

CISSP

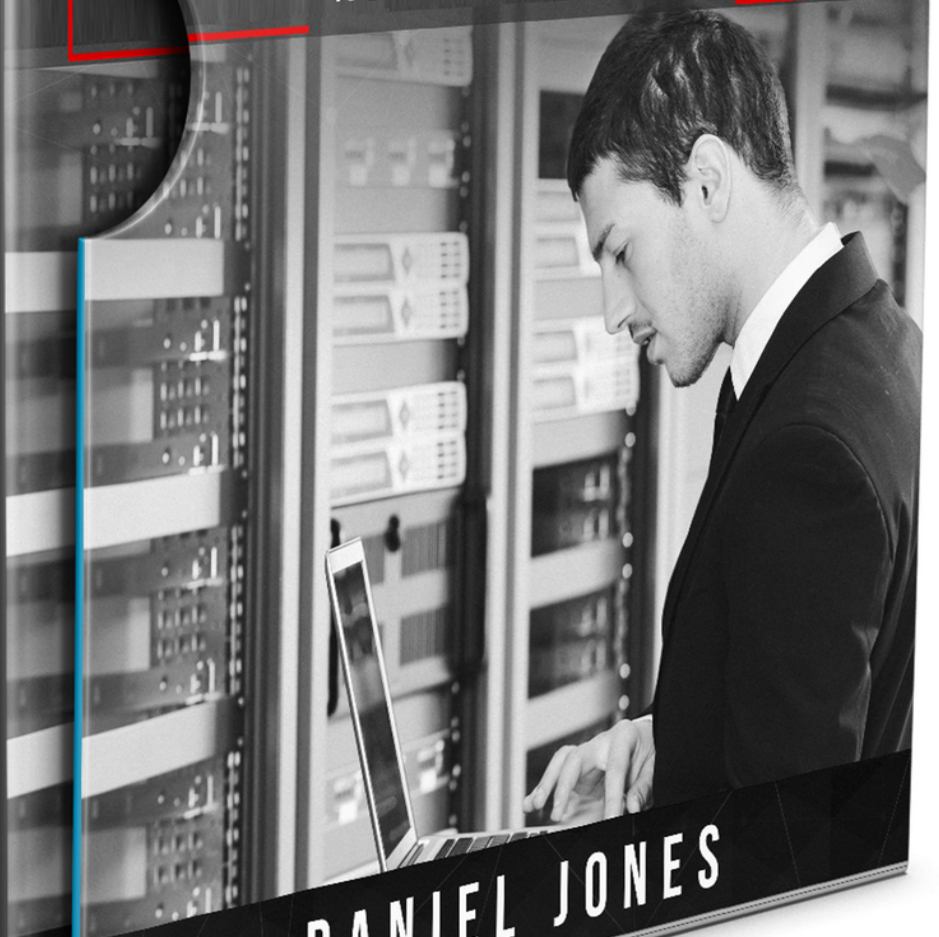
THIS BOOK INCLUDES

A COMPREHENSIVE BEGINNERS GUIDE TO LEARN AND UNDERSTAND THE REALMS OF CISSP FROM A-Z

A COMPREHENSIVE BEGINNER'S GUIDE TO LEARN THE REALMS OF SECURITY AND RISK MANAGEMENT FROM A-Z USING CISSP PRINCIPLES

SIMPLE AND EFFECTIVE STRATEGIES TO LEARN THE FUNDAMENTALS OF INFORMATION SECURITY SYSTEMS FOR CISSP EXAM

A COMPREHENSIVE GUIDE OF ADVANCED METHODS TO LEARN THE CISSP CBK REFERENCE



DANIEL JONES

CISSP

A COMPREHENSIVE BEGINNERS GUIDE
TO LEARN AND UNDERSTAND THE
REALMS OF CISSP FROM A-Z

DANIEL
JONES

BOOK 1

CISSP

A COMPREHENSIVE BEGINNER'S
GUIDE TO LEARN THE REALMS OF
SECURITY RISK MANAGEMENT FROM
A-Z USING CISSP PRINCIPLES

DANIEL
JONES

BOOK 2

CISSP

SIMPLE AND EFFECTIVE STRATEGIES
TO LEARN THE FUNDAMENTALS OF
INFORMATION SECURITY SYSTEMS
FOR CISSP EXAM

DANIEL
JONES

BOOK 3

CISSP

A COMPREHENSIVE GUIDE OF
ADVANCED METHODS TO LEARN THE
CISSP CBK REFERENCE

DANIEL
JONES

BOOK 4



CISSP

THIS BOOK INCLUDES

A COMPREHENSIVE BEGINNERS GUIDE TO LEARN AND UNDERSTAND THE REALMS OF CISSP FROM A-Z

A COMPREHENSIVE BEGINNER'S GUIDE TO LEARN THE REALMS OF SECURITY AND RISK MANAGEMENT FROM A-Z USING CISSP PRINCIPLES

SIMPLE AND EFFECTIVE STRATEGIES TO LEARN THE FUNDAMENTALS OF INFORMATION SECURITY SYSTEMS FOR CISSP EXAM

A COMPREHENSIVE GUIDE OF ADVANCED METHODS TO LEARN THE CISSP CBK REFERENCE



DANIEL JONES

CISSP

DANIEL JONES

© Copyright 2021 - All rights reserved.

This document is geared towards providing exact and reliable information in regards to the topic and issue covered. The publication is sold with the idea that the publisher is not required to render accounting, officially permitted or otherwise qualified services. If advice is necessary, legal or professional, a practiced individual in the profession should be ordered.

- From a Declaration of Principles which was accepted and approved equally by a Committee of the American Bar Association and a Committee of Publishers and Associations.

In no way is it legal to reproduce, duplicate, or transmit any part of this document in either electronic means or in printed format. Recording of this publication is strictly prohibited, and any storage of this document is not allowed unless with written permission from the publisher. All rights reserved.

The information provided herein is stated to be truthful and consistent, in that any liability, in terms of inattention or otherwise, by any usage or abuse of any policies, processes, or directions contained within is the solitary and utter responsibility of the recipient reader. Under no circumstances will any legal responsibility or blame be held against the publisher for any reparation, damages, or monetary loss due to the information herein, either directly or indirectly.

Respective authors own all copyrights not held by the publisher.

The information herein is offered for informational purposes solely and is universal as so. The presentation of the information is without a contract or any type of guarantee assurance.

The trademarks that are used are without any consent, and the publication of the trademark is without permission or backing by the trademark owner. All trademarks and brands within this book are for clarifying purposes only and are owned by the owners themselves, not affiliated with this document.

TABLE OF CONTENTS

CISSP

A Comprehensive Beginners Guide to Learn and Understand the Realms of CISSP from A-Z

Introduction

Chapter 1 : Security and Risk Management

- 1.1 Understand and Apply Concepts of Confidentiality, Integrity and Availability.
- 1.2 Evaluate and Apply Security Governance Principles
- 1.3 Determine Compliance Requirements
- 1.4 Understand Legal and Regulatory Issues that Pertain to Information Security in a Global Context
- 1.5 Understand, Adhere To, and Promote Professional Ethics
- 1.6 Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines
- 1.7 Identify, Analyze, and Prioritize Business Continuity (BC) Requirements
- 1.8 Contribute To and Enforce Personnel Security Policies and Procedures
- 1.9 Understand and Apply Risk Management Concepts
- 1.10 Understand and Apply Threat Modeling Concepts and Methodologies
- 1.11 Apply Risk-Based Management Concepts
- 1.12 Establish and Maintain Security Awareness, Education, and Training Program

Chapter 2 : Asset Security

- 2.1 Data and Asset Classification and Labeling
- 2.2 Determine and Maintain Information and Asset Ownership
- 2.3 Protect Privacy.
- 2.4 Ensure Appropriate Asset Retention
- 2.5 Determine Data Security Controls
- 2.6 Establish Information and Asset Handling Requirements

Chapter 3 : Security Architecture and Engineering

- 3.1 Implement and Manage Engineering Processes using Secure Design Principles
- 3.2 Understand the Fundamental Concepts of Security Models
- 3.3 Select Controls Based on Systems Security Requirements
- 3.4 Understand Security Capabilities of Information Systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- 3.5 Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements
- 3.6 Assess and Mitigate Vulnerabilities in Web-Based Systems
- 3.7 Assess and Mitigate Vulnerabilities in Mobile Systems
- 3.8 Assess and Mitigate Vulnerabilities in Embedded Devices
- 3.9 Apply Cryptography.

[3.10 Apply Security Principles to Site and Facility Design](#)

[3.11 Implement Site and Facility Security Controls](#)

Chapter 4 : Communication and Network Security

[4.1 Implement Secure Design Principles in Network Architecture](#)

[4.2 Secure Network Components](#)

[4.3 Implement Secure Communication Channels According to Design](#)

Chapter 5 : Identity and Access Management (IAM)

[5.1 Control Physical and Logical Access to Assets](#)

[5.2 Manage Identification and Authentication of People, Devices and Services](#)

[5.3 Integrate Identity as a Third-Party Service](#)

[5.4 Implement and Manage Authorization Mechanisms](#)

[5.5 Manage the Identity and Access Provisioning Lifecycle](#)

Chapter 6 : Security Assessment and Testing

[6.1 Design and Validate Assessment, Test, and Audit Strategies](#)

[6.2 Conduct Security Control Testing](#)

[6.3 Collect Security Process Data](#)

[6.4 Analyze Test Output and Generate Reports](#)

[6.5 Conduct or Facilitate Security Audits](#)

Chapter 7 : Security Operations

[7.1 Understand and Support Investigations](#)

[7.2 Understand Requirements for Investigation Types](#)

[7.3 Conduct Logging and Monitoring Activities](#)

[7.4 Securely Provision Resources](#)

[7.5 Understand and Apply Foundational Security Operation Concepts](#)

[7.6 Apply Resource Protection Techniques](#)

[7.7 Conduct Incident Management](#)

[7.8 Operate and Maintain Detective and Preventative Measures](#)

[7.9 Implement and Support Patch and Vulnerability Management](#)

[7.10 Understand and Participate in Change Management Processes](#)

[7.11 Implement Recovery Strategies](#)

[7.12 Implement Disaster Recovery \(DR\): Recovery Processes](#)

[7.13 Test disaster recovery plans \(DRP\)](#)

[7.14 Participate in Business Continuity \(BC\) Planning and Exercises](#)

[7.15 Implement and Manage Physical Security](#)

[7.16 Address Personnel Safety and Security Concerns](#)

Chapter 8 : Software Development Security

[8.1 Understand and Integrate Security throughout the Software Development Lifecycle \(SDLC\)](#)

[8.2 Identify and Apply Security Controls in Development Environments](#)

[8.3 Assess the Effectiveness of Software Security](#)

[8.4 Assess Security Impact of Acquired Software](#)

8.5 Define and Apply Secure Coding Guidelines and Standards

Conclusion

CISSP

A Comprehensive Beginner's Guide to Learn the Realms of Security Risk Management from A-Z using CISSP Principles

Introduction

How to Use This Book

A Brief History, Requirements, and Future Prospects

CISSP Concentration, Education and Examination Options

Chapter One : Security and Risk Management – An Introduction

Measuring Vulnerabilities

Threat Actors, Threats, and Threat Rates

The Cost

Chapter Two : Understand and Apply Concepts of Confidentiality, Integrity, and Availability.

Confidentiality

Integrity

Confidentiality

Chapter Three : Evaluate and Apply Security Governance Principles

In this chapter, you will learn:

Mission, Goals, and Objectives

Organizational Processes (acquisitions, divestitures, governance committees)

Acquisition and Divestitures

Organizational Roles and Responsibilities

COBIT

ISO/IEC 27000

OCTAVE

NIST Framework

Corrective Controls

Due Care/Due Diligence

Chapter Four : Determining Compliance Requirements

Contractual, Legal, Industry Standards, and Regulatory Requirements

Country-Wide Classification

Federal Information Security Management Act (FISMA)

Health Insurance Portability and Accountability Act (HIPAA)

Payment Card Industry Data Security Standard (PCI DSS)

[Sarbanes–Oxley Act \(SOX\)](#)

[Privacy Requirements](#)

[General Data Protection Regulation \(GDPR\)](#)

[GDPR – Array of Legal Terms](#)

[The Key Regulatory Point](#)

Chapter Five : Understanding Legal and Regulatory Issues

[Cybercrime](#)

[Licensing and Intellectual Property Requirements](#)

[Import/Export Controls](#)

[Trans-Border Data Flow](#)

Chapter Six : Understand, Adhere To, and Promote Professional Ethics

[\(ISC\)² Code of Professional Ethics Canons](#)

[Organizational Code of Ethics](#)

[Key Components of a Successful Code of Ethics Lineup](#)

Chapter Seven : Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines

[Standards](#)

[Procedures](#)

[Guidelines](#)

[Baselines](#)

Chapter Eight : Identify, Analyze, and Prioritize Business Continuity (BC) Requirements

[Develop and Document Scope and Plan](#)

[Planning for the Business Continuity Process](#)

[Business Impact Analysis](#)

[BIA Process](#)

[Recovery Strategy](#)

[Plan Development](#)

[Testing and Exercises](#)

Chapter Nine : Contribute To and Enforce Personnel Security Policies and Procedures

[Candidate Screening and Hiring](#)

[Employment Agreements and Policies](#)

[Onboarding and Termination Processes](#)

[Vendor, Consultant, and Contractor Agreements and Controls](#)

[Compliance Policy Requirements](#)

[Privacy Policy Requirements](#)

Chapter Ten : Understand and Risk Management Concepts

[Identify Threats and Vulnerabilities](#)

[Risk Analysis and Assessment](#)
[Risk Response](#)
[Countermeasure Selection and Implementation](#)
[Applicable Types of Controls](#)
[Security Control Assessment \(SCA\)](#)
[Asset Valuation](#)
[Reporting](#)
[Continuous Improvements](#)
[Risk Frameworks](#)

Chapter Eleven : Understand and Apply Threat Modeling Concepts and Methodologies

[Why Threat Modeling and When?](#)
[Threat Modeling Methodologies, Tools and Techniques](#)
[Other Threat Modeling Tools](#)

Chapter Twelve : Apply Risk-Based Management Concepts to the Supply Chain

[Risks Associated with Hardware, Software, and Services](#)
[Third-Party Assessment and Monitoring](#)
[Minimum Security Requirements](#)
[Service-Level Requirements](#)
[Service Level Agreements](#)
[Operational Level Agreements](#)
[Underpinning Contracts](#)

Chapter Thirteen : Establish and Maintain a Security Awareness, Education, and Training Program

[Methods and Techniques to Present Awareness and Training](#)
[Periodic Content Reviews](#)
[Program Effectiveness Evaluation](#)

Conclusion

References

CISSP

Simple and Effective Strategies to Learn the Fundamentals of Information Security Systems for CISSP Exam

Introduction

Chapter 1 : Security and Risk Management

[Maintaining Confidentiality and Various Requirements](#)
[System Integrity and Availability](#)

[Enhancing Security and Designating the Roles](#)
[Identifying and Assessing Threats and Risks](#)
[Risk Terminology](#)
[Risk Management](#)
[Cost/Benefit Analysis](#)
[Controls](#)
[Risk Management Framework](#)
[Business Continuity Management \(BCM\)](#)

Chapter 2 : Telecommunication and Network Security.

[Local Area Network \(LAN\)](#)
[Wide Area Network \(WAN\)](#)
[OSI Reference Model](#)
[The First Layer: Physical Layer](#)
[Network Topologies](#)
[Cable and Connector Types](#)
[Interface Types](#)
[Networking Equipment](#)
[The Second Layer: Data Link Layer](#)
[Logical Link Control \(LLC\)](#)
[Media Access Control \(MAC\)](#)
[Protocols in Local Area Networks and the Transmission Methods](#)
[Protocols in WLAN and WLAN Tech](#)
[Different Protocols and Technologies of WAN](#)
[Point to Point Links](#)
[Circuit Switched Networks](#)
[Packet-Switched Networks](#)
[The Networking Equipment Found in the Data Link Layer](#)
[The Fourth Layer: Transport Layer](#)
[The Fifth Layer: Session Layer](#)
[The Sixth Layer: Presentation Layer](#)
[The Seventh Layer: Application Layer](#)

Chapter 3 : Security of Software Development

[Security Workings in Distributed Software](#)
[Working with Agents in Distributed Systems](#)
[Object-Oriented Environments](#)
[Databases](#)
[Types of Databases](#)
[Operating Systems](#)
[Systems Development Life Cycle](#)
[Controlling the Security of Applications](#)
[AV Popping up Everywhere](#)

Chapter 4 : Cryptography.

[The Basics of Cryptography.](#)

[The Cryptosystem](#)

[Classes of Ciphers](#)

[The Different Types of Ciphers](#)

[Symmetric and Asymmetric Key Systems](#)

Chapter 5 : Operating in a Secure Environment

[Computer Architecture](#)

[Virtualization](#)

[Operating in a Secured Environment](#)

[Recovery Procedures](#)

[Vulnerabilities in Security Architecture](#)

[Security Countermeasures](#)

[Confidentiality](#)

[Integrity](#)

[Availability](#)

[Access Control Models](#)

[Trusted Network Interpretation \(TNI\)](#)

[European Information Technology Security Evaluation Criteria \(ITSEC\)](#)

Chapter 6 : Business Continuity Planning and Disaster Recovery Planning

[Setting Up a Business Continuity Plan](#)

[Identifying the Elements of a BCP](#)

[Developing the Business Continuity Plan](#)

Conclusion

CISSP

A Comprehensive Guide of Advanced Methods to Learn the CISSP CBK Reference

Introduction

[How to Use this Book](#)

[CISSP Domains, Learning Options, and Examination](#)

[CISSP Domains](#)

Chapter 1 : Domain 1 - Security and Risk Management

[The Role of Information and Risk](#)

[Risk, Threat, and Vulnerability](#)

[1.1 Understand and Apply Concepts of Confidentiality, Integrity, and Availability](#)

[1.2 Evaluate and Apply Security Governance Principles](#)

[1.3 Determine Compliance Requirements](#)

- [1.4 Understand Legal and Regulatory Issues that pertain to Information Security in a Global Context](#)
- [1.5 Understand, Adhere To and Promote Professional Ethics](#)
- [1.6 Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines](#)
- [1.7 Identify, Analyze, and Prioritize Business Continuity \(BC\) Requirements](#)
- [1.8 Contribute To and Enforce Personnel Security Policies and Procedures](#)
- [1.9 Understand and Apply Risk Management Concepts](#)
- [1.10 Understand and Apply Threat Modeling Concepts and Methodologies](#)
- [1.11 Apply Risk-Based Management Concepts to the Supply Chain](#)
- [1.12 Establish and Maintain a Security Awareness, Education, and Training Program](#)

Chapter 2 : Domain 2 - Asset Security

- [2.1 Identify and Classify Information and Assets](#)
- [2.2 Determine and Maintain Information and Asset Ownership](#)
- [2.3 Protect Privacy](#)
- [2.4 Ensure Appropriate Asset Retention](#)
- [2.5 Determine Data Security Controls](#)
- [2.6 Establish Information and Asset Handling Requirements](#)

Chapter 3 : Domain 3 - Security Architecture and Engineering

- [3.1 Implement and Manage Engineering Processes using Secure Design Principles](#)
- [3.2 Understand the Fundamental Concepts of Security Models](#)
- [3.3 Select Controls Based Upon Systems Security Requirements](#)
- [3.4 Understand Security Capabilities of Information Systems \(e.g., Memory Protection, Trusted Platform Module \(TPM\), Encryption/Decryption\)](#)
- [3.5 Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements](#)
- [3.6 Assess and Mitigate Vulnerabilities in Web-Based Systems](#)
- [3.7 Assess and Mitigate Vulnerabilities in Mobile Systems](#)
- [3.8 Assess and Mitigate Vulnerabilities in Embedded Devices](#)
- [3.9 Apply Cryptography](#)
- [3.10 Apply Security Principles to Site and Facility Design](#)
- [3.11 Implement Site and Facility Security Controls](#)

Chapter 4 : Domain 4 - Communication and Network Security

- [4.1 Implement Secure Design Principles in Network Architecture](#)
- [4.2 Secure Network Components](#)
- [4.3 Implement Secure Communication Channels According to Design](#)

Chapter 5 : Domain 5 - Identity and Access Management (IAM)

- [5.1 Control Physical and Logical Access to Assets](#)
- [5.2 Manage Identification and Authentication of People, Devices, and Services](#)
- [5.3 Integrated Identity as a Third-Party Service](#)
- [5.4 Implement and Manage Authorization Mechanisms](#)
- [5.5 Manage the Identity and Access Provisioning Lifecycle](#)

Chapter 6 : Domain 6 - Security Assessment and Testing

- [6.1 Design and Validate Assessment, Test, and Audit Strategies](#)
- [6.2 Conducting Security Control Tests](#)
- [6.3 Collect Security Process Data](#)
- [6.4 Analyze Test Output and Generate Reports](#)
- [6.5 Conduct or Facilitate Security Audits](#)

Chapter 7 : Domain 7 - Security Operations

- [7.1 Understanding and Support Investigations](#)
- [7.2 Understanding Requirements for Investigation Types](#)
- [7.3 Conduct Logging and Monitoring Activities](#)
- [7.4 Secure Provision Resources](#)
- [7.5 Understand and Apply Foundational Security Operation Concepts](#)
- [7.6 Apply Resource Protection Techniques](#)
- [7.7 Conduct Incident Management](#)
- [7.8 Operate and Maintain Detective and Preventive Measures](#)
- [7.9 Implement and Support Patch and Vulnerability Management](#)
- [7.10 Understanding and Participating in Change Management](#)
- [7.11 Implement Recovery Strategies](#)
- [7.12 Implement Disaster Recovery Process](#)
- [7.13 Disaster Recovery Plans \(DRP\)](#)
- [7.14 Participate in Business Continuity Planning and Exercises](#)
- [7.15 Implement and Manage Physical Security](#)
- [7.16 Address Personal Safety and Security Concerns](#)

Chapter 8 : Domain 8 - Software Development Security

- [8.1 Understand and Integrate Security Throughout the Software Development Lifecycle \(SDLC\)](#)
- [8.2 Identify and Apply Security Controls in Development Environments](#)
- [8.3 Assess the Effectiveness of Software Security](#)
- [8.4 Assess Security Impact of Acquired Software](#)
- [8.5 Define and Apply Secure Coding Guidelines and Standards](#)

Conclusion

CISSP

*A Comprehensive Beginners Guide
to Learn and Understand the Realms
of CISSP from A-Z*

DANIEL JONES

Introduction

CISSP: Certified Information Systems Security Professional is the world's premier cyber security certification (ISC)². The world's leading and the largest IT security organization was formed in 1989 as a non-profit organization. The requirement for standardization and maintaining vendor-neutrality while providing a global competency lead to the formation of the "International Information Systems Security Certification Consortium" or in short (ISC)². In 1994, with the launch of the CISSP credential, a door was opened to a world class information security education and certification.

CISSP is a fantastic journey through the world of information security. To build a strong, robust and competitive information security strategy and the practical implementation is a crucial task, yet a challenge that is entirely beneficial to an entire organization. CISSP focuses on an in-depth understanding of the components of critical areas in the information security. This certification stands out as proof of the advanced skills, and knowledge one possesses in terms of designing, implementing, developing, managing and maintaining a secure atmosphere in an organization.

The learning process and gaining experience are the two main parts of the CISSP path. It is definitely a joyful journey, yet one of the most challenging, without a proper education and guidelines. The intention of this book is to prepare you for the adventure by providing you a summary of the CISSP certification, how it is achieved and a comprehensive A-Z guide on the domains covered in the certification.

This is going to help you get started and become familiar with the CISSP itself. With a bit of a history, benefits, requirements to become certified, the prospects, and a guide through all the domains, topics, sub-topics that are tested in the exam. After you read this you will have a solid understanding of the topics and will be ready for the next level in the CISSP path.

A Brief History

In 2003, The USA Department of Defense (NSA) adopted the CISSP as a baseline in order to form the ISSEP (Information System Security Engineer

Professional) program. Today it is considered one of the CISSP concentrations. CISSP also stands as the most required security certification in LinkedIn. The most significant win it reached is to become the first information security credential to meet the conditions of ISO/IEC Standard 17024.

According to (ISC)2, CISSP works in more than 160 nations globally. More than 129,000 professionals currently hold the certification and this implies how popular and global this certification is.

Job Prospects

Information security as a carrier is not a new trend and the requirements, opportunities and salary has grown continuously. To become an information security (Infosec) professional takes dedication, commitment, learning, experimentation and hands on experience. To become a professional with applied knowledge takes experience, which is a critical factor. There are lots of Infosec programs and certifications worldwide. Among all the certificates, such as CISA, CISM etc., CISSP is known as the elite certification, as well as one of the most challenging, yet rewarding.

The CISSP provides many benefits. Among them, the following are outstanding:

- Carrier Advancements
- Vendor-Neutral Skills
- A Solid Foundation
- Expanded Knowledge
- Higher Salary Scale
- Respect among the workers, peers and employers
- A Wonderful Community of Professionals

The certification is ideal for the following roles:

- Chief Information Officer (CIO/CISO)

- Director of Security
- IT Directors
- IT Managers
- Network/Security Architects
- Network/Security Analysts
- Security System Engineers
- Security Auditors
- Security Consultants

Salary Prospects:

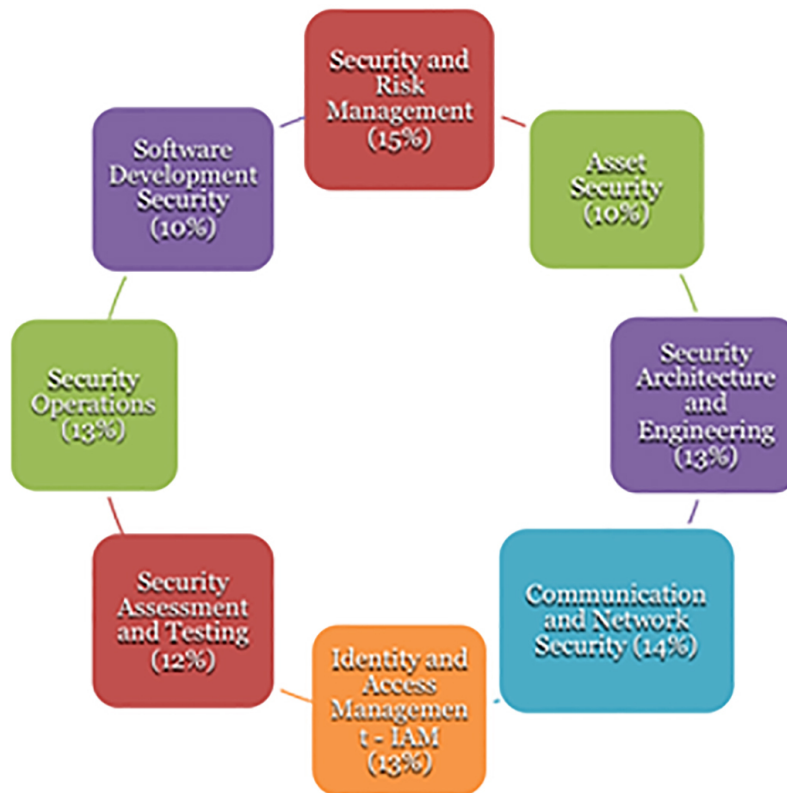
- The average yearly salary in the USA is \$131,000.
- Expected to grow by 18% from the year 2014 to 2024.

Industry Prospects:

- A high demand in Finance, Professional Services, Defense.
- A growing demand in HealthCare and Retail sectors.

More about the Education Paths and Examination Options

The CISSP concentrates on eight security domains. It critically evaluates the expertise across these domains.



Eight domains and the Weightings

- The CISSP is available in eight languages at 882 locations and in 114 countries around the globe.
- As of December 18, 2017, the English CISSP exam uses Computerized Adaptive Testing (CAT).
- It is provided in several languages: English, French, German, Brazilian Portuguese, etc. and even for the visually impaired.
- Non-English exams are conducted as a linear, fixed-form exam.
- The number of questions in a CAT exam can be between 100-150.
- The number of questions in the linear examination is 250.
- The CAT is 3 hours long, while the linear is 6 hours long
- Finally, you need to score 700 points to pass the exam.

CISSP Learning Options and Getting Ready for the Exam

There are a handful of options if you would like to learn CISSP from scratch. Here is a list of the options. The selection of a suitable method is up to the student.

- Classroom Based Training
- Online Instructor Lead
- On-Site
- Online Self-Paced

The classroom based training is good for the traditional learner who would like to obtain knowledge during classroom lead training in order to interact with the instructor, as well as the rest of the class. An (ISC)² trainer, or an authorized trainer in an (ISC)² office, or in an institute of one of the authorized training partners, will take the student through the course with well-structured courseware. The training will take 3-5 days, 8 hours per day. The training includes real-world scenarios and case studies.

The online learning option is one of the most popular and cost-effective choices nowadays, as it eliminates travel cost. For the people with a busy schedule, this is the best option. The courseware in (ISC)² is available for 60 days of access. An authorized instructor will be available. There are weekday, weekend and other options to select to for the requirements.

If you are looking for corporate training for an organization or an enterprise, (ISC)² provides on-site training. The training is similar to the classroom lead training. There will also be a dedicated exam schedule assistance.

If someone wants to self-learn CISSP in their convenience, this option is also available. This may be the most popular options available for many students who are geographically dispersed. Also, the best option to cut costs and time. There is instructor-created HD content and the materials are equivalent to the class-room content. Interactive games, Flash cards, exam simulations, all of these at a single place for 120 days if you select (ISC)². There are many other training providers to select from. This is also suitable for an organization.

Finally, if you want to register for an exam, review the exam availability by credential first. This is available at (ISC)² website. Then visit the Pearson VUE website, create an account, select the venue and time, make the payment and wait for the confirmation email. Once you receive the details, do some more quick studies, simulation practice tests (i.e. online) and go for it.

Chapter 1

Security and Risk Management

Risk is or can be defined as a step toward evolution. In day to day life, taking a risk to obtain a goal (i.e. a reward) is crucial. When it comes to information technology, the risk is something that comes along with the territory. There are many industries that integrate information technology into their daily operations. Take for example, the healthcare industry or the banking, information technology operates within the core levels. This comes with a huge risk in terms of information exposure, theft, and corruption. The calculation of assessing the associated risk, implementing and testing measures, mitigating the risks become a core responsibility of the security and management.

In the current information technology atmosphere, there are many risks associated with the components of a system. This can range from a simple display panel to complex machinery in a nuclear power plant. Risk management involves the process of understanding, assessing (analysis) and mitigating the risks to ensure the security objectives are met. Every decision-making process inherits the risks and the risk management process ensures the effectiveness of these decisions without having to go through the security failures.

Data/Information Security focuses on minimizing risks aforementioned, such as healthcare data, business documents, trade secrets intellectual properties, etc. The data/information security utilizes many preventive and detective tactics, such as data classification, IAM (Identity and Access Management), threat modeling/detection, and analytics.

As mentioned in the previous paragraph, a comprehensive understating of the basic and core security concepts is the best place to start the CISSP journey.

1.1 Understand and Apply Concepts of Confidentiality, Integrity and Availability.

Confidentiality, Integrity and Availability are known as the CIA triad (or AIC). This should not be confused with the Central Intelligence Agency. CIA is basically a model (more like the standard model) or a framework, technically speaking. It is intended to guide policies for information security within an organization while conceptualizing the challenges. This is something each employee of an organization must be made aware of. Without the building blocks it is unrealistic to think of a workable security plan.

Now let's look at the three components in more detail.

Confidentiality

Some people think this is the information security itself. Why? Information (or data) can be sensitive, valuable, and private. Falling into the wrong hands – people who do not have authorization or clearance - can lead to a disaster. If stolen, the information can be used to do multiple levels of abuse. Confidentiality is the process of keeping safe while preventing the disclosure to unauthorized parties. This does not mean you should keep everything a secret. This simply means that even if people are aware that such data/information exists, only the relevant parties can have access to it.

When it comes to confidentiality, it is also important to understand the need for data classification. When classifying data to determine the level of confidentiality, the level of damage it can cause in the event of a breach can be used as the classifier. By defining who should be able to access what set of data through what type of a clearance is the key. Then providing the least access with suitable awareness is the best way to ensure the confidentiality. The understanding of the risk involved when dealing with sensitive information is vital. Each person involved must be trained to understand the basics, to follow the best practices (i.e. password security, threats from social engineering, etc.), identify potential breaches and what ramifications are applied in a data breach.

By implementing access control measures, such as locks, biometrics, authentication methods (2FA), one can proactively mitigate the risks. For the data at rest or in motion, it is possible to apply various levels of encryption, hashing, and other types of security measures. We can utilize all

the physical security measures for data in use to screen the parties. Intelligent deny configurations can also save a lot of work.

Integrity

Now we know how to prevent unauthorized access in an information security perspective. But how do we ensure that the information is the original and not modified?

The integrity of the information means the information is and stays the original, accurate, unchanged accidentally or improperly by any authorized or an unauthorized party. To ensure the integrity, we need to make sure there are levels of access permission, and even encryption, thus preventing unauthorized modifications. This is, in other words, a measure of trustworthiness of data.

Validating the inputs can play a major role when it comes to maintaining the integrity. Hashing is important when it comes to the information/data in motion. To prevent human errors the data can be version controlled and must be backed up properly. Backups ensure the data is not lost due to non-human errors, like mechanical and electronic errors, such as disk corruption and crashing, thus provides a solid disaster recovery option. Data deduplication prevents accidental leaks. Finally, tracking the activity or auditing can reveal how data is accessed, modified and used, and it can also record all types of misuses.

Availability

Data availability means you are able to access the data or information you need when you need it without any delays or long wait times. There are lots of threats to the availability of data. There can be many disasters, such as natural disasters causing major loss of data. There can also be human-initiated threats, like Distributed Denial Of Service attacks (DDoS) or even simple mistakes or configuration faults, internet failures or bandwidth limitations.

To provide continuous access, it is important to deploy the relevant options. The routine maintenance of hardware, operating systems, servers, applications through fault tolerance, redundancy, load balancing and

disaster recovery measure must be in place. These will ensure high availability and resiliency.

There are technological deployments (hardware/software), such as fail-over clustering, load balancers, redundant hardware/systems and network support to fight availability issues.

1.2 Evaluate and Apply Security Governance Principles

Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives

The role of the information security is not to stand in a corner and safeguard a set of device or information. The need arises within the business itself, while planning. In any strategic planning phase, the business concentrates on its goals, the mission to reach one or more goals and the objectives toward each goal to reach the final outcome. To prevent and mitigate the risks the information security functions must be clearly identified, aligned and streamlined with the mission, goals, business strategy and objectives. If it is properly aligned, it will ensure the business continuity by attaining risk mitigation, disaster recovery and reaching objectives within the given time frame by fitting it to the business process.

In order to do so, these elements and the relationship to information security must be understood. When this is clearly understood it is easier to allocate organizational resources and budget to security initiatives. The outcome will be more efficient and effective security policies and procedures aligned with the entire business process.

Mission Goals and Objectives

When we speak of a mission, we might remember the mission to the moon and how it is accomplished. Every organization has a mission, and it is described in the mission statement. It states why the organization exists and what the overall goal is. The objectives can be thought of as milestones toward specific stages of a goal. Once you accomplish the objectives, you then reach a specific goal. When you accomplish all the goals, you accomplish the mission that is also the main objective. The security engineers or architects must have an understanding of the mission, goals,

and objectives. If the security framework isn't aligned and flexible, scalable, adaptive, there will be issues leading to failures as the business expands.

Governance Committees

When it comes to establishing an information security strategy, the decision must come from the top of the organization's hierarchy. The organization's governance or the governing body must initiate the security governance processes and policies to direct the next level management (executive management). Which means the strategy itself, the objectives and the risks are defined and executed in a top-down approach. The strategy must be in compliance with the existing regulations as well.

The executive management must be fully aware/informed of the strategies (visibility) and have control over the security policies and the overall operation. In the process, the teams must meet and review the existing strategy, incidents, introduce new changes when as required and approve the changes accordingly. This strengthens the effectiveness, and ensures that the security activities are continuing while mitigating risks, while the investment on security is worth the cost.

Acquisitions and Divestitures

During the lifecycle of a business, in order to maintain the competence, agility and focus, organizations tend to acquire other organizations or sell one of their own business units. Most of the acquisitions occur when there is a need for new technologies and innovation. Information security is a complex process when it comes to mergers, acquisitions and even divestitures.

When acquiring an existing organization, there are multiple security considerations. The existing organization also has a different hierarchy and security governance committee and executives, their strategy, policies and process, the differences between the organizations, as well as the nature, and current state of the operations. With any acquisition, there is a risk associated.

There can be many operations in an existing company in terms of information security such as threat management and monitoring,

vulnerability management, operations management, incident management, and other types of surveillance involved. Some of these can be linked to third-party. The existing security framework must be flexible to integrate the new business unit with a hassle.

When an organization divides into another or even multiple units, the security architecture can be moved by splitting the units with adequate changes and flexibility to better align with the new or changed process. Some reforms may need as the concentration of the business can change (mission, strategies, and objectives). There may be new regulations to adopt. Once the alignment is complete, the units can move forward with the new initiatives.

Organizational Roles and Responsibilities

The importance of being responsible as well as accountable must be an important issue to understand. The definition of roles has to be tied to the responsibilities. It also ensures the boundaries and accountability. When implementing a security policy, the responsibilities delegated to the parties involved must be defined in the policy and what roles are able to enforce and control the activities. These roles and responsibilities must be able to be applied to all the parties involved from the lowest level employee to the suppliers, stakeholders, consultants, and all the other parties.

As we discussed in earlier paragraphs, executive level management is responsible for and must demonstrate a strong allegiance with the security program in place. He/she is responsible for multiple functions and even wears multiple hats at certain times. As a manager, the responsibilities include implementing a proper information security strategy with the top-down approach and mandate. The person should also lead the entire organization when it comes to security by utilizing the skills, expertise, and leadership. There should be room for education, recognition, rewarding, and proper penalties.

On the other hand, as employees, they should honor the security framework. The compliance, gaining awareness of the policies, procedures, baselines and guidelines, legislations, through proper training programs are essential. By learning, understanding, and complying with the security program one can prevent compromization through due care. We will discuss

more in due care later in this chapter. This has to become the organization's security culture.

Security Control Frameworks

These frameworks are simply a set of practices and procedures that will help an organization to cover the overall security without any gaps. The selected framework also ensures risk mitigation. There are many frameworks to select from, and the followings are the most demanding.

- COBIT (Control Objectives for Information Technology).
- ISO 27000 standards.
- OCTAVE framework (Operationally Critical Threat, Asset, and Vulnerability Evaluation).
- NIST (US National Institute of Standards and Technology).

A noteworthy fact is that there are country-specific frameworks.

Features of a Control Framework

There are four types of frameworks.

- Preventive.
- Deterrent.
- Detective.
- Corrective.

Preventive Frameworks

These frameworks are the first line of defense and aims to prevent security issues through strategy (training, etc.). The followings are some examples.

- Security policies.
- Data classification.
- Security Cameras.

- Biometrics.
- Smart Cards.
- Strong authentication.
- Encryption.
- Firewalls.
- Intrusion Prevention Systems (IPS).
- Security personal.

Deterrent Frameworks

This is the second line of defense and intends to discourage malicious attempts by using appropriate countermeasures. If an attempt is made, there is a consequence. The following list includes several examples.

- Security personal.
- Cameras.
- Fences.
- Guards.
- Dogs.
- Warning signs.

Detective Frameworks

As the name implies, these are deployed when the activity is beyond the aforementioned controls. Only when an incident occurs are these effective. Therefore, it may not operate in real-time and can be used to reveal unauthorized activities. There are a few examples.

- Security personal.
- Logs.
- CCTVs.
- Motion Detectors.

- Auditing.
- Intrusion Detection Systems (IDS).
- Some antivirus software.

Corrective Controls

The final is responsible for restoring the environment to its original state or the last known good working state after an incident.

- Risk management and business continuity measures assisting backups and recovery.
- Antivirus.
- Patches.

In addition, there are other stages, such as Recovery and Compensative controls.

The recovery measures are deployed in order to recover (corrective) as well as prevent security and other incidents. These include backups, redundant components, high availability technologies, fault tolerance, etc.

The compensative or alternative control is a measure applied when the expected security measure is either too difficult or impractical to implement. These can be in the forms of physical, administrative, logical, and directive. Segregation of duties, encryption, and logging are few examples. PCI DSS is a framework where we can exhibit the compensating controls.'

Due Care/Due Diligence

Due Diligence is the understanding of governance principles and risks your organization has to face. This process involves the gathering of information, assessment of risks, establishing written policies and documentation, and distributing this information to the organization.

Due care is about the responsibilities. In other words, it is about your responsibility within the organization and the legal responsibilities to

establish proper controls, and follow the security policies to take reasonable actions and make better choices.

These two concepts can be confusing. For the ease of understanding, you can think due diligence as the practice by which the due care can be set forth.

1.3 Determine Compliance Requirements

Many organizations must satisfy one or more compliance requirements. There can be one or more applicable laws, regulations, and industry standards. The consequence of non-compliance can be severe, as the act directly violate regulations, which include state laws and regulations. The worst-case scenario is the end of business followed by a considerable fine. Therefore, compliance is a very important topic to discuss and understand.

Contractual, Legal, Industry Standards, and Regulatory Requirements

To have a better understanding of the legal requirements and to keep up with the changes are vital in this context. There can be nation-wide regulatory requirements, Governance within the organization laws, standards, etc.

There are two types of systems when it comes to legal systems. One is common law, and the other is the civil law system. Almost all of the civil laws are derived from the Roman law system. These laws come from legislative enactments. There are other religious laws such as Sharia.

On the other hand, common law is a new legal system based on new concepts. The constitutions allow judicial decisions to form or provision the statutes.

In the U.S. legal system, there are 3 branches. Namely, Criminal law, Civil law and Administrative law.

Laws, regulations, and industry standards are part of a compliance act or a policy. Some examples would be:

- Health Insurance Portability and Accountability Act (HIPAA).
- Sarbanes–Oxley Act (SOX).

- Payment Card Industry Data Security Standard (PCI DSS).
- Federal Information Security Management Act (FISMA)

Privacy

“Privacy is a concept in disarray.” – Daniel J. Solove, J.D.

It is a sociological concept, and it does not have a formal definition.

Privacy protection is the protection of Personal Identifiable Information (PII) or Sensitive Personal Information (SPI) in an information security perspective. Thanks to social networks, many people are aware of what privacy is and what measures can they take in order to protect the PII. There are several different laws and regulations when it comes to different countries, and within Europe, the laws are even tighter.

Some of the PII may not be sensitive, but there is hand full of sensitive information to protect. Social security number, credit card information, and medical data are just a few examples. Identity theft, abuse of information, and information stealing are common topics discussed nowadays. There are region-specific regulations. The best example is the GDPR act in the European Union. Here GDPR stands for General Data Protection Rule. PCI DSS and ISO standards also include guidelines to address certain areas.

1.4 Understand Legal and Regulatory Issues that Pertain to Information Security in a Global Context

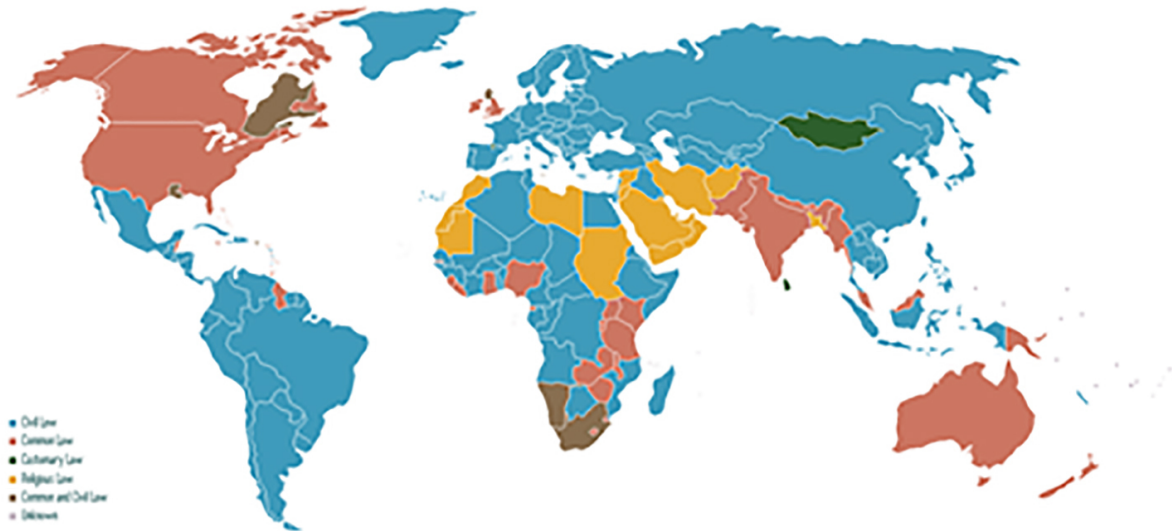
As a security professional, you must be familiar with the local as well as global context when it comes to laws, regulations, and standards.

Cybercrimes and data breaches

The organizations expand their business operations to different regions and countries. It is important to become familiar with the legal systems in order to determine the changes required. Different nations and regions follow different laws, acts and policies. Due diligence is what the security professional should exercise at this point.

As you may have already aware, in the USA, there are different state requirements when an incident occurs, such as a data breach. California

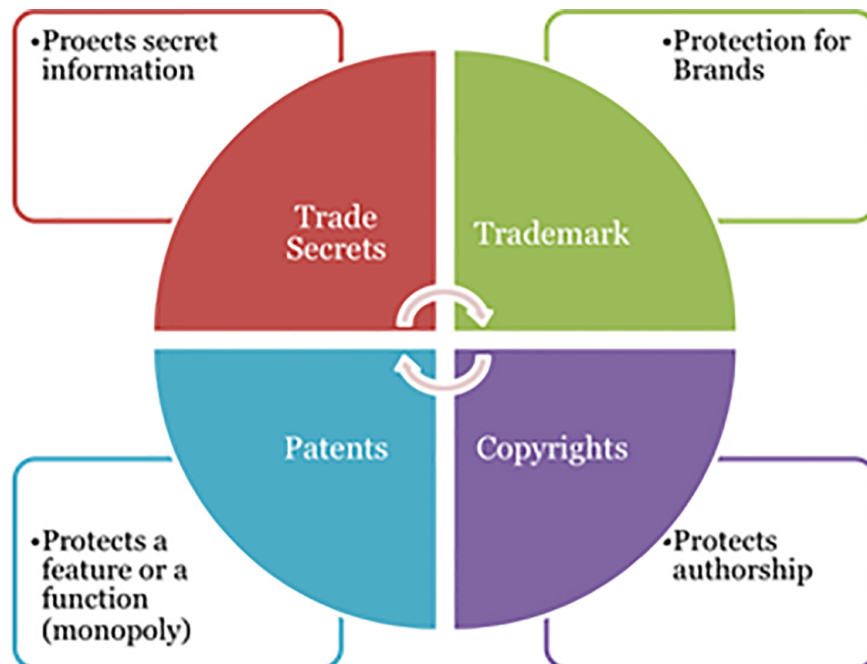
S.B. 1386 is an example. When arriving at a more nation-wide perspective, HITECH act in the USA has some requirements. In the European Union, GDPR introduced mandatory requirements. In the Asia Pacific, Australia, Philippine, China and some other countries have such laws.



(Law systems by country. Image credit: Wikipedia)

Licensing and Intellectual Property Requirements

There are 4 types of intellectual properties.



- An example of a trade secret is a formula to make a specific food or a drink (e.g., Coca-Cola).
- A trademark is a logo, symbol, or similar that represents a brand.
- A patent is a temporary monopoly provided for a unique product or a feature (e.g., iPhone).
- A copyright protects a creative work from unauthorized modification, distribution, or use. The copyright act can be different by country or region.

A license is an agreement/contract between a buyer and a seller. In an example, a software vendor sells a product with a license to the consumer (e.g., Microsoft Windows). In different regions or countries, there are different regulations controlling the nature of the licensing. This is intended to limit the unauthorized use, modification, or distribution.

Import/Export Controls

In any country, there are regulations on Importing and Exporting products or services. This helps an organization to control its information across multiple nations. As an example, many countries regulate the import of communication devices such as phones or radio transmitters.

There are export laws on cryptographic products and technologies. Other countries have import laws on encryption. This type of laws can restrict the use of a VPN technologies within a country, for example. If a VPN is running through a country where an encryption law is prohibited, or non-compliant, it must be regulated for the safety.

Trans-Border Data Flow

As the organizations expand their business, the data and information assets also expand the locations. Organizations follow specific security policies to control and secure the data. Therefore, the security professionals must be aware of the county specific laws, regulations and compliance, as well as where the data resides beyond the country. Especially with the current cloud network era this becomes an important consideration. A good example is the **EU-U.S. Privacy Shield Framework** .

Previously there was the **Safe Harbor** act between the U.S. Department of Commerce and European Union. The requirement originated as a response to the European Commission Directive on Data Protection. In 2015, the European Court overturned the agreement by stating that only the twenty-eight countries in the European Union should determine who controls how online information can be collected. In 2016, as a resolution to the new directive, the European Commission and the U.S. Department of Commerce established the **EU-U.S. Privacy Shield Framework** .

Privacy

With the evolution of social networks, privacy is a topic that is discussed and debated continuously. There are several laws established and being established in various countries to protect personal data. We already discussed GDPR act, and it has very stringent laws to protect personal data of European citizens. The data collection must be transparent if present. It should tell the users how the data is collected, for what purpose and to let them control (mechanisms) the degree.

1.5 Understand, Adhere To, and Promote Professional Ethics

There are two types of code of ethics you must understand. One is the (ISC)² code of ethics. The other is local to your organization.

(ISC)² Code of Professional Ethics Canons

(You can read more by following <https://www.isc2.org/Ethics>)

- Protect society, the common good, necessary public trust and confidence, and the infrastructure: This is about establishing and protecting the trustworthiness and confidence in the information and systems. In addition to promote the understanding and acceptance of security measures, to strengthen the public infrastructure and to do the right thing by following safe practices.
- Act honorably, honestly, justly, responsibly, and legally: Timely notify the stakeholders and deliver true information, observe the agreements, treat all the members fairly in resolving conflicts, giving prudent advice, and honor the different laws in different jurisdictions.

- Provide diligent and competent service to principals: To maintain and develop the skills to provide a competent and qualified service while avoiding the areas of expertise you are not an expert of. This to preserve the value of their assets and to respect the privileges they grant.
- Advance and protect the profession: This is all about maintaining the profession and its honor without diminishing it by not acting honorably; by keeping the skills and knowledge up to date. This also states how you should treat the other professions without an indifference.

Organizational Code of Ethics

This is about maintaining ethics in your organization. As a security professional, you should practice and establish the ethical framework by honoring, training, and guiding the others through documentation and other means necessary. It is also important to review and enhance the practices and guidelines. The frameworks may be different from one organization to another. In such cases, the flexibility and adaptability have to be there to align yourself and others.

1.6 Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines

In the beginning, we discussed the roles of security management, and the policies. This is part of the security management as you already know. The policies are defined by the management to describe how security is exercised in the organization. In other words, how the organization is expecting to secure its assets. The security policy is the first step to a structured and organized security architecture.

After outlining the policy, the next step is to define the **standards** . Standards are rules. These mandatory rules will be used to implement the policy.

To guide the implementation, there has to be instructions to follow. To do so, **guidelines** will be set. As the last step, the security team will create **procedures** by following the standards and guidelines.

A policy is not a specific, but it describes the security in general. It describes the goals. A policy is neither a set of standards, nor guidelines. It is also not specifically procedures of controls. An important thing to remember is that a policy does not describe implementation details. This is achieved through procedures.

The policy helps to define what is intended to protect and ensures implementation of proper control. Control means what is expected to protect and what restrictions should be set forth. During deployment, this ensures proper selection of products and follow best practices.

Standards

Setting standards is important because it helps to decide things such as software, hardware, and technologies and go on with a single, most appropriate selection. If this is not defined, there will be multiple selections, or choices, making it difficult to control and protect. By setting standards, even if the policy is difficult to implement, you can guarantee it to work in your environment. If a policy requires multi-factor authentication, the standard for using a smart card can make certain interoperability.

Procedures

As mentioned in an earlier paragraph, procedures are implementation instructions and are step-by-step instructions. The procedures are mandatory and therefore, well documented for reuse. Procedures can also save a lot of time as a specific procedure can serve multiple products. Some examples would be, Administrative, Access Control, Auditing, Configuration, and Incident Response.

Guidelines

Guidelines are instructions and are not mandatory in some cases. These are instructions to do a task or best practices if a user is expecting to do something. As an example, people tend to save passwords. A guideline can instruct how to safely store it by following a specific standard. But the user can keep it safe by other means.

Baselines

Baseline is a minimum level of security that is necessary to meet the policy. Baselines can be adapted to meet business requirements. In nature, these can be a configuration or certain architectures. For example, to follow a specific standard, as a baseline, a configuration can be enforced. This should be applied to a set of objects that are intended to perform a similar function (e.g., a set of Windows computers need to follow a security standard. A group policy can be applied to the computers or the users of these computers.)

1.7 Identify, Analyze, and Prioritize Business Continuity (BC) Requirements

Business continuity is to remain operational during any sort of outage with minimal impact. In other words, sustain the critical operations. There can be numerous threats or probability of failures due to many types of disasters. Some of these can be prevented, mitigated, or managed through careful and thorough planning. This process requires a considerable amount of planning and implementation.

According to the thebci.org, this is a holistic management process. During the process, the professional identifies the potential threats, provides a framework to build resilience, thus ensuring effective response while safeguarding the interests of the key stakeholders, reputation, brand, and value.

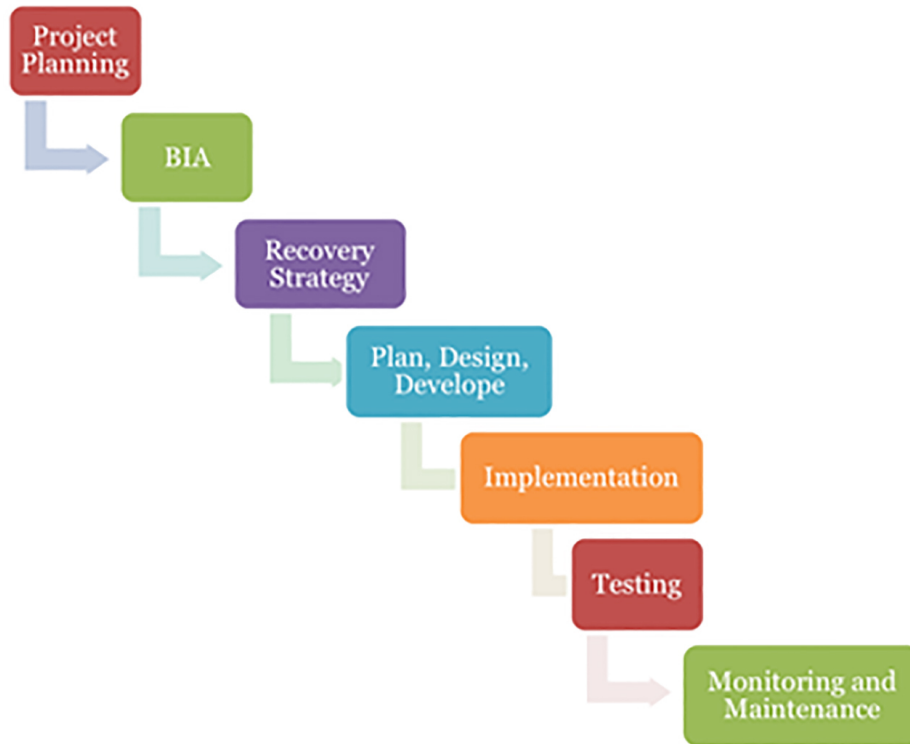
BCP is the planning process, while the Disaster Recovery Process (DRP) is the bottom level or implementation level. This lower level is a more technical level. If we take two examples, BCP is when we ask the question, “What should we do if our datacenter gets destroyed by a flood or an earthquake?” and it is DRP if we ask “What should we do if our perimeter firewall fails?” As you now understand the recovery measures from a more uncontrolled disaster is covered by DRP.

Develop and Document Scope and Plan

This is also a top-down process where the management gets approval from the top of the hierarchy by creating a business case. When it is approved, the plan can go to the next stage. Then it is the time to utilize the business and tech teams to formulate the plan. This often starts with a business

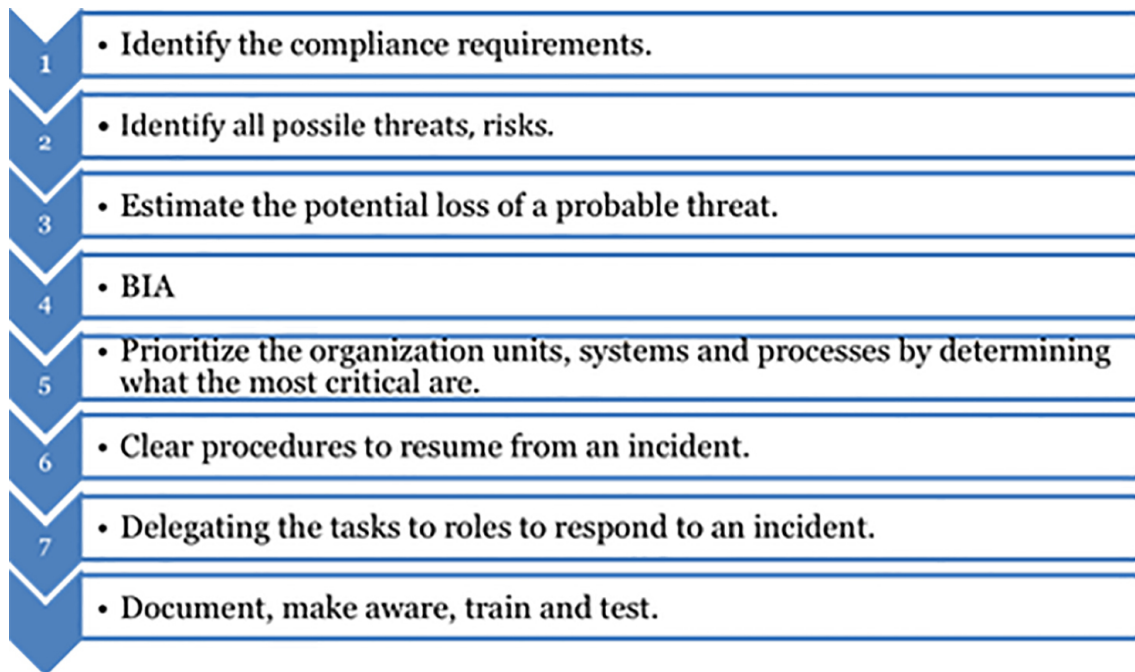
continuity policy statement followed by a **Business Impact Analysis (BIA)**. Once there is proper detail, you can create the rest of the components.

The BCP/DRP plan has several steps.



(BCP/DRP Main Processes)

Planning the BCP Process



Business Impact Analysis (BIA)

BIA measures the impact of disasters (each) on critical business functions. This acts as a catch-all. BIA is a complicated process as it requires a person or a team with the knowledge of all business processes, units, IT infrastructure, and interrelationships.

BIA Steps

Before we go into steps, we have to look at some important terms.

- RTO: Recovery Time Objective (the time it takes to recover).
- RPO: Recovery Point Objectives (how far you can go back).
- MTD: Maximum Tolerable Downtime (how long you can survive without this function).



(BIA steps)

In addition, you have to verify the completeness of the data and establish the recovery time. In this process, you have to also find the recovery alternatives and associated costs.

1.8 Contribute To and Enforce Personnel Security Policies and Procedures

In the IT environment, the top most risk is people. They can be employees, stakeholders, anyone who have access to the enterprise premises, including the network. Every user is a target for attacks such as phishing, social engineering, and similar yet sophisticated attacks. These policies and procedures are intended to reduce risks and potentials.

Candidate screening and hiring

This stage is the most crucial. The candidates must go through thorough background checks, educational verifications, certificate validation, past

jobs and track records, criminal records, and whatever is possible. If the candidate lists external referees, you must contact the person and obtain relevant information.

Employment agreements and policies

Upon a new hiring process, an employee agreement ensures the employee is bound to protect the policies. The agreement includes and sometimes defines the role (job duties), responsibility, pay-rates, how termination occurs, etc. The agreement also includes code of conduct, accountability, and consequences.

The agreement must clearly state and list the details. This reduces the risk and complexity. If an employee takes his work email when he leaves the job after a termination, he is violating a policy. These policies must be in place when such an incidence occurs.

Onboarding and termination processes

Onboarding is the welcoming phase in recruitment. It comprises of all the activities the person must go through. If the process is structured, logical, and easier to grasp, the risk is reduced greatly. To obtain the maximum results from all the of newbies, there must be a standard, documented process.

On the other hand, termination is a crucial part of the job of a manager. It is acceptable when a person retires after completing the required years. The other case is when the management is about to terminate an employee. This can be a high-stressed situation, especially if the termination is raised by cost reduction. In any case, the organization must revoke all the access to the systems.

Therefore, keeping policies and procedures documented can streamline this process.

Vendor, Consultant, and Contractor Agreements and Controls

These roles represent a worker who does not work full-time in an organization. Therefore, there is a need to take extra precautions. By selecting and make agreements with vendors, you are opening a path to your organization's data. Therefore, safeguards must be set.

In many organizations, a consultant is given a dedicated desktop and connectivity to the internal network/devices with limits because the person works for different organizations. This can result in accidental data loss, deliberate information corruption, and stealing information for profit. There must be a screening and verification process to identify these users, agreements, and put controls.

Compliance Policy Requirements

Organizations have to stay in compliance with different types of regulations and standards. During the onboarding process if the new employee is able to understand and follow the requirements, the risk is reduced. A well maintained set of documents can be used to guide new employees.

Privacy Policy Requirements

Personal Identifiable Information are sensitive to customers, employees, vendors, consultants and other parties. Therefore, such information must be kept safe. Only the indented party must be able to obtain and use the information. This process must also be audited to ensure trustworthiness. There must be a documented privacy policy to describe what types of information are covered and to who it is applied.

1.9 Understand and Apply Risk Management Concepts

Risk management is the process of determining the threats, and vulnerabilities, assessment of the risks, and risk response. The reports resulting after this process are sent to management to make educated and intelligent decisions. The team involved is also responsible for budget controls. A real-world scenario is that the organization management is spending less money and time to reduce the risks to a certain level.

Identify Threats and Vulnerabilities

A vulnerability is an exploitable problem. When a vulnerability is present, a threat is a possibility. These two are linked, as you understand now. There are known and unknown vulnerabilities. As an example, a computer may have a bug if it is unpatched. If this already has a patch, but not applied, it is a known threat. If no one except a malicious user knows it, it is an unknown threat. Identifying these is not easy in real-life situations.

Risk Assessment/Analysis

Assess Risks

Risk assessment is essential to determine if there are vulnerabilities and how those become threats. If exploitation happens, the resulting impact must be identified. There are several techniques to assess the risks.

- Qualitative: This is all about numbers and figures. This contains figures about the probability and its percentage of a specific threat to damage the organization, the loss in currency, the cost to deploy countermeasures and the effectiveness of the deployed as a percentage. The cost/benefit value governs the effectiveness of the control.
- Quantitative: This considers a scenario for each threat that may exploit a vulnerability. The probability, seriousness, and controls will be discussed in detail. After collecting necessary data occurs through surveys, meetings, brainstorming, and questionnaires. Once this is complete, the report ranks the threat, probability of occurring, and controls.
- Hybrid: Is a mixed approach of the two methods above. This offers more flexibility.

Response to Risks

There are four major actions.

- Risk Mitigation: Reducing the risk.
- Risk Assignment: To a team or a vendor.
- Risk Acceptance
- Risk Rejection

Countermeasure Selection and Implementation

Implementing **countermeasures** or **safeguards** or **controls** is important for risk mitigation. This could be by means of hardware or software. A password policy is a simple example. You can set the length, for example.

The password can be prevented from saving to a disk by preventing reversible encryption and utilizing hashing and salts. In addition, you can enforce the use of different types of characters. To further enforce, you can force the users to use multi-factor authentication. You must have a good understanding of the process of implementation.

Applicable Types of Controls

There are 6 major types of controls that we need to focus on.

- Preventive: This type of control prevents an action from happening. Intrusion Prevention Systems, Firewalls, Encryption, Least Privilege, etc.
- Detective: This type of controls detects during or after an incident. Intrusion Detection Systems, Cameras, Alarms, Software such as Antivirus.
- Corrective: Corrects things after an attack. Antivirus, Patches, and some types of IPSs.
- Deterrent: Deters or discourages someone from doing an action. Fences, Guards, Warning Signs, Warning Screens, Dogs.
- Recovery: Aids in recovering after an attack. Backups and Recovery, High Availability Clusters, Disk Arrays.
- Compensating: According to PCI-DSS terms, *"Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls."*

Security Control Assessment (SCA)

It is very good to have a security policy and controls in place. But what happens if you do not assess them periodically? The controls must be thoroughly reviewed, documented, manage changes, and implement upgrades as necessary!

Monitoring and Measurement

If you do not monitor and measure the safeguards, you'll never know if they perform as intended! This helps you to manage the safeguards, as well as ensure they perform effectively. Monitors and measures are an internal and active process that helps the management to get an idea of how and how well the controls operate.

If we take an example, this will be much easier to grasp. What if a security log indicates multiple failed attempts? You know obviously that the monitoring works but is it enough?

There has to be some way to measure the risk and impact to locate and remediate the threat. You also need to set up notifications to alert the responsible parties when an incident occurs. And you must ensure these monitoring service data is properly backed up.

A report of such an incident should contain the following details.

- Number of occurrences.
- Nature of the occurrence and end-result (success or failure, etc.)
- Duration.
- Location.
- The involved assets and parties.

Involved cost.

Asset Valuation

This is also an important part in the risk management process. The management and the team must be aware of the tangible and intangible assets and the values involved. The valuations involve the accounting department (i.e., balance sheets) as it is a measure of a value. There are several approaches to asset valuation.

- Cost Method: This is the basic method. It is based on the price for which the asset was brought.
- Market Value Method: Based on the value of the asset in the market place, especially when sold in the open market. If the asset is

now available in the market place, there is a greater difficulty to determine the value. There are two alternative steps at this stage.

- Replacement Value: If the same asset is bought, then the value can be based on that.
- Net Realizable Value: The price, if it is sold, deducted by the expenditure incurred.
- Base Stock Method: The organization maintains some level of stocks, and the value is based on the value of the base stock.
- Standard Cost Method: This method uses expected costs rather than the actual cost. The derivation relies on past experience by recording the difference between expected and actual costs.
- Average Cost Method: This is determined by dividing the total cost of goods available for sale by the units available for sale. This is applied when the valuation cannot be distinguished.

There are other methods as well as certain specific methods when it comes to the nature of the assets (i.e., tangible).

Reporting

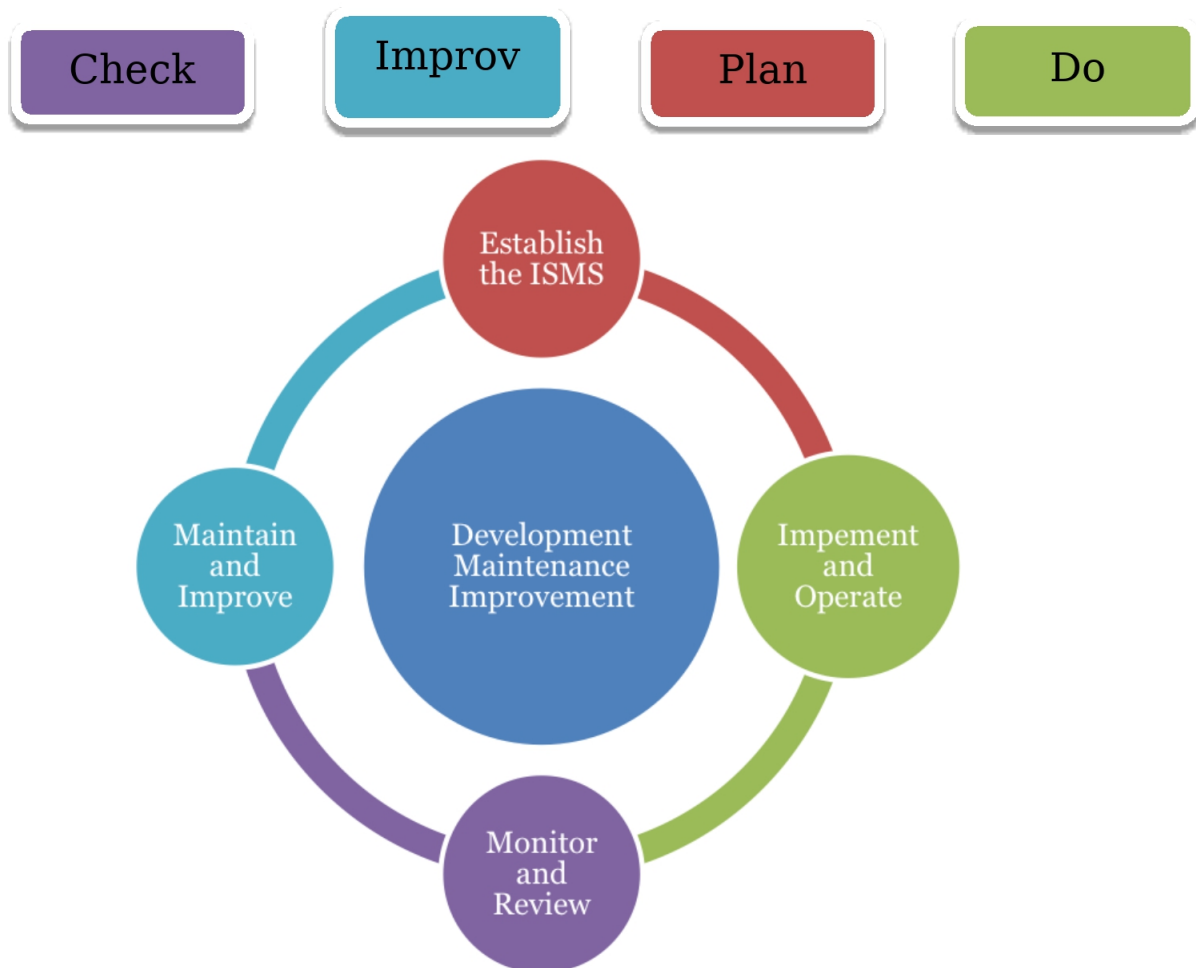
Continuous and timely reporting is a critical part of the process to prioritize the risk management needs. In any environment, reporting generates valuable information, and we can predict, proactively set measures for the future. The reports must not ignore or hide even a small piece of information. If there is a change to the risk posture, it must be clearly reported. When creating a report, also consider the requirements by understanding the laws, regulations, and standards.

Continuous Improvements

This simply means that you need to continuously improve the risk management process. This process is incremental and can be applied to process and products/services.

ISO/IEC 27000 family provides requirements for an Information Security Management System (ISMS) and an excellent guide. This includes the

requirements for continual improvements in clause 5.1, 5.2, 6.1, 6.2, 9.1, 9.3, 10.1, and 10.2.



ISO/IEC 27000, 27001 and 27002 for Information Security Management

Risk Frameworks

A risk framework is useful as the methodologies assist in risk assessment, resolution, and monitoring. Some of the frameworks are listed below.

- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE).
- NIST Risk Assessment Framework
(<https://www.nist.gov/document/vickienistriskmanagementframeworkoverview-hpcpdf>.)

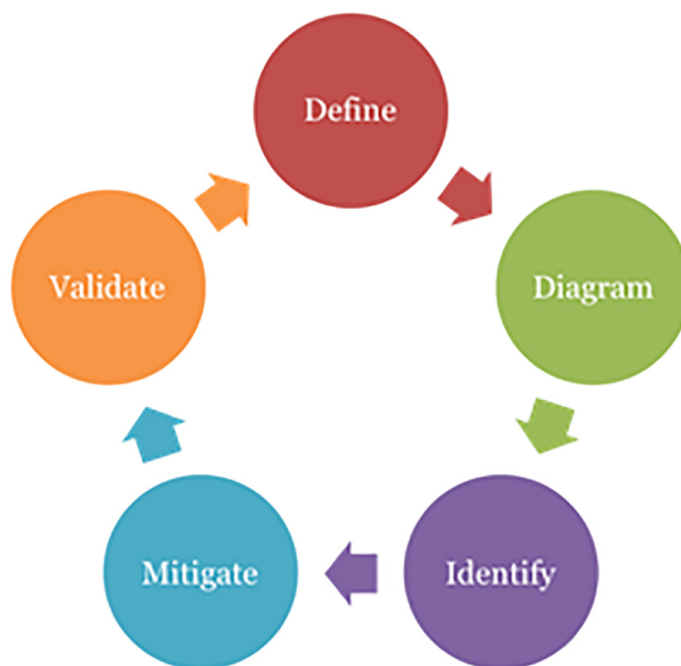
- ISO 27005:2008 (<https://www.iso.org/standard/42107.html>)
- ISACA (<http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx>)

There are individual tools and methodologies, such as OpenFAIR and TARA.

1.10 Understand and Apply Threat Modeling Concepts and Methodologies

Thread modeling is a technique used to analyze risks. Analyze means to identify and quantify the threats so that the threats can be communicated and prioritize. This is used extensively in software development. When modeling threats, you can focus on the **attacker** , on the **assets** or on **software** . Below there is a list of major threat modeling methods.

STRIDE : Invented in 1999 and adopted by Microsoft in 2002. STRIDE stands for **S** poofing Identity, **T** ampering, **R** epudiation, **I** nformation Disclosure, **D** enial of Service, **E** levation of Privilege (<https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling>).



(STRIDE Process)

PASTA : Developed in 2012, The Process for Attack Simulation and Threat Analysis is a risk-centric threat modeling technique.



VAST : Visual, Agile, and Simple Threat (VAST) is based on a threat modeling platform called **ThreatModeler** (<https://threatmodeler.com/> , <https://threatmodeler.com/threat-modeling-methodologies-vast/>).

There are others like OCTAVE, LINDDUN, CVSS (by NIST), Trike and so on. There are threat rating systems such as Microsoft DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability).

Now we will discuss the threat modeling steps in brief.

- Identifying.
- Describing the architecture.
- Breakdown the processes.

- Classify and categorize threats.
- Rate.

There is an excellent resource in which the models are compared by **Carnegie Mellon** University:

https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html

1.11 Apply Risk-Based Management Concepts

Risks

Any new hardware, software, or a service, can introduce risks to the existing security framework and posture unless properly evaluated. There will be integration difficulties as well.

- There are things to consider when evaluating the hardware such as integration, - availability (continuity) and updates.
- When it comes to software, there must be a framework to assess the security architecture. The software vendor support must be available with proper SLA schemes, and they must manage tasks such as patching.
- If it is a service, the following factors have to be considered. If the company provides the service to acceptable parties, to your competitors, if they follow security practices like you do, if they depend on third-parties for other services and can they guarantee the security as you do, etc.

Third-Party Assessment and Monitoring

If an organization is expecting to utilize a new third party, there are things to consider carefully. Agreements (e.g., non-disclosure, privacy), security agreements, and SLAs should be carefully reviewed before proceeding. When reviewing, you can match the requirements to your security architecture, standards, implementation, policies, procedures, etc.

Minimum Security Requirements

Having a minimum-security requirement specification is important in the occasion, such as mergers, acquisitions, and even during the procurement process. It serves as a baseline. This will aid in minimizing security gaps, conflicts, and counterstatements. It is better to update these requirements and set an expiration period if required, e.g., within 12 months.

There is also a requirement for a period of transition if there is a merger or acquisition. During the period, the architectures, configuration, processes, procedures, and practices can be assessed and adjusted to meet the new requirements.

Service-Level Requirements

Service levels and agreements are extremely important. The SLAs provide a guarantee of performance. Within an organization, there are internal SLAs and external or operating level agreements or OLAs. When considering the third-party software, hardware and services, their SLAs and subscription-based agreements must be reviewed and compared. During an incident, the response time depends on the SLA, and it can be critically affecting ongoing business operations.

The SLAs and OLAs must have realistic values based on certain metrics obtained by monitoring and analyzing the performance statistics and capabilities. There can be several levels based on who is being served and prioritized by the importance (e.g., software vendors provide agreements based on the subscription level. A good example is Amazon AWS).

1.12 Establish and Maintain Security Awareness, Education, and Training Program

The most vulnerable components of a security infrastructure are the human involved. If untrained and unaware, the users would not fit in and won't be able to exercise or maintain the standards, thus violating policies with or without knowing the impacts.

The need for awareness is the primary building block of communicating the security program to all the parties in the organization, especially to the employees. It can be started from basic awareness and develop the awareness through training and workshops. The guidelines and procedures

also assist in communicating the processes and best practices. The familiarity and trust can be built on the way to ensure the proper functionality.

Methods and Techniques to Present Awareness and Training

The difficult part with a security program is the beliefs of seniors that users are aware of the basic security practices and the belief of the users that they know everything. The awareness program should bring acceptance that they did not know and the will to participate. It can start from basic awareness and continue through training and education.

The security team must be confident in their understanding of security architecture. Once this is achieved, necessary training is required for non-security senior roles so that they are well aware of the architecture, policies, standards, baselines, guidelines, and procedures. This helps the business units to inherit and transmit the knowledge and practices through awareness. Moving forward, the awareness program requires the following in order to reach success.

- The senior management must actively engage in program design and presentation.
- The program has to deliver a clear perspective on how this program can secure the business objectives.
- Clear demonstration of how the program is beneficial for employees and their functions.
- The program must start from the basics focusing on building the awareness from bottom up.
- The training must be enjoyable and flexible so that the participants can actively participate.
- Measure and review the outcome, including tests.
- Update the training context.

Periodic Content Reviews

An effective security program is engaging and interesting. The content (material) has to be updated regularly along with the measurements and tests. If there are updates to the program, there has to be a program to educate the users.

The content can be changed to more engaging presentations, tests and videos. The social networks can be utilized to do campaigns and events as they are more compelling. The team can create new tests and simulations to review the level, or awareness and how it is practiced. There are many tools and techniques nowadays to achieve these goals.

Program Effectiveness Evaluation

The effectiveness is important because an organization spends money on the training program. Therefore, it must be assessed to measure effectiveness. The new allocations and budgeting depend on how secure the organization is, as well as the degree of the effectiveness of these programs.

To measure, a security team can implement metrics. Then the metrics have to be put in tests. If the outcome of the test provides positive results, the program is effective. For an example, if you put them into to test to determine if employees are vulnerable to scamming or phishing and if the resulting failure (getting scammed successfully) rate is lower than the previous, then the program is successful.

Chapter 2

Asset Security

When we use the word “Asset” it represents many types of valuable objects to an organization. In this scope, it includes people, facilities, devices, and information (virtual assets). In the previous chapter, we discussed more on assets. In this chapter, we are going to discuss about a specific asset. Information! Without a doubt, information or data is typically the most valuable asset that stays in the center. Safeguarding information becomes the main focus of a security program, with a decisive stance.

2.1 Data and Asset Classification and Labeling

What is **Data** ? In our scope, data is something that is bits and pieces that build **information** . Data can be at rest or ready to move. It is formatted from some electrical signal to a certain understandable, usable process-ready bits and bytes. We can transform this data to obtain a better understanding and a linguistic compatible version. Data that is combined to form meaningful facts or details.

Data goes through a complete lifecycle. During this lifecycle, we have to properly and precisely manage the data with security. In other words, by applying the CIA. In order to construct an effective security plan, we need to look at how important the information is and draw some lines to separate by priority and importance. This process of categorization is known as the Data Classification (or Information Classification).

Data Classification

As stated in the early paragraph, data classification is the most important part of this domain. Data must be properly classified, and there must be a way to apply a static identification. We call this **Labeling** .

The classified data will be assigned to appropriate roles to control and manage. This is called **Clearance** . If someone has no clearance and attempt to obtain it, there must be a process to obtain it. This process is

called **Access Approval** . Finally, the CIA is also applied and is served by practicing the **least privilege** (based on the **need-to-know** principle). A new user or role must have specific boundaries when accessing and dealing with such data. This is also defined in the classification and labeling process and then informed to the users upon granting access. They must stay in the boundaries to accept the provided authentication, authorization, and must be held accountable (AAA) for the actions they perform. To avoid security breaches, the least privilege is provided – to provide the necessary parts to perform the job.

If you are a U.S. citizen, you may already know the Executive Order 12356; EO 12356 (Executive Order 12356; EO 12356). This is the executive order followed as a uniform system in the U.A.S. upon classifying/declassifying and safeguarding national security information. Different countries follow similar directives.

There are some important considerations when it comes to data classification.

- Data Security: Depending on the type of data, regulatory requirements, and appropriate level of protection that must be ensured.
- Access privilege: Roles and permissions.
- Data Retention: Data must be kept ,especially for future use and upon regulatory requirements.
- Encryption: Data can be **at rest** , **in motion** or **being used** . Each stage must be protected.
- Disposal: Data disposal is important as it can lead to leak information/data. There must be secure and standardized procedures.
- Data Usage: The use of data must be within the security practices. It has to be monitored and audited appropriately.
- National and International Regulations, Compliance Requirements: The requirements must be understood and satisfied.

Labeling

We already described the labeling process. Let's take a look at the different classifications.

- Top Secret: This is applied mainly to government and military data. If leaks, it can cause grave damage to an entire nation.
- Secret: This is the second level of classification. If leaked it can still cause a significant damage to a nation or a corporation.
- Confidential: If leaked, it can still cause a certain level of damage to a nation or a corporation.
- SBU (Sensitive But Unclassified): This type of data does not cause damage to a nation, but can affect people or entities. Health Information is a good example.
- FOUO (For Office Use Only).
- Unclassified: Data/information yet to be classified or does not need a classification as it does not include any sensitive data.

Asset Classification

In this domain, assets are two-fold. We already discussed data as an asset. The other assets can be physical assets. The second type of assets are classified by asset type and often used in accounting. The same methodology can be used in information security.

2.2 Determine and Maintain Information and Asset Ownership

What is the need for an owner? An owner is a person who is responsible to keep, manage and safeguard an asset. Data also needs an owner to classify and secure the lifecycle of the data. If there is no clear owner, who would be accountable for the actions performed on data? How can you classify data, set permissions/rules/regulations, provide access through clearance, define the users, safeguard the stages, retention, and dispose securely?

2.3 Protect Privacy

There are several roles you need to learn in this domain. Let's look at the roles.

- **Business/Mission Owners:** The top-level hierarchy who have the ultimate responsibility to initiate, implement a proper security program, fund the program, and ensure the organization follows.
- **Data Owners:** This is usually the management who is responsible for the security of the data they own or manage. They have to classify the data, label the data, and determine the retention, backup, disposal requirements. The owners do the management operations, not the technical part.
- **System Owner:** Is responsible for the assets that hold the data, the computer hardware, and related technologies. He has to properly maintain these systems to the standards (patching, updating, configuring, etc.)
- **Data Custodian:** A custodian is a role responsible for delegated tasks. The person has to perform the hands-on duties such as backing up data, running recovery simulations, apply patches, and configuration.
- **Users:** The general users who are using the systems. This is the weakest link. Therefore, they must be informed and taught about the data and protection specifically. They are responsible for complying with the policies, standards, procedures, etc. If they fail to meet the policies, they have to bear the consequences. The management must educate the users about penalties.

Data Controllers and Data Processors

Data Controllers: Create and manage sensitive data. Human Resource team is an example that is responsible for sensitive personal data.

Definition of the European Commission : The **data controller** determines the **purposes** for which and the **means** by which personal data is processed. So, if your company/organization decides 'why' and 'how' the personal data should be processed, it is the data controller. Employees

processing personal data within your organization do so to fulfill your tasks as a data controller.

Data Processors: Manage data on behalf of the data controllers. This can be a third-party service.

Definition of the European Commission : The **data processor** processes personal data only **on behalf of the controller** . The data processor is usually a third party external to the company. However, in the case of groups of undertakings, one undertaking may act as a processor for another undertaking.

This definition says “in the case of groups of undertakings, one undertaking may act as processor for another undertaking”. This is an important fact. A data controller can become a data processor given different sets of data.

Another important thing to remember is the **joint data controllers** . One or more teams can join in this effort.

According to the European Commission “Your company/organization is a **joint controller** when together with one or more organizations it jointly determines ‘why’ and ‘how’ personal data should be processed. Joint controllers must enter into an arrangement setting out their respective responsibilities for complying with the GDPR rules. The main aspects of the arrangement must be communicated to the individuals whose data is being processed.”

Data Remanence

When we follow traditional data deletion techniques as an IT student, you may already know that the data on magnetic discs are still recoverable. This becomes a huge security risk as the organizations have to replace the disks when they fail. This is not limited to disks, and sensitive data that can be exposed.

There is a lot of storage types. RAM, ROM (there are many types and are either volatile or persisting data but can be deleted by electronic means), cache, Flash memory, Magnetic (e.g., hard disks), and Solid-State Drives (electronic).

Destroying Data

Now you are aware of the requirement regarding device disposal. You need to ensure the storage is not dumped while there is recoverable data. The following methods can be exercised before disposing of the storage devices.

- Overwriting: In this case, a series of 0s and 1s will be written so that the data is overwritten successfully. There can be a single pass or multiple passes. If multiple passes are applied, the recoverability gets close to zero.
- Degaussing: This is applied to magnetic storage. Once it is exposed to a strong magnetic field due to alterations, the disk will be unusable.
- Destroying: The physical destruction is considered to be the most secure method.
- Shredding: Is applied to paper data, plastic devices, and storage.

Collection Limitation

This is another important and cost saving option. If you limit storing sensitive data, such as certain employee information, you do not have to protect this set of data at all on your end. If an organization does not need certain data/information, it should not collect vat amount of unnecessary burden. If personal data is collection, there must be a privacy policy that determines what is collected, how the organization is intended to use it and all the relevant details. It must be transparent to the people who provide such data.

2.4 Ensure Appropriate Asset Retention

The retention of data is a need and a risk. An organization should have a specific policy to keep data for the current and future needs. This is either enforced by company policy, or to satisfy a specific law/regulation/compliance requirement. Once the period is over, the data must be destroyed in order to prevent any exposure.

The period of retention is also an important part. This raises issues such as the obsolescence of the storage device technologies and the people who have

the knowledge to operate such devices.

If the retention period is 10 years, the technologies will change, and the old data must be migrated, and it can be a difficult process. When it comes to the operators, after 10 years there may be difficulties in finding people with knowledge about old or obsolete technologies.

There is another important part when it comes to retention. You must ensure the data is available and recoverable. Therefore, the data/system owners and custodians must have a plan to go through the validity and usability of the data.

2.5 Determine Data Security Controls

To determine the data security controls, you must first understand the states of data.

Understand data states

- Data at Rest: When the data is unused and not transmitted, it is called data at rest.
- Data in Motion: When transferring/transmitting data.
- Data in Use: The data while it is used by any party.

Scoping and tailoring

This process intends to fine the scope and tailor on top of it. First, which controls are in and out of scope has to be determined. This is called **selecting standards** . Then the controls must be implemented tailored to the requirements.

According to NIST - Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication (SP) 800-53 Revision 4, tailoring process is as follows.

- Identifying and designating common controls in initial security control baselines.
- Applying scoping considerations.

- Selecting compensating control.
- Assigning specific values to organization-defined security control parameters.
- Supplementing baselines with additional security controls or control enhancements.
- Providing additional specification information for control implementation.

Standards selection

During this process, an organization selects and documents specific architecture or technologies. This provides a baseline for an organization to start and construct upon. Standards selection is focusing mainly on technologies. This should not be conflicted with vendor selection. This laid out framework does not change even if the people change. This helps an entirely new team to adapt and work through the same standards and scale the operations.

It is also important to know some of the standard frameworks. This has been discussed even before in previous sections.

- ISO 17999 and 27000 series.
- OCTAVE.
- PCI-DSS.
- COBIT.
- ITIL.

Data protection methods

We have discussed the stages of data previously. In each stage, the data must be protected.

- Data at Rest: Encryption can be applied to the data in various storage volumes. There are integrated memory and cache protection at the operating system level. Storage access can also be controlled by authentication controls. There are encryption standards to select

to encrypt partial or entire disk operations in an enterprise. BitLocker drive encryption is such a technology.

- Data in Motion: While communicating, data and information streams must be well protected. There are many methods. Using SSL/TLS, certificate authorities, PKI, and many others can be applied. End to end encryption can be used along with VPN technologies.
- Data in use: The data while in use can be protected with OS level security. Memory corruption and saving active memory with hibernation and other activities have to be discouraged. Selection of appropriate malware defense is also critical.

Now, in each step we need to keep logs to record the accountability. Auditing and audit logs keeping the logs safe and are a set of required tasks.

2.6 Establish Information and Asset Handling Requirements

As we discussed early applying classification through appropriate labeling is the place to start implementing the process. Labeling is important in other cases, such as someone accidentally getting access to data. If it is appropriately labeled the person is able to hand over the data to the data owner.

The assets should be labeled as well. Information assets such as disks, tapes, and backup devices can be protected while at rest and in motion. This can also be applied to the assets, such as papers, files, disks, CD/DVD ROMs, external drivers, etc.

The storage areas must be appropriately identified and informed to the roles and the users. The level of access can be determined by physical labeling and locking mechanisms, including security controls.

Destruction of data is another critical step in the final stage of the data lifecycle. Proper destruction requires standard methods. The classification levels must be tied to appropriate disposal stages and verification. The methods of data destruction are discussed previously and therefore, it will not be listed here.

Chapter 3

Security Architecture and Engineering

Now we have arrived at a more hard-core domain. This domain is highly technical than most of the other domains. This is a perspective on architecture and engineering that expand from fundamentals to aspects of other domains.

3.1 Implement and Manage Engineering Processes using Secure Design Principles

We have to employ a secure design principle for many reasons in the implementation and management process. Mainly, you need to stay within the proven methodologies and practices. This prevents unnecessary complications, risks and functionality issues while ensuring the budgetary requirements. To do so, we need to incorporate secure design principles to the engineering process.

Before going into the details, let's look at the components of an engineering process in brief.

- Design ideas and conceptualization: In this stage, a concept is developed to address a need and is documented the ideas and scope.
- Requirements: In this stage, the business and other requirements are documented. This includes the requirements from stakeholders and other parties. The nature of the requirements can be functional or non-functional (e.g., to meet regulations).
- System Design: In this stage, a design is made to meet the requirements. Here, designers must integrate security standards and concepts.
- Implementation: In this stage, the design is implemented part by part and gets integrated into the whole system.

- Testing: Initially, the tests will be carried out in the component level and arrive at modular testing. Finally, a more complete implementation will be tested in stages (i.e., Beta), followed by a full test, simulations, and acceptance tests. There can be 3 development environments; development environment for the engineers, test environment for the testers to test without mixing up with the business-critical systems, and a production test environment. The quality assurance process provides a guarantee that the implementation is bug-free, secure and compliant.
- Deployment: In this stage, there will be automated deployment processes and auditing processes to ensure the success.
- Maintenance and Support: Once the system is deployed, there must be a team to perform these tasks.
- There are other stages, such as training, and these are also important to bring awareness and familiarity with security practices.

3.2 Understand the Fundamental Concepts of Security Models

What is the purpose of using a security model? A model is like a Blueprint. It enables the design to address specific security boundaries. This also ensures classification and clearance. As a CISSP student, you should be familiar with the available security models and what type of plus points and complications exist.

Bell LaPadula (BLP) model: The model is a state-machine model implemented and formalized to become part of the U.S. DoD multilevel security policy (MLS). The model addresses one of the key elements of the CIA triad, the Confidentiality.

It ensures the **no-read-up** and **no-write-down** actions.

- A lower level clearance prevents reading objects from upper levels
- A higher classification cannot read security objects to a lower level.

To specify discretionary access control, a matrix is utilized.

The problem with this mode is the lack of write-up controls. Therefore, there is a need to integrate other models to ensure complete coverage.

Biba Model : This model was proposed after the BLP model. It addresses the gaps that existed in the BLP model while ensuring the Integrity. It ensures no-read-down and no-write-up.

- A higher-level clearance cannot read the lower integrity level of security objects.
- A lower-level cannot write to higher integrity level objects.

There are other models like the **Clark-Wilson** model.

3.3 Select Controls Based on Systems Security Requirements

In this section, we'll learn how to evaluate security systems by following a specific standard. The **Common Criteria for Information Technology Security Evaluation** (referred to as **Common Criteria** or **CC**) is an international standard (ISO/IEC 15408). This unifies the following older standards.

- The Information Technology Security Evaluation Criteria (ITSEC): This is the European standard developed in the early 90s.
- The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC): This was introduced in 1993.
- Trusted Computer System Evaluation Criteria (TCSEC): This was the U.S. DoD standard known as the Orange Book, which is a part of the Rainbow Series (a series of computer standards and guidelines introduced in 90s and 80s).

According to the <https://www.commoncriteriaportal.org/> , the Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA).

These certificates are recognized by all the signatories of the CCRA.

Now let's look at the CC in detail.

- The CC can be applied to both hardware and software.
- A Target of Evaluation (ToE) has to be selected first. For example, a server, a software product, or a security software.
- According to the National Information Assurance Partnership (NIAP), "Effective October 1, 2009, any product accepted into evaluation under the U.S. CC Scheme must claim compliance to a NIAP-approved PP". Here, a Protection Profile or a PP is a specific set of security features required to claim the compliance with the CC. Vendors may provide PPs and certain exclusions for evaluation purposes.
- ST or Security Target identifies the security properties with respect to the ToE. ST can be thought of as a set of security requirements used as a basis of an evaluation of an identified ToE.
- The evaluation procedure is aimed to assess the level of confidence.

The basis of the CC is functional and assurance security requirements. There are 7 Evaluation Assurance Levels. At the highest level, there is the highest confidence.

1. EAL1: Functionality Tested. This ensures only the functionality and does not view threats to the security in a serious manner.
2. EAL2: Structurally Tested. In this level, a low to moderate independently assured security, yet it is not for the complete development. This is usually applied to legacy systems upon securing.
3. EAL3: Methodically Testing and checked. This goes a level beyond EAL2, by assuring a moderate level of security and a through ToE check.
4. EAL4: Methodically designed, tested and reviewed. This goes a level beyond EAL3 by assuring moderate or high security. At this level, additional security costs are involved.

5. EAL5: Semi-formally designed and tested. High, independently assured security and rigorous development practices while preventing high cost situations.
6. EAL6: Semi-formally verified, designed and tested. Applied for high-risk situations where STs are developed and the security requirement justifies the cost.
7. EAL7: Formally verified, designed and tested. Applied when the risk is very high, and the cost incurred is also the same.

3.4 Understand Security Capabilities of Information Systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

This section focuses on the systems and components (e.g., hardware components) and their capabilities to secure the processes. Although the topics are covered in this section and other sections, you have to gain additional knowledge from your environment and outside of the book.

There are some important design concepts to become familiar with. One of these is Abstraction. There are functional levels of a chunk of data. Assume you are writing data to a notepad. You do not know about the layers below the application layer. Abstraction is a way of hiding unnecessary components, thus reducing risks.

Another is the Layering which goes together with abstraction. Layering separates modules into tiers. There is also abstraction built-in to differentiate the layers.

Finally, there are Security Domains. These domains limit access levels. We learned how we can label the data by classification. Each classification is also a domain. This domain concept also applies to the hardware. This model is called the Ring model, and it separates the Kernel mode and User mode in an operating system environment and also in a virtual environment (e.g., ring 0 is for the Kernel and ring 3 is for user applications).

Protecting the working memory

The memory of a computer is occupied by multiple programs and processes. Each segment of memory is allocated specifically to operating system operations and specific applications. An application or a process must not access a memory allocation that is not allocated to it.

- Hardware Isolation (Segmentation): Segmenting the hardware by importance and criticality during allocation (e.g., memory allocation).
- Process Isolation: Isolating the processes from each other during the operation (e.g., virtual memory, multiplexing, encapsulation).

Since we live in an age where virtual environments are common. In this case, the security of the host and the hypervisor are vitally important. By securing the host, isolating to high-security zones, by using a specific team to manage it can help protect the entire virtual environment.

There are two types of hypervisors.

- Type 1: Uses the operating system level (e.g., VMWare Esxi).
- Type 2: Runs on the operating system (e.g., VMWare Workstation).

A virtualized platform can be on-premise or cloud-based. For systems such as Amazon AWS, there are strict security implementation and practices.

Trusted Platform Module (TPM)

This is a hardware chip on a motherboard. Unlike any other chips, this has a specific task; to perform cryptographic operations. It can generate random numbers, generate and store cryptographic objects by running algorithms, and other security operations. A common example is the Windows BitLocker operation. To ensure the maximum-security operation, BitLocker must be used with the TPM.

Interfaces

Interface is another important concept. This is common in client-server systems. When a client is contacting the server, it uses an interface (e.g., VPN systems). These interfaces have specific security capabilities.

- Encryption: When a client wants to communicate with the end system, the end to end communication channel (called a tunnel in this example) can communicate privately without being transparent to the outsiders. If we take VPN, there are multiple ways of securing the end-to-end communication. SSTP, IPSec are a few examples. If you take file transfer as an example, there are multiple ways such as SFTP, FTPS, FTPES, etc.
- Message Signing: This method guarantees the non-repudiation. A sender digitally signs the message with his/her private key and sends the information. The receiver can open the message only from the sender's public key.
- Fault Tolerance: By engineering the fault tolerance and backup systems, within a system can prevent failures and availability issues.

3.5 Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements

In this section, we study various system architectures, security architecture with respect to the systems, how it is designed, mitigate and resolve security issues.

Client-based Systems : In any security design, the weakest link is the client end-point. The client can be a device, a computer or a smart phone. With the internet connected and the nature of the devices, they are extremely susceptible to attacks. Most of the users are unaware of patch management, vulnerabilities and required security practices.

The software load in any device widens the attack surface. Furthermore, even if protected, people are susceptible to social engineering attacks. Therefore, a specific consideration must be taken to protect the security and privacy. To protect the client, a good internet security suite with a client-side firewall is essential. This must be incorporated with built-in operating-system level defense mechanisms.

Server-based Systems : Even though it is difficult to compromise directly, through a client connection, it is not so difficult. This is why we emphasize on client security in the previous section. A server is a place where valuable

information is stored. If an attacker can gain access to a server, a large amount of valuable data can be stolen for commercial purposes.

It is important to follow standard procedures and security frameworks to ensure the security as defending a server is much more sophisticated than a client. In high-security environments, there are custom operating systems in place. In other sections, the servers must be properly patched (even the server image during deployment), the end-points must be secured, a remediation system with multi-layered authentication/authorization system must exist before permitting any operation.

Databases : This is the most critical asset of any information system. The databases hold the most important data such as mission-critical information, secrets, PII, statistical data and more. The databases are used to store information even in the client level (e.g., SAM database in Window clients) and these systems have certain protection built-in. This does not mean you need not to safeguard the systems.

If an attacker gains even a small level of access through a client or through an interface, he could use the same database techniques (querying, aggregation, inference, using mining and data analytics) to gain access to data. The security framework must be able to deploy the necessary techniques and mitigate potentials.

Cryptographic Systems : We briefly discussed encryption and digital signing earlier. Cryptography helps to increase the difficulty of finding a crypted message with success. It can be either time consuming or resource consuming. Either way, you can discourage the attackers. However, there are issues with such systems as well.

- Except for cryptographic system services, there is third-party software. Any software can have a bug, a security flaw, or a design flaw.
- There are well-known algorithms to generate cryptographic keys. The selected key must be a sufficiently large random number, and the permutations must be higher.
- A key is the most important part of this system. A key must remain a secret! It must be sufficiently long. If we take a symmetric

key, it has to be at least 256 bits long. For a symmetric key, the recommended key length is 2048 bits. When selecting a length, it should be based on your requirement and regulatory requirements.

- Protocols: There are protocols such as SSL (SSL/TLS), SSH, Kerberos, and IPsec. These protocols are capable of performing cryptographic functions.

Industrial Control Systems (ICS)

Supervisory control and data acquisition (SCADA) is a type of industrial control within a specific grid or a network. Within the scope, there are software and computer systems performing critical tasks. These are most of the time national level operations and the emergence of risks to such systems, including the decades older systems possess a real threat to the national-level operations. These systems are intended to monitor critical product parameters and provisioning of the critical services. If these systems are opened up or somehow connected to internet the lack of security can lead into catastrophic failures.

If you are following cyber security threats, Stuxnet is one of the most famous viruses created to attack Iran's nuclear power plants. There were other sophisticated malware such as Duqu which can damage these operations. These systems incorporate with powerline communication systems (PLC), and these systems are also vulnerable to attacks. Therefore, the risk is real, and proper layers of security must be implemented.

Cloud-based systems

There are many cloud-based systems. Let's look at some of these in brief.

- Public Cloud: This is when you outsource your infrastructure, storage, etc. for multiple benefits including maintenance cost, ease of integrations, high availability and to leverage economies of scale.
- Private Cloud: These are on-premise clouds or dedicated cloud networks for organizations and government.
- IaaS (Infrastructure as a Service): The infrastructure level operations and provisioning capabilities of networking, storage, etc.

are provided. The resources are highly scalable, easier to automate, manage, monitor and secure. An example would be Amazon AWS.

- PaaS (Platform as a Service): PaaS is a framework which provides a development environment for applications and application deployment. The underlying infrastructure is managed by the third-party. Windows Azure, Google App Engine are examples.
- SaaS (Software as a Service): Simply cloud-based applications, such as Google Apps, Dropbox, and Office 365.

Cloud-based systems are mostly managed by the service provider. As a security professional, you must focus on the areas you can access and control. Areas that you can control differs according to the levels. Identity and Access Management (IAM), multi-factor authentication, Remote Access Protection, End-point protection/firewalls, Load balancing, encryption, storage/databases, and even networking may be among the list and can be managed depending on the layers. For private clouds the owner will be able to manage even more. In any case, you should also collect security and analytical data. If there is logging support, enabling the logs is also a good practice. Some providers, such as Amazon, offer auditing and tracking. If your organization requires compliance, the provider must provide the service. If the services are geographically dislocated, compliance requirements such as HIPPA may not be available in such areas thus not implemented. Therefore, when evaluating the cloud services, be sure to compare the security strategies, regulations, and other core requirements with the services they provide.

Distributed systems

These systems are basically distributed across different geographical areas while working together to perform common tasks. Web services, file sharing, computing services can be among these. The main issue with these systems is that there is no centralized control or management. Additionally, the data is not in a single location and therefore, maintaining the CIA triad can be difficult.

Internet of Things (IoT)

This is one of the emerging areas and one of the crucial areas to manage protection. Such devices include embedded technologies and electronics. Devices such as health monitors (wearables), home defense systems, appliances, vehicle controls, and billing machines are a few examples. These implementations do not follow heavy standards, don't get updates in a controllable manner, security updates are not regular, and light authentication and security makes things worse. Therefore, a critical evaluation and looking into the history, in terms of security, is of utmost importance.

3.6 Assess and Mitigate Vulnerabilities in Web-Based Systems

Web-based systems

A web-based system is a web-server based service or an application. Many apps are browser-based. Some client-server apps are software-based as well as web-based. There are many varieties of software, applications, and services. As these systems exist on the internet, even a small vulnerability is enough to create lasting damage. Even if there is no vulnerability, these are susceptible to other types of attacks, including DDoS. The attack surface is wider, and attackers with less knowledge may tend to exploit because it is just there in the public space. The following areas must be assessed in order to set up the countermeasures to mitigate the vulnerabilities.

Web-servers

Web-based systems use a single-tier or multi-tier server system. There are millions of services and servers on the internet. The security threats and attack attempts are at the same or even a higher magnitude. The servers must be updated, patched, and must run the latest versions of the servicing software. In addition, the back-end, including the databases, must be protected from less-secure coding and weaker protection. There must be underlying mechanisms to mitigate the risks of denial of service attacks. It is possible to monitor, log, and audit the servers to find issues, flaws, attacks, and fix problems. Encryption must be utilized whenever possible.

Endpoint Security

End-points of a server-based system is obviously the clients. This is a weak link, and appropriate measures must be there to protect the servers from getting compromised. To mitigate, we can follow a layered-approach by securing the traffic (end-to-end), utilizing antivirus/internet security, a host-based firewall and up-to-date, mainstream web browsers.

The Open Web Application Security Project (OWASP) is a popular, world-wide, non-profit organization focused on improving the security of software. OWASP analyzes and documents the most critical web application security risks. More information can be found by visiting: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)

3.7 Assess and Mitigate Vulnerabilities in Mobile Systems

Mobile systems are widespread and taking over the computer era. The risk it poses is greater than and even more difficult to manage. There are many devices, operating systems, software repositories, versions and different security flaws. Such systems are difficult to manage centrally and apply a unified policy. However, the security policies, standards, baselines, and procedures must be applied whenever possible. Just like a client computer device, it must have all the security features enabled, configured, installed, and patched.

There are lots of integrated security features when compared with computers. These devices have biometric controls, multi-factor authentication, recovery, remote tracking, and wiping capabilities. There are locking mechanisms, even if the device is stolen.

3.8 Assess and Mitigate Vulnerabilities in Embedded Devices

There was a time when the computer accessories were connected or attached directly to the computers. As the semi-conductor technologies evolve, these devices became standalone devices. From a tiny hand-held scanner to large printer processing machines, projectors, smartboards, house-hold appliances, multi-functioning devices, embedded systems in vehicles and surveillance units, and many more exist today. This also includes the IoT devices. Although the risk is low, if these units are used within the organizations, security and protection have to be exercised.

Embedded devices with the technological advancements are able to involve in various communications, and these activities can pose a threat.

- Embedded devices are capable of communicating with the developer's networks. Some of these firmware applications tend to send crash data, debug logs, etc. These communications are dangerous, and the available options must provide means to block such activities for good.
- WPS and other connectivity methods must be disabled as the devices tend to initiate communication with a near-by device. Therefore, the protocols must be filtered whenever necessary.
- Finally, IoT devices are emerging and appearing in the enterprise. Such devices possess more threats, as they are incapable of access management and cryptographic operations. Therefore, you should understand that IoT is not suitable for every organization!

3.9 Apply Cryptography

Cryptography is a large area of focus and is a complex study which involves mathematics. There are many techniques and flavors. For this exam, you need to focus on the high-level details rather than technical implementation.

Cryptographic life cycle (e.g., key management, algorithm selection)

Cryptography depends on the numbers, complexity, and computation power. As you already know, it depends on the secrets, key length, and key space. With the technological development, the capabilities of computation including CPUs, mobile processors and GPUs threats are continuously evolving in parallel.

Although cryptography is safe given the strength of the algorithm and the key, there can be vulnerabilities in algorithms and cryptographic system itself.

Federal Information Processing Standards (FIPS) is developed by NIST in accordance with FISMA (Federal Information Security Management Act). According to FIPS, there are certain categories that you need to understand.

You have to avoid using weak cryptographic algorithms, weak key lengths, deprecated algorithms, and legacy algorithms. Instead, you can rely on approved and accepted standards. However, there are restrictions on key lengths given the use and the organization type.

Cryptographic methods

There are some cryptographic methods you need to become familiar with.

Symmetric: In symmetric cryptography, the same key is used to encrypt and decrypt the data. As you can see, the danger is the exposure of the encryption key. In this case, you have to select a longer key length. However, depending on the requirement, you can select a smaller key, and it can prevent heavy resource consumption.

Asymmetric: This is basically a public key encryption standard. There are two keys to do the encryption and decryption. One key is private which must be kept as a secret, and the other is a public key and anyone can use it. If someone outside encrypts the data using another's public key, only the owner of the private key can decrypt it. This can be used to ensure CIA triad and non-repudiation. However, to achieve this we have to depend on trust.

A **PKI** (Public Key Infrastructure) has multiple tiers. It has a **Root Certification Authority**, and sub-level functions performed by down-level servers. After the root server, there is a set of **Policy CAs** and an **Issuing CAs** . In normal operations, there will be **Subordinate CAs** online and serving while the root server is disconnected (offline) and kept secure. The rest of the servers manage the policing and issuing/revocation tasks.

The public keys must be trustworthy, and we rely on public certificate authorities (or even a CA within the organization). If you take PGP, however, it depends on the web of trust (individual endorsements). The PKIs and certificate authorities provide policies, procedures, templates and configuration so that we can customize and use it to fit our requirements.

A PKI must have a **Certificate Policy** and a **Certificate Practice Statement (CPS)** . The CPS must describe how the PKI is using the identities, the how private keys are stored and how certificates will be used.

When we consider certificates, it has an expiration. Even before the expiration, an authority can revoke the certificate. This can be due to other reasons including legal issues or due to vulnerabilities. In such cases, the certificates must be revoked, and a revocation list must be available for public access.

Key management practices

- **Key Creation and Distribution:** The creation and distribution must be made through a secure channel as the information must be kept secret between the two parties. If you are a Windows user, you can store the keys in the certificate store.
- **Key Protection and Custody:** The requirements for key protection is self-explanatory. You can keep the keys safe with passwords and other methods. You can even share the access to keys called **Split Custody** . By this method, you can share parts of an access key so that only the aggregation can unlock the key.
- **Key Rotation:** To increase the randomness and odds, you must rotate the key in specific time intervals.
- **Key Destruction:** As you are now aware, the keys have a specific lifetime. A key can be suspended or revoked. Furthermore, a key can reach its expiration and destruction unless renewed. Each of these processes must follow specific guidelines and avoid any exposures.
- **Key Escrow:** This is also known as the Fair Cryptosystem. The keys need to encrypt and decrypt are held in an escrow. In certain circumstance, an authorized third-party can access the keys by this method.
- **Key Backup and Recovery:** As with any data keys can be lost or get corrupted due to technical issues or even a recovery is required upon legal issues. Many PKIs provide such facilities, and it is the best to use it and keep the keys safely backed-up.

Digital Signatures

We already discussed how this can be useful under the message signing section. By digitally signing, you can prove that you are the original owner of the sending object.

Non-repudiation:

Non-repudiation is the purpose of digitally signing an object. The origin of the object is logically certain. However, if someone is sharing the private key or if someone has stolen it, it is difficult to rely only on this. Therefore, it should be combined with confidentiality.

Integrity

To obtain this characteristic, we use a mechanism called **Hashing**. Hashing is different from encryption. Encryptions can be decrypted. Hash is a one-way function and is generated by a specific algorithm. There is no private key to unlock the hash and decrypt the content. This is a very secure method, however, is susceptible to brute forcing methods by attempting collision attacks, pre-image attacks, birthday attacks, and so on. If you try generating hashes by using a random input string and matches to the hash, eventually you will be able to find the match. However, it can take a very long time. This is why passwords are protected by hashing techniques rather than encryption.

To obtain additional protection by introducing randomness, we can use something called a **Salt**. A salt is another sub input string which is random and can be rotated. This ensures stronger protection against attacks.

Understand methods of cryptanalytic attacks

- Cipher Text Only: The attacker knows the algorithm and ciphertext to be decoded.
- Known Plain Text: The attacker knows the above and one or more plain-text-cipher text pairs formed with the secret key.
- Chosen Plain Text: The attacker knows the algorithm, cipher text to be decoded and a chosen plain text together with its correspondent cipher text generated with the secret key.

- Chosen Cipher Text: The same as above except for the last part. The cipher text is chosen by the cryptanalyst together with the decrypted plain text generated with the secret key.
- Chosen Text: Chosen plain-text + chosen cipher-text combination.

Digital rights management

Rights are basically what you are allowed to do and not do against any data object. In the enterprise, this is known as Digital Rights Management, Rights Management, Information Rights Management, and so on. To manage rights per object, we have to utilize the classification techniques, clearance, authorization and permissions. This is also applied to portable data. The main intention is to protect the organizational data and assets, especially during the sharing process. Some organizations permit external access (e.g., another organization) to certain assets and resources. Therefore, a separate set of rights have to be managed for the outsiders, e.g., through federation services, and so on.

As we are familiar with cloud concepts to a certain extent, rights management has to be integrated accordingly. There are many RM solutions enabling you to track and audit actions, pass and edit the rights on-demand.

3.10 Apply Security Principles to Site and Facility Design

In this chapter, we are looking into secure design principles when it comes to sites, such as organization facilities, data centers, server rooms and network operation control centers, etc. Why do we even take this into account? Because the selection and design can mitigate the risks associated with the land (natural disaster concerns), position, environment, and other factors.

From the construction plan, a security plan must be considered. To take advantage of natural properties is essential. One of the methods used in constructing secret operation facilities is Urban Camouflage. To blend with the surroundings and avoid unnecessary attraction are the key parameters.

The location being an area facilitating natural surveillance is another important consideration. By eliminating the hidden areas, dark corners, by

utilizing the opportunity to set observatory points (e.g., from above) a certain level of defense can be assured.

Another important consideration is the territorial control. In an organization, there will be different locations where people need clearance and stay away if they do not have it. By using specific signs and other means (e.g., cameras), the organization can prevent and detect any security threats.

Specific consideration on access zones, access controls, parking lots, standoff distance, warehouse access, lighting, and signage are required.

Access Control is one of the most prominent considerations. By importance, each entrance can be guarded with fences, security people, and so on. If the areas require multiple levels of clearance, appropriate signs, access control mechanisms, including biometrics with surveillance.

The overall goal of this section is to focus on deterring attacks and disaster prevention.

You should also have an idea about Crime Prevention Through Environmental Design (**CPTED**). According to the CPTED,

“Crime Prevention Through Environmental Design (CPTED) is defined as a multi-disciplinary approach for reducing crime through urban and environmental design and the management and use of built environments. CPTED strategies aim to reduce victimization, deter offender decisions that precede criminal acts, and build a sense of community among inhabitants so they can gain territorial control of areas and reduce opportunities for crime and fear of crime. CPTED is pronounced ‘sep-ted’ and it is known around the world as Designing Out Crime, defensible space, and other similar terms.”

You can find more information by visiting <http://www.cpted.net/>

3.11 Implement Site and Facility Security Controls

In this section, the focus is on internal facility conditions, securing and mitigating incidents. In other words, we concentrate on physical security and how it should be implemented.

Wiring closets/intermediate distribution facilities

A wiring closet is a place or a room where there is hardware and wiring. Once a person gains access, he or she can perform MITM and data access/modification. The closets must be restricted to a specific team of technicians. When someone accesses the areas, there must be a proper area to enter, obtain the clearance, and use an electronic mechanism to record access to the internal areas. The doorways can be secured and used for monitoring.

Server rooms/data centers

A server room is a dedicated space to keep wiring, network equipment, servers, and all the peripherals together. This is a bigger version of a wiring closet. There are specific security protocols when considering security and access controls. The room is locked, and specific clearance is required to access it. It has other locking mechanisms to lock cabinets and other hardware. There can be motion sensors, emergency exits with controls, biometric access controls, HVAC controls, and so on. Each module is specifically focuses on one or more risks and to mitigate the risks.

A data center is a larger version of a server room. It can spread across an entire area, even acres. A data center has specific and rigid physical security measures starting from exit/entry points, surroundings, security guards, dogs, clearance sections, cameras, sensors, sophisticated HVAC controls, live monitoring, and biometric controls to prevent access to specific areas. Only a recognized team of users will be able to gain access under strict surveillance.

Media storage facilities/Evidence storage

This is similar to a storage room. It has to be protected from fire, water, any kind of disaster, and the risks such as unauthorized access has to be mitigated. Access controls and surveillance are necessary requirements.

Restricted work area

A restricted work area means it is dedicated to a critical operation; A server room, a mainframe, a NoC, or even a vault. These areas must utilize access control. In addition, access points must be monitored and logged.

Utilities and HVAC

Heat, Ventilation, and Air Conditioning are important controls. Especially in a data center environment. To run these systems in optimal conditions it is necessary to keep the temperature (to keep warm in certain weather conditions), ventilation (heat control), air conditioning (heat control, particle removal), humidity conditions and corrosion controlled.

These auxiliary systems must have backups on standby. Furthermore, the electricity must have backups. The electric supply for the internal server farms must be restricted to a limited area as much as possible with access protection. The backups must focus on powering the server farms and internals rather than powering outside areas (keep additional generators). These units must be tested on drills to make sure they are fit for the task.

Environmental issues

There are lots of environmental conditions threatening continuity. However, these are not regular occurrences. The environmental selection must be made after a complete background check to determine the possibilities.

- There can be weather conditions and floods, water leaks, drainage issues, and many more. Any supplies must be built with emergency cut-off mechanisms. Proper distance is also important.
- There are possibilities of disasters from fire. In such cases, using water may cause even more damage. Therefore, remote cut-off mechanisms, necessary fire-control mechanisms must be set with ease of access (yet not to compromise the protection).
- There are possibilities of winds, tornados and lightning. Each of these conditions must be simulated (does not mean you have to call “Thor” the god of thunder) and appropriate backups must be in place.
- Earthquakes can cause even more damage to the entire areas. In such cases, there must be a backup to take over and proceed until the restoration. There are engineering methodologies to reduce such damages by design. Therefore, the design must be fit to tolerate acceptable impacts.

Fire prevention, detection and suppression.

- Fire Prevention: As we briefly discussed earlier fire can cause a lot of damage. There may be instances where electricity, lightning and accidents lead to such incidents. The prevention process must address the potentials. In this process, the sensors, alarms, and prevention equipment must be placed properly with a clear strategy. Simulations and random drills can ensure workability. Fire suppressing areas, doors, and firewalls can be integrated into the facilities.
- Fire Detection: In this process, the mechanisms and technologies are installed to detect a fire during a minimal duration from the start.
- Fire Suppression: Suppression of a fire once it is started in a minimal time can save the facility from the disfunction. Warning systems, and alarms (to trigger appropriate persons) can be installed so that either a system or a user can detect it and alert the appropriate teams and the fire department.
There are fire suppression systems, and each targets a specific type of fire, and not all the types can be used to combat any type of fire. There are gas-systems (FM200 – ideal for data centers), foam-based, Halon-based, and other traditional water-based, water-mist based and other types of extinguisher. You need to know the advantages and disadvantages of each technique and use a combination as appropriate.

Chapter 4

Communication and Network Security

Networks are the building block of any communication technology. If you are doing CISSP then you need to learn more about communication and network architectures and how security is impacting the architectures. If you have a networking background, this is your domain.

4.1 Implement Secure Design Principles in Network Architecture

In this section we will look into the communication and networking while focusing on security. Security is important to ensure the confidentiality, integrity, authentication, authorization and to prevent all kinds of internet originated threats but not limited to these, as networks are susceptible to other types of local attacks.

Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models

This section focuses the on building blocks of and standard models related to networking communication. There are 2 models named, OSI and TCP/IP. The OSI model is the ISO/IEC 7498 model and is the conceptual and standard model. The intention of this model is to provide a seven-layer approach beyond the underlying technologies in order to simplify and standardize the communication. The other model is the TCP/IP model and this is the widely used model in almost every implementation nowadays. It is a more simplified version of the OSI model. The following table compares these 2 models and layers respectively.

Type	OSI Model	Protocols	TCP/IP Model	Type
DATA	Application	HTTP, FTP, SSH, DNS etc.	Application	DATA
DATA	Presentation	SSL, SSH, other compression and encryption	Application	DATA

DATA	Session	SMB, RPC, P2P, Sockets	Application	DATA
Segments	Transport	TCP/UDP	Transport	Segments
Packets	Network	IP, ARP, IGMP, ICMP	Internet	Packets
Frames	Data Link	Ethernet	Network Access Interface	Bits and Frames
Bits	Physical	RS 232, Cables	Network Access Interface	

OSI versus TCP/IP

IP – Internet Protocol Networking

IP is the foundation of network addressing and internet work communication. This facilitates other protocols to communicate with each other. By working with TCP, it provides a reliable end-to-end data transfer. TCP is a connection-oriented protocol. In other words, it provides end to end reliable communication with timers and sequence numbering, error correction and a reliable buffer windowing mechanism.

IP works with TCP or UDP. The difference with UDP is the reliability. TCP is a connection-less protocol. It provides faster and the best effort communication when compared with TCP. IP can work with either one to facilitate communication between two or more devices.

IP now comes with 2 options. For 32bit computers TCP/IP version 4 was used. Since the address space was already used, a 128bit version 6 is being used now.

When it comes to communication, you should be familiar with how TCP/IP works together to form an end-to-end communication channel called a socket. Each of these protocols have a unique port number. A port is a service identification number or a virtual service identifier. By using the address and port, a socket is formed. The entire communication is then based on sockets. This is the regular method used by connection-oriented protocols.

Implications of multilayer protocols

A multi-layer protocol uses more than one OSI or TCP/IP layers at a given time. If we take an example, **Asynchronous Transfer Mode (ATM)** is a switching technique (cell-switching based, non-IP) utilized by telecommunication providers. In this operation a multi-layer communication occurs. ATM has 3 layers and operates in corresponding Physical and Datalink layers. The layers are used simultaneously in its operation. To utilize layers together, a technique known as **Encapsulation** is used. In this operation, the information of one layer is encapsulated in the other layer and additional data is appended to a header section (or even a header and a trailer). ATM is commonly used with **Synchronous optical networking (SONET)** . This is used to transfer large amounts of data, voice and video over long distance networks.

DNP3 is another multilayer protocol. If we take TCP/IP together, it can also be thought of as a multilayer protocol, conceptually.

Converged protocols

This can be thought of as merging of different protocols (e.g., proprietary protocols) with general or standard protocols. This is advantageous because the existing TCP/IP networking infrastructure and protocols can be used to facilitate different services without changing the infrastructure (e.g., hardware). This is basically achieving extensive amounts of cost savings, especially with multimedia services. Managing, scaling and securing the services is easier than building a proprietary network to serve the customers. Some examples would be:

- Fiber Channel over Ethernet (FCoE).
- SIP protocol used in VoIP operation.
- iSCSI.
- MPLS.

Also, remember that combining multiple technologies has its own pros and cons when dealing with security. By using the existing infrastructure, securing the new services is not difficult.

Software-defined networks

With the arrival of the cloud networks, software-defined networks emerged by replacing certain physical infrastructures. Software controlled designs were taking place due to many reasons including cost efficiency, flexibility, scalability, adaptability and dynamic nature.

Now we will take a look at the SDN architecture. It intends to decouple the hardware controls and forwarding functions from the architecture, and can program the controls manually. This also separates the underlying infrastructure for network services.

Features of the SDN

- Programmable: The entire network control is directly programmable due to decoupling from the forwarding functions.
- Programmatically Configured: The administrators can fully configure the SDN and is the best feature. They can manage, optimize and secure at their will.
- Agile: The ability to abstract control from forwarding – this results in a greater control over the network-wide traffic.
- Centralized Management: SDN controls are responsible for managing and maintaining a global view of the entire network. Policy engines and applications see this as a logical switch.
- Vendor-Neutral: The simplification of the network design and operation is achieved through the open standards.

Wireless networks

Wireless networks maintain its own standard (802.11) and security protocols. We will have a look at the standard, versions and security protocols. For details information, please visit http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

Protocol (802.11)	Frequency (GHz)	Data Rate
a	5	54 Mbps
b	2.4	11Mbps (TCP: 5.9 and

		UDP: 7.1)
g	2.4	54 Mbps
n	2.4 – 5	600 Mbps
ac	5	6.93 Gbps

Wireless Protocols

Wireless Security Protocols

- WEP: WEP stands for Wired Equivalent Privacy. This was the legacy wired-like security algorithm used in the past. This was a weak security algorithm and has now deprecated. It was replaced by later standards, such as WPA. WEP used RC4 for confidentiality and CRC-32 checksum for integrity. There were flavors, such as 64-bit, 128-bit, 256-bit WEP keys. After successfully developing a method to find the WEP key in a cryptanalysis, WEP is no longer secure.
- WPA: Wi-Fi Protected Access version 1 implemented as much as 802.11i standard. It uses Temporal Key Integrity Protocol (TKIP). It generates a per packet key with a 128-bit key length. WPA is also designed to perform packet integrity checks. Unfortunately, WPA relied on a weakness that had in WEP and found it was vulnerable to spoofing and re-injection.
- WPA2: WPA2 is Wi-Fi certified. The version 2 of WPA comes with strong security and support for Advanced Encryption Standard (AES). It also supports TKIP if the client is unsupported. WPA2 can use a pre-shared key for home users, but it supports advanced methods for enterprise use. This is the most secure out of the 3.
- WPA3: This is the next generation Wi-Fi Protected Access. There is a handful of information here: <https://www.wi-fi.org/discover-wi-fi/security>.

Other than these protocols, wireless uses IPSec and TLS for security and protection.

There is one important thing to remember. Insecure services, such as WPS (Wireless Protected Setups) must be discouraged.

4.2 Secure Network Components

A network is the heart or the backbone of the digital business operations. If at least one component fails or is compromised, there can be a colossal loss of data and income. This is why it is of the utmost importance on top of others. In this section, we will dive into the network components and security implementation.

Operation of hardware

The hardware devices are integrated and controlled in many ways in different networks. However, there is always a standard to follow. If we look into networking hardware, there can be communication hardware, monitors, detectors and load balancers in general.

- Modems: Modems are used to do the digital to analog/analog to digital conversion. In the old days, it was used to connect a PC to the internet.
- Hubs: Hubs are used to implement topologies, such as star. Every port of a hub is in a single collision domain and therefore it is not very reliable and secure.
- Concentrators and Multiplexers: These devices aggregate and convert different signals into one. A Fiber Distributed Data Interface (FDDI) is an example.
- Layer 2 Devices: Bridges and switches operate in the OSI layer 2 (Datalink layer). To connect through a bridge the architectures must be identical. Furthermore, it cannot prevent attacks in the local segment. On the other hand, a switch is more efficient. It divides the collision domains per port, and has a number of security features including port locking, port authentication VLANs and many more.
- Layer 3 Devices: Routers are more intelligent than the counterparts. It can make decisions based on the protocols and algorithms. Further, it also acts as an interconnecting point where

different technologies can operate collaboratively. A router can be used to segment a network. Not just routers, but they are high performance layer 3 switches. Layer 3 devices also provide a lot of enterprise-level security features, such as integrated packet filtering firewalls, authentication technologies and certificate service integrations.

- Firewall: Firewall is the main security guard in a network. It can make decisions based on the packets. The filtering/forwarding decisions can be configured. There are two methods employed by a firewall to filter the packets. One is **static filtering** and the other is the **stateful inspection**. The advantage of stateful inspection is that the decision is based on context.

Transmission Media

There are different categories of transmission media. We can mainly categorize the two by the material: copper and fiber. Let's look at the general media types in brief.

- Twisted Pair: By the name, it implies the twisted pair has pairs of twisted wires. The twist eliminates the interference and crosstalk. The number of twists determine the quality. In addition, the insulation and conductive material enhance the resistance to the outside issues.
- Shielded Twisted Pair (STP): This uses grounding to protect the signal from interference. These are used in high-interference environments, such as factories, airports and medical centers. Especially when microwaves and fluorescent lights are used.
- Unshielded Twisted Pair (UTP): This cable is susceptible to interference, unlike STP, so an additional level of protection is required. These are generally used in phone wiring and internet works.
- Coaxial Cable: This cable is far more superior in dealing with interference and environment issues. It has insulation, as well as a non-conductive layer, to attain a robust level of strength and

protection. Such cables are used as antenna cables in day-to-day use.

- **Fiber Optics:** This is the most superior type of the transmission media in terms of the stability, dependability, security and speed. The media is made of fiber and the signaling medium is a ray of lights (either Laser or LED). The single mode fiber cables reduce the number of reflections while increasing the speed. This is ideal for long distance transmissions. On the other hand, the multi-mode fiber cables can deliver the data with higher speeds without covering miles. There are plastic fiber cables as well, but it is not as reliable as the traditional fiber.

Network Access Control (NAC) devices

These devices are not exactly 100% physical. You definitely need physical devices, but to control access and prevent intrusions, there must be logical controls. Let's look at some of the NAC devices types.

- **Firewalls:** We have already discussed stateless/stateful firewalls in a previous section. These firewalls are driven by policy configuration.
- **Intrusion Prevention/Detection Systems (IPS/IDS):** We have discussed what these systems do in a previous lesson. The preventive measures are taken before an intrusion and the detective measures work during and after the attack. These systems can prevent or detect – help detecting us, an intrusion accordingly.
- **Proxy/Reverse Proxy:** A proxy or a **forward proxy** acts as a middle man. It intercepts the requests from the internal network and acts on-behalf of the internal computers or devices by screening certain information (e.g., PII). In addition, a proxy can filter certain traffic. On the other hand, a reverse proxy does the reverse process of a proxy server. It will work as the middle-man by intercepting **incoming traffic** . It provides features, such as load balancing, attack mitigation, global server load balancing and caching.

Endpoint security

An endpoint device is something like a client computer in a network. It can be a mobile device or any other similar device. This is the most vulnerable point of a network, given the larger attack surface, due to a variety of running software and services. An endpoint can be breached easily, and this is why most attackers target an endpoint.

To protect the endpoint from any type of a breach or an intrusion a number of technologies can be used. By preventing and restricting actions through policies, deploying multifactor authentications technologies, rights-management technologies, mitigation networks, remote access protection, configuring VPN security, installing anti-virus/internet security programs and host-based firewalls we can ensure a maximum level of protection. There must be awareness training and best practice guides to prevent social engineering and other types of attacks. The following methods can assure additional protection for your endpoints.

- Automated patch management.
- Device restrictions – such as USB and removable media device policies.
- Application white/blacklisting.

Content Distribution Networks (CDN)

A CDN is utilized to distribute content globally in order to reduce the download/upload speeds. Amazon CloudFront is a perfect example. Content, such as documents, files, and media content, take considerable download time, and a CDN can distribute the content upon first request and keep it for the rest of the requesters. These CDNs spread across the globe and therefore, the reduction of time improves the user experience significantly because caching the access to this contents is faster and even secure; these networks do not appear directly to the users. Therefore, direct attacking possibilities are less than the front-facing systems.

Physical devices

Just like the network security, physical security is one of the utmost important aspects of organization security. There are physical assets to secure, such as buildings. A variety of methods can be employed, such as security personal, CCTV, reception and more. Beyond the basic or digital

locking mechanisms, physical access controls can be based on access codes and cards. There can be other mechanisms as well, such as biometric devices. Certain high security environments even apply physical locks to computer systems.

Mobile device protection is also important. To prevent stealing or to prevent lost information, we can apply encryption, and other mechanisms to lockdown and prevent easy access to the system.

4.3 Implement Secure Communication Channels According to Design

We discussed security aspects of the data at rest. In this section, we will discuss on securing data in motion.

- Voice: In an organization, communication through audio streams are considered as strong collaborative means. Many companies utilize VoIP to reduce the costs, and to reduce the time consumption. In such use, end to end encryption is important. These streams are real-time data. In other words, the streams must receive priority. In order to prioritize, the Quality of Service (QoS) can be applied to the networking configuration. One real challenge is that the use of software-based services, such as audio enabled instant messengers, such as Skype, Whatsapp, IMO, Viber, and the list goes on and on. Again, even these programs support encryption and other security measures.
- Multimedia Collaboration: To take part in meetings, conferences and seminars can be difficult as the organizations widen their operations around the globe. With multimedia technology, the collaborative business efforts have entered into a new era. Now, voice, video, multimedia conferencing tools, online webinar tools, and collaborative tools, such as Microsoft 365, Helpdesk tools, software, such as Slack, TeamViewer, instant messengers, help businesses to achieve their goals in an increasingly fast-phased environments. With thousands of applications there are more and more advancements, however, it widens the attack surface.

- Remote Access: There are many ways to access the organizations assets remotely. One can use SSH, VPN technologies, RDS, and RDP. There are many third-party tools, such as TeamViewer. Technologies, such as Microsoft VDI, VMWare and similar virtualization tools, aid in creating fully virtualized, remote accessible, scalable remote infrastructures or farms. With the emergence of cloud technologies, remote access is becoming a de-facto standard. As the end users are accessing the remote devices through insecure network, there are greater challenges when it comes to communication security.
- Data Communication: The most logical solution to apply to a certain network is the least privilege. You should restrict access to only the required areas whenever possible and keep others away from the space. This is acquired through the use of VLANs. The organization network can be segmented with VLANs. The classification of VLANs can be based on business functions, workplace areas, or teams. In any case, the communication channels must be made secure with TLS, IPsec and other security protocols, including the certificate-based enterprise deployments.
- Virtualized Networks: Virtual networks have evolved as much as the physical networks (or even more). With advanced hypervisor technologies and SDNs it can control and secure the virtual networks with clinical precision. The control of ports, virtual switching, bandwidth control and other services can be managed centrally with ease. Both host and desktop environments can be virtualized. Therefore, such internal systems must follow operating system-based security standards. For other things like VLANs, general physical security approach can be applied tailoring to the requirements.

Chapter 5

Identity and Access Management (IAM)

In this chapter, we will look into the identity and access management. In other words, authentication, authorization and related areas. Let's briefly discuss what these are.

We have another important set of letters to learn. It is known as IAAA. IAAA stands for Identification, Authentication, Authorization and Accountability. This is a combination of identification with the AAA (triple A). Identity is self-explanatory. It can be your name, SSN, ID number and so on.

Authentication: Authentication is the first level of access control. Before you access a system, the system challenges you so that you have to provide a user id and a password. This is the traditional authentication mechanism. LDAP is a common protocol used to handle and store authentication and authorization data. New systems integrated multilevel systems into a single authentication. This is called Single Sign On (SSO). Many cloud apps and services rely on such service. Moving forward in high security facilities biometrics and authentication systems work together to provide a unified access control system.

Authentication Factors:

- Something you know – A password or something similar.
- Something you are – Biometrics.
- Something you have – A smartcard; a token.

Authorization : Once someone gets authentication approval, the user or the process can reach the resources. However, to view, use and remove resources, there must be another set of permissions. Otherwise, any user/process can gain access and abuse the data. To control this, authorization is implemented. Once a user is authenticated, authorization provides necessary access so that the object or a set of objects can be

viewed, executed, modified or deleted. Traditionally, LDAP was used to manage and store authorization information. With automation, there are now new intelligent and dynamic methods to authorize users or processes based on the location, etc.

Accountability: We will discuss this later in the chapter.

5.1 Control Physical and Logical Access to Assets

As you understand up to this point, access to an IT asset is mainly two-fold. Either physical or logical, and sometimes it can be both. Let's look at the assets and how you should approach.

Information

We discussed how data and information become assets and how you should approach in securing them in previous chapters. We should specially focus on authentication and authorization. Authentication can be of many types and it controls the main access to data/information resource. However, what a user can perform is really determined by the level of authorization he/she receives. Authorization governs the actions a person or a process can perform on a data object. Therefore, this must be thoroughly calculated and applied to prevent issues. The clearance level can control both authentication and authorization in a conceptual level. Necessary auditing is also required.

Systems

A system can be either a server - hardware, operating system - or a service. This can be either physical or virtual. In each case, controlling access by physical and virtual means is necessary. If you integrate on-premise and the cloud, you have to use a federation services to manage access. In this case, you can get a clear and transparent image of centralized operation. There are different systems to deploy and manage such services. System monitoring and auditing can provide details on how efficient and effective the controls are.

Devices

A device can be a computer, mobile device, or a peripheral device. There are different types of authentication mechanisms, either hardware or

software so that multi-factor authentication is a reality. In an organization, authentication must be centrally managed. Local authentication (administration) to a device in the network must be discouraged and limited to a specific team of administrators.

Facilities

In this area, the access control can be managed through a front-desk. Each user can be provided with a badge, stating the clearance level and role. If it is an electronic device, it can also serve as an access control device (e.g., smartcard). Depending on the security requirements, multi-factor authentication can be integrated. High security environments, such as power plants, labs, military operations and datacenters follow these procedures.

5.2 Manage Identification and Authentication of People, Devices and Services

This is an extension to the previous section. In this section, the previous topics are discussed in greater detail focusing on the technical aspects and implementation.

Identity management implementation

Lightweight Directory Access Protocol (LDAP)

LDAP (RFC 4511) allows services to share information about users and authorization in a standard format. In a Windows Active Directory environment, Kerberos handles the authentication, while LDAP manages the authorization and querying. LDAP supports encryption, which is an excellent feature.

LDAP stores information about users, groups, computers and other objects. It can also store metadata. The best example of LDAP is Microsoft Active Directory.

AD Directory Service (AD DS) utilizes LDAP with Kerberos for authentication. You should also remember that LDAP uses port 389 for unencrypted and 636 for encrypted communication. Kerberos uses port 88.

LDAP is used in Microsoft, Sun, Apache and Novell eDirectory.

Kerberos

Kerberos is heavily used in Windows and Network File Stream (NFS) in - Sun systems. Kerberos is any symmetric, ticket-based authentication protocol. The name comes from an ancient myth about a three-headed dog guarding the gate to the underworld – the hound of Hades. However, Hades himself did not develop the protocol. It was the effort of a team of researchers at MIT.

Kerberos is not a simple process to understand. Let's look at the process and learn.

1. Once logged in, a Windows client requests the user to input credentials. It uses a one-way hash function to generate a secret key using the credentials. Only the User ID is sent to the **Kerberos Key Distribution Center (KDC) Authentication Server (AS)**. The password is not sent.
2. The KDC matches this to a principle and verifies it exists in its Database. **The ticket Granting Service (TGS)** issues a ticket to the client. This is encrypted by using the secret key. It also generates a **Ticket Granting Ticket (TGT)** consisting of the identifier of the subject, the network address, validity period and TGS session key. Then TGS encrypts TGT using its own secret key. The TGS session key and TGT are sent to the client.
3. The client decrypts TGS using the secret key, completes the authentication and deletes the secret key. The client is unable to decrypt TGT.
4. When subject requires access to a principle (e.g., let's assume it is a server), it sends the identifier of this object, an authenticator (is generated by using the client ID, timestamp and encrypted using the TGT session key) to the TGS.
5. The TGS on KDC generates a client/server session key and encrypts it using the TGT session key for the client and a service ticket. The service ticket consists of subject's identifier,

network address, validity period and client/server session key. TGS encrypts these using the secret key of the object (server) and then sends these back to the object (server).

6. The client (in this case, the server) decrypts the client/server session key using the client/TGS session key. Remember the client (in this case, the server) cannot decrypt the service ticket as it is encrypted by TGS using the secret key of the requested object.
7. Now the client (Windows client) can directly communicate with the requester (server) and sends the service ticket and an authenticator consisting of the identification and a timestamp. Client encrypts the authenticator with the client/server session key generated by TGS. The object (server) decrypts the service ticket encrypted with its secret key. Now the service ticket is revealed to the object (server) which includes the client/server session key which allows the object (server) to decrypt the authenticator. Once it is decrypted, it can access the subject's identifier and the timestamp. If both are valid, then the object establishes the communication with the client and to secure the communication the client/server session key is used.

SESAME

This stands for **Secure European System and Applications in a Multi-vendor Environment** . It is developed by European Computer Manufacturers Association (ECMA). SESAME is similar to Kerberos, yet more advanced, and is another ticket-based system. It is even more secure, as it utilizes both symmetric and asymmetric encryption for key and ticket distribution. As it is capable of public key cryptography, it can secure communication between security domains. In order to do so, it uses a Privileged Attribute Server (PAS) at each side and uses two Privileged Attribute Certificates to provide authentication. Unfortunately, due to the implementation and use of weak encryption algorithms, it has serious security flaws.

RADIUS

RADIUS stands for **Remote Authentication Dial-In User Service** . This is an open-source client-server protocol. It provides the AAA triad (Authentication, Authorization, Accounting). RADIUS uses UDP for communication and it operates on the application layer. As you already know, UDP is a connection-less protocol and therefore, less reliable.

RADIUS is heavily used with VPN and Remote Access Services (RAS). Upon authentication, a client's username and password are sent to the RADIUS client (this process does not use encryption). It encrypts the password and sends both to the RADIUS server. The encryption is achieved through PAP, CHAP or a similar protocol.

DIAMETER

This is developed to become the next generation RADIUS protocol. The name DIAMETER is interesting (Diameter = 2x Radius if you remember mathematics). It also provides AAA, however, unlike the RADIUS, DIAMETER uses TCP and SCTP (Stream Control Transmission Protocol) to provide connection-oriented and reliable communication. It utilizes IPsec or TLS to provide secure communication and it focuses on network security or transport layer security. Since RADIUS is the popular application, DIAMETER still needs to gain popularity.

RAS

The Remote Access Service is mainly used in ISDN operations. It utilizes the Point to Point Protocol (PPP) in order to encapsulate IP packets. It is then used to establish connections over ISDN and serial links. RAS uses the protocols like PAP/CHAP/EAP.

TACACS

The Terminal Access Controller Access Control System (TACACS) was originally developed by the United States Military Network. It is used as a remote authentication protocol. Similar to RADIUS, TACACS provides AAA services.

The current version is TACACS+ which is an enhanced TACACS version, which however, does not provide backward compatibility. The best feature

of TACACS is the support for almost every authentication mechanism (e.g., PAP, CHAP, EAP, Kerberos, etc.). It uses port 49 for communication.

The flexibility of TACACS makes it widely used, especially as it supports a variety of authentication mechanisms and authorization parameters. Furthermore, unlike TACACS, TACACS+, it can incorporate dynamic passwords. Therefore, it is used in the enterprise as a central authentication center. It is often used to simplify administrative access to firewalls and routers.

Single/multi-factor authentication

Traditional authentication utilizes only a single measure such as passwords, passphrases or even biometrics, but without a proper combination. Integrating 2 or multiple factors makes a stealing attempt much more difficult.

As an example, if we take a user who has a password and a device, such as a smartcard, or a one-time access token, an attacker would need both to gain access. This is also known as the type2 authentication.

A password can be integrated with a finger-print or a retina scan. In the second case, it is even more difficult, as something you are cannot be stolen. This is also known as type3 authentication.

When you do bank transactions via ATM machines, it requires the card and a pin. This is a common example of multi-factor authentication. A more secure approach can be the use of a one-time password along with the device. There are two types.

- HMAC-based Onetime Password (HOTP): This uses a shared secret and a counter, which increments. The counter is displayed on the screen of the device.
- Time-based Onetime Password (TOTP): A shared secret is used with the time of the day. This simply means it is only valid until the next code is generated. However, the token and the system must have a way to synchronize the time.

The good thing is that we can use our mobile phones as token generators. Google Authenticator is such an application.

You should also remember that you can deploy certificate-based authentication in enterprise networks. A smartcard or a similar device can be used for this purpose.

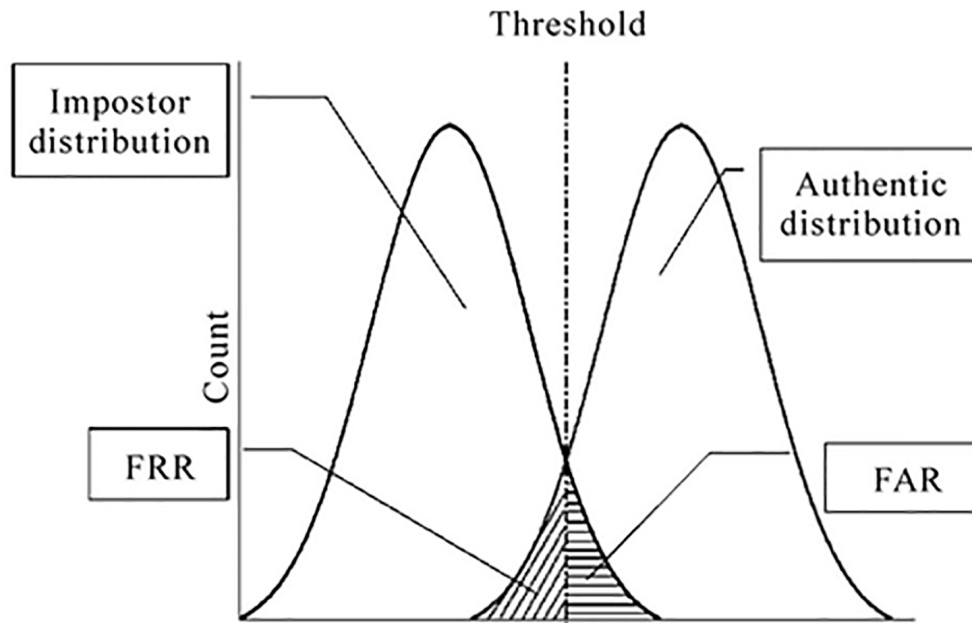
Let's discuss a bit more on biometrics and type3 authentication.

There are 2 steps for this type of authentication. First, the users must be enrolled. Their biometrics (e.g., fingerprint) must be recorded. Then, a throughput must also be calculated. Here, the throughput means the time required for each user to perform this action, e.g., swiping the finger. The following is a list of biometric authentication methods.

- Fingerprint scans.
- Retina scans.
- Iris scans.
- Hand-geometry.
- Keyboard dynamics.
- Signature dynamics.
- Facial scans.

Biometrics raises another issue. There are 2 factors governing the strength of the techniques.

- One is the **False Acceptance Rate (FAR)** . It is the number of false acceptances when it should be rejected.
- The other is the **False Rejection Rate (FRR)**. This is when a legitimate user is rejected, although the user should be allowed.
- Crossover Error Rate (CER) – You must increase the sensitivity until you reach an acceptable CER where the FAR and FRR intersects.



Accountability

Accountability is the next most important thing in the triple A (authentication, authorization and accounting). The accountability is the ability to track user's actions, such as login, object access, and performed actions. Any secure system must provide audit trails and logs. These must be stored safely and even backed up if necessary. Audit information helps troubleshooting, as well as to track down intrusion attempts. If we take a few examples, continuous password failure is something you need to monitor and configure alerts. If a person accesses an account from one location and within a few minutes he accesses it from a different location, it is also considered suspicious activity. If you are familiar with social networks, like Facebook, even these platforms now challenges users when this occurs.

Audit logs can be extensively large. In such cases, it must be centrally managed and kept in databases. Technology, such as mining and analytics, can provide a better picture of what is happening in the network.

Session management

A session can be established once you connect from a client to a server, in general. However, we are taking about sessions that require and succeed authentication into the account. As an example, a VPN session, an RDP

session, an RDS session or an SSH session. A browser session can last until the session is expired and it would use a cookie to handle this. Browsers provide configuration options to terminate sessions manually.

Sessions can be hijacked or stolen. This is the danger associated with it. If you log into an account and leave the computer to let others access, a mistake or deliberate misuse may occur. To handle such instances, there are timers that can be configured. An example is the idle timeout. Once it reaches a certain threshold, the session expires. To prevent denial of services, multiple session from the same origin can be restricted. If someone leaves a desk after a browser-based session, it can be configured to end the session by expiring the cookies when he closes the browser.

Registration and proofing of identity

If you are familiar with email password registration, you may have seen prompts for security questions and answers. This is heavily used for the password resetting process and account recovery. However, you must remember that your answer to these questions must be tricky. You do not have to use exact answers to these questions. Instead, you can use any sort of answer (things you need to memorize, of course) and increase the complexity, thus making a guess difficult.

There are other instances, such as your ID, driving license, etc. If you are a Facebook fan, you may have encountered such events. It asks you to prove your identity through an ID card or something similar.

Federated Identity Management (FIM)

Federated identity management system is useful in order to reduce the burden of having multiple identities across multiple systems. When two or more organizations (trust domains) share authentication and authorization, you can establish a FIM. For an example, there is an organization that can share resources with another organization (two trusted domains). The other organization has to share user information to gain access. The organization that shares the resources trusts the other organization and its authentication information. By doing it this way, it can cut the requirement for multiple logins.

This trust domain can be another organization, such as a partner, a subsidiary or even a merged organization.

In IAM, there is an important role known as the Identity Broker. An identity broker is a service provider that can offer a brokering service between two or more service providers or relying parties. In this case, the service is access control. An Identity broker can play many roles including the following.

- Identity Provider.
- Resident Identity Provider – This is also called the local identity provider within the trust domain.
- Federated Identity Provider – Responsible for asserting identities that belong to another trust domain.
- Federation Provider – Identity broker service that handles IAM operations among multiple identity providers.
- Resident authorization server – Provides authentication and authorization for the application/service provider.

What are the features?

- A single set of credentials can seamlessly provide access to different services and applications.
- Single Sign-on is observed in most cases.
- Simplify storage costs, and administrative overhead.
- Manage compliance and other issues.

Inbound Identity: This provides access to parties who are outside of your organization's boundary and let them use your services and applications.

Outbound Identity: This provides an assertion to be consumed by a different identity broker.

Single Sign-on (SSO)

Almost all FIM systems have a SSO type login mechanism, although the FIM and SSO are not synonymous because not all SSO implementations are FIMs. If we take an example, Kerberos is the Windows authentication protocol. It provides tickets and SSO like access to the services. This is called IWA (Integrated Windows Authentication). But it is not considered as a federations service.

Security Assertion Markup Language (SAML)

This is the popular web-based SSO provider. In a SAML request, there are 3 parties involving.

- A principle: The end-user.
- Identity Provider: The organization providing the proof of the identity.
- Service: The service, which is the user who wants to access.

SAML has two types of trust relationships. One way or two way.

- If a one-way trust is existing between domain A and B, A will trust authenticated sessions from B, but B never trusts A for such requests.
- There can be two-way trusts.
- A trust can be **transitive** and **intransitive** . In a Transitive trust between A, B and C domains, A trusts B, and B trusts A. If B trusts C, then A trusts B.

OAuth

OAuth is another system that provides authorization to APIs. If you are familiar with Facebook, GitHub, major public email systems, they all utilize OAuth. A simple example would be importing contact to Facebook via email (you must have seen it asks you to). Many web services and platforms use OAuth and the current version is 2.0. It does not have its own encryption scheme and relies on SSL/TLS. OAuth has the following roles – all are self-explanatory.

- Resource Owner (user).
- Client (client application).
- Resource Server.
- Authorization Server.

OpenID

OpenID allows you to sign into different websites by using a single ID. You can avoid creating new passwords. The information you share with such sites can also be controlled. You are giving your password to the identity provider (or broker) and the other sites never see your password. This is now widely used by major software and service vendors.

Credentials management systems

Simply, a credential management system simplifies credential management (i.e., User IDs and Passwords) by centralizing it. Such systems are available for on-premise systems and for cloud-based systems.

A CMS creates accounts and provisions on the credentials required by both individual systems, and identity management systems, such as LDAP. It can be a separate entity or part of a unified IAM system.

A CSM or even multiple CSMs are crucial for securing access. In an organization, employees and even customers join and leave rapidly, changing roles as business processes evolve. Increasing privacy regulations and others demands the demonstrated ability to validate the identities of such users.

These systems are vulnerable for attacks and impersonations. Revoking and issuing new credentials in this case can be a tedious task. If the number of users is high, the performance issues may also exist. To enhance security, Hardware Security Models (HSM) can be utilized. Token signing and encryption make such systems strong, as well as such systems can be optimized for performance.

5.3 Integrate Identity as a Third-Party Service

Third-party identity services can be utilized for managing identities, both on-premise and in the cloud. Such systems are important and also pose a security risk. When considering such systems, you have to focus on Identity Lifecycle Management, Authentication, Authorization, Privilege access, provisioning and governance. Providers, such as Microsoft, has its own services, such as Forefront Identity Management (FIM) or Azure, while others, such as Oracle, Okta, OneLogin, Auth0, RSA Secure ID, WSO2, SailPoint and DigitalPersona. As a third-party service we can call such services Identity and Access Management as a Service (IDaaS).

On premise: On premise applications often require servers, appliances or service integration in the existing setup. Integration services are made simple and can be optimized for organizational requirements. For example, to provide SSO you can integrate your existing Active Directory environment with a third-party system.

In the cloud: There are two favorites when it comes to the cloud. You can either select federation services to federate the on-premise systems to the cloud. Or else, you can use the services the cloud providers already crafted. Microsoft Azure, Amazon IAM and Google IAM are excellent options. There are some advantages to such systems.

- The vendor manages the infrastructure, service and security.
- Less time-consuming.
- Scalable.
- Reduced cost.
- Rich in features and extensions.
- Greater performance.

However, there are some drawbacks too.

- For a full feature-set you may need to provide additional fees.
- You do not control the infrastructure and it may not fit well with your organization policy, government regulation or compliance requirement.

- Legacy services may not be able to cope with these systems.
- The learning-curve may consume time and cost.

Federated: We have discussed federation in detail in the previous sections. You can use your organization's credentials and the database to facilitate user access to external platforms. As an example, an organization could use the existing credentials and SSO to provide access to a cloud-based service. The most important fact is the user experience so that users do not have to remember multiple credentials into each system, which also enhances the security.

5.4 Implement and Manage Authorization Mechanisms

The sole purpose of this section is to give you an understanding of different access control mechanisms.

Role Based Access Control (RBAC)

Role-based access control is the default approach for many organizations. There are clearly defined roles and responsibilities. When a new user or a service needs access, a role is assigned to the new instance. This technique is, however, a non-discretionary access control method. In other words, the role has static boundaries and is a coarse-grain access control, yet easier to manage and strong in terms of protection. It offers the reduction of administrative overhead, ease of delegation and control, operational efficiency and compliance. For example, you can implement a role-based access control with Microsoft Active Directory and Azure using users, groups and principles. Microsoft Exchange server is also a good example, and it is based on RBAC.

Rule Based Access Control (RuBAC)

In this mechanism, a set of pre-defined rules will be used. Rules can be used to simplify and automate the access management. A common example is a firewall. Firewalls and routers have rule-based access control mechanisms to filter packets, make decisions and apply actions. Network Access Control platforms also use rule-based models.

The logic is more like “If A then B”. If a user named John is allowed to access a remote desktop machine when his IP matches a specific IP in a whitelist, he is granted access. If he is accessing it from a different location, he is denied. This is a simple example of how it works.

Mandatory Access Control (MAC)

MAC does not stand for Apple’s most popular computer system in this case. In a high-security environment, discretionary controls are highly limited. Users cannot determine or control objects like in DAC. This model is based on the information classification and clearance, which we discussed in previous chapters. For an example, Alex has a security clearance for a secret access level and is able to access a specific set of files. He has read and write access. Jason has confidential access to a set of files he manages. By MAC, Jason cannot access files that Alex has clearance for. Likewise, Alex does not have clearance for files managed by Jason. Although the MAC is inherited, it is not a threat, as in such environments you are not provided a chance to deploy software or any other nasty thing, unlike in some Sci-fi or action movies.

To implement MAC, a customized operating system is often used. DAC seems to be the best security solution, but the reality is unfortunately, far from it. Such systems come with a huge administration overhead, including implementation and clearance, very expensive, limits the ability to function, and not user-friendly. Therefore, MAC is used for special purposes and used with military applications.

Discretionary Access Control (DAC)

This is something you are familiar with. In day-to-day work you must have accessed properties of a file or a folder and looked at security settings or permissions on Windows, Linux-based or any other operating system. This is where DAC is used in practice. You can control the permissions, such as read, write, execute, modify and delete. To provide permissions to others, you add the user or a group and provide necessary control. In the enterprise network, you can have your own control to the information you manage within your folders. Just like RBAC, this is widely used in the enterprise, as it is easy to understand, manage and ensure security. One problem is the inheritable permissions. If an intruder or a process gains access, it will be

with certain level of control. However, the inheritance can be disabled or modified in a such way as to prevent unnecessary actions.

Attribute Based Access Control (ABAC)

Each user, device, and network has characteristics that can be turned into attributes of the entity. If we take a user named Sophia, for an example, she needs to be given access to a secret project. The project is called NuX, which is research based on nuclear reactors. She is a senior executive who handles a team of individuals. She must access a specific lab while she is in the office premises and the timeframe is also known.

Now in this description you can find a list of attributes. If you can take these attributes and construct a rule, you will be able to provide access if her request for access matches the rule. However, if you utilize RuBAC, this will become complex, as it affects multiple users (not specific). Instead, by taking RuBAC into the plate you can create more specific rule-based control called ABAC on top of it.

One important thing to remember is the simplicity and clarity with this design. As you know, a user will not wait for hours until the system searches and matches attributes. For an example, in an active directory environment, you can use a user's or a group's attributes and combine it with another permission to gain fine-grained access control.

5.5 Manage the Identity and Access Provisioning Lifecycle

This is the last topic of this domain and chapter. Each user, service or a device has a lifecycle. If we take an employee for example, an employee joins an organization and after few years he/she will leave the organization. This lifecycle must be planned, implemented, provisioned, administered, assisted and so on until the revocation is reached. Let's look at this in detail.

- Let's take a person called Jane. Jane is hired by a company to perform as a creative designer. Now Jane is about to start working at this company. She must be given with proper access to carry on her duties.
- The formal process starts at the HR department. They are responsible for enrolling and onboarding this person, so they are

going to create a user account, a role, and a set of permissions with the help of other sections in the firm. Let's assume there is an integrated system where a HR can create a profile with attributes, then another system is able to create a user profile by matching these. In the provisioning process, such accounts will be created and provided access. Many organizations use automated tools to make the process easy and less time consuming.

- The user will be provisioned in the directory service environment next.
- IT and administration can apply user's role and attributes.
- IT department is also responsible of automating or a manual assisting process regarding password resetting and changing roles (e.g., Jane gets a promotion and appointed as a senior executive).
- When Jane is about to leave the company, her access must be revoked, company assets must be relocated, and the user account is kept on hold.
- Once the migration of user information is complete, the account will be deleted. There is a retention period, such as a week or a few weeks.

During the lifecycle, you must focus on these stages.

Provisioning and De-provisioning

This is the process where you create an account and at the end of the lifecycle you terminate the account. These are the key tasks that you perform. If you create and reserve accounts, or keep stale accounts, you are introducing vulnerabilities. If you use template accounts and do not review them, you may provide unnecessary permissions. If you remove the accounts too early, you may not revoke all the assets and might lose important information. Therefore, this process must execute through proper clearance and guidelines.

User access review

When a user is granted access, a team of security and auditing must review the access with the help of team managers and supervisors. This will reveal if the user has more than enough rights to perform a job, if the company policy controls the access, and if the process of granting is documented. You also need to evaluate the best practices policies and how it is effective in terms of this process. Once you identify stale accounts, you also need to take the necessary steps to revoke access and terminate these objects. The main intention is to review if a user is granted access beyond his requirements and if the stale users are still accessing the resources. This activity can reveal any access violations performed by users and intruders.

System account access review

System accounts or service accounts are used to manage system processes, services and tasks. These accounts sometimes have superuser privileges. For example, the System user on Windows can control many actions on a Windows platform. If this is hijacked by malware or an intruder, he can perform many things beyond the control. In Linux systems, the root user is often unused and on mobile devices it is disabled to mitigate security vulnerabilities and breaches. Periodically, you must review these accounts, control the level or permissions if possible, and document these findings, including the actions it performed, on who's accounts and what level of access was provided.

Chapter 6

Security Assessment and Testing

This chapter is about security assessment strategies, testing, techniques and technologies utilized.

6.1 Design and Validate Assessment, Test, and Audit Strategies

Each organization needs to establish a proper audit strategy to keep track of security events. The strategy depends on the organization's size and the requirements. Auditing is something that must be developed in parallel to the security policy and strategy. Therefore, it is an integral part and must be assessed continuously. The policies, procedures and processes are the core focus here. Now let's look at the strategies you can employ.

- Internal strategy: This is the same as the company policy that is aligned to the internal structure and the business operations. Therefore, depending on the structure, size and operation, the strategy can be complex and frequent. We also need to take the stakeholder requirements and common interests into account. Furthermore, if there is a specific compliance or regulatory requirement it must be satisfied.
- External strategy: External auditing is a way to determine how an organization follows its security policy, regulations and compliance requirements.
- Third-party strategy: This is best suited when a neutral and objective review of the existing design, testing framework, and the complete strategy. It can also reveal if internal and external auditing is effective and following the procedures.

If we take a look at the steps in brief, we can list some of the important stages.

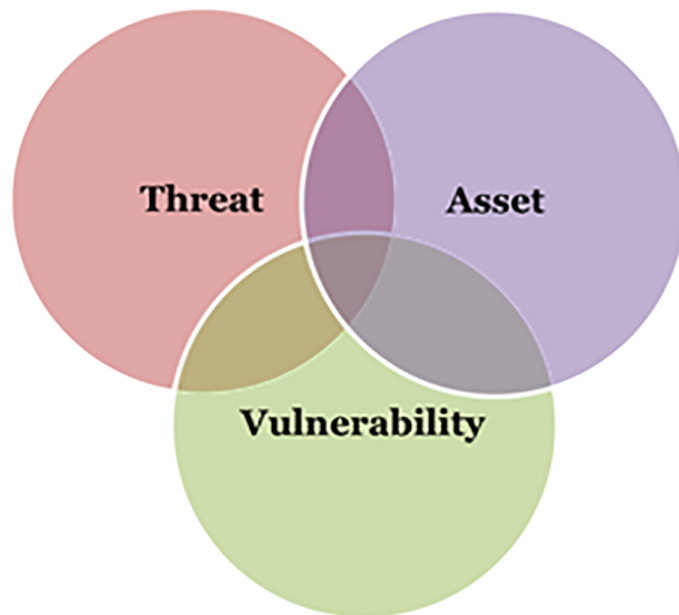
- Assessing the requirements

- Assessing the situation
- Document review
- Identification of risks
- Identification of vulnerabilities through scans
- Analysis
- Reporting

6.2 Conduct Security Control Testing

Now we'll discuss the existing methods that you can employ with your strategy.

Vulnerability assessment: This is an interesting topic isn't it? It's like you are in a Sherlock Holms role. Well, a **vulnerability** is an open security hole or a **weakness** that can be **exploited** by a **threat** . **Risk** is the potential damage if a vulnerability is exploited by a threat. During the process of testing, threats and vulnerabilities are determined and identified. Risk mitigation countermeasures will be applied once it is complete.



Vulnerability assessment processes can be highly technical and non-technical. For an example, physical security can be assessed by looking at it from different perspectives.

Penetration Testing : This is the most interesting phase of the testing, as it attempts to attack a system forcefully in order to find a hole and breach. In other words, to exploit vulnerabilities if they exist. The sole purpose is to uncover possible weaknesses in security. Penetration testing is a whole topic and it involves highly technical activities. There are multiple methods and tools to use to plan and deploy a penetration test. The following includes the common penetration testing stages (model).

- Reconnaissance – In this stage, identification and documentation of the organizational information is accomplished.
- Enumeration/Scanning – In this stage, more information is collected by employing techniques and technologies.

- Vulnerability mapping – In this stage, the information collected during the 2nd stage is mapped to the vulnerabilities.
- Exploitation/Gaining Access – You know what occurs in this stage.
- Maintaining Access.
- Clearing Tracks.

Now let's look at some of the penetration testing scenarios and types. We will look at the testing in details in next chapters.

- Application layer testing.
- Network layer testing.
- Social engineering testing.
- Client-side testing.
- War dialing – In this test, the penetration focuses on models and modem pools and then exploits the vulnerabilities.
- External testing – Testing from the outside of a company, mainly through the internet.
- Internal testing – Simulates a malicious user on the inside.
- Blind testing – A tester knows about the target's name and the security person/team knows about the upcoming attack.
- Double-blind testing – A tester knows the target's name and the security person/team is unaware of the upcoming attack.
- Targeted testing – in this case, both the security person and the tester works together to test for vulnerabilities.

Log reviews

Log review is a crucial part of the practical security management process. Any organization collects logs and even backs them up. However, it is imperative that you review logs frequently. Any unusual patterns or a series of denied requests most probably indicate a failed attempt, or a weakness. A series of success states do not really indicate anything. In this case, it is

extremely difficult to determine any intrusion attempts. However, a success attempt can indicate a succeeded exploitation if it is deliberate, or even due to a mistake. This information is valuable, as it displays the clues, and also serves as a witness.

You must always remember to back up the logs and enforce simplex communication to avoid compromising logs. You could also use write-once media and backups to further protect the logs.

Synthetic transactions

The focus of these transactions is to test the system level performance and security, while the others focus on real-time actions.

Code review and testing

This focuses on the application development lifecycle. Code review and testing are extremely important in order to secure applications and fix vulnerabilities. The attack surface can be reduced by introducing applications if the application is free of vulnerabilities. These tests can focus on functionality, as well as on units.

Misuse case testing

Software applications may exist with certain erroneous code. Such implementation issues or flaws in the logic may lead the application to be misused. These issues may lead to password stealing, privileged escalations and accessing unauthorized resources, including memory areas.

Fuzz testing

Fuzz testing is a quality assurance technique used to discover coding issues, security holes and vulnerabilities in a software program. Fuzz is a massive amount of random data. The intention is to crash the system. A **fuzzer** is a software that can perform such tests. This technique can uncover vulnerabilities subjected to DDoS attacks, Buffer Overflow attacks, XSS and Database Injections.

Test coverage analysis

The following is a list of coverage testing types.

- Static tests: The system is not monitored during this test.
- Dynamic tests: The system will be monitored during this test.
- Manual tests.
- Automated tests.
- Functional tests: The functional response and reactions are analyzed during this test. Certain tests are aimed to trigger abnormal behaviors (expecting) given the inputs and is called anti-normal tests. Such tests run in order to validate the functionality, stability and reliability.
- Structural tests: Such tests focus on code structure and hierarchy. It can be thought as a Whitebox test.
- Negative tests: In this series of tests, a software is tested against invalid and unexpected inputs, sequences and against malicious data.
- Whitebox testing: Whitebox testing is a test performed while the tester is fully aware of the structure and processes. This does not aim on testing functionalities. The test will review the coding as well and therefore, the tester must have a solid understanding of coding. Some drawbacks exist in the tests, such as complexity, duration, scalability, and code disclosure leading to security issues. A few advantages would be code optimization, anticipation and the possibility to fully review the code.
- Blackbox testing: In this scenario, the tester's role is similar to a hacker (or a cracker). The tester has no knowledge of the system and structure. Unlike the Whitebox test, the person has minimal knowledge about the target. The attack is more dynamic in nature, as real-time or slow analysis is required in the reconnaissance period. The mapping is also created once this step is complete. The downside of this approach is that it does not reveal internal vulnerabilities.

- Gray-box testing: During this process, the tester has certain knowledge about the system, and is similar to a regular user. This can speed up the process and the testing is similar to a MITM attack in some cases. This test evaluates both the internal and external networks together and provides great detail on vulnerabilities and risks.

Interface testing

An interface is more like an exchange point between a user and a system. During the test, such exchange points will be evaluated to locate the good and bad exchange points. These tests are mostly automated. Before the test, all the test cases are documented for reuse. During the integration testing, this test is used extensively. The following is a list of the test types.

- Application Programming Interface.
- User Interface.
- Physical Interface.

6.3 Collect Security Process Data

Security systems create lots and lots of data. Systems, such as Security information and event management (SIEM, combination of SIM - Security Information Management - and SEM - Security Event Management), process such data.

Security process data include electronic data, as well as paper records. These processes are set forth by an organization to ensure the CIA triad. Since these reports are important, it must be maintained and tested consistently. Your organization must perform vulnerability assessments and account reviews regularly. The overall process must be documented. You could use an Excel or a similar spreadsheet.

Account management

An organization must have a proper and consistent procedure to maintain the account, as these accounts are used to access systems and assets. In addition, another sub system must exist to manage vendor and other accounts. In any case, from the creation of the account, expiration, logon

hours and other attributes must be collected. The access can be both physical and logical. In case of physical access, access hours, and other attributes, can be matched before allowing access.

Management review and approval

As we already discussed, management plays a critical role to ensure proper information delivery to employees, and if directions are followed. Process data can be collected by an administrator or a team of employees. Management must support the individual or a team to accomplish this process by approving the techniques to be utilized and by performing periodic checks.

Some of the activities during this process are listed below.

- Reviewing recent security incidents.
- Reviewing and ratifying policy changes.
- Reviewing and ratification of major changes relating to the business process.
- Reviewing the Risk Indicators and key metrics.
- Budget reviews.

Key performance and risk indicators

Key Performance Indicators or **KPIs** and **Key Risk Indicators** or **KRIs** are highly important. To measure the risks, we employ RIs in order to calculate the risk associated with process, account and other actions. Similarly, KPI is utilized to measure the success of a process, as well as how it can affect the regular operations in the organization.

Some of the key areas of focus when selecting the KRIs are listed below.

- Incident Response: Incidents provide valuable information about weaknesses and areas an organization need to focus on. The number of similar incidents display trends and possible issues. The key findings here or risk indicators are dwell-time (time required to realize an ongoing incident) and time required to rectify and resolve.

- Vulnerability Management metrics: In this area, the stages are performing scans, identifying the vulnerabilities, and release fixes or patches to resolve the issue. The KRIs focus on public awareness of the vulnerability and time required to release a resolution.
- Logging/Monitoring: This is also similar to vulnerability management. Upon reviewing logs and monitored areas, trends and potentials can be found. The event types, number of occurrences and severity are key parameters here. KRIs focus on actual start time and the time when a security person realizes the incident and starts to take action.

Backup verification data

Regular backing up, restoring, verification and assessing the efficiency is vital. You should keep the backups out of reach and delegate the authority to a trustworthy partner. The data must not be modified during any sort of process in order to maintain the **integrity** .

Training and awareness

We have already discussed the benefits of training and awareness in previous chapters in great detail. No matter how neat a policy, implementation and control, without a proper training program the challenge is still there. This affects the entire organization, rather than just the data collection team. There are three main components of an effective program. We will look into the learning framework in brief.

	Awareness	Training	Education
Purpose	To give a basic idea on what security is and what an employee should do	How to react/respond to situations where threats are encountered	Why the organization exercises security and why it responds to events as it does
Level	Basic	Intermediate	Advanced
Outcome	Ability to identify general threats and respond proactively	Formulate effective responses using the skills	To understand organization objectives, active defense and continuous improvements

Learning Methods	Informal training, web, media, videos, newsletters, etc.	Formal training plus workshops and hands-on	Theoretical knowledge, webinars/seminars/discussions, reading of related work, case studies
Assessment	MCQ and short tests	Ability to apply the learning	Architecture/design level essays
Impact	Short-term	Medium	Long-term

Disaster Recovery (DR) and Business Continuity (BC)

This is another area that requires extensive documenting. Backups can be confusing if not labeled correctly. The purpose and sets must be documented with the strategy. If there is automation and multiple vendors, such information with other standards introduced can also be documented. Recovery strategies and “when to use what” is an important part, given the infrequent nature of use for recovery. In addition, the service accounts and credential requirements must be kept accounted and safe to use whenever needed.

During the security assessment and testing process, DR and BD must be reviewed to ensure the strategy is consistent, complete and that recovery can be restored at any point in the long run, and to verify that the business can continue after the recovery process without having to worry about gaps and holes.

The key areas to focus are the following.

- Data Recovery.
- Disaster Recovery.
- Integrity of Data.
- Versioning.
- Recovery Environments.

Information security continuous monitoring (ISCM) - NIST SP 800- 137 – strategy greatly assists organizations to implement and maintain an

effective and systematic security monitoring and management program in ever changing environments.

6.4 Analyze Test Output and Generate Reports

There are tons of tools to generate, capture logs, and even statistical data. Unfortunately, without a proper reporting system and representation, such data is difficult to draw a picture or to make sense of. Meaningful information is the key to get the best out of the tests performed regularly. The interpretation of the data must provide accurate indicators and statistics in order to uncover ongoing issues, performance problems and outdated controls.

There must be multiple reports in order to deliver the information to the appropriate person or team. If a technical report targeting system administrators is given to a senior manager who does not have such background, he may not be able to understand and interpret the situation and make appropriate decisions. Instead, these must be converted to meaningful KRIs and business metrics. The security team must be able to understand different perspectives and format the information to match the requirements in order to make sense in terms of the business. This is the key to an evolving security strategy and to gain more budgetary allocations, staff, and assets to enhance the security program.

For example, SSEA 18 auditing standard requires several reports known as **Service Organization Control (SoC)** reports. This was developed by **American Institute of Certified Public Accountants (AICPA)** .

- SoC 1 Type 1: This is an attestation of controls at a service organization within a given timeframe or a specific point in time.
- SoC 1 Type 2: Same as SoC 1 over a minimum of six-month period.
- SoC 2: According to AICPA SoC 2 is a “Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy.”
- SoC 3: According to the AICPA, “These reports are designed to meet the needs of users who need assurance about the controls at a

service organization relevant to security, availability, processing integrity confidentiality, or privacy, but do not have the need for or the knowledge necessary to make effective use of a SOC 2® Report. Because they are general use reports, SOC 3® reports can be freely distributed”.

More information about SoC reports can be obtained from <https://www.aicpa.org/content/aicpa>

6.5 Conduct or Facilitate Security Audits

Auditing is both examining and a measuring the process focusing on systems, as well as business processes. It can reveal information on how well these are planned, how these are being used and how effective these processes are. Auditing must be free of bias in order to gain accurate results. In order to achieve this, many organizations use third-party audits or they utilize a separate, specific team of individuals.

Audits are also important in order to find out if the organization operates within the policies, standards, government laws, regulations, legal contracts and compliance requirements.

There are three different types of audits.

- Process audit: This gives an idea of processes and if they are working within the limits. An operation is evaluated against certain pre-determined standards or instructions to measure conformance.
- Product audit: This is an evaluation of a specific product, such as hardware, software, etc. to check if it conforms to the requirements.
- System audit: This is an audit conducted on a management system.

Depending on the interrelationship among the parties it can be also classified as,

- Internal (First-party) audit: Performed internally (using a team within the organization) to measure strengths and weaknesses against its own internal standards, procedures and methods or against external standards.

- External (Second-party) audit: This is an audit performed by a customer (or on behalf of a customer) against a supplier or a service provider.
- Third-party audit: In addition to external audits, this procedure assesses the validity of internal and external audits and to perform in-depth audits in specific areas. There is no conflict of interest. Such audit may result in recognition, registration, certification, license approval, a fine, or even a penalty issued by a third-party.

Difference between performance audits, compliance and conformance audits

The key difference is the collection of evidence related to organizational performance versus evidence to verify conformance (or compliance).

What is a Follow-up audit?

This is also an important audit because of a very specific reason. Previous audits may have revealed the problems with applications of standards etc. and the set of actions required to resolve the issues. A follow-up audit is exercised in order to verify if the corrective actions are taken and how effective those are.

There are four different phases of auditing. The following is a brief on these phases.

- Preparation: The preparation is all about meeting the prerequisites to ensure the audit complies with the objective. Parties involved can be clients, lead auditor, an auditing team and audit program manager.
- Performance: This is more of a data gathering phase, and also known as fieldwork.
- Reporting: As we discussed, in this phase the findings will be communicated with the various parties.
- Follow-up and closure: According to ISO 19011, clause 6.6, "The audit is completed when all the planned audit activities have been carried out, or otherwise agreed with the audit client."

There is a critical difference between staying compliant versus a comprehensive security strategy. You can definitely follow compliance standards and stay within. However, this does not mean compliance is security. Assuming that the compliance brings effective security-policy isn't a great strategy. It is important to understand the difference and develop strategies to stay secure and compliant in parallel.

Chapter 7

Security Operations

In this domain, we are focusing on an operational perspective. Therefore, this is not exactly a theoretical section. In other words, this is more hands on and discusses how to handle situations instead of planning or designing.

7.1 Understand and Support Investigations

This section walks you through the learning, understanding and supporting security investigations. The sub topics here cover the stages of this process.

Evidence collection and handling

Every organization should have an incident response policy and strategy. For an example, if you are to investigate if a digital crime occurred within your organization you need to have a specific guideline for the organization users in order to protect relevant evidence by ensuring the integrity and usability. Therefore, incident response and reporting policy procedures and guidelines must be established targeting the key business areas, with clear guidelines, and it must be communicated and rehearsed.

It is important for an organization to have a trained incident response team. It can be either dedicated or an ad-hoc team (on call).

Evidence collection is performed relevant to the nature of the incident. There can be different types of evidence, such as physical, behavioral, logical and digital. No matter the type, the evidence must be properly documented. This document must record the actions performed on the evidence and each party who handles the evidence, along with the tracking to locate where the evidence is. This is also known as the chain of custody (who, what, where, when and how). It assures the accountability and protection of evidence.

If a physical investigation is required, e.g., an employee is suspected, along with the inquiry, there must be relevant business units involved, such as HR. The inquiry information must be documented properly.

We will also briefly look at the types of evidence below. There are four major types of evidence.

- Real evidence: Tangible things – e.g., weapons.
- Demonstrative: This is similar to a model, such as a chart or a diagram demonstrate the testimony of evidence.
- Documentary: A textual evidence.
- Testimonial: Witness testimony.

Seizure of digital assets is difficult. An organization must follow specific laws in order to seize and obtain the assets as evidence. Ethics are also an important practice. Such criminal investigation laws are different from country to country and state to state in some countries. Law and enforcement units can also take such assets into custody under different circumstances. Anyhow, the identified evidence must be properly marked (with who, when, where and circumstances).

Analysis of such information is a very sensitive task. Only certified, qualified team must handle the task.

During this process, such data at rest must be properly stored in a secure facility with proper access controls. During the transportation, the involved parties must be accountable and trustworthy. The storage facilities must be free of hazardous or contaminations.

In the final stage, the data must be presented in a court in some cases. This must be also handled with careful supervision. After the investigation, the assets are often released to the owner. However, in certain cases, a court might order a person to destroy the evidence and assets. Such tasks must be handled according to proper procedures.

Reporting and documentation

Some information about the reporting procedure was discussed in the previous section. When considering internal reports, there are two types of reports: technical and non-technical (i.e., for management).

Investigative techniques

These techniques are used to determine whether a crime has been committed or not. An investigation process is initiated with the collection of data within the legal framework. Such collection of data must be preserved and presented to an authority with intelligent information to make an impact. The way of the presentation also matters, as it should make sense and it must be rational.

During an investigation, actions such as collection of evidence, preserving it, examining and analyzing the evidence to determine what can be presented to authorities or in a court can be observed. The analysis also helps to determine the root cause or motives behind a crime.

From a top-level view, the stages involved are:

- The use of proven scientific methods.
- Collection and preservation.
- Validation.
- Identification.
- Analysis.
- Interpretation.
- Documentation.
- Presentation.

Digital forensics tools, tactics and procedures.

Digital forensics is similar to forensics, but the nature and involvement of the assets, parties and evidence are digital most of the time. Forensic is a scientific investigation carried out in order to determine the criminal who committed a crime and when, where and how it is committed. It helps to find and document valid evidence for use in legal proceedings. There can be instances, such as internal malicious activities, criminal activities, and lawsuits.

Digital forensics uses complex and sophisticated tools, techniques and methodologies. In order to become an investigator, you need to have in-depth knowledge of hardware, networking devices and operations, operating systems (such as client, server, device firmware and systems used in routers, mobile devices, etc.), databases, applications and coding. In addition, you need to have experience using specific sophisticated tools and applied knowledge of strategies.

The process involves the following procedures.

- Acquiring.
- Examination.
- Analysis.
- Reporting.

There are mainly 4 categories of forensic tools.

- Hardware/Digital forensics: This focuses on computer and hardware devices, and the processes would be identification, preservation, recovery and investigation by following the standard procedures.
- Memory forensics: This is a crucial step in forensics. If there is little evidence on static storage devices, memory devices are analyzed in order to find traces.
- Software forensics: This mainly focuses on the legitimate use of software in order to determine if it was stolen. The litigation process is related to intellectual property rights in well-known cases.
- Mobile forensics: Focuses on mobile devices, as this is the next generation technology.
- Live forensics: This is performing real-time analysis on processes, file history, memory, network communication and

keystrokes. This can affect the performance of any system.

7.2 Understand Requirements for Investigation Types

If you are into forensics, you have to understand that the investigation depends on the type of the incident. Let's look the types of investigations.

Administrative

This type of an investigation is often carried out to collect and report relevant information to appropriate authorities so that they can carry out an investigation and take necessary actions. For an example, if a senior employee compromises the accounting information in order to steal, an administrative investigation is carried out at first. These are often tied to human resource related situations.

Criminal

These types of investigations occur when there is a committed crime and when there is a requirement to work with law enforcement. The main goal of such an investigation is to collect evidence for litigation purposes. Therefore, this is highly sensitive, and you must ensure the collected data is suitable to present to authorities. A person is not guilty unless a court decides so beyond a reasonable doubt. Therefore, these cases require special standards and to follow specific guidelines set forth by law enforcement.

Civil

Civil cases are not as tough or thorough as criminal cases. For example, an intellectual property violation is a civil issue. The result in most cases would be a fine.

Regulatory

This is a type of an investigation launched by a regulating body against an organization upon infringement of a law or an agreement. In such cases, the organization must comply and provide evidence without hiding or destroying it.

Industry Standards

These are investigations carried out in order to determine if an organization is following a standard according to the guidelines and procedures. Many organizations adhere to standards to reduce risks.

7.3 Conduct Logging and Monitoring Activities

Intrusion detection and prevention

Intrusion detection is a passive technique used to detect an attempt or succeeded intrusion. There are three types of intrusion detection systems used.

Host-based Intrusion Detection Systems (HIDS)

HIDS is capable of monitoring an internal system, as well as the network interfaces hosted by that system, including the communication from/to it.

Network-based Intrusion Detection Systems (NIDS)

NIDS is more like a network scanner that is capable of scanning (listening) an entire network for intrusion activity.

Wireless Intrusion Detection Systems (WIDS)

Today, wireless networks are more prone to intrusions and attacks, as it is difficult to contain network signal within a premise. These systems are capable of detecting intrusions targeting wireless networks.

Other than these, there are perimeter intrusion detection systems (PIDS) and virtualization-based intrusion prevention systems (VMIDS).

As you see there are actually host-based and network-based IDSs. These systems utilize several methods to detect an intrusion.

Signature-based

By using a static signature file network, communication patterns are matched to certain signatures to identify an intrusion. The problem with this method is the requirement to continuously update the signature file. This method cannot detect zero-day exploits.

Anomaly-based

In this method, variations or deviations of the network patterns are observed and matched against a baseline. This does not require a signature-file, which is the advantage. However, there is a downside. Anomaly-based systems report many false-positive identifications and it may interrupt regular operations.

Behavior-based/Heuristic-based

This method uses a criteria-based approach to study the patterns or behaviors/actions. It looks for specific strings or commands or instructions that would not appear in regular applications. It uses a weight-based system to determine the impact.

Reputation-based

This method, as you already understand, is based on a reputation score. This is a common method of identifying malicious web addresses, IP addresses and even executables.

Intrusion Prevention

Intrusion Prevention systems are active systems, unlike IDSs. Such systems actively sit and monitor all the network activities in the network. It monitors packets deeper, proactively, and attempts to find attempts by following a few methods. Also, remember that an IPS is able to alert and communicate with administrators.

- Signature-based.
- Anomaly-based.
- Policy-based: This method uses security policies and network infrastructure in order to determine a policy violation.

By using these methods, it can prevent system network intrusions, system intrusions and even file intrusions.

Security information and event management (SIEM)

We have already discussed things about SIEM in a previous chapter (6.3). Security systems create vast amounts of data across multiple systems and

stores this data. Systems, such as Security information and event management (SIEM, combination of SIM - Security Information Management - and SEM - Security Event Management) is a centralized log management approach. This is a critical requirement for large-scale organizations. SIEM process is listed below.

- Collect data from various sources.
- Normalize and aggregate.
- Analyze data: In this stage, the existing threats and new threats will be uncovered.
- Reporting and alerting.

SIEM provides two main capabilities.

- Security incident reporting with forensics.
- Alerting if a certain rule-set is matched during the analysis.

Continuous monitoring

As you may have already understood, continuous monitoring and logging are two critical steps to proactively identify, prevent and/or detect any malicious attempt, attack, exploitation or an intrusion. Real-time monitoring is possible with many enterprise solutions. Certain SIEM solutions also offer this service. Monitoring systems may provide the following solutions.

- Identify and prioritize vulnerabilities by scanning and setting baselines.
- Keeping an inventory of information assets.
- Maintaining competent threat intelligence.
- Device audits and compliance audits.
- Reporting and alerting.
- Updating and patching.

Egress monitoring

As the data leaves your network, it is important to have a technique to filter sensitive data by monitoring it. **Egress monitoring** or Extrusion Detection is important for several reasons.

- Ensures the organization's sensitive data is not leaked.
- Ensures any malicious data does not leave or originate from the organization's network.

There are several ways to monitor such information.

- Data Loss Prevention (DLP) systems: Such systems monitor for the leakages of PII and other sensitive data such as Personal Health Information (PHI). By utilizing deep packet inspection and decryption technologies these systems are capable of combating such situations.
- Egress Traffic Enforcement Policy.
- Firewall rules.
- Watermarking.
- Steganography: Steganography is hiding a file within another file. You may have heard attackers hiding malicious files within an image file or a similar. There are ways to detect such files. However, there is the possibility of hiding organizational data within important files by employing the same method.

7.4 Securely Provision Resources

Any business entity or an organization inherits a common characteristic. That is the dynamic nature. In the constant change, the business operation must be consistent. The security posture and standing must also be consistent with the changes. Provisioning and deprovisioning are two critical integrations. For example, if you introduce a new application to the existing computer network, it can bring positive and negative impacts. If there is an exploitable vulnerability, the security posture of an organization

will be at a great risk. The provisioning is the process of the lifecycle of such an asset. However, in this process, if an organization fails to ensure the protection, the entire organization is open to an intrusion attempt and there is a possibility that one might succeed.

The resource provisioning and de-provisioning process must integrate security planning, assessment and analysis. Let's look at some important considerations.

Asset inventory

Keeping an asset inventory help in many ways.

- Protect physical assets, as you are aware of what you own.
- Licensing compliance is a common goal.
- Ease of provisioning and de-provisioning.
- Ease of remediation or removal upon any security incident.

Asset Management

Every asset has a lifecycle. Managing the assets means managing the lifecycle of each and every asset. With asset management, you can keep an inventory, track resources, manage the lifecycle, as well as security as you know what you own, how you use it, and who uses it. This also helps to manage costs and reduce additional costs.

In an organization there can be many assets, such as physical assets, virtual assets, cloud assets and software. Provisioning and de-provisioning processes are also applied here with a security integration in order to mitigate and prevent abuses, litigations, compliance issues and exploitation.

Change Management

Change management is the key to a successful business. As business evolves the dynamic nature of the business is inevitable. The changes are in a flux and an organization must manage it to make the operations consistent and adapt new technological advancements. This is also part of the lifecycle management.

Configuration Management

Standardizing configurations can greatly assist in change management and continuity. This must be implemented and strictly enforced. There are configuration management tools, but the organizations must have implemented the policies. A configuration management system with a Configuration Management Database (CMDB) is utilized to manage and maintain configuration data and history related to all the configurable assets, such as systems, devices and software.

If we take for example, a configuration management software will enforce all computers to have internet security software applied and updated. If a user (e.g., using a mobile computer) does not have his mobile computer updated, the system has to remediate the system. This process has to be automated to cut-down the administrative overhead. Having a single, unified configuration management system reduces workloads, prepare the organization for recovery, and secure operations.

7.5 Understand and Apply Foundational Security Operation Concepts

In this section, we are going to look into some foundational security concepts you can apply to organizational operations. Some of the concepts are discussed in-depth in some sections.

Need-to-know and least privilege

There is a difference between “need” and “want. Need is something you require to do a task. On the other hand, want is more of a desire. Therefore, in order to prevent misuse and information leakages we need to enforce the need-to-know principle. People with valid and validated business justification should be provided access to the necessary data and functionalities.

Least-privilege is closely related with need-to-know principle. This concept is about providing only the necessary privileges to perform the assigned task. In this case, it can be a permission or a right. The least-privilege when provided is enough to perform the duty without a problem. If there is a need for escalation, there has to be a procedure to make it happen. If you have

worked with enterprise level permission management approach, the best policy is to start from **deny all** and then proceed forward.

In RBAC, **aggregation** is often used to unify multiple pieces. In addition, there is also a concept known as **transitive trust**. This is employed in Windows Active Directory when creating child domains. It is like a parent child automatic trust relationship. Even though it makes things simpler, it is dangerous in high-security environments, as it can cause security issues.

Separation of duties and responsibilities

Why separation of duties is important? In any organization, this is common practice. However, a duty with enough power can lead to complete chaos. Let's assume a person has enterprise administrator privilege and has access to all the root accounts. There are several negative impacts.

- The user may become a single point of failure, as he may be the primary authority.
- He might overuse his authority and misuse the organizational assets.
- If an attacker gains enough control of his accounts, the entire enterprise is in jeopardy.

This is why we need to split responsibilities. You may have seen separate administrators exist in system and network infrastructure services. Each person is responsible for his/her task. Sometimes, a team of two or multiple people are required to complete one critical task. This is also applied in the military when it is required to activate security countermeasures – two keys are required to activate certain weapons and there are two people, each having a key and a password that is known to one person each.

If there is a need of a single IT admin, accountant or a similar role, you can either utilize compensation controls or third-party audits.

Privileged account management

Privilege accounts are not uncommon. In an enterprise network, there can be multiple admin roles handled by a single person or a business role. These

accounts can perform a variety of duties. During the process, such privileges can lead to abuses. Therefore, the actions taken from such accounts must be closely monitored. Every action must be logged with all the relevant details so that another party can closely monitor and take actions whenever necessary. Automated monitoring systems can be deployed in enterprise environments where accountability is a key success factor.

Job Rotation

Job rotation is an important practice employed in many organizations. The purpose of this is to prevent a duty becoming too formal and too familiar. Job rotation ensures that the responsibilities are not leading toward mistakes or ignorance, malicious intents and a responsibility becoming an ownership. In other words, job rotation reduces opportunities to abuse the privileges, as well as eliminates single point of failure. If multiple people know how to perform a task, it does not need to depend on a single contact. This is also useful in cross-training in an organization and promotes continuous learning and improvement.

Information lifecycle

This is a topic we have discussed in detail in previous chapters. Let's look at the lifecycle and what the phases are.

- Plan: Formal planning on how to collect, manage and secure information.
- Create: Create, collect, receive or capture.
- Store: Store appropriately with business continuity and disaster recovery in mind.
- Secure: Apply security to information or data at rest, in-transit and at other locations.
- Use: Including sharing and modifications under policies, standards and compliance.

- Retain or Disposal: Archive or dispose while preventing any potential leakages.

Service Level Agreement (SLA)

This is another topic we discussed previously (Chapter 1).

An SLA is a critical agreement between a service provider and a service receiver in order to ensure the provided service and response are acceptable – to guarantee a minimum level of standards. It is a quantified statement. When an organization depends on SLAs of external parties, contractors and vendors, they must ensure the SLA meets the business requirement during the provisioning process. If an organization has to provide SLAs to its customers, the service quality, such as uptime, and the incident handling time frames, must not violate the agreements. If an organization violates such agreements, there will be penalties and the consumer can take legal actions.

For example, let's take an organization that provides internet and storage services with a 99.9 uptime and a response-time with urgent priority is 15 minutes and to a case with high priority is within an hour. If the uptime goes below 99.9 it is a problem with the service quality. In order to resolve the issue, they may need to ensure fault tolerance and resiliency by applying an appropriate technology, for an example, failover clustering, load balancers or firewalls if the problem was caused by a security breach. They must respond to incidents within the given time-frame in order to help the clients with business continuity by providing true details of the incident and possible alternatives.

The following parameters may exist in such standards.

- Mean Time Between Failures (MTBF).
- Mean Time to Restore Services (MTRS).
- Incident response time.
- General response time.
- Escalation procedures.

- Available hours.
- Average and peak concurrent users.

There are important document considerations when it comes to the SLAs. The OLA (Operational-Level Agreement) and Underpinning Contracts (UC). An OLA is an internal operation level agreement (e.g., between groups) and UC is there to manage third-party relationships.

You also need to remember that you need to employ critical assessment of the parties involved in order to measure the efficiency and effectiveness of SLAs. Setting up and analyzing Key Performance Indicators (KPIs) will greatly assist.

7.6 Apply Resource Protection Techniques

This section will walk you through the application of protection techniques to resources, such as hardware, software and media.

Among hardware/firmware, there are communication devices, such as routers, switches, firewalls and more sophisticated devices and their operating systems.

Data, such as system (operating systems, configuration and audit data), and business data need critical protection. We have already discussed the nature of such data.

Storage systems and media need critical consideration, as all the data is stored on such devices. Storage services, such as DAS, SAN and NAS and media/backup media devices, such as tapes and cartridges, external devices, such as removable media, fall under this category.

In addition to these resources, operating system images and source files must be free from vulnerabilities, especially bugs and 0-day vulnerabilities. There are tools that apply patches and updates by injecting those into system images and deploying with software packages during installation.

Hardware and software asset management

This is something we discussed earlier, if you remember inventory management topics. Without such databases, assess and manage

vulnerabilities become more and more difficult. This inventory helps to identify what is being used in the organization and the inherent risks involved.

7.7 Conduct Incident Management

In this section, we are going to have a look into a critical process in the management lifecycle of almost every business: incident management. However, we are going to focus on security related incident management. Let's analyze the stages of security incident management in detail.

Proactiveness

A successful incident management is formed by identifying, analyzing and reviewing the current/future risks and threats and by forming an incident management policy, procedures and guidelines. This must be well documented, trained, rehearsed and evaluated in order to create a consistent and efficient incident management lifecycle.

Detection

Detection is the first phase of the incident management lifecycle. A report or an alert may have generated from an IDS, a firewall, an antivirus system, a remediation point, a monitoring system – hardware/software/mobile, a sensor, or someone may have reported an incident. If this is detected in real-time, it is great, however, that not always the case. During this process, the response team should have an initial idea of the scale and priority of the impact.

Response

With the detection process, the responsible team or an individual must start verifying the incident. This process is vital. Without knowing if this a false alarm, it is impossible to move to the next phase.

If the incident occurs in real-time, it is advisable to keep the system on in order to collect forensic data. The communication is also a crucial step. In such a situation, the person who verifies the threat must communicate with the responsible teams so that they can launch their procedures to secure and isolate the rest of the system. A proper escalation procedure must have been established before the incident happens. Otherwise, it will take time to

locate the phone numbers and wake up multiple people from their bed at midnight.

Mitigation

Mitigation include isolation to prevent prevalence and contain the threat. Isolating an infected computer from the network is an example.

Reporting

In this phase you start reporting to the relevant parties the information about the ongoing incident and recovery.

Recovery

In this process, the restoring process is started and completed so that the organization can continue regular operations.

Remediation

Remediation involves rebuilding and improving existing systems, placing extra safeguards in line with business continuity processes.

Lessons learned

In this final phase, all the parties involved in restoring and remediating gather to review the entire phases and processes. During this process, the effectiveness of the security measures and improvements, including enhancing remediation techniques will be discussed. This is vital, as the end result should be to prepare the team to face a future incident.

7.8 Operate and Maintain Detective and Preventative Measures

In this section we will look into how detective and preventive measures are practically operated and maintained.

Firewalls

Firewalls are deployed often at the perimeter, DMZ, in distribution layer (e.g., web security appliances), and in high-availability networks. These are few examples and there are many other scenarios. To protect virtualized and cloud platforms, especially from DDoS and other attacks, firewalls must be in place, both hardware appliances and software-based. For web-based

operations and to mitigate DDoS and other attacks, the best method is to utilize a **Web Application Firewall (WAF)** . To protect the endpoints, it is possible to install host-based firewalls, especially if the users heavily rely on the internet. It is also important to analyze the effectiveness of the rules and how logging can be proactively used to defend the firewall itself.

IDS/IPS

Just placing an IDS/IPS is not going to be effective, unless you continuously evaluate the effectiveness. There must be a routine check in order to fine-tune the systems.

Whitelisting/blacklisting

This is often used in rule-based access control. These lists may exist in firewalls, spam protection applications, network access protection services, routers and other devices. This process can be automated but requires monitoring. On the other hand, whitelisting can be a manual process in order to ensure accuracy.

Security services provided by third parties

It is possible to integrate third-party service providers in order to implement a security operation. This isn't going to hurt if you know and understand the technologies in-depth. There are several services and we will look into each service. Some of these services involve AI services, audits and forensics.

- Managed Service Providers (MSS) – Security: An MSS monitors, evaluates and analyzes an organization's in order to detect functional issues and they also provide incident management.
- SIEM: We discussed SIEM in depth in previous chapters.
- Web filtering.
- DDoS prevention and mitigation.
- Vulnerability management services.
- Spam filtering.

- Cloud-based malware detection.

Sandboxing

This technique is mainly used in the software development process – during the testing process. If you are familiar with development platforms, an organization would have a production platform for the actual operation, while a development and test environments to do development and testing respectively. A sandbox environment can be an isolated network, a simulated environment or even a virtual environment. The main advantage is the segmentation and containment. There are platforms to test malware in sandbox environments in order to analyze it in real-time.

Honeypots/honeynets

A honeypot is a decoy. An attacker may think a honeypot is an actual network. It helps to observe the stacking strategy of an intruder. A collection or a network of honeypots is called a honeynet.

Anti-malware

Anti-malware applications fight with malicious applications or malware. Malware can be of many types yet all focus on one thing; to break the operation – disrupt, destroy or steal. A basic malware protection application depends on signature-based detection. However, there are other methods and the integration of AI and machine learning. Such software can also mitigate spam issues and network pollution. These services can send alerts to the users. If it is an enterprise class solution, it sends alerts to an operations control center.

7.9 Implement and Support Patch and Vulnerability Management

Patch management and vulnerability management may sound identical but there are some differences.

Patch management focuses on fixing bugs and security flaws in software applications. These issues are caused by the developer or vendor due to their coding practices or integrated technologies. In such cases, they release advisory, release updates and fixes for ongoing threats.

- Software applications are capable of automatic patch management. Detecting and obtaining updates automatically and installing it by itself are some of the capabilities.
- In a large network, if you manage end-point patch management, it is a resource consuming process, especially when considering the internet costs and internal network congestion. Therefore, it is important to obtain and distribute patches through a central server. Microsoft WSUS is a good example of centralized update and patch management.
- To assess if patch management is effective, patch compliance reporting is essential. The statistics will reveal if it is successful or if certain devices have failed to comply.
- Once you install the patches, it may lead the current operation into chaos if it is not tested for all the possible cases. In such cases, automatic rollback capabilities can save the day.

If we arrive at vulnerability management, there is a key difference. Vulnerabilities may arise, not only due to software, or system-level bugs or fixes. They can be due to misconfiguration, installation methods, missing updates and conflicts. Therefore, it has a broader perspective, but the management techniques and technologies must provide a unified approach. When it comes to vulnerabilities, zero-day vulnerability can cause massive damage to systems if it can be exploited – zero-day exploit. The security teams must be proficient and proactive in order to manage such vulnerabilities by deploying countermeasures to mitigate the future threats effectively.

7.10 Understand and Participate in Change Management Processes

Change management is a major process in business, infrastructure, security and in almost all management areas. If there are no flexible and adaptable settings, it is difficult to reach scalability and expandability. There are several important steps in change management and let's discuss it here.

- Identify the change: The identification process of the change is the first phase of a change management lifecycle. The requirement may arise due to different objectives, incidents, reports or obsolescence.
- Design: In this process, the required change is planned and designed.
- Review: The solution must be realistically tested before it is forwarded to the board in order to obtain approval.
- Change request: This is a formal request explaining the requirement and to get approval before the implementation process. A change request consists of the date planned to release the change, root cause and reasons, impacted areas, how it is going to change in contrast to the existing, notification information, test results, deployment plans and recovery/rollback plans.
- Approval: In this stage, a board of control or a committee receives the request, arranges meetings, reviews the request and studies the business and other impacts and decides whether it is feasible or not. There will be interviews and other methodologies to analyze the impact and cost involved. If the requirement is unavoidable or a realistic need, the change request will be approved.
- Notifications: Either the board or the implementation management is responsible for sending notifications of incoming changes.
- Implementation/Deployment: In this phase, the change is fully implemented and pushed to the production environment. It is followed by a series of tests.

7.11 Implement Recovery Strategies

In this section, we will look into more of a strategic perspective on implementing recovery procedures. The recovery strategy is vital to recovering a business from security incidents, outages and unplanned disasters. Minimal downtime and rapid recovery are the expected end-results.

Backup storage strategies

A proper backup strategy requires a policy, standards and procedures. It should clearly answer the what (what to back up), when and how (techniques) and where (on-premise, offsite, cloud) questions. For the role requirements (who) there has to be custodians and operators. Security must be integrated to the backup strategy to protect backups from damages, to avoid single point of failure and to protect backups from being misplaced.

It is also important to reduce costs by applying retention policies. The retention must not, however, destroy the important data. Furthermore, an organization might think of reducing costs on storage. In such cases, they may look for an alternative. If the organization is thinking about archive costs, they may look for archive solution (offsite). Nowadays, there are cloud services that offer intelligent backup strategies (e.g., Amazon storage and archive services) with best grade security.

Recovery site strategies

For datacenters, it is important to have one fully operational site, one recovery site (warm site) and a cold site (a site that has the equipment but not configured yet). The recovery site must be able to operate if the main center is down. However, in order to provide services from the recovery site, it requires regional sites to obtain the copies and provide continuous operations. These sites may be geographically distant in order to reduce the impact of a natural disaster. With the expansion of cloud technologies, this is not a difficult goal to achieve.

Multiple processing sites

With the expansion of technologies, running several datacenters is no longer a complex process. Therefore, site resiliency is no longer a difficult goal. Today there are multiple datacenters across the globe and the communication is much faster, secure and reliable. The ability to reach

availability through synchronization and replication through multiple datacenters allows vendors to offer backup-free technologies. If an organization lacks additional datacenters they can think of public cloud solutions.

System resilience, high availability, Quality of Service (QoS), and fault tolerance

System resilience

To build system resilience, we must avoid single point of failure by incorporating fail-safe mechanisms with redundancy in the design, thus enhancing the recovery strategy. The goal of resiliency is to recover the systems as quickly as possible. Hot-standby systems can increase the availability during a failure of primary systems.

High availability

Resilience is the capacity of quickly recovering (minimize downtime), while high availability is having multiple, redundant systems to enable zero downtime for a single failure. High availability clustering is the operational perspective. If you take a server or a database cluster, even if one node fails, the rest can serve the clients while the administrators fix the problem.

Quality of service (QoS)

This technique is used to prioritize traffic within the network. For instance, streaming media will receive higher priority than web traffic or torrents. Often, network control traffic, voice and video get top priority. Web traffic, gaming or peer-to-peer traffic gets lower priority.

Fault tolerance

Fault tolerance is the ability to withstand failures e.g., hardware failures. For instance, a server can have multiple processors, hot-standby hardware, hot-pluggable capabilities to combat these situations. A repository of hardware is also important.

7.12 Implement Disaster Recovery (DR): Recovery Processes

Disaster recovery planning and a clear disaster recovery procedural documentation at the end is vital to any form of business. This is a process that takes time and careful analysis of all the possibilities. The procedures must be exercised and verified for effectiveness.

Response

Responding to a disaster situation depends on few main factors. The verification is important to identify the situation and the potential impact. The process is time-sensitive, and it must be set in motion as soon as possible. In order to minimize the time to realize a situation, there must be monitoring systems in place with a team dedicated for such activities.

Personnel

As mentioned in the previous section, in many organizations there is a dedicated team of professionals assigned for this task. They are responsible for planning, designing, testing and implementing DR processes. In a disaster situation, this team must be made aware – this team is usually responsible for monitoring the situations and in such case, they are the first to know. If the communication breaks there must be alternative methods and for that reason, the existing technologies and methods must be integrated to the communication plan which should also be a part of the DR planning.

Communications

Readiness (resourcefulness) and communication are two key factors of a successfully executed recovery procedure. Communication can be difficult in certain situations, such as earthquakes, storms, floods and tsunami situations. The initial communication must be with the recovery team and then they must collaboratively progress through any available method of communication. If the method is a reliable media, it is less disturbing. The team must communicate with the business peers and all the key players and stakeholders. In this process, they must inform the general public about the situation as needed.

Assessment

In this process, the team engages with the relevant parties, incorporate technologies in order to assess the magnitude, impact, related failures and get a complete picture of the situation.

Restoration

Restoration is the process of setting the recovery process and procedures in motion once the assessment is complete. If a site has failed, the operation must be handed over to the failover site. And then the recovery must be started so that the first site is restored. During this process the safety of the failover must also be considered. This is why the organizations keep more than one failover.

Training and awareness

The training and awareness are vital factors contributing to a successful recovery process. Without awareness, the employees, stakeholders and even general public do not know what sort of actions will be taken during a disaster situation. Training the relevant teams and personal makes the familiarity a reality, thus greatly enhances the effectiveness. All these methods are relating to the readiness (resources and financial) and practical approach with respect to the utilization of available resources, as mentioned before.

7.13 Test disaster recovery plans (DRP)

As we iterated in multiple sections, without testing the plan it is impossible to measure how effective and realistic the plan is. In this section we are going to look into this in more detail.

Read-through/tabletop

This process is a team effort where the disaster recovery team with other responsible teams gather, read through the plan and measure the resources and the time requirements. If all the requirements have met, the teams approve the plan as realistic. If it does not meet certain criteria, the DR team has to redesign or adjust specific areas. The change management process is also an integral part of the DR plan.

Walkthrough

A walkthrough is a tour of a demonstration. It can be also thought as a simulation. During this process, the relevant team and also perhaps certain outsiders may go through the process and look for errors, omissions and gaps.

Simulation

An incident can be simulated in order to practically measure the results and the effectiveness. During a simulation, an actual disaster situation is set in motion and all the parties involved in the rehearsal process participate.

Parallel

In this scenario, teams perform recovery on different platforms and facilities. To test such scenarios, there are built-in, as well as third-party solutions. The main importance of this method is to minimize the disruptions in ongoing operations and infrastructures.

Full-interruption

This is an actual and a full simulation of a disaster recovery situation. As this is closer to an actual situation, it involves significant expenses, time and efforts. Although there are such drawbacks, the clinical accuracy cannot be assured without at least one of these test simulations. During this process, the actual operations will be migrated to the failover completely and an attempt will be made to recover the primary site.

7.14 Participate in Business Continuity (BC) Planning and Exercises

Business continuity is the most important and receives the utmost priority of any business operation. Disaster recovery is actually a part of this process, in other words, a tactic. During an actual disaster, the process will help to continue the business. However, even without disasters, there are challenges to overcome. BC planning has a highly broad spectrum and it must address even more prevailing issues than DR.

The planning process should identify mission critical business processes. Identified the financial requirements is also a part of this process. This can be achieved by performing a business impact analysis (BIA). In the next

stage, it is important to have your technologies reviewed with a well-formed plan with a review on vendor support contacts.

The communication is vital, as mentioned before. It is important to build a robust communication plan with failover in order to use during an actual event.

The BC process is not something you can do alone. You need to get assistance from local authorities, police, fire-department, government agencies, partners and general public.

7.15 Implement and Manage Physical Security

Perimeter security controls

Perimeter security involves securing the perimeter areas of your organization, datacenter or of the sites. Basically, this focuses on the physical access control.

Access Control can be installed or deployed. To protect the perimeter we could use fences, guards, signs, and electronic access controls, such as cards, sensors, surveillance, or even biometrics. As you understand, monitoring is a critical process of access control and serves as both a preventing and detective method. For instance, if an electronic door is not closing automatically, the door may have been tampered with. If a vent appears dislocated, it is something to investigate. If someone is trying to access a second door with failures, although he/she should have used the same key card to gain access from the first door, he/she may have gained access from an illegal way. If someone is using a card to access a restricted area with a key card and unable to proceed, he/she may have stolen it. These are some of the possibilities. Monitoring systems can alert and also evaluate incidents by matching the historical events. Such automation is something we may need in the long run.

Internal security controls

The internal controls deal with securing internal physical assets and locations. It can be a sensitive area, a wiring closet, a file cabinet, a server room, or even a corridor that provides access to internal areas.

If there are visits from outsiders and if it is required, it is important to have a proper procedure to escort the visitors.

Securing individual office spaces, storage cabinets and desks are also contributing to uplift internal security.

7.16 Address Personnel Safety and Security Concerns

In this section we'll look at the personal safety of employees while working and traveling.

Travel

This mainly focuses on the safety of the user while traveling inland or abroad. While traveling, an employee should focus on network safety, theft and social engineering. This is even more important if the employee has to travel to other countries. The government laws, policies and other enforcements may be entirely different from the country where a person lives. This can raise legal actions, penalties, and even more severe issues, if someone is unable to comply or does have no awareness of such issues.

During the travel it is important to install/enable device encryption and anti-theft controls. This is important especially for mobile devices. During communication with the office, the communication must also use encryption technologies or secure VPN setup. It is also advisable to avoid public Wi-Fi networks and internet facilities, such as cafes. If there is even more risk, advise the employees not to take devices with sensitive information with them when traveling to such countries. If the mobile device is needed while in the other countries, it is possible to provide an alternative device or a backed-up and re-imaged device that does not include any previous data.

Security training and awareness

Each organization may have different security risks and may need different campaigns. The threats may emerge while you are at a different place, in a different country or even at home. To deal with each most important company specific scenario, users must have adequate training and simulations. For instance, if an employee is expected to join a meeting with a set of people in the foreign country, he should travel with assigned or

reputed travel services. The person should not disclose personal and official information to unknown people. It is also important to train them to prevent the use of any external devices they buy or are given during the visits. The awareness and training campaigns can do a lot in order to prevent information leakage and intrusions, as end-point devices as well as people, are the most vulnerable.

Emergency management

This is something an organization needs to focus on during the DR/BC planning process. During an emergency situation, such as a terrorist attack, an earthquake or a category 3-4 storm, there may arise huge impacts and chaos. The organization must be able to cope with the situation, notify the superiors, employees, partners and visitors about the situation. There must be ways to locate and recover employees, alert them no matter where they are. Sometimes, during such incidents, employees may be traveling to the affected location. The communication and emergency backup communications are extremely important. Nowadays, there are many services, from SMS to text messages, social media, emergency alert services, and many more that can be integrated and utilized. All of these requirements can be satisfied with a properly planned, evaluated emergency management plan.

Duress

Duress is a special situation where a person is forced to coerce an act against his/her will. Pointing a gun at a guard or a manager who is responsible for protecting a vault is a scenario in a robbery. Another is blackmailing an employee in order to steal information by threatening to disclose something personal and secret about him. Such situations are realistic and can happen to anyone. Training and countermeasures can tactically change the situation. If you were watching an action movie, you may have seen how the cashier uses a mechanism to alert the police. Such manual or automated mechanisms can be really help. There are certain sensor systems that can silently alert or raise an alarm when someone enters a facility in an unexpected hour. It can be either an outsider or even a designated employee. However, in such situations, you must make sure the employees are trained not to attempt to become heroes. The situation can be less intensive and traumatic if one can comply and allow the demands, at

least until help is arrives. The goal here is to set countermeasures and effectively manage such situations without jeopardizing personal safety.

Chapter 8

Software Development Security

This is the last domain in the CISSP examination. Software development lifecycle and security integrated design are highly important because most of the electronic devices used in organizations are controlled by some kind of a code-based platform. It can be embedded code, a firmware, a driver, a component, a module, a plugin, a feature or simply an application. Therefore, you should think about how significant the secure design is and how it widens the attack surface if you simply install a simple application.

Therefore, the security must be focused on the software development lifecycle in every stage. The development environment should also be secure and bug free. The repositories should be well protected and the access to such environments must be monitored thoroughly. When an organization merges or splits, it is important to assure the governance, control and security.

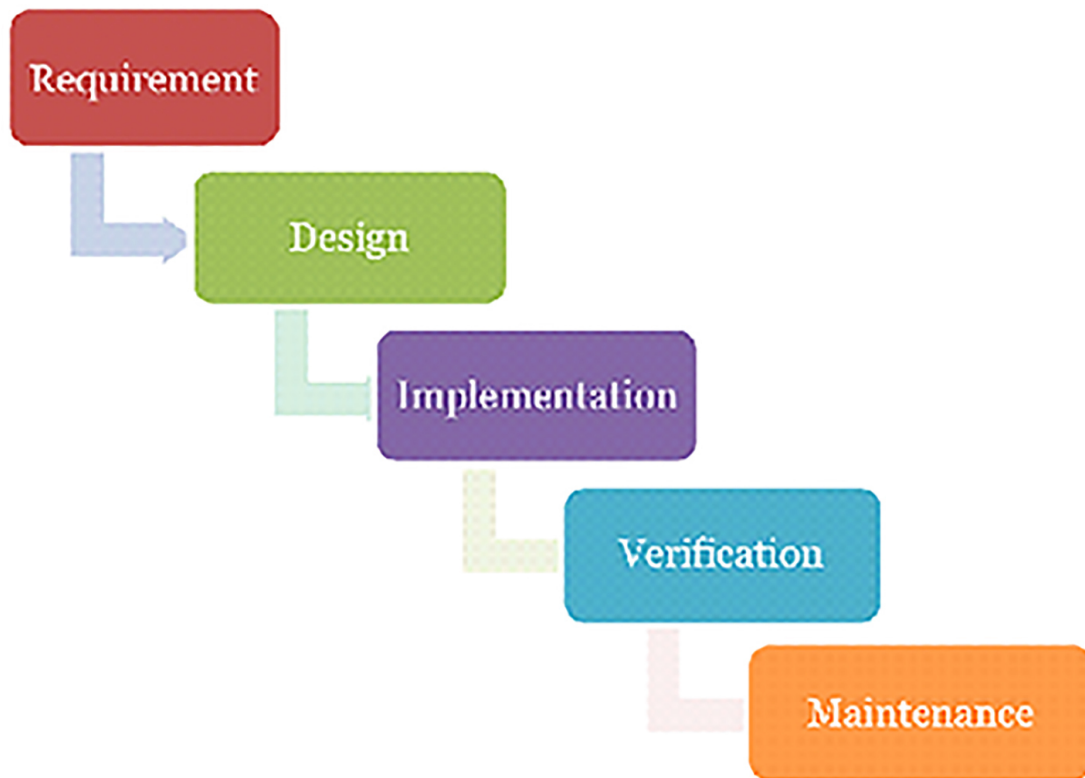
8.1 Understand and Integrate Security throughout the Software Development Lifecycle (SDLC)

Development methodologies

There are many software development methodologies, both traditional and new. In order to get an idea of the development lifecycle, let's have a look at them one by one.

Waterfall model

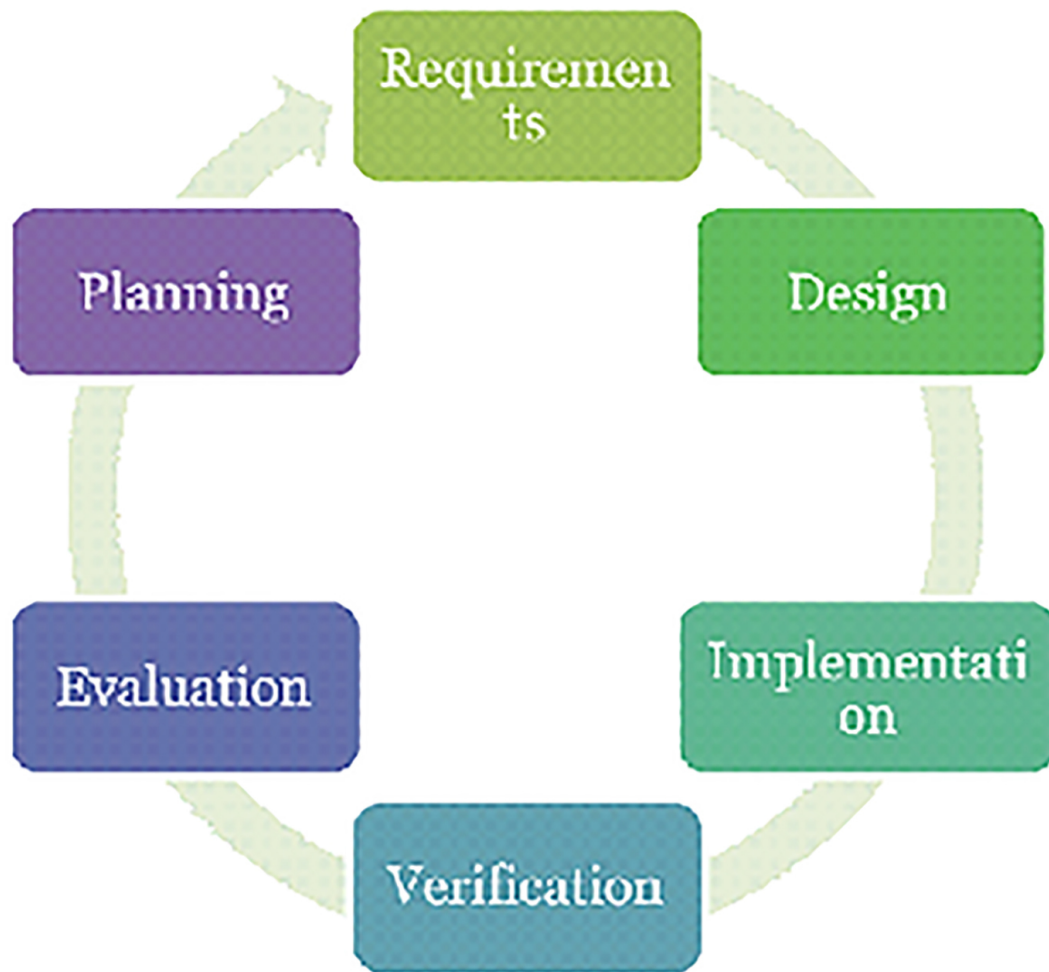
This is one of the oldest SDLC models and it is not even used in recent developments. The model was not flexible enough, as it requires all the system requirements to be defined at the start. Then at the end of the process, the work has to be tested and the next requirements are assigned, and it resets the process. This is a rigid structure and most of the development work requires more flexibility, except for certain military or government applications.



The Waterfall Model

Iterative model

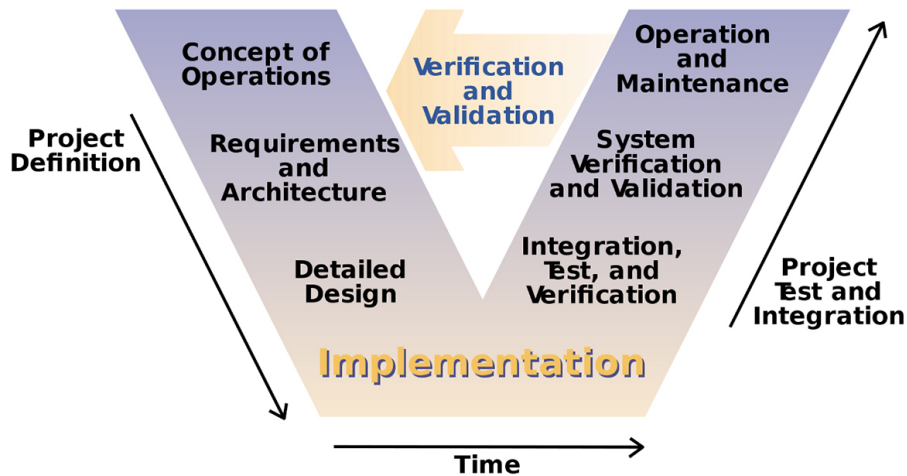
This model takes the waterfall model and divides it into mini cycles or mini projects. Therefore, it is a step by step or a modular approach rather than all at once in the waterfall model. It is an incremental model and somewhat similar to the agile model (will be discussed later), except for the involvement of customers.



Iterative model

V-model

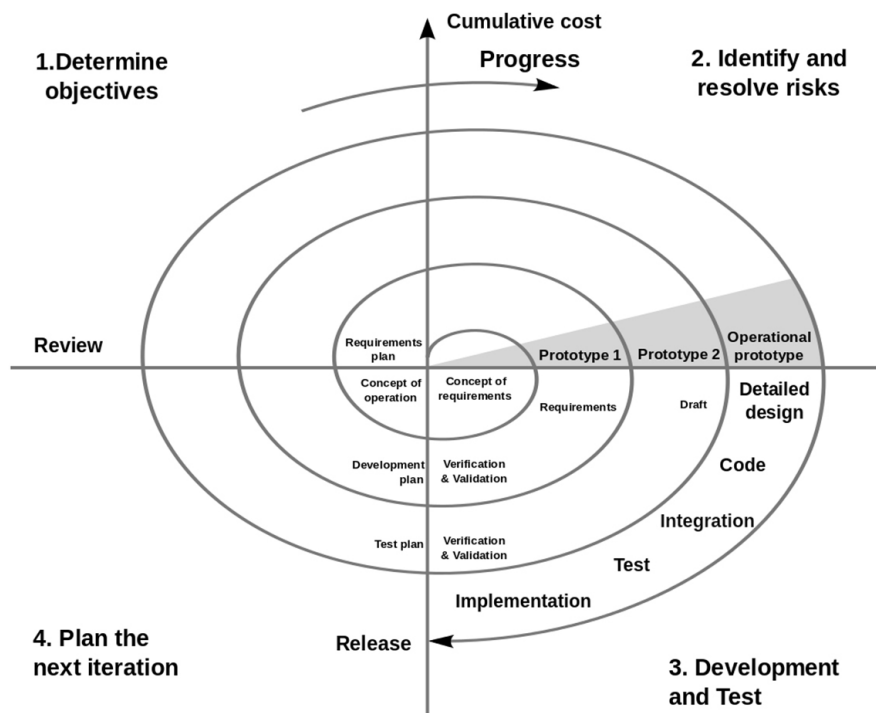
This is an evolved model out of the classic waterfall model. The specialty is that the steps are flipped upward after the coding (implementation) phase.



(V-model – image credit: Wikipedia)

Spiral model

The spiral model is an advanced model that helps developers to employ several SDLC models together collaboratively. It is also a combination of waterfall and iterative models. The drawback is to know when to move on to the next phase.



(Spiral model – image credit: Wikipedia)

Lean model

As you should have understood, the development work requires much more flexibility. Lean approach focuses on speed and iterative development, while reducing the waste in each phase. It reduces risk of wasting effort.

Agile model

This model is similar to the lean model. We can think of this as the opposite of the waterfall model. This model has the following stages.

- Requirement gathering.
- Analysis.
- Design.
- Implementation (coding).
- Unit testing.
- Feedback: In this stage, the output is reviewed with the client or customer, the feedback is taken and made into new requirements if it requires modification. If it is complete, the product is ready to release.

Prototyping

In this model, a prototype is implemented for the customer's review. The prototype is an implementation with the basic functionalities. It should make sense to the customer. Once it is accepted, the rest of the SDLC process continues. There may be more prototype releases if required. This is most suited for emerging technologies so that the technology can be demonstrated as a prototype.

DevOps

DevOps is a new model used in software development. However, it is not exactly an SDLC model. While SDLC focuses on writing the software, DevOps focuses on building and deploying. It bridges the gap between the creation and use, including continuous integration and release. With DevOps, changes are more fluid and organizational risk is reduced.

Application Lifecycle Management (ALM)

ALM is a broad idea that helps integrating others. It involves the entire product lifecycle until the end of life. ALM incorporates SDLC, DevOps, Portfolio Management and Service Desk.

Maturity models

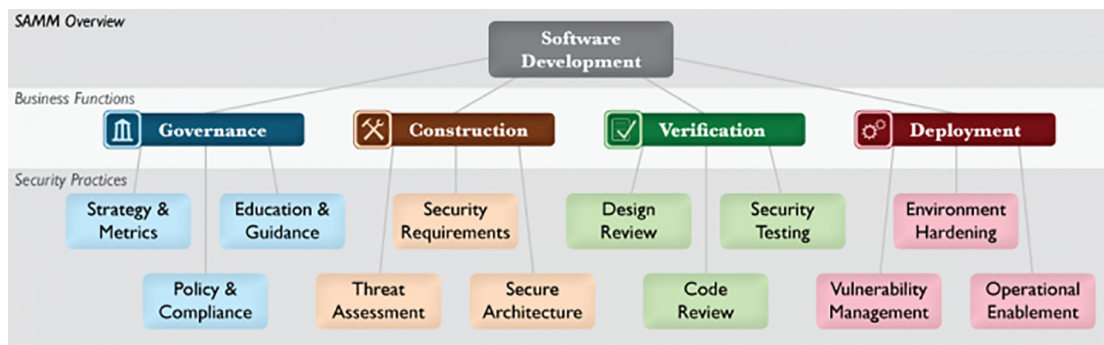
The **Capability Maturity Model (CMM)** is a reference model of maturity practices. With the help of the model, the development process can be made more reliable and predictable, in other words, proactive. This enhances the schedule and quality management, thus reducing the defects. It does not define processes, but the characteristics, and serves as a collection of good practices. This model was replaced by **CMMI (Capability Maturity Model Integration)**. CMMI has the following stages.

- Initial: Processes are unpredictable, deficiently controlled, and reactive.
- Repeatable: At the project level, processes are characterized and understood. At this stage, plans are documented, performed and monitored with the necessary controls. The nature is, however, reactive.
- Defined: Same as the repeatable at the organizational level. The nature is proactive rather than reactive.
- Quantitatively managed: Collects data from the development lifecycle using statistical and other quantitative techniques. Such data is used for improvements.
- Optimizing: Performance is continuously enhanced through incremental technological improvements or through innovations.

We will also look at the **Software Assurance Maturity Model (SAMM)**.

This is an open-source model developed to assist in implementing a strategy for software security. SAMM is also known as OpenSAMM and is part of

the OWASP. You will be able to find more information at <https://www.opensamm.org/>



(OWASP SAMM model – image credit: OWASP)

Maturity Levels of OpenSAMM

- Level 0: Starting point – unfulfilled practice.
- Level 1: Initial understanding with ad-hoc provisioning of security practices.
- Level 2: Increase the efficiency and effectiveness of security practices.
- Level 3: Comprehensive mastery of security practices.

Operation and maintenance

The next phase of the software development lifecycle is the operation and maintenance. In other words, to provide support, updates and upgrades (new features).

Change management

Change management is an alien term now if you have been following this CISSP book from the start. This is a common practice in software development. A well-defined, documented and reviewed plan is required to manage changes without disrupting the development, testing, and release activities. There must be a feasibility study before starting the process. During this study current status, capabilities, risk and security issues will be taken into account within a specific time frame.

Integrated product team

In any environment, there are many teams beyond the dev team. The infrastructure team, general IT operations department, and so on. These teams have to play their roles during the development process. It is a team-effort and if teams are unable to collaborate, the outcome will be a failure. As we discussed earlier, DevOps and AML integrate these team in a systematic and effective way so that the output can be optimized to gain maximum results.

8.2 Identify and Apply Security Controls in Development Environments

In this section, we are going to look into the protection of code, repositories and intellectual property rights. To secure the development environment multi-layered risk mitigation strategy is required.

Security of the software environments

A development environment utilizes many services and layers. It is comprised of application servers, web, connectivity, development platforms and databases. An organization must protect this environment with sensitive data, code, and other important components.

Security weaknesses and vulnerabilities at the source-code level

In the development process, most vulnerabilities occur due to poor coding practices. In each programming language and development guide, there are specific guidelines to write code by eliminating the security holes. For instance, if you use buffers in a program and if you are unable to handle errors by using appropriate methods, you are creating a vulnerability and opening the application to buffer-based exploits. This is also the same for web-based applications with a database at the backend. Input validation issues are also among common mistakes. Secure code practices are vital to implement best quality software. Once you release a software, releasing bugs and patches can take lots of time and resources.

Configuration management as an aspect of secure coding

Configuration management must be accomplished through a centralized system with version control in mind. When there are development processes to implement new features, editions or even fixes, and proper documentation, as well as a central code repository are important.

Security of code repositories

Code repositories must be isolated from the internet. Furthermore, there must be separate repositories for development, testing and release. The code must be free from unauthorized modifications. Nowadays, organizations hire outsourced services. An extra-precaution must be taken in such cases. If the repos can be accessed remotely by developers from distant areas, it must occur through highly secured SSH, RDS or VPN service implementation.

Security of application programming interfaces

The API is a way to interconnect different platforms and applications, as well as to control an application programmatically. You can think of an API as a set of programmatic tools and procedures to build communicating applications.

When dealing with APIs we employ different security concepts and categories for specific API interface and provisioned services. We will be utilizing the following methods to secure APIs.

- Authentication and authorization.
- Encryption and digital Signature.
- Use tokens.
- Use quotas and throttling.
- Use an API gateway.
- Apply vulnerability management.

There are security guidelines specifically for APIs such as REST and SOAP APIs. These guidelines must be followed during the integration process.

API security schemes in brief.

- API Key.
- Authentication (ID and Key pair).
- OpenID Connect (OIDC).

8.3 Assess the Effectiveness of Software Security

Assessment is the key to effective security framework, and it is iterated many times in many chapters. Continuous assessment is required in order to verify if the deployed security strategies are working efficiently. Routine checks and reviews of implementations are the two high-important processes.

Auditing and logging of changes

Without changes there will be no development. Therefore, auditing must review the change control process for its effectiveness and efficiency. Changes cannot be announced and integrated on the fly. Therefore, if there is a change it must be logged properly to keep track and test thoroughly.

Risk analysis and mitigation

Without taking a risk there will be no progress. Risks are necessary during the development phase. However, it must be addressed during the development lifecycle before releasing an implementation. When a risk is found, there is a need to apply mitigation techniques. During the previous chapters we have discussed the risk analysis and mitigation techniques. This process must be inherited by the software development process and procedures.

8.4 Assess Security Impact of Acquired Software

This section is critically important so that you can integrate the techniques to the provisioning and de-provisioning.

When an organization acquires a software development firm, or even when an organization decides to obtain software rather than the development environment, it opens the doors for incoming and unknown threats. It can

be either a continuation or a new emergence. Therefore, if an organization acquires software, the software development process including coding practices, repository security, design and implementation, and intellectual property rights must be carefully reviewed.

8.5 Define and Apply Secure Coding Guidelines and Standards

We have arrived to the final section of the 8th domain of CISSP. In this section we will discuss the technical approach to applied security in coding.

In the past, code security was integrated in later stages. However, this outdated concept is no longer practiced. As an organization, it should protect the infrastructure, as well as the development lifecycle. There are multiple strategies, as well as tools available to make the developer's coding security easier. However, also remember that some vulnerabilities cannot be found through automated tests.

Security weaknesses and vulnerabilities at the source-code level

A practitioner with security in mind follows standards, procedures, guidelines and best practices. At a modular level, testing and reviewing can reveal any missed concerns. Source code analysis tools, also known as **Static Application Security Testing (SAST)** tools, aid in analyzing code and complications in order to find security flaws. OWASP provides SAST tools and can find issues, such as buffer overflows, SQL injections, and XSS issues at a highly complex stage. These tools can be integrated with many IDEs. The drawbacks of these tools are the false positive rate and the inability to find certain vulnerabilities.

There are new approaches like **Interactive Application Security Testing (IAST)** which is an enhanced version of SAST. These technologies are faster, accurate, and able to integrate with new platforms.

Security of application programming interfaces

There can be several types of attacks on APIs. The most common is **perimeter attacks**. To mitigate such attacks, all the incoming data must be validated. By setting up threat detection tools, it is possible to monitor and prevent issues. The second threat is stealing the API Key, also known as

identity attacks . Securing and preventing leakage are two critical steps in preventing the leakage. In addition, any attacks can appear in between the communicating devices. In order to prevent such MITM attacks, it is possible to use encryption such as TSL.

There are lot of API security platforms, such as Google Apigee, CA API gateway, IBM API Connect, RedHat 3scale, Amazon API gateway, Microsoft Azure API gateway, and SAP API management are enterprise-level examples.

Secure coding practices

- Input validation.
- Pay attention to compiler errors and warnings.
- Output encoding.
- Secure authentication and access control methods.
- Cryptographic practices.
- Error handling and logging practices.
- Database security practices.
- File handling best practices.
- Communication handling practices.
- Information protection schemes.
- System level protection.
- Installer protection.
- Memory management and protection.
- Code and platform-based best practices.

Some of the practices can be found in detail at OWASP coding practices page here:

https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide

Conclusion

At the end of the 8 chapters, we hope you have gained a proper understanding of the topics and content. We advise you to go through the available resources to gain additional knowledge, as this book is intended to give you an introduction to A-Z subjects related to and covered in the CISSP learning path. Now that you have reviewed the book you will be able to apply your knowledge to organizational requirements and research more into the domains.

If you are getting ready for the examination, make a plan and approach it well. You will need to register for the exam at least 2 months before and study hard. Most of the information related to examination and resources can be found here on the ISC2 website - <https://www.isc2.org/Certifications/CISSP>

You can find Flash cards here

<https://enroll.isc2.org/product?catalog=CISSP-FC>

It is also useful if you join a CISSP study group. There are many community forums and platforms. You will be able to experience an extensive amount of useful information, technical skills from your peers and friends who have a common interest.

Taking video training, and seminars/webinars can scale your knowledge and perspectives. Once you gain as much as you need, it is the time for practice tests.

Finally, it is the time to sit for the exam. Remember, the exam is 3 hours long. Therefore, you must get a good night's rest. Have a good meal before you leave for the exam. You can also bring drinks or snacks to consume during a break. Collect what you need to bring, including your identity card, emergency medicine, etc. Dress comfortably and arrive early at the examination center. Leave what is not permitted, such as your mobile device, before you arrive at your desk. During the exam, take breaks whenever necessary, and keep yourself hydrated.

If you find the book useful, we would appreciate a positive review. We would like to hear it from you. We appreciate your feedback very much!

CISSP

*A Comprehensive Beginner's Guide
to Learn the Realms of Security
and Risk Management from A-Z
using CISSP Principles*

DANIEL JONES

Introduction

International Information Systems Security Certification Consortium” - (ISC)² is undeniably the world’s largest security organization. It is an international non-profit organization for information security professionals. With more than 140000 certified members, it empowers the professionals who touch every segment in information security. Formed in 1989, it had fulfilled the requirement for vendor-neutral, standardized, globally competent information security certification, networking, collaboration, leadership, and professional development in every aspect.

Certified Information Systems Security Professional (CISSP) is the most premier, internationally recognized, and mature cybersecurity certification. (ISC)² launched CISSP in 1994, and to the date, it provides world-class information security education and certification. Along with it comes the prestigious recognition among thousands of top-level security professionals, enterprises and vendors. The certificate provides an extensive boost to your carrier along with other countless benefits. Today (ISC)² offers a wide range of exceptional information security programs under different categories including CISSP.

CISSP is the first information security certificate meeting the ISO/IEC Standard 17024 requirements. It is globally recognized, and the exam is available in different languages other than English. As of May 31, 2019, there are 136,480 members. The certification is available in 171 countries.

CISSP is not just another certification. It is a journey through your passion for information security as a student and a professional. It is for the people who are committed and dedicated and live the information security life-style. This does not mean it is boring and tedious. In reality, it is the most challenging, enjoyable journey through cybersecurity. The CISSP certification is the insignia of your outstanding knowledge, skills, and commitment in terms of designing, implementing, developing and maintaining critical and overall security strategy in an organization.

This book was written to provide you with a good head-start by introducing the CISSP curriculum and its first chapter, “Security and Risk Management.” CISSP certification requires an in-depth understanding of

critical components in 8 major domains. Security and risk management is the largest topic taking 15% of them all.

“A Comprehensive Beginner's Guide to learn the Realms of Security and Risk Management from A-Z using CISSP principles” lines up the CISSP chapter one, “Security and Risk Management.” This is one of the most important and a theoretical chapter. It introduces why we would need an effective information security program through understanding threats, risks, and business continuity. The fundamentals covered here answers questions such as,

- What a threat and a risk is, why is there a risk?
- What are fundamental security principles?
- What risks are there? Why would we require effective security architecture?
- What are the big words such as governance, compliance, and regulations?
- What are professional ethics?
- What implementations have to be there?
- What is the importance of a security awareness program?

This book walks you through A-Z of risk and risk management while laying out a solid foundation toward the rest of the CISSP topics. It includes complete and comprehensive information and examples on each topic, subtopic, and even the smallest detail that you need not just to pass an examination but to provide you with extensive knowledge, understanding, and utilization. More about using the book is included in the following chapter.

How to Use This Book

As a CISSP student, you have to cover a lot as the subject areas are extensive. This requires your dedication, studying every area in-depth, experience from the field, and commitment. The focus of this book is the areas of security and risk management. This does not mean the content is strictly concentrating on this specific topic. It starts by introducing the field of information security and its principles then walk you through the security and risk management while covering other related areas whenever necessary.

I intend to provide a simple and concise book to help you get started your CISSP journey. I also expect you to master the topic and get organized. At the end of the studies, you will be able to get through the other topics with ease and complete the CISSP examination. The respect and the benefits await.

The book has 12 sub-topics or chapters covering the latest CISSP curriculum. There are also tips and useful information. Some graphs and images are included as with images; it is easier to understand and remember rather than chunks of text.

Although this book covers a specific topic, I always encourage you to do further research and update on the latest information. You can find complete CISSP study guides if you wish to pursue it. When you study, do not forget to keep short-notes, highlight important areas, use mind-maps, build stories, and try to organize everything so that you can memorize the content quickly and efficiently. Critical thinking is the best tool you have here. Read, understand, apply, and evaluate – these are key areas of a successful learning program. Gaining experience is also important to earn your recognition as a CISSP professional.

Wishing you good luck with your CISSP learning program!

A Brief History, Requirements, and Future Prospects

You are already aware of the foundation of (ISC)2. By 1990 the Common Body of Knowledge (CBN) was formed by the first working committee. By 1992, the first version of the CBK was finalized. The launch of CISSP credentials occurred by 1994. In 2003, the ISSEP program of the U.S. National Security Agency (NSA) started using CISSP as a base-line program. Since then, it was adopted by many programs. Today (ISC)2 offers a variety of CISSP programs including HCISSP for healthcare industry.

CISSP is not for everyone. It is specifically designed for industrial, enterprise, and government requirements. To join the CISSP rank, you must have a minimum of five-year paid work experience in two out of the eight domains. If you already earned a four-year college degree or earned (ISC)2 approved additional credentials, it is equal to one-year experience. The education credit only satisfies one-year of experience in the field.

If you do not have the necessary work experience, you can still complete the examination. However, you have to become an Associate of (ISC)2 and satisfy the experience requirements within six years. You can work full-time or part-time as long as you work 35 hours a week or 2080 hours as a part-time worker. It is also important to note the ability to work as an intern. In this case, your company must be able to produce a letter of confirmation.

For more information, visit

<https://www.isc2.org/Certifications/CISSP/experience-requirements>

Now is the million-dollar question! “Is entering the field information security can secure fun and profit?” Well, if you like good challenges, to involve in serious and critical decisions, able to think critically and outstand among others, have a passion for managing critical situations on time, and mitigating those proactively, ready to take serious responsibilities, yes! Then this is the best choice for you. However, you still have to spend time in a room, learning and experimenting. This is the life of an ICT worker/enthusiast and an information security expert.

Selecting information security as a profession is not a new trend. It is a high-risk, high-reward situation per se. But with the recent developments in the information and communication areas, Infosec professions stand among others due to the high paygrade and recognition. This does not occur in a single day but takes time and requires maturity in the areas. You can pursue the same career by following other highly recognized infosec certifications such as CEH or CISM. With time it may take you to a six-figure income if you grind it like a pro.

CISSP provides many benefits, and the following aspects are among them.

- A robust foundation.
- Professional advancements.
- Professional aid.
- Vendor-independent skills.
- Extensive knowledge.
- Outstanding paygrades.
- Respect among the communities.
- Multiple career opportunities.
- A wonderful and active community of professionals.

As a student, you must be having another question about the fields you can enter once you complete (or even during the internship) the studies. CISSP is the path to become one of the professionals below.

- Chief Information Officer.
- Head/Director of Security.
- Security Consultants.
- IT Directors and Managers.
- Security Architects.

- System/Network Engineers – Security.
- Security Auditors.

Let's now look at the salary and industry prospects.

According to a study of Global Knowledge, CISSP is one of the highest-paid IT certifications in 2019. It is at the 10th place (in the top 10).

Source: <https://www.globalknowledge.com/us-en/resources/resource-library/articles/top-paying-certifications/>

The average salary, according to the study, is \$116,900. According to the “Annual Cyber Security Ventures” report, worldwide spending on information security in 2019 is expected to grow by 8.7 percent (it does not include IoT, IIoT and Industrial Control Systems). Cybersecurity Ventures predict a growth in spending on cybersecurity products and services from 2017 to 2021. It will exceed 1 trillion according to the forecast. Meanwhile, global spending for security awareness programs is predicted to reach 10 billion by 2027.

Source: <https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf>

Therefore, when taking everything into account, Cybersecurity Ventures predicts a massive 3.5 million unfilled cybersecurity jobs by 2021.

Source: <https://www.herjavecgroup.com/2019-cybersecurity-jobs-report/>

CISSP Concentration, Education and Examination Options

CISSP concentrates on eight security domains. The syllabus may change time to time according to the needs. As per 2019, the domains and the content as a percentage are listed below.

- Security and Risk Management: 15%
- Asset Security: 10%
- Security Architecture and Engineering: 13%
- Communication and Network Security: 14%
- Identity and Access Management (IAM): 13%
- Security Assessment and Testing: 12%
- Security Operations: 13%
- Software Development Security: 10%

More on the CISSP examination

- CISSP is accredited in 114 countries, 882 locations in 8 languages.
- English CISSP examination uses CAT (Computerized Adaptive Testing) as of December 18, 2017.
- CISSP is available in French, German, Brazilian Portuguese, Spanish, Japanese, Simplified Chinese, Korean, and Visually impaired.
- Examinations in other languages are conducted as fixed-form, non-linear exams.
- The number of questions in a CAT examination can be from 100 to 150.

- In a linear examination, the number of questions is 250.
- The duration of CAT is 3 hours, and the linear examination is 6 hours.
- To pass the exam, you need to score 700 marks or above it.

What is the Best Learning Method?

Do you think about the CISSP learning paths? Yes, this is the next important question. The good news is CISSP offers many learning methods you can follow to learn at your phase. Here is a list of options.

- Class room-based.
- Online, instructor-led.
- Online self-phased.
- On-site.

For more formal learners who prefer classroom training can select the first option. As a student, you have to select a training provider in your country. It can be an (ISC)2 trainer, an (ISC)2 office or an authorized training partner. The fees may differ depending on the country you live in, and you will also receive well-structured, official courseware. The training may take three to five days, 8 hours per day. It will comprise real-world scenarios and case studies.

The online option is the most popular and, of course, cost-effective. It also saves a lot of time and effort. (ISC)2 courseware is available for 60 days. An instructor will be available to suit your schedule and you can select both weekdays and weekends as you prefer. With or without an instructor-led training, you can learn CISSP online at your phase. There are training programs and videos provided by your learning partner at a specific price. You will most probably receive access to discussion forums and emails so that you can ask questions from an instructor. Support options and learning help is available such as games, exam simulators, target questions and flashcards. If you chose (ISC)2 these are available for 120 days.

If your organization is willing to arrange on-site training, this is also an available option. This is similar to the classroom-based training. In addition (ISC)2 will provide an exam schedule assistant.

How about books? There are great books written specifically on CISSP studies as well as on examination. Even when you follow the other options, I encourage you to read whatever you can about CISSP. There are printed books, e-books, and other resources. If you are looking for official resources, please visit <https://www.isc2.org/Training/Self-Study-Resources>

Chapter One

Security and Risk Management

– An Introduction

An asteroid or a supervolcano could certainly destroy us, but we also face risks the dinosaurs never saw: An engineered virus, nuclear war, inadvertent creation of a micro black hole, or some as-yet-unknown technology could spell the end of us – Elon Musk

In information, a security risk is a **potential adverse impact** that may occur in the future. The undesired impact can affect an organization and its stakeholders raising business continuity issues. The potential can be a threat or a vulnerability associated with operations, the systems which are responsible for the operations and the environment in which those systems operate.

We live in an era of information and communication technology at the peak of its utilization. Many small to large scale operations involve implementation, control, monitoring, and maintenance through at least one piece of information technology or an electronic device. For instance, if we consider a healthcare operation or a banking operation, it heavily depends on information and communication technologies. It can be a customized or in-house implementation of software, servers and networking, wireless technologies, internet and other electronic devices which depend on such infrastructures. Or else it can be a small restaurant using a few point-of-sales systems and connected to the internet to serve online requests such as Uber. There are many examples but the important point here is the utilization of information, transfer of information through different devices, systems and networks, relying on underlying systems which these organizations have neither visibility nor control, and the potentials it has to disclose important information to entities which are willing to compromise these systems and abuse information for various intentions.

Risk has potential, and it also has a probability. Two main factors are form a risk. Those are threat and vulnerabilities.

- **Threat:** A threat is a human-made or a naturally occurring event that has the potential to cause an undesirable impact on an asset, process, or organization. We can call it the frequency of potentially undesirable events. The impact can be large or small and the complexity level can be different.
Examples: Natural disasters, man-made threats such as explosions, a fire (man-made or wildfire), malware, DDoS attacks, phishing, MITM (Man in the middle attacks).
- **Vulnerability:** A vulnerability is an opportunity or a likelihood of success of a threat. It is an undiscovered or unresolved weakness in safeguarding a process or an asset. When there is a vulnerability, there is a higher probability for a threat to **exploit it** . This may cause intensive damage financially or by other means and it may frequently occur in iterations.
Example: If you heard about remote code execution incidents, unpatched remote code execution in a system (i.e., in an operating system) could bring catastrophic damages to an entire operation.

Measuring Vulnerabilities

You can definitely disclose vulnerabilities if you perform routine checks or have deep knowledge in certain systems, processes, or activities. For instance, if you are closely monitoring a shift change of security personal, you may find out a new vulnerability. You may be able to exploit this vulnerability if you implement a strategy that works. This may require months of surveillance, planning and testing. However, this is how attackers monitor, identify, design, implement, test and release an exploit for them to use or for others. The probability of success is difficult to measure but you can always measure vulnerability prevalence. Prevalence is the

Threat Actors, Threats, and Threat Rates

We already know what a threat is now. In simple terms, a threat is anything that can exploit a vulnerability. A threat doesn't propagate or execute by itself. It requires a threat actor. An actor is a person or an entity responsible for an incident resulting in an impact now or the future. For instance, a Black Hat hacker who has the potential to successfully exploits a vulnerability causing an impact is a threat actor or a threat agent.

Note: Some define a threat agent as the path taken by a threat actor rather than the actor himself/herself.

There are many human threat-actor groups, but we can categorize them into a few groups. Those are,

- Cyber Criminals: The main motive of a cybercrime is money. These groups or individuals are well equipped with sophisticated tools and knowledge and well-funded.
- Hacktivists: The main motive of a hacktivist is not known. It can be a financial reason or a personal. Such individuals are difficult to disclose, predict, and are the main source of cyber vandalism.
- Have you ever heard about cyber espionage? The main goal of cyber espionage is to steal information for competitive advantage. The act involves stealing information without knowing and authorization from individuals, competitors, rivals, enemies, and governments for personal, political or economic advantages and in some cases military advantages. This third category is about the state-sponsored attackers.
- Local or Insider Threats: In an organization or a similar entity, there is also the human factor and human errors. For instance, sensitive information may be disclosed due to the work of an uneducated employee or someone who has an unresolved issue with the organization.

Threats can be calculated based on the frequency, known as the threat rate. It is calculated based on historical evidence. For instance, we can calculate the threat rate of an earthquake of a certain country, state, or province, by the frequency and the magnitude.

A threat rate can be categorized into two. Those are,

- Local Threat Rate.
- Global Threat Rate.

An organization's local status, geographic location, political stance, competitiveness, and economic perspectives can expose it to local threats

and more or less to global threats. Even though it is difficult to determine what comes first but it is always the best to have an estimation of the possibilities.

What is a Zero-day Vulnerability or an Exploit?

Now you are familiar with the terms except for the zero-day. A zero-day vulnerability is an undisclosed vulnerability that exists in an entity that can be exploited. Once exploited, it becomes a zero-day exploit and a successful one. It is not easy to implement detective and preventive measures to fully resolve the potentials, but it is always possible to proactively mitigate a possibility or a risk.

Risk can be defined as an equation.

$$\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Cost}$$

The Cost

The cost can be defined in three ways according to the impact and recovery. Basically, it is the total cost of the impact of a threat experienced by the vulnerable target.

- Hard Costs: This includes the repair/replacement cost of actual damaged assets. Work hours of IT staff and other quantifiable resources are also included.
- Soft Costs: Includes end-user productivity, reputation, public relations, etc.
- Semi-hard Costs: The loss incurred during the downtime.

Now, if you look at the equation again, if you mitigate or eliminate threats, vulnerabilities and costs, the risk is zero or minimal. This is often the goal of any organization but the success depends on the efficiency and effectiveness of the strategy. As you may have already learned or experienced about the nature of information security, it is always possible to mitigate threats but not fully eliminate even for a longer period.

In reality, we cannot achieve a 100% secure environment; it is a mere theory. We cannot control the evolution of information technology, the tools

and the techniques, and the facts like the environmental changes. Do you believe you can predict or control the full impact of an earthquake and save your data-center headquarters? Even if we mitigate such risks, there will always be insider threats, like mistakes the humans make. Therefore, building a formidable strategy and tactics is the best defense against threats, vulnerabilities and exploits. As a start, it is the time to dig deeper into the risk and risk management.

At present, information technology is utilized in almost every component in an organizational environment. Therefore, there can be more threats than we are aware at component level as well as the whole. The utilization can range from a simple alarm to complex machinery in a nuclear power plant, or high-security government complex, or to manage a massive physics experiments in a laboratory-like NASA or CERN. In any of these utilizations, there are many risks involved, inherently, and externally.

Risk management is a sensitive and complex process that involves the process of identifying, assessing, and mitigating risks to ensure an organization meets its safety and security goals. The end result should be eliminating, mitigating, or minimizing to an acceptable level. This process involves identifying threats and vulnerabilities, risk assessment, risk response, setting up countermeasures and controls, asset valuation, monitoring and reporting. In the end, after successful evaluations, it requires continuous improvement. We will be looking into the entire process and current frameworks with which you can start building your risk management strategy.

Now it's the time to utilize the knowledge you obtained so far to identify the vulnerabilities, threats/threat agents, and risks. Fill this table correctly using the following lines as appropriate. Each line consists of a vulnerability, threat agent, and risk but in the wrong order.

Vulnerability	Threat Agent	Risk

- Fire, Damage to the building and assets, absence of fire sensors, and alarms.
- Malware, Absence of malware protection, Infection.
- DDoS and brute-forcing, hackers, lack of safeguards, and validation.
- Social Engineering attacks and exposure of sensitive information, using insecure protocols, hackers.

Chapter Two

Understand and Apply Concepts of Confidentiality, Integrity, and Availability

Before moving into the risk and risk management, you should have a proper understanding of the ABCs of security in general as well as at the organizational and governmental levels. It is imperative that you thoroughly understand security concepts, governance, compliance, legal and regulatory aspects, implementation of policies, and business continuity requirements. In this chapter, we will look into the first section, the concepts of CIA.

In this chapter, you will learn:

- Pillars of information security.
- Approaches to confidentiality, integrity, and availability.
- Cryptography – Basics.
- Cryptographic services (confidentiality, integrity, authentication, authorization, and non-repudiation).

No, this isn't a study of the Central Intelligence Agency. The short term for Confidentiality, Integrity, and Availability is CIA (some use the term AIC to avoid confusion). CIA triad is the classic venerable model of information security. The establishment of the three fundamental and the three most critical pillars ensure and helps develop information security policies and countermeasures. The mandate of every information security team is to protect the CIA of the assets (systems and information) that the company holds.

Confidentiality

Some used to refer the confidentiality itself (or with the combination of privacy) as information security. Data or information has different values, use cases, and not everyone should know everything. Information can be a

tool as well as a weapon. It can be, stolen, used against an entity, alter the integrity, alter the meaning, erased, and used to construct strategies to destroy a business or an entity. That is when fallen to the wrong hands. Confidentiality ensures the level of disclosure (not the integrity) and safeguards the information against unauthorized entities. In reality, you cannot hide everything and assume it is secure. The information must be available but only the relevant parties must be granted access.

In the previous paragraph, you learned that information has different values to different people and functions. Therefore, the sensitivity of such information also varies. This raises questions about how information should be categorized. To answer this question, confidentiality comes with the idea known as information classification. Information classification is a broad topic. It is easier to start from how data can be classified and what the simplest criterion is. The impact level of a breach is a widely used classifier. Although this is the foundation, with any classifier, three key factors govern the classification.

- What value the information holds?
- Who should have access or clearance to which set (who needs it)?
- What is the impact if it is disclosed? The value of the information defines the risk factors.

Based on the answers to these questions, it is possible to draft a confidentiality classification table and assign values to each set. Then it is possible to calculate the final value and determine the clearance level, groups, safeguards, countermeasures, and regulations.

With this, another set of questions arises. What is the next step upon a data breach or disclosure? What are the regulations and penalties if a person or a group is involved? These questions will be answered in the next chapters.

When implementing the classification and clearance levels, the best practice is to start with the need to know and least privilege principles. This means the entity or the person who requires access must be limited to the information he/she requires to carry on the tasks or operations. There is a difference between the need to know and the least privileged.

- Need to Know: For instance, in an HR department, a worker requires access to profiles of the employees to perform certain tasks. In technical terms, the person needs to access the user-profile section in the HR database. Does this mean he/she requires to access all the profiles? Not necessarily. This ensures confidentiality.
- Least Privilege: Now the HR worker has the necessary clearance. Then again, must he be allowed to perform any task on these profiles or data? Definitely not! This is when an organization needs to employ the least privilege principle. The user must not be able to perform any adverse actions.

When someone is provided with privilege, this person can alter the data, meaning and therefore, the value and the sensitivity. The information or data must be original and should remain free of unnecessary alterations. In the next section, let's look into the next pillar, the integrity.

Before moving into that section, if we consider safeguarding confidentiality, there are many strategies, technologies, and techniques to ensure it. Mainly the implementation of secure physical environments, authentication systems (humans, devices and software) and protocols such as passwords, locking mechanisms, multi-factor authentication an organization can defend against and combat the threats. Upon a successful implementation of a well-architected strategy, it is not impossible to maintain prevention and mitigation.

The important thing to remember is the nature of the information or data. Data or information has several stages – it can be at rest, in motion, or use. In each case, the necessary confidentiality is required and it must be implemented. If you are familiar with encryption technologies, hashing, public key infrastructures (PKI), certificates, you may have an idea of safeguarding the data in motion and even in use. Data encryption is one of the key techniques used to ensure confidentiality.

What are the Threats to Confidentiality?

The main threat to confidentiality is the disclosure. Below are some of the instances when confidentiality is compromised.

- Theft: A laptop containing confidential or sensitive information is stolen.
- Malware: A host is infected by spyware.
- Configuration Fault: Sensitive data in a database is posted to a website or leaked.
- Human Error: A password is written on a desk.

Integrity

The next pillar of this model is the integrity. Do not confuse with data security and integrity. Integrity is the assurance of accuracy, trustworthiness, and consistency of information during its existence as well as in each stage of data. The accuracy and trustworthiness ensure the data or information is unmodified by unauthorized means. This does not however, mean that an authorized person cannot alter data for malicious purposes. It will be addressed by a different layer of security layer in this chapter.

In technical terms, keeping integrity is the next difficult task. To ensure integrity, both access controls, permission, and authorization techniques can be implemented - mainly the permissions (e.g., file permissions) and user access control. Most of the hardware and software systems use version control and it contributes to maintaining integrity. These measures prevent human errors and malicious intent.

Apart from that, incidents like data corruption (during transmissions), storage corruption, failures, server crashes, and other physical damages cause integrity violations. If a web application is unable to properly validate the input, as well as the data before entering to the database, it can lead to data corruption and eventually loss of integrity. It is also apparent the requirement of proper backups to recover (to ensure business continuity). However, another challenge arises with duplicate data as it may contribute to integrity issues. Data deduplication is utilized to resolve this problem.

To track the sources of integrity violations, it is important to audit the actions or activities in object level, system-level as well as user level. Nowadays, there are strong encryption techniques but you cannot ensure integrity using encryption directly. For instance, you can ensure the

integrity of a file transferred through the internet. The technique used here is known as the message digest and it involves cryptography.

Using Encryption – Cryptography Basics

Encryption is the technique used to hide the cognitive meaning of information. For instance, when a piece of data is encrypted, it is converted into a certain secret and meaningless code. The science behind this is known as cryptography. Cryptography is the science of encryption and decryption. This is a broad topic and requires certain skills in mathematics. Since it is important at a conceptual level, we are going to look into it briefly.

Encryption has the following features or services.

- Confidentiality: Ensures the secrecy.
- Authentication: Verifies the integrity as well as the source of information.
- Authorization: Authorization is the permission required to perform a task or an activity.
- Integrity: Ensures the accuracy and trustworthiness.
- Non-repudiation: This prevents the sender from rejecting or denying the *sent* action.

Data encryption can be performed on a piece of data, information, a database, a disk, or even between networks. It mainly ensures confidentiality. It can also be used to ensure integrity in a later stage. Let's look at an example.

John wishes to send a confidential file over a network to his manager Jeff. How does he ensure the confidentiality of the file?

Confidentiality

To prevent information disclosure to unauthorized parties, confidentiality is required. Cryptography is used to encrypt information to make it incomprehensible to everyone except for those who are authorized.

In the previous scenario, the file is in plaintext. What we need here is a secret code that Jeff and only Jeff can uncover. With the help of encryption, this is achieved, and the end result is known as a cyphertext. The encryption process itself involves a mathematical calculation with the use of a specific algorithm. This algorithm is known as the encryption algorithm or cipher. However, using the message and an algorithm does not guarantee uniqueness of the ciphertext. To maintain the uniqueness of the output, a variable called the **key** is used.

The ciphers fall mainly into two categories.

- **Symmetric Cipher:** In symmetric cryptography, a shared secret is used to encrypt as well as decrypt data. When someone is using a specific, unique key, the receiving party must also have it to decrypt the data. The challenge here is sharing the secret key without getting disclosed. The Advanced Encryption Standard or AES is the most widely used symmetric block cipher. In contrast to asymmetric ciphers, symmetric ciphers have less overhead and faster.
- **Asymmetric Cipher:** This is also known as public-key encryption. There are two keys involved. One is unique and known only to the owner, called the private key, and the other is a public key that is shared among the others. Prime numbers are used to generate the private and shared key. For instance, person A is using public-key encryption. He has his private key X and public key Y. If someone wishes to send 'A' a confidential message, he uses Y and encrypts the data. Only the one with the related private key can decrypt it. The X and Y keys are logically linked but you cannot reverse engineer and obtain a key. At present, the RSA (Rivest-Shamir-Adleman) is the most widely used. In many cases, this is used to exchange secret keys securely.

You must also remember that the strength of the encryption depends on the size of the key as well as the strength of the algorithm.

Authentication

Cryptography provides two types of authentication.

1. Integrity Authentication: To assure data integrity.

2. Source Authentication: This can be used to verify the identity of who/what created the data/information.

Authorization

Authorization is often enforced in an organization to perform a security function or an activity. Therefore, cryptographic functions are often integrated with authorization. Authorization is granted after successful processing of a source authentication service.

Integrity

Data integrity is the assurance that data has not been modified in an unauthorized manner during creation, transfer, and at rest.

To achieve integrity, the technique used is known as a message digest and digital signature. A message digest is a fixed-length numerical representation of the content, generated by a hash function. A hash function is an integral part of modern cryptography, taking an arbitrary numerical input and converts it into another compressed numerical value of a fixed length. Now, if two things can produce the same hash, then we are confident that the prices of content identical.

A hash function is one-way, meaning the hash is not reversible. Unlike encryption, hashes cannot be decrypted to obtain the key. Furthermore, it must be computationally impossible to find two messages that hash to the same digest.

At first, we obtain the hash from the message we need to send to someone. We can share the hash with the message so that the other party can generate the same hash. When both matches, with confidence, we can call, there are no integrity issues with the message. A message-digest generated using a symmetric key is known as a Message Authentication Code (MAC). As you now understand, it assures the integrity as well as message authentication.

Non-Repudiation

The last section of the encryption focuses on non-repudiation. In technical terms, it is the process of binding of a subject of a certificate through the

use of a digital signature key and certificate to a public key. This also means that the signature created by this specific key has the support of both the source authentication and integrity of a digital signature. It is important to remember that there are many aspects to be considered in making a decision

This ensures that the user cannot deny sending a message. It is important to verify the origin and the person who sends a message, file, or something else. In legal matters, it is required to prove who the owner and sender is. A digital signature serves this purpose.

To create a digital signature, we use the message digest that we created previously. It is the hash, in other words. To create a digital signature, the sender uses his private key (only known to him) to encrypt the hash. Then the message is sent to the other party. The receiving party obtains the public key of the sender, decrypts the message. Only the public key of the related private key can decrypt it. Therefore, non-repudiation is met. Once we obtain the hash, we can generate a hash from the message and compare it against the sender's hash. If two matches we can confidently say the integrity and non-repudiation goals are successfully met.

Availability

The final critical pillar in the CIA triad is the availability. What is availability? Now the information has its classifications, confidentiality, and integrity. But what if the information is not available for access when it is required? The next biggest threat is the consistent availability of information to the required parties. For instance, if a database holds certain business information gets unavailable (here unavailable also means a long delay or partial availability) during a decision-making process that will affect the decision, the business development as well as the continuity.

There are multiple threats to availability. It can be a natural disaster, network breakdown, congestion, an intrusion (exploitation), a malicious intent to destroy the reputation, or even a human error causing an adverse impact.

To mitigate the risks of losing reputation and business opportunities, many organizations develop strategies to establish routing checks, maintenance, fault-tolerant placements, redundancy (includes branch networks), load

balancing and other disaster recovery measures. It can be a security breach or a natural disaster, and there may be downtimes. The strategy should be able to withstand the effects while minimizing the downtime. Many trending technologies offer fail-over clustering, load-balancing, redundancy, monitoring and reporting to prevent, defend, mitigate and recover from such disasters.

Chapter Three

Evaluate and Apply Security Governance Principles

In this chapter, we are looking into the business perspectives in terms of security. Security isn't something standing outside of the gate and safeguard the entrances. It should be determined by analyzing the nature of the business, current, and future risks. The business strategy and functions must align with information security to gain effective and collaborative results. It also reduces the complexities and enhances the transparency. To get a substantial idea, the chapter covers various organizational processes, roles and responsibilities, methodologies and frameworks available to design, develop and enhance security controls.

In this chapter, you will learn:

- Business strategies, goals, missions, and objectives and the role of security and alignment.
- Organizational processes such as acquisitions.
- Organizational roles.
- Responsibilities.
- Security control frameworks.
- Due care, due diligence.

What is a principle? A principle is not a law or a rule. It is different from a protocol or practice. It is more of a behavior toward or a belief on a fundamental truth. Therefore, it isn't a specific standard. With the evolution of the corporate world, good corporate principles have evolved over the decades. Through the ups and downs, the survival required fluidity. Fluidity is required to adapt, survive as well as to evolve. Hence, corporate governance must also remain flexible to adapt to the ever-changing needs.

The corporate governance, therefore constructed by incorporating such principles.

In a corporate environment, there are often well-defined and exercised governance principles. Why would an organization require good governance principles? Any organization requires to formulate a business strategy and policies to establish a business framework. Within the framework, a business operation can be executed, controlled with precision and it can be standardized. To formulate policies, policymakers to evaluate as well as enhance the institutional, regulatory and legal framework for corporate governance. It should carry a prospect to support economic efficiency, financial stability and sustainability.

Let's look at some good corporate governance principles universally.

- Efficiency and effectiveness.
- Sound decision-making.
- Financial Transparency and Disclosure.
- Adhere to Law, Regulations, and Compliances.
- Integrity and Ethical Conduct.
- Rights and Equity.
- Openness to Change.
- Continuity and Sustainability – this includes risk management.
- Financial Efficiency.
- Corporate Responsibilities and Accountability.
- Cultural Diversity.

An organization comprises a hierarchy of management and control. The business roundtable supports the following core principles.

- CEO at the top is responsible for establishing a sustainable, long-term corporate strategy. With the senior manages the CEO plans,

allocate resources while assessing the long- and short-term growth potentials. Another critical act is assessing and mitigating risks.

- Under the board's oversight, the management develops and implements the strategy to meet the long-term and sustainable business goals.
- Management produces fair and accurate financial statements under the supervision of the board and the audit committee. This reveals the actual financial state and necessary and timely disclosures so that investors get the ability to analyze financial prospects, business soundness, and risk.
- The audit committee, with the involvement of other parties' oversees the annual audit process, internal controls over financial reporting. It also oversees the compliance and risk management.
- The corporate governance committee plays a key role in corporate governance as well as shaping the board with diverse figures whose composition is required in light of the needs of the company.
- The board with the compensation committee develops a philosophy with which the company can reward the hierarchy for achieving business goals, evaluate the performance, and further develop meaningful goals and keep the active contribution physically and psychologically.
- Long-term value creation is critical for a business. The board and the appropriate parties must engage with long-term shareholders and resolve the existing issues. For accountability, shareholders who engage in corporate decision making and strategic changes are encouraged to disclose appropriate identifying information for the long-term interests of the company.

This is an overview of the corporate governance principles. Information is a valuable asset. Information and communication technology plays a critical role in assisting business functions. Therefore, there must be a strategy to incorporate information and communication technology assets and resources while maintaining security, control, and governance. This is where the need arises for security governance principles. This is initiated at

the strategic planning phase. Any corporation during the start and continuation concentrates on business goals. A mission of any business is to fulfill the objectives and achieve the goals. During this process, there will be requirements to safeguard the information and encounter risks. Therefore, it is important to clearly define the security strategy, objectives, and policies ensuring the business continuity through preventive, mitigative, reactive and corrective measures. Both risk management and disaster recovery come as the top requirements. With a properly aligned business and information security strategies and through continuous monitoring, reviews and updates, it is possible to bring the mission into a reality.

Mission, Goals, and Objectives

The term mission became popular after the mission to the moon. This event was a good example of corporate success through a collaborative effort. Every organization has these vision and mission statements and are published on the web sites they own and manage. These statements are not fancy displays. The truth is, the actual operation and the corporate goals are represented and expressed through the two statements. The mission statement expresses why an organization exists and its overall goal.

An objective is one step of a ladder toward a goal. At the end of the accomplishment of all the objectives, the final goal is reached. Accomplishing the mission is the main objective. It is divided into smaller objectives. Why would a security engineer need to understand these? You have already learned that information security must be aligned with the business strategy and functions. The strategies exist to accomplish this mission by reaching the goals through objectives. Therefore, information security auxiliaries the process by providing assurance in terms of safety and security. Risk and disasters are inevitable. It is the task of a streamlined and proven to work information security and disaster recovery plan to continue the business process while minimizing the business continuity issues. There is also the need to emphasize the flexibility, scalability, and adaptiveness of the security framework so that it can be aligned properly (while achieving a flexible change management approach).

Organizational Processes (acquisitions, divestitures, governance committees)

As previously mentioned, the establishment of information security governance must emerge from the top of the corporate hierarchy – the CEO, the board of directors – as a well understood, defined, and funded long-term goal. Once initiated, the security governance process and policies will aid the decision-making process and policy establishment of the executive management. It is a top-down process. In addition, the strategy must sound compliant with the current laws, regulations, and other requirements.

In the next stage, the executive manages to have the responsibility of implementing the strategy. They must have sound awareness, and transparency and delegated control over security policies and the overall operation. The formal way of doing this is by arranging AdHoc and weekly/monthly meetings. During the meetings, the top persons and teams must meet and review the existing strategy, the recorded incidents, request new changes, approve the changes and push them to the execution phase. This is the most efficient method as it assures the continuous development of security activities and effectively mitigates the risks, and in turn, the investment in security makes a positive contribution and worth the cost.

Acquisition and Divestitures

During the corporate lifecycle, many organizations acquire other organizations to maintain agility, competency and concentration. At times, an organization may acquire all or a single business unit that belonged to another organization. In most fields, especially the technology-oriented business entities, acquire innovations and emerging technologies. Such acquisitions, mergers and divestitures raise complex security questions and concerns as the outside organization or business unit may have followed a different strategy under different corporate security governance or none at all.

Acquiring existing organizations raise multiple security concerns.

- They most probably have utilizing a different strategy under a different set of people and cultures.

- Their policies, procedures, and processes may differ significantly.
- They may bring risks and loopholes.
- They may or may not use a robust and trustworthy framework and principles.
- There may be people and devices with undesired states.
- The devices may bring open threats and vulnerabilities.

As you see, there is a high risk associated with the process and the impact can cause the organization to walk into serious issues. There can be many operations and practices to synchronize with the existing organization and that includes but not limited to,

- Risk management strategy and architecture.
- Operations management.
- Incident management.
- Security monitoring, management, and auditing.
- Third-party involvements.
- Other stakeholders and impact.

The existing organizational security and risk management framework must be able to open the door for the new entity. The flexibility governs the adaptability here.

When an organization splits into two or multiple units, the security strategy may move along with the units. Necessary changes and/or reforms may be required to make the mergers or acquisitions cope with the existing architecture. For instance, there may be new laws or regulations to adapt to. Therefore, to move forward as a single organization, the alignment must be completed at a satisfactory level.

Organizational Roles and Responsibilities

In a previous chapter, you were introduced to the corporate hierarchy and how the decision-making process flows. The roles represent the overseer of a specific business function or a set of function. With it comes the need for responsibility and accountability. When designing a security policy along with-it roles and responsibilities must be clearly defined such that the responsibilities can be delegated and the activities can be enforced and controlled as expected.

If you go back and take a look at the governance principles section, executive level management has the top priority to move the information security program forward. They must demonstrate a strong allegiance with the current security program. The executives are responsible and held accountable for multiple roles and even wear multiple hats. The CEO and the boards form the security program while executives mandate the implementation program. They should lead the security program by utilizing leadership qualities, skills, and expertise. Most importantly, they need to understand the requirement for awareness education, recognition and rewarding. To address policy violations, appropriate measures must be formed, documented, informed and monitored.

On the other hand, an employee should honor the corporate governance framework and security program. To expect results and maintain the standard, there must be training programs such as awareness training. These programs cover the following areas in general.

- Awareness of the requirement of information security and business continuity (including risk management) programs.
- Awareness training for specific business units about corporate governance structure and their responsibility and accountability – information specific.
- Information security awareness training on policies, procedures, baselines, laws, regulations, compliance requirements, and legislations.
- Application training – teaches how to utilize best practices.
- Evaluations and reviews.

- Based on the performance results, training should be provided to executives in case of lack of expertise or proficiency.
- Such programs should cover stakeholders as well as customers and third-parties.

The next chapter is about security control frameworks. As you may have already figured, this process is not straight forward. There are difficulties in determining and covering all the aspects without proper structure or guidelines. Therefore, the requirement urged the emergence of security control frameworks and standards. We are going to look into the prominent frameworks and their characteristics.

- Control Objectives for Information Technology (COBIT).
- ISO 27000.
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE).
- National Institute of Standards and Technology (NIST) Cyber Security framework.

Note: Some of these are country-specific frameworks.

Let's have a brief look at these frameworks.

COBIT

COBIT (version 5) is a leading framework for governance and management of enterprise IT. It is a leading-edge growth-roadmap and business optimization, providing a breadth of tools, guidance, and resources; COBIT leverages proven practice and global thought leadership. It provides groundbreaking tools to fuel business success and inspire IT innovations.

COBIT helps organizations to align IT strategy with business goals while addressing the business challenges in the following areas.

- Audit assurance.
- Risk management.

- Information security.
- Regulatory and Compliance.
- IT governance.

COBIT is at its 5th version released on 2012. You can learn more by following the link below.

COBIT online: <https://cobitonline.isaca.org/>

COBIT is based on the following five principles. These are the essentials for governance of information and security and effective management.

1. Meeting stakeholder needs.
2. Covering enterprise end-to-end.
3. Applying a single integrity framework.
4. Enabling a holistic approach.
5. Separating governance from management.

In the five principles, there is the principle of enabling a holistic approach. The holistic approach is required to build a *holistic framework* for governance as well as management of IT. This framework is built upon seven *enablers* . Those are,

1. Principles, policies, and frameworks.
2. Processes.
3. Organizational structure.
4. Culture, ethics, and behavior.
5. Information.
6. Service, infrastructure and applications.
7. People, skills, and competencies.

The enablers aid in aligning the business objectives with the investment on IT.

ISO/IEC 27000

ISO 27000 is a series of standards tiered to standardize information security practices. The standards were developed and published by the International Organization for Standards (ISO) and the International Electrotechnical Commission (IEC). The family of standards has an extensive broad spectrum and is applicable to all sizes and sectors of an organization. ISO, along with other bodies, continuously develop the standards, and there will be new standards as well as the removal of obsolete standards. Let's look at the existing standards.

- ISO/IEC 27000: Is about Information Security Management Systems (ISMS)
- ISO/IEC 27001: Is about Information Security Management Systems requirements (3-part series)
- ISO/IEC 27002: Code of practice for information security controls (3-part series)
- ISO/IEC 27003: Information security management system implementation guidance
- ISO/IEC 27004: Information security management – Monitoring, measurement, analysis, and evaluation
- ISO/IEC 27005: Is about Information security - Risk management
- ISO/IEC 27006: Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007: Guidelines for information security management systems auditing
- ISO/IEC 27008: Guidelines for auditors on information security controls

- ISO/IEC 27009: Sector-specific application of ISO/IEC 27001 (requirements)
- ISO/IEC 27010: ISM for inter-sector and inter-organizational communication
- ISO/IEC 27011: ISM guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013: Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27014: Information Security Governance
- ISO/IEC 27016: ISM – Organizational economics
- ISO/IEC 27017: Code of practice for information security controls - based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27023: Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002
- ISO/IEC 27031: Guidelines for ICT readiness for business continuity
- ISO/IEC 27032: Guidelines for cybersecurity
- ISO/IEC 27033: Network security (6-part series)
- ISO/IEC 27034: Application security (8-part series)
- ISO/IEC 27035: Information security incident management (2-part series)
- ISO/IEC 27036: Information security for supplier relationships (4-part series)
- ISO/IEC 27037: Guidelines for identification, collection, acquisition, and preservation of digital evidence

- ISO/IEC 27038: Specification for digital redaction
- ISO/IEC 27039: Selection, deployment, and operations of intrusion detection systems (IDPS)
- ISO/IEC 27040: Storage security
- ISO/IEC 27041: Guidance on assuring suitability and adequacy of incident investigative methods
- ISO/IEC 27042: Guidelines for the analysis and interpretation of digital evidence
- ISO/IEC 27043: Incident investigation principles and processes
- ISO/IEC 27050: Electronic discovery (3-part series)

In addition to these standards and supplements 27103 and 27701 standards there for Cybersecurity and ISO and IEC standards, guidelines for cyber insurance, electronic discovery and privacy management enhancements

ISO/IEC 27014:2013 is specifically about the governance of information security and guides concepts and principles. Organizations can use the guidelines to:

- Evaluate.
- Direct,
- Monitor,
- Communicate

the information security content within an organization. This assures the alignment of information security with organization strategy, goals, objectives, accountability, and value delivery. In turn, it supports,

- Visibility.
- Agility.
- Efficiency.
- Effectiveness.

- Compliance.

OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation is a risk management framework developed by Carnegie Mellon University, SEI (Software Engineering Institute) on behalf of the Department of Defense. This risk assessment framework is flexible and self-directed. The framework suites are small to large business operations. The fundamental difference between this and other frameworks is that OCTAVE is not driven by technology. Instead, it is driven by operational risk and security practices.

This framework can be used to,

- Develop qualitative risk evaluation criteria. This is useful to get an image of operational risk tolerance.
- Identify mission-critical assets.
- Identify threats and vulnerabilities to the assets.
- Determine and evaluate the impacts if such threats are realized.
- Risk mitigation through continuous development.

There are three phases of OCTAVE, and these are,

1. Build asset-based threat profiles.
2. Identify infrastructure vulnerabilities.
3. Develop strategy and plans.

Current OCTAVE version is 2.0.

NIST Framework

President of the United States issues an executive order 13636, Improving Critical Infrastructure Cyber Security in February 2013. This is after realizing the fact that the reliable function of the critical infrastructure is a critical part of the national and economic security. National Institute of

Standards and Technology (NIST) received the order, and they started creating a voluntary framework by working with stakeholders. The framework is based on existing standards, guidelines and practices. The goal is to reduce the cybersecurity risks on information infrastructure and as an aid for owners and operators. Later, The Cybersecurity Enhancement Act of 2014 made reinforcements to NIST's role. This was a collaborative effort between the government and industry.

NIST framework has the following characteristics.

- Prioritized.
- Flexible.
- Repeatable.
- Cost-effective.

You can learn more about the NIST framework by following the link below.

NIST framework for new users: <https://www.nist.gov/cyberframework/new-framework>

Another advantage of this framework is fostering cybersecurity and risk information communication between internal and external stakeholders of organizations.

The framework has three primary components. Those are,

- “Core: Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls.”
- “Profiles: Alignment of an organization's requirements and objectives, risk appetite, and resources using the desired outcomes of the Framework Core.”
- “Implementation Tiers: A qualitative measure of organizational cybersecurity risk management practices.”

The followings are the key attributes of the NIST framework.

- Identity.

- Protect.
- Detect.
- Respond.
- Recover.

The current NIST framework version is 1.1.

NIST also works on the FISMA implementation project. You can obtain more information on the related risk management framework by following the link below.

FISMA – RMF Overview: <https://csrc.nist.gov/projects/risk-management/rmf-overview>

That was an overview of the frameworks. We can categorize these *frameworks* into four *types* . They are,

- Preventive.
- Deterrent.
- Detective.
- Corrective.

Now let's look at the characteristics of these *types* .

Preventive Frameworks

Prevention is always better than detection if successful. It is also efficient and hassle-free — such frameworks aid in laying out the first line of defense. However, there is still a requirement for strategic and tactical use, and it may require adequate training and expertise.

The followings are some examples.

- Bio-Metrics.
- Data Classification.
- Encryption.

- Firewall.
- Intrusion Prevention System (IPS).
- Security cameras.
- Security personal.
- Security policies.
- Smart cards.
- Strong authentication.

Deterrent Frameworks

These frameworks can be considered as the second line of defense. The expectation is to discourage malicious attempts with appropriate countermeasures. There would be a consequence if an attempt was made.

- Security cameras.
- Dogs.
- Guards.
- Fences.
- Security personal.
- Warning signs.

Detective Frameworks

This is the next strategic framework. If the threat is beyond the previous implementation of the frameworks, this is where it requires detection and neutralization. This, however, comes with a price. To detect something, it must enter and make some impact. Furthermore, sometimes it may become difficult to detect real-time threats. Hence, the frameworks may work as surveillance units and activities.

- Auditing.
- CCTV.

- Intrusion Detection System (IDS).
- Motion detectors.
- Fire detectors.
- Environment sensors.
- Security personal at specific areas or levels.
- Certain antivirus software.

Corrective Controls

The need of corrective controls is understandable. Risk mitigation, detection, and other activities cannot always defend certain disasters. When a disaster occurs digitally or physically, there must be a way to,

- Detect and determine the impact.
- Steps required to identify and isolate the incident.
- Steps needed on how to stop the expansion and/or recover from the damage.
- To operate and continue with acceptable downtime or availability.
- To restore the operation back to the original state.

The following corrective measures will be commonly utilized within this framework.

- Antivirus.
- Repairing tools.
- Backup and recovery.
- Updates and patch management.

In addition, there are two other frameworks. One is the recovery controls or measures. Such measures are deployed to recover as well as prevent related incidents. These include,

- Backups.
- Fault-tolerant controls.
- High-availability (e.g., clustering).
- Redundancy (e.g., additional measures that are placed to take over, such as hot-swap, hot standby and other techniques).

The other is compensative (or alternative) controls. This is applied when the application is either too difficult or impractical. Compensative controls have four types in general.

- Physical.
- Administrative.
- Logical.
- Directive.

PCI DSS framework provides options to deploy compensative controls. Some examples of this type of control are segregation of duties, logging, and encryption.

Due Care/Due Diligence

Due diligence is the understanding of governance principles and risks an organization has to face during the lifecycle. This process includes the following phases.

- Information collection.
- Risk assessment.
- Establishing well-written policies and procedures.
- Communicating the establishments to the organization.

On the other hand, due care is the organizational responsibilities. In other words, your responsibilities as a stakeholder of the organization and legal responsibilities. This helps to establish appropriate controls and follow the policies, thus taking reasonable actions and better decision making. It's

important to remember that the two terms are not interchangeable. However, it is worth noting that people tend to misunderstand these two concepts.

In simple terms, due care is in a given situation, doing the *right thing* as a person. For instance, you rent a car, and before you drive, you spot a damaged parking light. As a reasonable person, you should report it before you take the car. Otherwise, you will have to take the penalty. That is due care.

The action created out of due care is called due diligence. Technically speaking, it is the management of due care. Let's look at the first example. You informed the car rental company an hour ago but the repairing is not underway. Then you have to follow up and find out why.

Let's take a scenario in which you are a security consultant of an organization. During the analysis, you find certain vulnerabilities due to patch management issues. At the end of the data collection and analysis, you document the findings. You find more than half of the machines have the vulnerability unpatched. You request the internal IT team to install and configure the patch updates. This is due to care. Next week, you arrive and perform another test and a follow up to enhance the security. The analysis will find no existing vulnerabilities. This is due diligence.

Chapter Four

Determining Compliance Requirements

In this chapter, we will be looking into the legal frameworks, how and why compliance is critical to information security. To stay in compliance with the regional, national, state, and other legislation, regulations, and standards always provide efficient and secure governance and control. Other than these requirements, an outstanding and critical requirement is the privacy and the protection of privacy. With the digital information networks, social media, digitized healthcare and other services provide millions of opportunities for external parties to steal and abuse private information of not only the organizations but of the individuals. Chapter four covers these topics comprehensively and gives you an understanding of everything you need to know.

In this chapter, you will learn:

- Contractual, legal, industry standards, and regulatory requirements.
- Classification of legislations and current frameworks.
- Privacy requirements.
- Privacy and data protection frameworks.

For some, the term compliance is not a familiar one. Therefore, first, it is better to start at this point. In the CISSP learning path, the 8th domain is all about Legal, Regulations, Investigations and Compliance. As it sounds, it is about legality and justice. Yes, indeed. As a security professional, one must acquire knowledge on laws and regulations. That is to bring wrongdoers to justice. There are laws about privacy, civil and criminal activities.

In this chapter, we are not going to go deeper into cyber-crime and cyber laws but the organizational requirements about laws, regulations and compliance. Regrettably, the laws were unable to keep up with the phase of

technology in terms of development. This is causing a serious issue when we talk about cybercrime.

From an organizational standpoint, it must adhere to national laws, regulations and standards while building and encouraging professional ethics and code of conduct. This is followed by encouraging responsibility and accountability. All of these activities are for the safety and security of the organization as well as to set examples of lawful operations - staying **compliant** to the enforcements for betterment in other words. This also discourages the unethical and illegal operations from the inside as well as from the outside. This is what compliance is all about. It's a practice and a discipline.

In addition, an organization must have a legal framework, a staff including information security professionals, and an auditing process. This is to justify the legality as well as preventing the organization from knowingly or mistakenly committing illegal and criminal activities. Furthermore, it is required to identify and bring internal offenders (illegal operations) to justice.

Contractual, Legal, Industry Standards, and Regulatory Requirements

A vital step for long-term sustainability and continuity is to have a better understanding of legal requirements and stay up to date with the changes. During the operation, an organization must understand and stay compliant with global or country-specific national laws. These are not something an organization can simply avoid. Before going into the details, it is better to clarify the systems of law.

There are two types of law systems; one is a common law, and the other is civil law. Almost all the civil laws were derived from Roman law system and arose from legislative enactments where-as common laws can be traced back to the old England monarchy which used to order writs. Writs are formal orders issues when justice is needed. Later the writs could not cover the requirements and cases and the system evolved to have courts of equity. Appropriate remedies were based on equitable principles that were developed. These principles were taken from many sources of authority including Roman and other laws (natural laws for instance). As the previous

decisions and collective cases are published, the court system was able to use these cases in future hearings. This is how the common law developed. On the other hand, the roots of civil law go back to the Roman era. Roman Emperor Justinian around 600 C.E., compiled the code of laws, and over the years in many countries, authoritative legal codes have been developed and matured.

When looking at the existing law systems, we can identify several different classifications. Those are,

- Civil.
- Criminal.
- Internal.
- Natural.
- Public.

When it comes to an individual, it does not mean the individual is specifically assigned to a specific law. Instead, a need arises, a combination of each is utilized toward a workable and acceptable resolution.

Note: There are other systems, for instance, Sharia law. This is a civil law system and it is enforced within the specific religious context and among followers. However, there are nations where certain laws are derived from such laws (e.g., middle-eastern countries).

To get a more specific understanding, the following article provided by the World Bank can be used.

Key-features of Common Law or Civil Law Systems:
<https://ppp.worldbank.org/public-private-partnership/legislation-regulation/framework-assessment/legal-systems/common-vs-civil-law>

Country-Wide Classification

Civil Law by Country : Most of the central and eastern European countries follow a civil law system. In addition, the countries that were former Dutch, German, French, Portuguese, and Spanish colonies also follow civil law

systems. Much of the Central and South America as well as some Asian countries, follow the same.

Common-Law by Country : Most of the countries are former British colonies or protectorates. The countries include England, the United States of America, Canada, and India. It is worth mentioning that in the U.S. legal system, there are three branches namely Criminal, Civil and Administrative law.

What is a regulation? Although the effect of the law and regulation is the same, it is important to know the difference. Laws are written statutes passed by legislatures or a congress (in the U.S.). Next, bills are created by legislatures and when passed by a voting procedure becomes statutory law.

A regulation, on the other hand, is a standard or a set of standards or even rules. In fact, it is adopted by administrative agencies. These agencies govern how laws are enforced. Hence, the regulations become specifics (own set of internal rules and regulations). Both are codified and published so that any party can get informed. The other important fact is that law and regulation have the same force. Otherwise, for instance, an administrative agency won't be able to enforce a law.

These laws, regulations, industry standards are part of a compliant act or a policy. The following list includes some examples.

- Federal Information Security Management Act (FISMA).
- Health Insurance Portability and Accountability Act (HIPAA).
- Payment Card Industry Data Security Standard (PCI DSS).
- Sarbanes–Oxley Act (SOX).

In the next section, there is an overview of these examples.

Federal Information Security Management Act (FISMA)

FISMA is a federal information security management act. The United States Congress passed the E-Government Act (Public Law 107-347) in 2002. The title III of this act, FISMA, requires federal agencies to develop, implement

and document information security plans (agency-wide programs). The main goal of this is to provide information security information/systems that support the agency's assets and operations. This also includes information and systems provided or managed by another agency or a contractor. FISMA act 2014 is an amendment to the 2002 act. This provides several modifications to cope with the evolving security concerns by modernizing federal security practices. The new change results in the following advancements.

- Less reporting.
- Continuous monitoring is strengthened.
- More focus on compliance.
- Reporting focuses more on the issues caused by security incidents.

FISMA works along with two other acts, the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996. The emphasize is on risk-based policy for cost-effective security.

The entire focus of the collection of these acts and Office of Management and Budget (OMB) through Circular A-130 enforcing these legislations is to manage federal information as a strategic resource. It expects the agents to understand the risk and other factors, their adverse impact, and the status of their security program (present and the future) to make informed judgments to mitigate the risk to acceptable levels, thus protecting the investments.

In 2003 NIST started implementing the FISMA project and was responsible for the standards and guidelines that include minimum requirements for federal systems. However, these standards and guidelines won't apply to national security systems immediately. It requires approval of the federal official handling the policy authority over such systems.

As FISMA is risk-based approach, NIST also developed a risk management framework. This brings all the FISMA and related security standards/guidelines to leverage the development of broad and uniform security program by agencies.

FISMA requirements set by NIST are:

- To maintain an information security inventory.
- To do Risk categorization (FIPS, 199).
- To have a system security plan.
- To set security controls (20 security controls are defined by NIST 800-53).
- To perform risk assessment using NIST risk management framework.
- Accreditation and certification – to demonstrate the ability to implement, monitor, and maintain FISMA.

Violation of FISMA may result in an agency baneful consequence and for a contractor at the end of the business. It may also result in loss of reputation, missing future bidding opportunities, and other problems. Therefore, if an organization depends on federal funds, it must be FISMA compliant.

Health Insurance Portability and Accountability Act (HIPAA)

As the name implies, HIPAA is related to health and health information. HIPAA (Public Law 104-191) is a legislation that provides information privacy. It also provides security provisions for safeguarding the health and medical information. The act was signed by the U.S. president Bill Clinton in 1996.

HIPAA consists of five titles. The tiles are listed next.

- Title I: Protects health insurance coverage for workers and their families that change or lose their jobs. It limits new health plans the ability to deny coverage due to a pre-existing condition.
- Title II: Prevents Health Care Fraud and Abuse; Medical Liability Reform; Administrative Simplification that requires the establishment of national standards for electronic health care transactions and national identifiers for providers, employers, and health insurance plans.

- Title III: Guidelines for pre-tax medical spending accounts. It provides changes to health insurance laws and deductions for medical insurance.
- Title IV: Guidelines for group health plans. It provides modifications for health coverage.
- Title V: Governs company-owned life insurance policies. Makes provisions for treating people without United States Citizenship and repealed financial institution rule to interest allocation rules.

source: <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>

When considering the Health and Human Services (HHS), the act enforces the secretary of HHS to publicize standards for the electronic exchange, security, and privacy of health information. The act required HHS secretary to issue privacy regulation over personal identifiable health information. That was if the congress did not institute privacy legislation in three years. As it did not occur, HHS moved forward and established the privacy rule in 1993. In 2002 they modified the act and published the final form.

HIPAA had focused on two main outcomes.

- To continue health-insurance for workers upon losing or changing the job.
- To standardize electronic transmission of administrative as well as health transactions. This also reduces administrative costs.

Other than that, it aimed to repel abuse, fraud, and waste in health care and insurance thus improving access to long-term healthcare services and insurance.

In 2009, Health Information Technology for Economic and Clinical Health (HITECH) Act was released, and it required HHS to implement modifications to HIPAA and placed the omnibus rule in 2013. This concerns the business associates. HIPAA violation has penalties and with this, it was increased to 1.5 million USD per incident.

Another HIPAA enforcement is the HHS Office for Civil Rights (OCR); it issued guidance in 2016 on cloud service providers and other associates of healthcare organizations. They are covered by HIPAA security, privacy, and breach notification rule.

The omnibus regulations and the breach notification rules are important. These require covered entities and affected businesses to inform patients upon a data breach. This ensures the transparency of the operation. The notification rules were extended in 2010 to cover the organizations not covered by HIPAA. This includes vendors of electronic health records (EHR).

In 2016, the HHS Office for Civil Rights (OCR) released a crosswalk between NIST's cybersecurity framework and HIPAA to identify cybersecurity gaps and align it with the national security standards.

There are no official HIPAA related certifications. OCR currently offers several education and training programs on HIPAA compliance. Organizations for the employees create internal training programs focusing on their current policies, HITECH act, and others.

As a CISSP enthusiast, you may focus on HIPAA privacy rule. HIPAA was the first national act to establish protections for personal health information (PHI). The rules issued by HHS limit sensitive personal health information that limits the use and disclosure. The doctors have to provide what is disclosed with accountability for administration and billing. In addition, the patient can request PHI from HIPAA-covered organization.

What is the protected information of a patient under HIPAA?

- Personal information, such as names, birthdate, and social security number (SSN).
- Physical and mental health status.
- Any type of care provided.
- Payment details that might disclose all these.

The following list is about the administrative requirements that the covered entities must have in place.

- A privacy official to implement and manage the policies and procedures.
- All the employees must be trained on policies and procedures.
- Establishment of safeguards employing administration, physical and technical.
- A HIPAA covered entity must have a center to accept patient complaints on violations.
- If PHI is disclosed in a violation of policies and/or procedures, the entity must mitigate as much as possible.

The HIPAA security rule comprises the security standards for PHI. It establishes national standards to safeguard stored and digitally transferred health

information. When addressing electronic PHI (ePHI) associated risks and vulnerabilities, an organization must focus on three key questions. Those are,

- Are we able to identify the PHI and ePHI sources, including the PHIs you create, send, receive and maintain?
- Are we able to identify external sources of PHI?
- Are we able to identify threats to ePHI and PHI handling systems (natural, environmental, and man-made)?

HIPAA violations can have devastating consequences. However, it is not the intention of the book to provide a full course on HIPAA. For more information, refer the following page.

HHS HIPAA page: <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>

Payment Card Industry Data Security Standard (PCI DSS)

At this point, you have learned about two legislations, one on federal information and the other on health information. What about the payment account data? Yes, that is not only sensitive but a prominent target

sometimes beyond the threat that federal information and health information face.

Do you trust an organization to hold your payment card information securely? Many have doubts and uncertainties. Breach of such information may cost millions. Therefore, accepting, storing, transferring, and processing credit card information must be carried out in a secure environment.

In 2006, the Payment Card Industry Security Standards Council (PCI SSC) was launched. The requirement was already there because PCI security needed a security transformation. The main focus of the standardization is to improve payment account security throughout the entire transaction processing*. PCI SSC administrates and manages the PCI DSS. It is important to remember that PCI SSC was formed by the major credit card brands such as VISA, Master Card, Amex, JCB, and Discovery, as an independent body. The responsibility of the payment brand (or acquirers) is to implement PCI DSS. It is not the responsibility of PCI SSC.

Note: By processing, it means electronic transactions including online and web operations as well as mobile and voice operations (e.g., taking credit card information over the phone).

PCI DSS applies to any organization that holds payment data cards regardless of the size. However, there are four PCI compliance levels. This is based on Visa transaction volume over twelve months.

1. Merchant Level 1: Any merchant processing six million Visa transactions per year.
2. Merchant Level 2: Any merchant processing one to six million Visa transactions per year
3. Merchant Level 3: Any merchant processing twenty-thousand to one million Visa transactions per year.
4. Merchant Level 4: Any merchant processing fewer than twenty-thousand Visa transactions per year.

The next section lists the goals and requirements for PCI security standards.

GOALS	PCI DSS REQUIREMENTS
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

Source:

https://www.pcisecuritystandards.org/pai_security/maintaining_payment_security

There are some requirements for level four merchants to become PCI DSS compliant. This is ideal for small merchant and services that are not required to submit compliance reports. For them, there is a validation tool to execute a Self-Assessment Questionnaire (SAQ). The tools are in fact, a questionnaire that has yes or no questions. If an answer is a no, then the company may be required to state the future actions and remediation date. Since there can be different merchant environments, there are different questions to meet this requirement. You can find the list of requirements below.

QUESTIONNAIRE	HOW DO YOU ACCEPT PAYMENT CARDS?
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. <i>Not applicable to face-to-face channels.</i>
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. <i>Applicable only to e-commerce channels.</i>
B	Merchants using only: <ul style="list-style-type: none"> • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
D	For Merchants: All merchants not included in descriptions for the above types.
D	For Service Providers: All service providers defined by a payment card brand as eligible to complete a Self-Assessment Questionnaire.

Source:

https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

In addition to PCI DSS, there are other specific standards to meet different scenarios and roles. Those are,

- PCI PTS: PCI PIN Transaction Security Requirements (PCI PTS)
 - This focuses on protecting card holder's PIN and related processing activities. This applies to design, manufacture, and transport of such devices.
- PA-DSS: Payment Application Data Security Standard – This is provided for software vendors and developers who implement payment applications processing transactions, store data, and sensitive authentication data.

- P2P Encryption: This targets point-to-point encryption solution providers.

Sarbanes–Oxley Act (SOX)

Sarbanes-Oxley Act isn't exactly about information security, but overall it is about corporate governance. In fact, it's about financial reporting, audit and management. It was established to regulate financial practices and corporate governance; the act is named after two architects, Senator Paul Sarbanes and Representative Michael Oxley. The legislation came to force in 2002.

In the 21st century, with the emergence of large corporations, high-tech facilities came along corporate scandals and cybercrime. Therefore, there was a need for legislation that can improve financial reporting reliable and in case of a high-profile corporate crime, restore investor confidence. It sets a number of deadlines for compliance. Regardless the size, any corporation must comply with the act.

The act is arranged to eleven sections (or titles). In terms of compliance, the most important ones are 302, 401, 404, 409, 802 and 906. These are more pertinent than others. The eleven sections and sub-sections are as follows.

TITLE I - PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

- Section 101: Establishment; administrative provisions.
- Section 102: Registration with the Board.
- Section 103: Auditing, quality control, and independence standards and rules.
- Section 104: Inspections of registered public accounting firms.
- Section 105: Investigations and disciplinary proceedings.
- Section 106: Foreign public accounting firms.
- Section 107: Commission oversight of the Board.
- Section 108: Accounting standards.

- Section 109: Funding.

TITLE II - AUDITOR INDEPENDENCE

- Section 201: Services outside the scope of practice of auditors.
- Section 202: Preapproval requirements.
- Section 203: Audit partner rotation.
- Section 204: Auditor reports to audit committees.
- Section 205: Conforming amendments.
- Section 206: Conflicts of interest.
- Section 207: Study of mandatory rotation of registered public accounting firms.
- Section 208: Commission authority.
- Section 209: Considerations by appropriate State regulatory authorities.

TITLE III - CORPORATE RESPONSIBILITY

- Section 301: Public company audit committees.
- Section 302: Corporate responsibility for financial reports.
- Section 303: Improper influence on conduct of audits.
- Section 304: Forfeiture of certain bonuses and profits.
- Section 305: Officer and director bars and penalties.
- Section 306: Insider trades during pension fund blackout periods.
- Section 307: Rules of professional responsibility for attorneys.
- Section 308: Fair funds for investors.

TITLE IV - ENHANCED FINANCIAL DISCLOSURES

- Section 401: Disclosures in periodic reports.

- Section 402: Enhanced conflict of interest provisions.
- Section 403: Disclosures of transactions involving management and principal stockholders.
- Section 404: Management assessment of internal controls (the most costly to implement).
- Section 405: Exemption.
- Section 406: Code of ethics for senior financial officers.
- Section 407: Disclosure of audit committee financial expert.
- Section 408: an Enhanced review of periodic disclosures by issuers.
- Section 409: Real-time issuer disclosures.

TITLE V - ANALYST CONFLICTS OF INTEREST

- Section 501: Treatment of securities analysts by registered securities associations and national securities exchanges.

TITLE VI - COMMISSION RESOURCES AND AUTHORITY

- Section 601: Authorization of appropriations.
- Section 602: Appearance and practice before the Commission.
- Section 603: Federal court authority to impose penny stock bars.
- Section 604: Qualifications of associated persons of brokers and dealers.

TITLE VII - STUDIES AND REPORTS

- Section 701: GAO study and report regarding the consolidation of public accounting firms.
- Section 702: Commission study and report regarding credit rating agencies.

- Section 703: Study and report on violators and violations
- Section 704: Study of enforcement actions.
- Section 705: Study of investment banks.

TITLE VIII - CORPORATE AND CRIMINAL FRAUD ACCOUNTABILITY

- Section 801: Short title.
- Section 802: Criminal penalties for altering documents.
- Section 803: Debts non-dischargeable if incurred in violation of securities fraud laws.
- Section 804: Statute of limitations for securities fraud.
- Section 805: Review of Federal Sentencing Guidelines for obstruction of justice and extensive criminal fraud.
- Section 806: Protection for employees of publicly traded companies who provide evidence of fraud.
- Section 807: Criminal penalties for defrauding shareholders of publicly traded companies.

TITLE IX - WHITE-COLLAR CRIME PENALTY ENHANCEMENTS

- Section 901: Short title.
- Section 902: Attempts and conspiracies to commit criminal fraud offenses.
- Section 903: Criminal penalties for mail and wire fraud.
- Section 904: Criminal penalties for violations of the Employee Retirement Income Security Act of 1974.
- Section 905: Amendment to sentencing guidelines relating to certain white-collar offenses.

- Section 906: Corporate responsibility for financial reports.

TITLE X - CORPORATE TAX RETURNS

- Section 1001: Sense of the Senate regarding the signing of corporate tax returns by chief executive officers.

TITLE XI - CORPORATE FRAUD AND ACCOUNTABILITY

- Section 1101: Short title.
- Section 1102: Tampering with a record or otherwise impeding an official proceeding.
- Section 1103: Temporary freeze authority for the Securities and Exchange Commission.
- Section 1104: Amendment to the Federal Sentencing Guidelines.
- Section 1105: Authority of the Commission to prohibit persons from serving as officers or directors.
- Section 1106: Increased criminal penalties under Securities Exchange Act of 1934:
- Section 1107: Retaliation against informants.

One of the important provisions of the act is the Whistleblower Protection Act. This is more of a witness protection program. Whether it is an employee or even a contractor, if reports fraud and testifies against an organization they work for/with, this act protects against dismissal or discrimination.

Another important improvement is the change in corporate auditing practices. The new requirement states that a corporation should hire independent auditors to audit the accounting practice. Furthermore, it creates rules for separation of duties and what duties can and cannot perform by the internal auditor during an audit process. For Audit Reports, SOX laid the foundation for the Public Company Accounting Oversight Board (PCAOB). This sets standards and rules for audit reports. It requires

all the accounting companies that audit public companies to register for PCAOB.

SOX provides long-term benefits, including achieving great transparency and accountability, better financial allocations and utilization of investments, and investor protection from financial fraud.

Privacy Requirements

Privacy requirements have been there for a long time. Since humans began to become more civilized, they had this requirement, privacy, and it is a sociological concept. Both privacy and confidentiality are related but not the same. Privacy is about personally identifiable information while confidentiality can be an attribute of property, asset or piece of information. Nowadays, privacy is a big concern as large corporations are required to share private information with governments and the potential to keep the information private on the internet.

With the arrival of social networks, and third-parties are getting the opportunity to use certain private content of people, there are debates on how to keep the privacy. These corporations and businesses are required to follow standards and compliance requirements to ensure privacy, and they are obliged to provide privacy options for their customers or subscribers. In terms and conditions of any online service, privacy is explained and transparent. However, people are still concerned about how online platforms reveal private data to governments and third-parties. There is also the concern on information stealing and abuse of private information for benefits and to commit a crime.

Personal Identifiable Information (PII) or Sensitive Personal Information (SPI) are the terms we use in the information security context. There are many different universal, regional, and country-specific laws to help protect private and sensitive information. A recent example would be the GDPR act in the European Union. GDPR stands for General Data Protection Rule. Other than that, IOS and PCI DSS address certain issues and offer guidelines.

Privacy must be part of the information governance strategy. There can be issues, for instance, one's trust in a bank and his personal information

should be shared with the government to find evidence or locate the person if he is questioned by law enforcement. Therefore, it can be controversial about information disclosure. Then again, if the person actually committed a crime, the bank should reveal evidence if it is helpful to bring the person to justice. That may appear as a privacy violation in a different perspective. It is a sensitive matter and must be integrated with confidentiality and compliance to make correct decisions. Therefore, a holistic approach is required.

Privacy protection must go beyond the aspects that overlap with security to place protective measures that focus on collecting, preserving and enforcing customer choices with respect to how and when their personal information is collected, stored, processed and used and how likely to and how it gets shared with third-parties.

As you are aware, data comes from many sources to an organization. Various functional teams handle human resource, financial, IT, and legal departments. Therefore, setting privacy protection for PII requires a collaborative approach. In previous years it is thought that protecting privacy is more of an atomistic approach but this isn't the case any longer.

There are a few, more focused frameworks to address privacy requirements as a holistic approach. One is European General Data Protection Regulation (GDPR). Another is Data Governance for Privacy, Confidentiality, and Compliance (DGPC) framework developed by Microsoft. In this chapter, we briefly look into the GDPR framework.

General Data Protection Regulation (GDPR)

Privacy is a human right. European Convention on Human Rights (1950) states that "Everyone has the right to respect for his private and family life, his home and his correspondence." European Union was already in the process of ensuring privacy for a long time, not just through ethics but through legislation.

In the 90s technological advancements raised the need for data protection. In 1995 European Union passed the European Data Protection Directive (UDPD). It comprised minimum data security and privacy standards to ensure the member states can establish their own laws based on UDPD.

With even more serious concerns such as popularity of online banking, social media giants like Facebook, the need for more robust and comprehensive legislation was prominent. In 2011, Google had to pay the penalty for scanning user emails. In 2016 GDPR was published and enforced after passing European Parliament. All organizations were required to be compliant as of 25, 2018.

There are some key points to understand here.

- If an organization processes personal data of a European citizen, then GDPR applies to that organization, whether it is in Europe or not.
- The penalty for violating GDPR is extensive. There are two tiers, one which max out at 20 million Euro. The other is 4% out of the global revenue (even higher). The subjects can seek compensation for damages.

GDPR – Array of Legal Terms

- **Personal data** : Any information that can be used to identify a person directly, indirectly, or pseudonymously. Other than names, emails, ethnicity, gender, biological data, religion, web-cookies, and personal opinions such as political ideas.
- **Data Processing** : Any action performed on manual or automatic data such as collecting, storing, organizing, recording, structuring, using, deleting, etc.
- **Data Subject** : The owner of data or the person whose data is processed.
- **Data Controller** : The organization (e.g., owner) or the person (e.g., employee) who decides why and how such data is processed.
- **Data Processor** : Third-parties that involve processing such data for the data controller. For instance, a cloud service or an email service is a data processor.

The Key Regulatory Point

Data Protection Principles

1. Lawfulness, fairness, and transparency.
2. Purpose limitation: Purpose is explicitly specified to the subject and for legitimate purposes only.
3. Data minimization: Only the absolutely required and none other than that.
4. Accuracy: Must be accurate and up to date.
5. Storage Limitation: Stored until the purpose is fulfilled and no longer from that point onward.
6. Confidentiality and Integrity: Using appropriate measures, e.g., encryption.
7. Accountability: Data controller must be responsible and accountable.

Accountability

Under GDPR, data controllers must demonstrate the ability to stay compliant. Therefore, just being compliant is not enough. To demonstrate an organization can,

- Designated data protection responsibilities.
- Document everything, including how it is collected, used, erased, and actions of responsible parties.
- Implement the measures and continuously update them while training the employees.
- Initiate comprehensive data protection agreements with third-parties.
- Though not all organizations require, appoint a data protection officer (DPO).

Data Security Implementation

- Technical Measures: For instance, individual data security measures such as two-factor authentication, data protection agreements, and measures such as cloud-based end-to-end encryption.
- Organizational Measures: Privacy policy, need to know the principle, least privilege, staff training, and other things.
- Upon a breach, you have 72 hours to inform the data subjects. Otherwise, there will definitely be a penalty.

Under GDPR, the processing of data is possible if and only if the following conditions are met.

- You must have received unambiguous consent from the data subject.
- To enter into a contract in which the data subject is a party, first, you need to do processing, for instance, background checks.
- When you have to process it to comply with a legal obligation.
- When you need to save someone's life.
- When you perform tasks for public interest or to carry out an official function (e.g., private garbage collector).
- When you have a legitimate interest – In this case, however, your personal interest is overridden by fundamental rights and freedom of the data subject, e.g., child's data.

Consent is a critical part of GDPR. The following rules must be satisfied.

- Unambiguous, freely given, specific, and informed.
- Requests for consent must be clear, specific, distinguishable, and unambiguous.
- Consent can be withdrawn whenever the data subject requests, and you cannot, by any means, stand against it.

- A subject under the age of 13 can only give consent if parents agree.
- Evidence of the consent must be documented.

In a previous paragraph, it is mentioned that in certain cases, an organization has to appoint a Data Protection Officer (DPO).

- You do not possess a judicial capacity as a court but a public authority.
- There is a requirement to monitor people on a large scale, systematically and regularly (e.g., companies like Facebook, Google).
- Large scale processing of special categories of data – listed under Article 9 (<https://gdpr.eu/article-9-processing-special-categories-of-personal-data-prohibited/>) or Article 10 (<https://gdpr.eu/article-10-personal-data-relating-to-criminal-convictions-and-offences/>) - relating to criminal convictions and offenses).

Everyone is a data subject at a point in time. For instance, you can be a data collector or a processor. If you use the internet, you are a subject as well. Therefore, fundamental privacy is a right of everyone. GDPR identifies new privacy rights for data subjects to offer individuals more freedom and control over the data they share with organizations. As an organization, these rights must be understood and be compliant.

- The right to be informed.
- Access right.
- Rectification right.
- Erasure right.
- The right to restrict processing.
- Data portability right.

- The right to object.
- Rights in profiling and automated decision making.

All the GDPR information can be found here: <https://gdpr.eu/>

Chapter Five

Understanding Legal and Regulatory Issues

In this chapter, we will look into chapter four in a different perspective. The risks and threats to information security is a significant issue. The issue gets even worse when there are legal issues such as corporate compliance issues, regulatory issues as well as external threats like cybercrime. Most of these issues end up in compromised states of businesses, information disclosures, privacy violations, and abuse of intellectual property. In addition, we have to learn how import/export controls and trans-border data-flow pertain to information security.

In this chapter, you will learn:

- Cybercrime and data breaches.
- Intellectual property requirements.
- Licensing.
- Import/export controls.
- Trans-border data flow.
- Privacy.

Information security can be categorized simply as personal, national, regional, and global. In this chapter, we are going to have a global perspective on security-related issues, legal and regulatory boundaries and measures.

Cybercrime

In most countries, there is information relating laws and regulations to protect personal information, finance and health information, organizational information, and national security. An organization has to understand,

regulate and comply with national laws and regulations for its own as well as stakeholders' protection. When the operation of the organization when it expands beyond the country, it has to stay compliant with international laws, regulations, and standards. These can be interdependent or sometimes entirely different. For instance, an act in a state in the U.S. may enforce an organization to comply with a set of requirements while in Europe, there may be different or even tighter requirements. Due diligence is an applied approach here.

The most prominent intention of cybercrime is stealing information. From an organizational perspective, the term “data breach” is used. When an intruder gains access to data without authentication and authorization for misuse or even for no intension other than either causing bad reputation or availability, we call it a breach (for instance, a DDoS attack does not breach data but affect availability while a ransomware attack may compromise or erase data).

When such incident occurs, however, there are strict procedures enabled through laws and regulations in most countries. For instance, in the U.S. in a global context, there are procedures to follow upon such a breach and in different states, there are certain different requirements. From a nation-wide perspective, an act such as HITECH requires an organization (e.g., a company that provides EHR system for instance) to follow a set of procedures upon a data breach. This also requires the business associates to stay compliant. In the European Union, GDPR sets mandatory requirements from a regional perspective. GDPR was discussed in a previous chapter in detail. In other regions such as the Asia Pacific, and as countries Australia, China and the Philippines enforce similar laws and requires the appropriate organization to stay compliant.

Next, we will look into the violations that can occur more often and the requirements to protect these entities. Among these licensing and intellectual property are at the top.

Licensing and Intellectual Property Requirements

What is intellectual property? Intellectual property refers to creations of the mind. It can be a design, an aesthetic work (a painting, literature, a movie), a symbol, a name, an image, or an invention. Since these springs up in

mind, the creator and the creation have to be protected from misuses such as copying, redistribution, recreation, selling under different names, stealing of ideas, inappropriate modifications, etc.

There are four types of intellectual properties, and those are,

- Protect secret information.
- Protection for brands.
- Protects a feature or a function.
- Protect authorship.

The following list comprises some examples of intellectual property and the terms used to categorize them.

- Trade secret: For instance, recipes used by companies like Coca-Cola or KFC is a formula to prepare a specific food with a specific taste. Such entities are known as *trade secrets*.
- Trademark: A symbol, logo, or a text or something similar, which represents a brand or a business entity such as an organization.
- Patent: It can be thought of as a monopoly provided for a unique idea, product, or feature.
- Copyright: Protects a creation from unauthorized modifications, distribution, and use. There are country-specific regulations and may somewhat differ from one another.
- License: A license is a bond, an agreement, or a contract between a buyer and a seller. In the IT world, you must be familiar with the term subscription options and service level agreements. All of these are catered through a license. It also stands as a legal right to use or even modify and redistribute in some cases. License terms can be different from nation to nation or based on the region. For example, you might find different agreements when a license is offered for European subscribers in contrast to other regions. Therefore, the license agreements must be compliant with such laws and regulations.

Import/Export Controls

Import and export goods and services can have a significant impact on confidentiality, integrity, and availability, as well as privacy and governance.

Therefore, strict rules are applied upon importing goods. There are legislations and taxes to prevent, control, and quarantine incoming entities if the entities don't follow standards. The entity can be for instance, a hardware device such as a computer system or a surveillance camera. If the provider or logistic services do not follow standards, there can be adverse impacts. Some of these entities may face restrictions if a country prevents importing such. For instance, a county may prevent certain transmission equipment or healthcare equipment from entering due to legislative concerns.

If we take certain entities such as cryptographic products and technologies, some export laws are dependent on the country. Certain countries impose restrictions on encryption standards as well. This is an instance where a service is prohibited. Such laws also prohibit using VPN technologies (China is a good example). The danger with services such as VPN is you do not see the underlying activities yet you depend on these services to transfer sensitive information to avoid controls put by governments to ensure the safety. Therefore, sometimes it is a dangerous deal when someone is having concerns with state-backed information stealing and depending on a service that he may not know anything about.

If your organization utilizes services such as VPN or even cloud and provides services by relying on top (for instance, PaaS or SaaS), you must consider the international laws and regulations on certain technologies these service use. If you provide services to Europe for instance, you must find out the services you rely on are also compliant. Otherwise, you may violate a country law and the penalty can be significant. Therefore, planning for risk and business continuity involves these activities. With third-parties, an organization must have reliable and compliant agreements so that it does not break laws.

Trans-Border Data Flow

There are many instances where organization data resides in many places other than in the specific country. When data resides beyond a country, there are considerations to make as the data security and privacy may fall under different laws, regulations and standards and even not in parallel with the country-specific protocols. With the popularity of cloud-based networks, this problem became a serious issue and certain countries and regions started drafting frameworks and agreements so that they govern the data outside the country if the other countries agree to maintain their standards. An example is the EU-US Privacy Shield Framework.

The U.S. Department of Defense (DoD) and the European Union had such an agreement called the *Safe Harbor* act. European Commission Directive on Data Protection required other countries to enter such agreements if they have to hold and process data relating to European citizens. In 2015, the European Court overturned the agreement by stating only the twenty-eight European countries (European Union) are the ones to determine how online information and data can be collected. As a resolution, in 2016, a new directive formed another framework between the European Commission and the U.S. Department of Commerce. This is known as the EU-US Privacy Shield Framework.

Privacy

As you are aware, at this point, privacy is one of the most prominent issues during the internet era. Personal identifiable data is at risk and it raises multiple concerns. Especially social media opening personal information to third-parties (companies like Google and Facebook) people are getting more and more nervous about security and privacy. Therefore, many countries are pushing legislation and require these companies to be compliant for these companies to stay transparent, informative and bring them to justice if required in information related incidents.

Chapter Six

Understand, Adhere To, and Promote Professional Ethics

In this chapter, we will look into personal contributions pertaining to the information security. These characteristics greatly assist corporate governance, compliance, and risk reduction. The weakest link in information security is none other than people. Therefore, individual thinking patterns, professionalism in judgment, conduct, commitment, responsibility and accountability have to cultivate in an ethical framework. As a CISSP professional, you are a leader of this process. Ethical boundaries must exist throughout your professional practice and you must be able to inspire the organization to conduct the practices ethically.

In this chapter, you will learn,

- What are ethics?
- (ISC)² Code of Professional Ethics.
- Organizational Code of Ethics.

Understand, Adhere To, and Promote Professional Ethics

If you are following CISSP, you must be aware of two types of professional ethics. One is the (ISC)² code of ethics. The other is local to each organization.

What are ethics or good conduct?

The etymology of the word “ethics” comes from the Greek word “ethos.” This resembles the character of an individual as well as the culture of a community.

Ethics can be defined as moral principles governing a person’s behavior or conduct. Ethics shape how people make decisions and how they conduct activities and also how they judge things. In fact, ethics is a branch of

philosophy. In the philosophical world, it is called *moral philosophy* . In general, ethics cover the following thought processes:

- Good choices during life.
- Rights and responsibilities.
- Moral decisions.
- Right and wrong.

Ethics fall into three categories in modern philosophy. Those are,

- **Meta-ethics** : It looks into the origins and meaning of principles and deals with the nature of moral judgment.
- **Normative ethics** : Criteria for right and wrong – moral judgment.
- **Applied ethics** : Looks into areas like capital punishment, war, and rights of other species.

What do ethics do, and what don't they do?

- Ethics provides a moral map.
- Provides the ability to pinpoint disagreements.
- Ethics clarifies more and eliminates confusion – It does not give the right answer but lays a foundation toward better choices.
- It may not provide the right answer but several answers.

Why is ethics important to individuals and organizations?

- Ethics paves for thinking about others and about empathy.
- Ethics can enhance the strength of groups – if a group believes in moral justification about something positive, it is good for the individuals, group, and society.
- Virtue ethics can shape the moral character of individuals.

Now it is time to look at professional ethics. In CISSP, you learn about two codes of professional ethics.

(ISC)² Code of Professional Ethics Canons

As a CISSP student or a professional practitioner, you must honor the (ISC)² code of professional ethics. There are four canons. Those are,

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

Source: <https://www.isc2.org/Ethics>

Why a Specific Code of Ethics?

We need to adhere and visibly practice (inspiration) the highest ethical standards of behavior so that we can empower the safety and welfare of our societies, and the common good, for us and for others. Therefore, a condition of this certification is strict adherence to (ISC)² code of professional ethics.

Organizational Code of Ethics

This applies to an organization itself to maintain the code of professional ethics within. As a security professional, you should stand on these principles, encourage and inspire the teams as well as the organization. An ethical framework secures strong moral conduct among organizations and professionals. It also motivates customers to depend on and build trust upon the professional conduct. As a result, the corporate practice gains trust as well as builds a strong ethical society. This can lead to shaping moral judgment. Many information security incidents are a result of bad ethics of people and even professionals. Therefore, this is the line that separates you and the rest who do not believe in ethics.

In this section, we are looking into how your organization can develop a code of ethics targeting roles and functions. In addition, we will look into the key components and how to create code of ethics for an organization.

Leadership and Ethics

Ethics is something you cannot really be taught in a day. It has to be learned through examples and inspirations. A leader with good ethics or the good ethics displayed by a leader has a significant impact on morale and the loyal values of workers. Good ethics means good business and higher standards of ethics can stimulate others to reach the same standards. As already pointed out previously, this as a whole will increase the reputation of the company in the financial market as well as in the community. Strong and stable ethics and integrity in the community may boost the business.

Ethics and the Employees

Ethics among workers ensure honesty, commitment, and integrity. It also keeps professional relationships understandable and strong. Employees can use ethics to keep aligned with company policies and rules while fulfilling company objectives and meeting personal goals along the way. An ethical employee almost always produces quality output. As a result, the company's reputation is enhanced as the products and services sustain the quality.

Cultural Role

In the previous two sections, we discussed the code of ethics of the leaders and employees. This is the foundation of ethical organizational culture. As you notice, leaders initiate the culture by exercising what they want the employees to follow (or what they want to see in employees). In psychology, such developments can be motivated by a reward program. This reinforces ethical structure, and eventually, the rewarded employees become leaders in ethical standards. They will lead their co-workers and if someone is lagging behind, he/she outstands among others for not following ethics and leaders may initiate disciplinary actions.

Organizational Code of Ethics

Ethics can also be thought of as a holistic approach toward business goals. The code of ethics sets out the business objectives, values, responsibilities, and ethics as a whole. It should reflect ethics, values and business perspective. This can be produced as a written guidebook. If it is well-written, it should also provide guidelines to deal with certain ethical situations. Some codes can be long/lengthy such as manuals addressing multiple situations and some can be shorter general guidelines.

Key Components of a Successful Code of Ethics Lineup

In general terms, ethics are a set of controlled behaviors. Adhering it reflects the values of the company and betterment for the society. Ethics can be set up fairly easily. But to practice, lead and monitor can be difficult at the start. The workers must feel comfortable and enjoy the environment while upholding values. Without closely monitoring, it is difficult to evaluate the performance of the ethical culture. Therefore, appropriate measures to monitor it and take disciplinary actions are also important for a sustainable, ethical framework. The key components are lined up below.

Values

The primary objective of the ethical framework is to define what an organization is about and what degree of honesty, integrity, and fairness it values. These aspects of business values are expressed by how the organization performs regular interactions with key stakeholders. There can be many values that have psychological and humanistic perspectives (i.e., rights) such as respect, prevention of discrimination, equity and equality. No matter what the circumstance is, these values will uplift the goodwill of the organization.

Principles

There can be many business principles that support values. Some success factors, such as customer satisfaction, continuous improvement, and business profitability, plays a key role in documenting principles. At the corporate level, the responsibility to the sustainable environment, friendly use of natural resources, environment-friendly waste management etc. are often found in code of ethics.

Personal Responsibility

Every worker in a corporate environment has a personal responsibility to uphold the code of ethics. If a worker violates the code of ethics, it may raise legal issues and moral consequences on not only the individual but also the organization itself. There must be room to report ethical violations. Such volunteers must be protected by the organization for their effort and goodwill. This is also part of the monitoring program, and it does not require mechanical means.

Management Support

As security programs, ethical regulation programs must start from the top. Their support of values and principles are documented in the code of ethics. As previously stated, it must also include how to report ethical violations in a risk-free environment anonymously. The program should sound how serious the consideration of the management. It can be expressed by signing (signed by management) important sections of code of ethics and display it, for instance, in the break room.

Compliance

Staying compliant with regional, national, and corporate laws, regulations, and standards is a critical part of the business. The requirements are initiated by the top tables and push it down through the hierarchy to the rest of the employees through the management. In history, there are multiple compliance violations and ethical violations, i.e., acts like Sarbanes-Oxley formed directly to address these issues. For instance, the truthfulness and transparency of the financial reports are requirements made through legislation. Standards like ISO 9000 are specifically geared toward customer satisfaction, to meet regulatory requirements and to achieve continuous improvement. We have discussed other frameworks during the previous chapters. The code of ethics can heavily influence compliance standards as it is everyone's responsibility.

How to create an Organizational Code of Ethics

Chapter Seven

Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines

In this chapter, the area of focus is on a more practical approach. In other words, implementation of the security strategy by developing the security policies, developing or adopting standards, documenting procedures, and making guidelines. This is the formal process of the implementation of an organizational security program.

In this chapter, you will learn,

- Why must an organization implement a security policy?
- Why policies?
- What are standards, procedures, guidelines, and baselines?

In the first topic, we looked into how the hierarchy of an organization decides, forms and funds the information security frameworks within an organization. When moving on to the implementation and development, it is the area of security management. This process often starts with architecting a security framework and within the framework the formation of security policy development. The policy requires the oversight of the CEO and the approval. It may require the approval of the board if it introduces changes to the current policies.

Information security policies define and describe how security and safety practices are exercised within an organization. There can be one or more policies to address levels of employees, classifications of information, auditing, risk management, and other functions. When employees comply and stay in the limits by practice, it greatly reduces risks and vulnerabilities. Therefore, policies are the first step toward well-organized security architecture.

Once the policies are developed, next step is to define the standards. Standards are required to deliver accepted practices, for interoperability, measure the outcome and mitigate risks. Standards can be thought of as rules or mandates and are also part of the policies - policies can adopt standards.

When it is time to implement the policies, there is, however, a lack of assistance if guidelines are not formed and documented. Once the guidelines are documented, the security management and teams will create procedures by following the policy standards and guidelines.

Although there can be multiple policies, a policy is not there to answer a specific question. It describes security practices and goals - a policy is neither a set of standards nor guidelines. It isn't a specific procedure of control. Another important thing is that a policy does not describe implementation details (this is achieved through procedures).

A policy helps to define what is intended to safeguard and ensures the implementation of appropriate controls. The control here means how to protect and what restrictions are to be set forth. The proper definition of controls assures proper selection of products and employment of best practices.

Next, let's look at the reasons you should have a security policy.

Who is responsible for safeguarding the information of an organization? Is it the CEO's responsibility, or of the board, perhaps the management information systems department? Or else is it a responsibility of the senior management? Well, part is true, and part is false. Ultimately, everyone is responsible and accountable. Not only the individual employee or departments but the institution itself. Therefore, to protect the best interests of an institution, planned by senior managers, initialized through the management process (senior and other managers) with the collaboration of information technology department and administration develop and deploy an effective security policy. This is applied to the entire organization.

As you know, policies don't solve problems; in fact, they can make things worse and complicated unless policies are clearly written and observed. The policy must stay aligned with the business process. The policy defines the

direction toward which all the organization's efforts should be. By definition, a security policy has the following characteristics.

- Clarity.
- Comprehensiveness.
- Well-defined plans.
- Required set of rules.
- Best practices.

These characteristics regulate access to information and information systems of an organization. A clearly planned policy protects not only the information and systems but individuals as well as the institution, and this is a vital component of risk management, business continuity and disaster recovery. A well-defined and effective policy is a prominent statement to the outside world as it resembles the commitment of the organization to information security.

Standards

Implementation-wise adhering to standards is important. It helps to shape security framework as well as procedures. External standards often come with guidelines and sometimes procedures. A standard helps with decisions on selections such as software, hardware, and technologies. It helps to select a specific and appropriate standard and move forward. If a process does not follow standards, there can be either no standard or multiple standards causing multiple issues. Even with a difficult policy to implement by settings a standard guarantees the selections will work in your environment. For instance, if a policy requires multi-factor authentication and if the organization decides to move forward by selecting smart-card as the choice, adhering a specific standard ensures interoperability.

Procedures

As stated in the previous paragraph, procedures directly control the implementation. Procedures are step-by-step implementation instructions

and are mandatory. Therefore, documenting the procedures is critically important.

Well written and documented procedures save a significant amount of time as it is possible to reuse procedures (and even update as required). Examples for procedures are,

- Access Control.
- Administrative procedures.
- Auditing.
- Configuration.
- Incident response.

Guidelines

Guidelines servers as instructions and, in most cases, not mandatory. For instance, you can compile a set of guidelines to follow when using removable drives in an office. In the guidelines, you can also set examples of best practices and alternatives if required. You can deliver standards practically and with ease of understanding.

Baselines

As the word implies, a baseline is a performance measure. It is ground zero. In terms of security, a baseline is the minimum level of security that needs to meet the policy. Baselines can also be adopted from external entities and align with the business process. There are baselines for configuration, or architectures if you are familiar with system administration or software engineering. In practice, a configuration can be enforced to follow a specific standard as a baseline. It can serve as a scale as well as a building block. For instance, it can be applied to a set of objects that are intended to perform a similar function.

Security baseline serves as a secure starting point for an operating system. To create a baseline, it requires creating a written security policy. Once the policy is there, administrators may use different methods e.g., group policies, templates, or images to deploy security baselines. These baselines

are then securely stored and backed up. Later, administrators or auditors can use these baselines to compare with the existing systems. The result will express the level of security.

If we look at a practical example, let's assume an organization has a policy mandate governing the use of USB thumb drives. None of the users are allowed to bring such drives from outside. Administrators deploy security policy by enforcing this restriction. Later, they can compare the existing system to a baseline and verify if the policy is still intact.

An organization, in most cases, uses multiple baselines. If we look at the first example, the operating systems, general end-user operating systems may have one baseline, computers in the accounting department may have a different baseline, administrator computers may have another, general servers may have another and specialty servers may have another. Major vendors develop tools to create baselines. For instance, Microsoft provides options to create a baseline.

Chapter Eight

Identify, Analyze, and Prioritize Business Continuity (BC) Requirements

Now we arrive at a point where we can actually look at risk management and business continuity in depth. In this chapter, we are looking into how an organization identifies and analyzes the business continuity requirements. In business continuity identifying business objectives and prioritize the critical components needed for the long-run is essential. Many topics are covered in this chapter and intend to provide an implementation-level understanding to you.

In this chapter, you will learn,

- What is business continuity?
- What is disaster recovery?
- What is the process of integrating these into an organizational security program?
- What are the steps?
- A practical approach to the implementation.

Business continuity is a primary objective of a business entity, such as an organization. This basically means to remain operational during outage while maintaining the operation to an acceptable level and with minimal impact on the business as well as clients. This also means that you must recover to continue. In simple terms, business continuity is the sustainment of critical operations. There are many risks affecting businesses no matter how carefully planned and threats due to the vulnerability of at least one person or a component. Sometimes natural disasters cause significant impact. Some of these can be prevented, mitigated or managed through thorough and careful planning. Therefore, the process requires a significant amount of planning and implementation.

Business continuity and disaster recovery are part of a holistic management process. During this process, the security team creates a framework to identify potential threats and build resiliency. This ensures effective response while safeguarding the interests of key stakeholders – reputation, value and brand.

If we look into the two terms business continuity and disaster recovery, the first is the planning process, and the latter is the implementation process. As you understand, the latter engages technical implementation and deployments. For instance, in business continuity planning, you may get questions like what we can do if our datacenter headquarters stops functioning during an earthquake due to extensive damage. During disaster recovery planning and exercise, you may get questions like, “What should we do if our perimeter firewall is breached?”

Develop and Document Scope and Plan

Developing a scope and plan involves the top levels in an organization hierarchy. This requires the approval of top tables, including the board. When a plan is approved, it is allowed to move to the next stage. To formulate the plan, both business and technical team collaborate. In reality, this process starts with a Business Continuity Policy Statement (BCPS) followed by a Business Impact Analysis (BIA). Once this is successfully finished, the teams can create rest of the components.

The business continuity and disaster recovery plan comprise of several stages. Those are,

1. Project Planning.
2. BIA.
3. Formulating the Recovery Strategy.
4. Plan, Design, and Develop.
5. Implementation.
6. Testing.
7. Monitoring and Maintaining.

Next, we will have a look at the main processes of the Business Continuity Process (BCP) and Disaster Recovery Process (DRP).

As stated in the previous chapters, business continuity and disaster recovery are two steps of a holistic approach. We can identify the processes of the holistic approach and classify it into NCP and RDP.

1. Business Continuity.
 - a. Business continuity policies and strategy.
 - b. Risk Management.
 - c. Business continuity planning.
2. Validating and Testing (this is part of the BCP as well).
 - a. IT recovery processes.
 - b. Alternatives sties.
 - c. Backup and replication (onsite and offsite).

Planning for the Business Continuity Process

This planning process comprises the following phases.

1. Identify compliance requirements.
2. Identify and document potential risks and threats.
3. Estimate the potential loss if a probable threat succeeds – for each threat, for instance.
4. Business Impact Analysis.
5. Determine and prioritize organizational resources such as units, systems, and processes, according to criticality.
6. Determine clear procedures to resume from an incident.
7. Task delegation to appropriate roles to respond to incidents.
8. The document, review and create guidelines and procedures to bring awareness through training. This phase also includes

training processes.

Business Impact Analysis

Business Impact Analysis is a process that measures the impact of a disaster or each impact of multiple disasters on critical business components or functions. You can also have a perspective on BIA as a catch-all process. Since BIA is a complicated process, to perform, it requires a team with a good knowledge of all the business processes, business units, infrastructure and interrelationships. Therefore, this is also a holistic process.

For most CISSP students, BIA is an unfamiliar process. Therefore, it is better to look at some terms.

- Recovery Time Objective (RTO): The time that takes to recover from a disaster.
- Recovery Point Objective (RPO): To what point it can be recovered (how far can you go back?)
- Maximum Tolerable Downtime (MTD): How long a company can survive without the lost function or component.

The following list outlines the BIA process.

1. Select the individuals to collect data – data sources. In this process, tools like questionnaires can be utilized.
2. Form data gathering techniques using quantitative and qualitative approaches.
3. Identify critical business functions.
4. Identify all the resources that rely on these functions.
5. Calculate the duration that a business can survive without these functions.
6. Identify potential threats and vulnerabilities.
7. Risk assessment and calculation.

8. Document the final findings and submit the reports to management.

These are the main steps of a BIA. In addition to these, there are some other steps as well. Those are,

- Verification of the completeness of data.
- Determine the recovery time.
- Find recovery alternatives.
- Calculate the associated costs.

The business continuity process follows the process outlined below after conducting a successful business impact analysis.

- Develop the recovery strategy.
- Plan development.
- Testing and exercises.

Let's take a real-world example to simplify the process. Let's assume your organization is required to perform a BIA. How do you practically implement the process? The following example outlines the process.

BIA Process

- Develop the questionnaire.
- Train business functions and managers on how to complete the BIA through workshops and other means necessary.
- Collect the completed BIA forms.
- Review.
- In the final stage, the data must be validated through follow-up interviews. This ensures no gaps will be present in the collected data.

Once the BIA phase is complete, you should move to the recovery strategy phase.

Recovery Strategy

- Based on the BIA results, identify the resource requirements, and document them.
- Perform a gap analysis to determine the gaps between the recovery requirements and capabilities at present.
- Explore the strategy and obtain management approval.
- Implement the strategy.

Plan Development

- Develop the framework.
- Form the recovery teams with roles and responsibilities.
- Implement a relocation plan.
- Compile and document business continuity and disaster recovery procedures.
- Document alternatives and workarounds.
- Validate the plan and obtain management approval.

Testing and Exercises

- Determine and develop testing plans, exercises as well as maintenance requirements.
- Conduct training – this is an iterative process.
- Orientation exercises.
- Conduct the tests, document the results, and create a report.
- Refine the business continuity process by incorporating lessons learned through this final phase.

This is how you conduct a real-world business continuity and disaster recovery plan. Thorough and unique tests and exercises can greatly

influence the entire process. Once you implement everything, you must assess and test the process with a better schedule to ensure the effectiveness of the process in a timely manner.

Chapter Nine

Contribute To and Enforce Personnel Security Policies and Procedures

In this chapter, we are going to look at some aspects of individual contributions to the security and business continuity program. No matter how comprehensive a security program is, the ones who drive the program are workers. Without their contribution and commitment, no security program is going to achieve success. We will be looking into these vectors in the next sections. This chapter covers the strategies and procedures use to hire workers, how to manage the employee lifecycle, how to find the right candidates, and how to build effective personal security policies and procedures.

What is the weakest entity in a work environment in information security or risk management perspective? Is it an operating system with obsolete updates? Perhaps the internet? Or maybe mobile apps? Any of these may indeed bring threats. But the weakest link in even a most secure environment is none other than humans. People.

There are lots of stakeholders linked to an organization. Each person poses a risk as people are always vulnerable through their awareness and practices. Any user can be a subject to attacks such as social engineering, phishing scams, etc. and can be maneuver toward goals of the attacker. To reduce potential risks, personal security policies and procedures are developed and deployed.

Candidate Screening and Hiring

Candidate screening is a crucial process of identifying the legitimacy of the applicant, who he/she is, and whether the claims of his/her are true or false. There are different types of screening and some are mandatory. In certain countries, there are procedures enforced by government legislation to utilize when hiring candidates for certain types of jobs. The following sections explain the screening process further. The main goal of this process is to

eliminate the risks when the employee has to take part in managing resources of an organization including financial assets without jeopardizing the organization.

Pre-Employment Screening

This type of screening is mainly designed to verify the claims provided by the candidates on resumes. These investigations can reveal character flaws and criminal tendencies of a candidate that may tarnish the reputation of the organization in the future while endangering the staff. It can also uncover issues limiting the effectiveness of the candidate.

Screening for Criminal Activities (History)

In many countries, laws dictate how criminal information can be used for screening activities when evaluating clients. In the U.S.A., there are state laws. State Identification Agencies and Federal Bureau of Investigation (FBI) provide services to help businesses during the process.

Drug Screening

Drug testing is becoming a common practice, giving an idea of the trustworthiness of prospective candidates. It also reduces risks such as workplace injuries, financial abuse, and other illegal activities. If an organization conducts a drug test, it has to do in accordance with existing laws.

Tracing Social Security Number (SSN)

This is used to validate the social security information, and useful to conduct criminal and credit checks.

Compensation Claims History

This would reveal any disabilities of the candidates by investigating the compensation claims in the past.

Credit History

Credit status of a candidate can determine if financial issues might impact the trustworthiness. It can also reveal evidence of irresponsible behavior.

Lie Detectors

Not all the hiring processes utilize lie detectors, and it is prohibited by legislation such as the Employee Polygraph Protection Act. Only in special cases, lie detectors can be used to validate the truthfulness. Can you guess what these special cases are? Yes, I am sure you have an idea. Security and national defense-related organizations utilize lie detectors if required. Security guard services, security vehicle services, and pharmaceutical services are few examples.

Screening for Sex Offenses

Organizations avoid hiring candidates who were sex offenders previously. This is to prevent endangering the staff and reputation.

Employment and Education Verifications

Previous employment can be verified through the references the candidates provide. In addition, there will be other checks through the previous organizations. However, past employers may limit their response to these queries if policies are preventing them from doing so. There are national level verifications; for instance, all workers in the U.S. must prove their identity and work eligibility by completing an I-9 Employment Verification Form (<https://www.uscis.gov/i-9>).

It is not so difficult to verify the education qualifications. Most universities, institutions, schools, and other education providers can be queried legitimately to obtain such information. However, some countries may require the consent of the candidates for such education providers to release the information. For instance, the Family Rights to Privacy Act (FRPA) in the U.S. enforces the consent requirement.

Other acts are protecting the candidate. Employees may use third-parties to run background checks on candidates. These checks are covered by legislation such as The Fair Credit Reporting Act (FCRA), and also others like FRPA).

Employment Agreements and Policies

An employee agreement secures the organization as well as an employee. An employee is bound to protect the policies set forth by an organization.

The agreement provides cover for the employees, the organization and also includes certain criteria, limitations, and so on. Let's have a look.

What is included in an employment contract? The following sections and statements are included.

- Identification of the parties.
- Title.
- Type of employment: Full or part-time, paid hourly or fixed, and type of service.
- Wages and relating compensation types.
- Benefits the employee is going to receive.
- The effective date of the employment.
- Probation period (or onboarding period).
- Duration of the employment, if any.
- Work schedule.
- Duties and responsibilities.
- Severability: If one part of the contract is found to be illegal, the others still remain active.
- Confidentiality (if required).
- No-compete agreement: An employee should not start his own company to compete against the organization he works for.
- Communication: Ownership of content such as social media posts.
- Dispute process.
- Applicable law: This is a statement about the state in which a dispute about the contract is adjudicated.
- Notices: How notices of actions are transmitted.

- Termination process.

The agreement must express clarity, low complexity, and guidance. If it is too hostile, the user may start to spring a negative influence. This may eventually justify an act of survival that corrupt the integrity of the data as well as systems. If the statements are complicated, the agreement may still start but without consent.

Onboarding and Termination Processes

Onboarding is a critical part of the employment lifecycle. Onboarding is not the orientation process. During the onboarding process, the employee learns about the objectives, responsibility and culture in the organization. If the process is structured, logical and easy to understand, it influences the new employee to inherit and adopt the policies and practices, including security. The onboarding process must be well-written and documented.

Normally the onboarding can last for a few months, but nowadays, it can last up to 12 months. To establish a properly aligned program, top tables must formulate, evaluate and approve an onboarding program. There are some questions an employer should ask before creating an effective strategy.

- What is the starting point of the process?
- What is the duration?
- At the end of the first day, what impression do you want the employees to have?
- What part of the process will each role-play (role means the HR, Senior Managers, Team-leads, Co-workers)?
- What goals would you like to set for new employees?
- How would you collect performance data and measure the effectiveness?

Both onboarding, as well as the termination, are crucial parts of a job, especially as a manager. A natural retirement process is acceptable. However, an unwelcoming termination is a high-stress situation. For

instance, certain organizations may terminate employees to minimize the cost (known as reduction in force or RIF). During the process, the employee must feel no hostility. Improper procedures may lead employees leaving an organization and start vandalism against it. As you notice here, the process must be legal and ethical.

An employee who is not focusing on enhancements, efficiency, and principles can be a burden as well as a future risk. If the person does not follow policies, standards and security practices, it can lead to grave damages and loss of reputation as he/she is neither reliable nor accountable. There is no choice but to terminate the employees even after fair warnings and putting the person through training programs. This is now however, always the case.

The human resource department should maintain the credibility by displaying proactiveness and identifying potential failing employees (this identification has to be a collaborative effort). There have to be the following practices to empower employees, especially if they are failing.

- Provide feedback directly but without hostility. The method differs from person to person.
- Performance Improvement Strategies.
- Coaching.
- Performance Enhancement Planning Process – specifically for this employee, if the employee is still a valuable asset, you will need to introduce him/her a performance improvement plan.
- Performance Improvement Plan (PIP): This facilitates constructive discussion between the staff member and the supervisor so that they can clarify the work performance that needs improvements.

Disciplinary Termination

Most states in the U.S. follow the “employment at will” doctrine. Except for the reasons prohibited by law, employers are free to discharge an employee for any reason. If the reason is unclear and seems unreasonable, it may be

deemed as a pretext. This may end up in litigation. Therefore, the employer must carefully document the reason for termination.

During a termination, there is a procedure to follow. The employee must handover everything that belonged to the organization. Otherwise, it opens the door to a serious security risk in the future. For the best interest, it is always better to have a checklist. A sample checklist is provided below.

1. Record termination details.
2. Request/receive a letter of resignation.
3. Notify the HR department.
4. Notify the system/network administrators.
5. Terminate all online and offline accounts.
6. Revoke access to perimeters and physical assets.
7. Revoke the company assets.
8. Maintain a document to validate the received assets.
9. Request/receive benefit status letters from HR.
10.
Review signed agreements.
11.
Release the final payment.
12.
If required, conduct an exit interview confidentially and obtain written permission for reference.
13.
Update the information and close the profile.
14.
A farewell party, if required.

It is worth noting that keeping policies and procedures documented can streamline the entire process.

Vendor, Consultant, and Contractor Agreements and Controls

These roles are also essential for business operations in times. However, none of these entities work on a full-time basis and may have different agreements. They are external parties, and an organization must take extra precautions. The selection and agreements open up the organizational data to third-parties. Therefore, managing risks and setting up safeguards are vital.

Although vendors and contractors do not use internal corporate resources, consultants may receive their own dedicated desk, a computer, and connectivity to the internal network with certain restrictions. Consultants are not dedicated workers to a specific organization. Therefore, there are possible instances such as accidental data loss, deliberate comptonization, integrity violations, confidentiality violations and stealing information. Hence, the selection of consultants must go through a screening process, background check and a verification process to identify, make necessary agreements and place effective controls to prevent adverse impacts.

Compliance Policy Requirements

During many previous chapters, there have been discussions on compliance. In this chapter, it is specific to personal policies. Organizations have to be compliant with different legislations, regulations and standards. These drive the foundation of company-specific policies. These policies also raise the requirement to pave user-specific policies. During the onboarding process, new employees are introduced to and walked through these requirements. Understanding and adhering to these assures employee discipline and risk reduction. During the orientation and onboarding, well-maintained compliance policy documents can be utilized to guide new employees.

Privacy Policy Requirements

In a previous chapter, we were looking into the privacy laws, policies, and requirements in depth. In this chapter, we focused more on individual policies or the building blocks in other words. There are two sides to this

specific case. One is the privacy requirement of the customers who engage with the company in day-to-day operations. The workers must honor the confidentiality and privacy requirements for the sake of the clients. It is a responsibility as well as accountability as an employee.

For instance, the sales department handles extremely sensitive information, including personally identifiable information as well as payment information. Another example is a health insurance company holding both PII and PHI. They are the first line of defense as well as they can be the first line of failure. Therefore, organizational policies, standards and procedures must be well taught to them, monitor and take actions if anything goes wrong. A better way is to roll these boundaries as ethics. There is also a requirement for training programs to uplift the positive motives and a reward program to empower the committed.

The next important thing is the right to privacy as an employee. An employer can keep an eye on employee's actions, speech, and even know some information about their personal lives. But to what extent? The protection of such information has become a greater concern in recent years. Especially with the rise of social media and digitalization. With these changes in recent times, although things appear as private in reality, it isn't the truth.

Sufficient laws are covering many rights and obligations in the employer and employee relationship regardless of the status of the employer (current, former, or future). These laws address legal issues such as unlawful terminations, workplace safety concerns, job safety, discrimination, wages and taxation. In many countries in the world, there are national laws, federal and state laws. For instance, an employer and an employee agree to terms upon recruiting and the agreements are formed by following such laws. Contract law alone or with support of other laws dictate the rights and duties of all parties involved. However, the rights of a private employee may differ from the public employee.

Passwords, information segregation, or using electronic lockers may give an impression of subjective expectations of privacy. In reality, employer policies may eliminate objective expectations of privacy. Especially some technologies do not follow any type of law.

An organizational policy often includes employee rights for privacy. That comprises work information and personal information to some extent. There are many legal monitoring activities, and many technologies exist supporting such decisions. Most technologies track the digital footprint of the employee and facilitate to have insights. For instance, an employer can monitor a work PC by every mean necessary, even without regulations. Workplace communication can be monitored along with the systems. Employees must keep in mind that they use company properties and they are obliged to allow monitoring procedures. And another important thing to remember is that as an employee, one must not attempt to evade or compromise such setups by bypassing the policies. This puts the company in danger.

Let's look at some privacy concerns below.

- Internet and email privacy: Employee emails can be monitored and is legal if the employees use company properties. However, the monitoring activity must be known to them. Employers can monitor and track emails, monitor activities, idle time, keystrokes, and other relevant activities.
- Telephone privacy: Electronics Communications Privacy Act (ECPA) prohibits employers from monitoring personal phone calls. They have to disclose the monitoring of phone calls and voice messages. In fact, they can monitor, disclose, prevent access, and delete the entities. Mainly it is used to track phone activities and quality control.
- Video Surveillance: Employers have the right to monitor the premises as well as the parks for safety and security. Again, they have to inform the employees about the act. Video recording must not include audio and is illegal in many countries. Surveillance recording must be used only if there is a legitimate need, such as to deter theft or monitor employees for productivity. Normally video surveillance is not deployed in restrooms, break rooms and lockers.
- Screening: Employers use screening when recruiting and, if necessary, during the employment but with restrictions set by laws. For instance, private firms can require drug tests but they are not

allowed to release reports. However, laws restrict drug screening of employees for instance, in the U.S.

- GPS tracking: Employers can use GPS devices to monitor the locations of the employees during work, especially they use company-provided vehicles and phones. Beyond that, there are U.S. state laws barring employers from monitoring GPS on a personal level.
- Social media: Many employers track the social media activities of the users during work hours and on the premises. And some restrict users publishing posts or comments about the company. Furthermore, some recruiters force candidates to provide social media account credentials. There are state laws in the U.S. barring employers from restricting social media use outside of company hours. In addition, The National Labor Relations Board (NLRB) outlines the rules regarding these issues. This includes protecting the fair use of social media, protecting employee freedom to discuss things like salaries and other sensitive information, and protecting them from being asked to provide social media credentials.

In addition to these issues, there may be other cases, such as an employee having certain medical conditions. The organization has to know if the worker can sustain. However, it should not lead the situation to discrimination. Employer-employee awareness, trust forms mutual understanding that is required in governance and risk management programs. When an employee understands why and how governance, risk and business continuity requirements are important for the organization as well as the individual benefits, many problems and disagreements will be resolved.

Chapter Ten

Understand and Apply Risk Management Concepts

The main goal of this study guide is to help you with understanding, developing, and mitigating risks through risk management concepts. In this chapter, we are going to deep dive into risk management. Risk management is a process of determining the threats and vulnerabilities, followed by an assessment of risks and develop risk responses. The outcomes such as comprehensive reports are used by the managers to make intelligent decisions (including taking future risks) through the entire operation. A part of this process is budget-control. In fact, the final successful outcome is to save resources and time while mitigating risks up to an acceptable level to maintain business growth and sustainability.

In this chapter, you will learn,

- Threats and vulnerabilities and how to identify these.
- Risk assessment.
- Risk response.
- Controls and countermeasures.
- Asset valuation techniques.
- Reporting and refining.
- Risk frameworks.

Identify Threats and Vulnerabilities

In the first chapter, there was plenty of information on a threat and a vulnerability. A vulnerability is an opportunity and possibility of exploitation. Therefore, a vulnerability may become a present or a future threat. Taking such a risk is not a good business practice.

A threat is a circumstance – a man-made or natural- that may adversely impact a business or business continuity. It can be a known threat or an unknown (known to none or someone). On the other hand, a vulnerability is either a weakness or a missing safeguard that may cause a threat more likely to occur or to occur repeatedly in a frequent manner.

Risk Analysis and Assessment

Assessing a Risk

Risk assessment is a process of determining the degree of future or existing vulnerabilities, and the potential a vulnerability has so that it can evolve into a threat. If there is a real risk, then the next step is to calculate the impact. Recovery procedures often follow the second step to achieve business continuity.

There are several ways to assess a risk.

- Quantitative Analysis: As you may already know, quantitative means numbers and currency amount. A qualitative analysis reports the figures. The figures represent the probability and percentage of a specific threat to succeed and cause damage. It comprises other figures such as loss in currency, the cost of countermeasures and the effectiveness of the deployed measures as a percentage.
- Qualitative Analysis: A qualitative analysis uses a pre-defined rating scale. It prioritizes the identified risks using this rating system. Then the risks are scored based on their probability of occurring and the impact on objectives. Normally, the probability scale is a binary system (zero to one), while the impact scale is organization-specific. This also makes categorization easy based on the source or effect.
- Hybrid Analysis: This is a blend of qualitative and quantitative analysis methods. This often offers more flexibility and accuracy.

Now let's look into these methods and practical use of it in examples.

Performing a Quantitative Analysis

This assessment uses cost to the elements of risk assessment as well as assets and threats. To fully execute a qualitative risk analysis, you have to quantify the values of assets, impact, frequency of a threat, cost of the measures, the effectiveness of the measures, probability, and uncertainty). The main problem with this approach is the difficulty of assigning a monetary value to all the elements. This is when you need a qualitative approach (this makes the entire analysis a hybrid). The steps for quantitative analysis are as follows.

1. Calculating Single Loss Expectancy (SLE): $SLE = \text{Asset Value (AV)} \times \text{Exposure Factor (AF)}$. Asset value may vary with inflation and market value. Exposure factor is the potential loss (subjective) to a specific asset if a threat is realized as a percentage.
2. Calculate Annual Rate of Occurrence (ARO): This calculates the frequency (in other words, repetition) of an adverse event. This process is in fact the threat analysis stage.
3. Calculate the Annual Loss Expectancy (ALE): $ALE = SLE \times ARO$. This combines the potential loss and annual rate to calculate the magnitude of the risk.

Do not forget that you need to include the associated costs such as,

- Repair cost.
- Loss of productivity.
- Lost assets or value of the damaged assets.
- Cost required to replace the hardware or reload the data.

Example: In this example, we are going to calculate ALE on a database. Let's assume that the database is a risk. Here, the *risk* is information stealing. It may also cause the database to lose integrity. It may become corrupted and unusable in some cases.

- Asset value: \$500, 000
- Exposure factor: 57%

$$\text{SLE} = 500000 \times 0.57$$

$$\text{Therefore, SLE} = \$285,000$$

Let's assume the ARO (annual frequency) is 20% and calculate the ALE.

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

$$\text{ALE} = 285,000 \times 0.2$$

$$\text{Therefore, ALE} = \$57,000$$

A list of Quantitative Techniques are as follows:

- Sensitivity analysis.
- Expected Monetary Value (EMV) analysis.
- Decision Tree Analysis.
- Expert Judgement.
- Tornado diagrams.

Performing a Qualitative Analysis

As mentioned in the previous section, whenever a quantitative approach is not realistic, a qualitative approach can be used. There are assets that you cannot assign monetary values to. In such a situation, you have to depend on a qualitative scale. For instance, in NIST 800-26, a qualitative approach is performed based on confidentiality, integrity, and availability. The scale comprises three states, low, medium and high.

- Low: Minor impacts that may not cause a serious impact.
- Medium: Medium impacts on businesses, and it may incur a certain level of the repair cost.
- High: This may cause loss of revenue to a greater degree, and may also result in legal actions and loss of goodwill between the company and the customers.

Example: In this example, based on the scale mentioned above, we are going to do a basic analysis of a specific asset. The asset is a Subscriber Database. Let's calculate the impact based on the CIA triad.

- Loss of Confidentiality: High
- Loss of Integrity: High
- Loss of Availability: Low

A list of Qualitative techniques are as follows:

- Facilitated Risk Assessment Process (FRAP).
- The Delphi Technique.

What are the goals of risk analysis?

- Identification of available assets and its value.
- Identification of vulnerabilities and threats.
- Quantify the probability as well as the business impact.
- Obtaining a balance between the impact in a situation when a threat succeeds and the cost of the countermeasures.

Risk Response

Response to risk is a critical process in risk management, and the degree of success is the major contributing factor to business continuity.

There are four major actions you need to be aware of. Those are,

- Risk Mitigation: Risks cannot be prevented by 100% in the real world. Mitigation means reducing the risk to a minimal and acceptable level.
- Risk Assignment: This is the process of assigning the potential loss of a risk to another party (often to a third-party) such as an insurance company.

- Risk Acceptance: This is the prudent way of handling risk; by accepting loss and cost if a risk occurs.
- Risk Rejection: This is not exactly a prudent way of managing risks. However, in some cases, it is possible to pretend that the risk does not exist.

Risk assessment formulas can be used to calculate the total risk and deploy countermeasures to reduce the risk. The following formulas reflect this concept.

- $\text{Total Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Asset value}$
- $\text{Residual risk} = \text{Total risk} - \text{Countermeasures}$

Countermeasure Selection and Implementation

Risk mitigation requires countermeasures (a.k.a controls or safeguards). A countermeasure can be either a physical implementation or a logical decision. If we take a simple example such as a password, using a password policy with hardened requirements (extended length, using a combination of alphanumeric characters, special characters, etc.) In addition, you can place biometric devices to harden the access further. By this, it is possible to reduce unauthorized access and false acceptance rate thus reducing the risk surface.

Applicable Types of Controls

There are six types of major controls. In previous chapters, these controls were introduced in different sections.

- Preventive controls: The main objective of such controls is preventing action. Some examples are intrusion prevention systems (IPS), firewalls, least privilege, need to know principle, and encryption.
- Detective controls: These controls are there to detect an action or event as it happens or even after. Therefore, it does not prevent actions. Some examples are intrusion detection systems (IDS), anti-virus systems, surveillance cameras, and sensors.

- Corrective controls: These measures correct or fix things during or after an attack. Some examples are antivirus, patches, and certain IPS functions.
- Deterrent controls: These controls prevent actions by discouraging the attempts. For instance, warning signs, warning screens, watchmen, and dogs are deterrent measures.
- Recovery controls: The sole responsibility of these measures is providing aid in recovery. For instance, backups high availability clusters, disk arrays serve this purpose.
- Compensating controls: When an entity cannot meet a requirement due to legitimate technical or business constraints, it is possible to mitigate risks through the implementation of other controls sufficiently. For instance, if placing a security measure is either too difficult or impractical, an alternative measure can be utilized. Some examples would be segregation of duties (SoD), logs and audit trails, and measures applied when encrypting mass data is impractical.

Security Control Assessment (SCA)

The measures or controls must be reviewed periodically and tested for efficiency and effectiveness. During this process, a documented plan is required with procedures; in addition, change management and upgrading/replacing are necessary. SCA is the principle that ensures the policies enforced are meeting their objectives and goals. It helps to evaluate managerial, operational and technical security measures and determine the effectiveness and accuracy.

There are tools and techniques used to conduct an SCA. NIST Security Control Assessment opens the door to perform a comprehensive SCA. NIST Special Publication 800-53 (currently, 800-53A, revision 4 – source: <https://csrc.nist.gov/Projects/risk-management/Security-Assessment>) provides guidelines to assess controls.

Monitoring and Measurements

A critical part of security controls is the continuous monitoring and tuning for performance and precision. Without monitoring security measures and review the performance, it is impossible to expect sustainable mitigation of threats. It is an active process and operated within an organization by a designated team of professionals.

If we take a simple scenario such as a security log is reporting about multiple failed attempts to log in to a server remotely means there is an ongoing intrusion attempt. If there is a vulnerability, and if you do not notice it, the attacker may eventually succeed. Therefore, it does not always work like automated sentry-guns in a movie. There must be a way to measure the risk and impact as well as to locate and remediate the threat. For instance, you could install a notification or alerting mechanism to alert all the responsible parties.

Another important thing to keep in mind is the protection of logs and relating data. For instance, an intruder upon success may attempt to clear the traces, including logs. There are methods to save logs, use a special location to write only and other advanced strategies to keep integrity. Log rotations may occur in some cases due to save the space, but in such cases, backing up and reviewing are necessary steps before something goes wrong. Simply, you need logs for auditing and tracking the performance of security measures.

In an organizational environment, the reviews of measures and logs occur weekly basis. The outcome of a review comprises the following details.

- The number of occurrences.
- Nature of the outcome (success/failure).
- Duration of the event or activity.
- Assets affected.
- Impact on cost.
- Parties involved (customers, business units, departments, etc.)
- Location.

Asset Valuation

Asset valuation is an important stage in the risk management process. Management and executives must be aware of every value (tangible and intangible) involved in specific incidences. In most cases, the account department is responsible for asset valuation, and it can come from the balance sheet. However, it is not as simple as it seems. If an organization has to replace an obsolete hardware device that was involved in an incident, the new replacement may cost higher than the depreciated value of the old hardware. In addition, the work hours required for the replacement, downtime and other facts are needed to be considered.

There are several approaches to asset valuation:

- Cost method: This is the basic valuation method used for many years. It is based on the purchased value of the asset.
- Market Value method: This method uses the market value of the asset is to be sold in the open market. If the asset does not exist in the open market, it is difficult to rely on this method. In that case, there are two additional steps to consider.
 - o Replacement Value: If the same asset is the one to purchase, the value is calculated based on this fact.
 - o Net Realizable Value: This is the cash amount that an organization expects to receive upon sales. This is sometimes referred to as cache realizable value.
- Base Stock method: In this method, an organization maintains a baseline of stocks, and the value depends on this fact.
- Standard Cost method: In this method, instead of using actual costs, the value depends on the expected cost. The expected cost is substituted from the actual cost, and variances are recorded subsequently. The variances show the difference between the expected and the actual costs.
- Average Cost method: This method is also known as the weighted-average cost method. In this method, the total cost of good available

is divided by the units available. It comes useful when the valuation cannot be distinguished. For instance, if there are three access points worth \$100, \$150 and \$ 200, the average method dictates the value as \$150 as the average cost of all three items.

Other than these methods, there are more specific methods if it is a tangible asset.

Reporting

Reporting is another critical requirement in risk management because of two reasons. One is that reporting incidents and/or requirements relating to risk management are the key to a sustainable risk management program. The other is that the reports remind the management of how important the risk management process is. The second keeps reminding the managers to keep the priority of the risk management is at the top of the mind.

Another key success factor is to disclose every incident or issue. If things are hidden, it is impossible to mitigate as it does not appear as a critical requirement. In addition, changes to the risk posture of the company must be included in the report. For instance, events such as acquisitions, mergers, zero-day vulnerabilities, bleeding-edge technologies, and any type of failure must be reported promptly and comprehensively.

There are law and regulations that require adhering to specific reporting structures or specific reports. The following list includes some entities that may exist in a report.

- Changes to the risk ledger.
- Internal and external audit reports.
- Information relating to risk treatment.
- Monitoring of measures and key performance metrics.
- Changes to measures.
- Any changes to team members who are responsible for managing the program.

Continuous Improvements

There are no risk management program or framework that you can apply to an organization and forget. Risks evolve with time, and the vital responsibility of the relevant parties is to review and refine the process. Besides, if the program lags behind the technologies and advancements, it will become obsolete and incapable. Therefore, the improvement process must be incremental and can be applied to processes, products and services.

If we take a look at the ISO/IEC 27000 series (especially in 27001:2013), it provides an excellent guide. It outlines the requirements for an Information Security Management System (ISMS). The requirements for continuous improvement are included in clauses 5.1, 5.2, 6.1, 6.2, 9.1, 9.3, 10.1, and 10.2. It helps an organization to demonstrate continually improving adequacy, effectiveness and suitability.

ISMS Process

The process comprises four stages; namely, Plan, Do, Check and Improve. In each process, the following steps are executed.

1. Establish the ISMS.
2. Implement and Operate.
3. Monitor and Review.
4. Maintain and Improve.

Risk Frameworks

There are methodologies to assist the organizations in designing, developing, operating, and maintain risk management programs. These frameworks provide proven methodologies to achieve risk assessment, resolutions and monitoring. Some of these frameworks are listed below.

- NIST Risk Assessment Framework (for more information, please visit <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>)

- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE – for more information, please visit <https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419>). OCTAVE Allegro is a methodology developed by Carnegie Mellon University.
- ISO 27005:2008 is another information security risk management guidelines provided by the International Organization for Standardization (for more information, please visit <https://www.iso.org/standard/42107.html>).
- The Risk IT framework by ISACA fills the gaps between generic and detailed information technology risk management frameworks for more information, please visit <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx>). It also works with their COBIT framework.
- For the organizations who wish to obtain individual tools, there are others like TARA and Open Group Open Fair risk analysis tools.

Chapter Eleven

Understand and Apply Threat Modeling Concepts and Methodologies

This chapter is about threat modeling concepts and methodologies that are used to identify and quantify threats so that the risks can be communicated properly and prioritize accurately. These techniques are widely used in the software development industry. There are several perspectives when you model threats. You can focus on the asset, or the attacker, or even the software.

In this chapter, you will learn,

- Threat modeling methodologies.
- Threat modeling concepts.

In this chapter, we are going to look at the industry standard methodologies utilized to conduct threat modeling and analysis. The chapter also briefly looks into the process or operation of each technique.

Why Threat Modeling and When?

Threat models are used mainly in the software development industry. These models are often designed during the system design. In reality, threat models are often created for existing systems. It plays a major part in the maintenance process. In the information technology area, it is a risk analysis and used to identify security defects. Similar to software development, threat modeling, in this case, is used during the design phase. Therefore, it can be applied to software as well as operating systems and devices.

In most cases, threat modeling has an attack-centric approach. In other words, it is used to identify exploitable vulnerabilities. And it is most effectively used in the design phase, although it can be used in other phases. At this point, by using these methodologies, it is possible to identify threats

as well as mitigations. It is also flexible when it is used in the design phase because, after the implementation and deployment, a lot of efforts have to be taken to patch these issues.

General threat modeling steps would be,

- Identification of threats.
- Determining the attack potentials.
- Reduction analysis: Avoids duplicate efforts.
- Remediation.

Threat Modeling Methodologies, Tools and Techniques

Attack Trees

This is another oldest model and is also widely used. It can be applied to cyber, cyber-physical and physical systems. Although it was a standalone method, it is now used in collaboration with other methodologies and frameworks (e.g., STRIDE, PASTA). As the name implied, attack trees are diagrams in a tree form. It depicts attacks on a system. For complex systems, attack trees can be created for each component. It helps to determine vulnerabilities and to evaluate specific attack types.

hTMM

Another more recent threat modeling method developed in 2018 by Security Engineering Institute (SEI) is known as hTMM (Hybrid Threat Modeling Method). It uses SQUARE (Security Quality Requirements Engineering Method), and security cards. Features of this method include no false positives, no overlooks, consistent results, and cost-effectiveness.

PASTA

Does the name PASTA sound familiar? Indeed, but this is not about your favorite meal. PASTA stands for Process for Attack Simulation and Threat Analysis. This is a fairly new modeling technique (developed in 2012). The method is attacker-centric. PASTA provides a seven-step process and is platform insensitive. The main goal of PASTA is to align business

objectives with technical objectives, compliance requirements, and business impact are carefully considered. In addition, this method takes software development focused threat modeling to new heights. The risk and business impact analysis turn the method into a strategic business exercise and involves key decision-makers.

The following list outlines the process.

1. Define Objectives.
2. Define Technical Scope.
3. Application Decomposition.
4. Threat Analysis.
5. Vulnerability Analysis.
6. Attack Modeling.
7. Risk and Impact Analysis.

OCTAVE

OCTAVE was introduced in a different chapter; it stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation. The framework and methodologies were developed at Carnegie Mellon University – Software Engineering Institute (SEI) with CERT. The methodology focuses on assessing non-technical risks in an organization. By using it, an organization can identify information assets and the datasets held by the assets. One of its main goals is eliminating the confusion about threat modeling scope while reducing excessive documentation.

STRIDE

STRIDE is a Microsoft product, invented in 1999 and adopted in 2002. It is also the most mature and evolved to address more threat specific tables and variants such as STRIDE-per-Element and STRIDE-per-Interaction. It uses data-flow diagrams and is used to identify system entities, boundaries, and events. Below list outlines the steps.

- S: Spoofing the Identity – In this case, authentication is violated.
- T: Tampering – In this case, integrity is violated.

- R: Repudiation – In this case, non-repudiation is violated.
- I: Information Disclosure – Confidentiality is violated.
- Denial of Service (DoS) – Availability is violated.
- Elevation (of privileges) – Authorization is violated.

STRIDE is successful in cyber and cyber-physical systems. Currently, it is part of the Microsoft Security Development Lifecycle (MSDL). Another methodology developed by Microsoft is DREAD (Damage Potential, Reproducibility, Exploitability, Affected, Discoverability) and it is also another approach to assess threats.

STRIDE use the following stages in general.

Define > Diagram > Identify > Mitigate > Validate

For more information, please visit <https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling>

Trike

Trike is an open-source threat modeling tool developed in 2006. It uses threat modeling as a technique and is a security audit framework. The perspective of this tool is based on risk management, and it looks at threat modeling in a defensive approach. It is based on a requirement model. In 2006 the main goal was to improve the efficiency and effectiveness of the existing methodologies. Currently, there are three versions of this methodology. Since this is a complex process, it is not the intention of the book to go through the entire process. You can learn more by visiting <http://www.octotrike.org/>

VAST

VAST stands for Visual Agile and Simple Threat. It was developed based on a platform known as *ThreatModeler*, an automated platform. It is a highly scalable platform and adopted by large organizations. It helps to produce reliable and actionable results. VAST requires two types of models.

- Application threat model: This uses a process flow diagram, and it represents the architecture.

- Operational threat model: This is created based on the attacker's point of view.

VAST can be integrated into DevOps and other software development lifecycles.

Other Threat Modeling Tools

- Microsoft Threat Modeling Tool (2016):
<https://www.microsoft.com/en-us/download/details.aspx?id=49168>
- IriusRisk community and enterprise tool:
<https://iriusrisk.com/threat-modeling-tool/>
- Mozilla SeaSponge, a web-based threat modeling tool:
<https://github.com/mozilla/seasponge>
- OWASP Threat Dragon Project:
https://www.owasp.org/index.php/OWASP_Threat_Dragon
- SecuryCAD Vanguard, an automated threat modeling and attack simulation tool based on SaaS service. It is widely used with Amazon AWS. More information can be found at
<https://www.foreseeti.com/>

Each of these methodologies has pros and cons, and there is no specific model to address every aspect of an organization. Sometimes you may have to depend on one or more methodologies in collaboration.

Chapter Twelve

Apply Risk-Based Management Concepts to the Supply Chain

Risk management concepts are used whenever an organization deals with external parties relating to the supply chain. This includes contractors, suppliers, transportation services, and any other relevant party. When acquisitions and mergers occur, these concepts can be applied. From a different perspective, you may think of it as applying due diligence.

In this chapter, you will learn,

- Risks associated with hardware, software, and services.
- Third-party assessment and monitoring.
- Minimum security requirements.
- Service-level requirements.

Before applying the risk management concepts, you have to have a clear idea about the risks associated with the information technology assets.

Risks Associated with Hardware, Software, and Services

Information technology is driven mainly by hardware systems, including networking equipment, software and services associated. Any of these entities can have vulnerabilities hidden or known. Proper maintenance programs including testing, updating and upgrading, are required to mitigate the risks. If an organization purchases new hardware, software or services (especially third-party), it must have a good idea about the risk and attack surface these entities bring. In addition, if these entities violate laws, regulations and standards, the organization may end up in serious situations. If an entity violates a standard, you may lose interoperability as a result. Therefore, proper evaluation is required.

- Consider the following when evaluating the hardware: compatibility with an existing security program, integration, continuity, updates, and obsolescence.
- When purchasing software, there must be a proper framework to assess the architecture of security and compatibility. Since the software is used to run mission-critical services, vendors must provide appropriate Service Level Agreement (SLA) schemes. They must also have a proper update and upgrade programs to mitigate risks and to keep up with the technological changes (continuity).
- If the entity is a service, consider the following factors.
 - o The reputation of the company gained through providing services to similar business functions and organizations.
 - o If the company is providing services to your competitors.
 - o If they follow laws, regulations, and standards as you do in your organization and compatibility between these standards.
 - o If the company relies on third parties (e.g., cloud-based service infrastructures), to what degree the third-party services follow these standards and protocols.

Third-Party Assessment and Monitoring

If an organization decides to hire third-party services, it must consider the following facts carefully.

- Non-disclosure agreements.
- Privacy agreements.
- Security agreements.
- Service level agreements (SLAs).

These must be thoroughly reviewed before proceeding to a purchasing or hiring decision. Upon review, you have to match the requirements to your

organizational security architecture, policies - compliance, standards, integration and interoperability.

Minimum Security Requirements

In a requirement specification, you must have minimum security requirements. This acts as a baseline security and compliance filter. It is very useful in important events such as a merger or an acquisition and during the procurement process. Having minimum security requirements helps to avoid security gaps, conflicts and to decide on security measures. It is important to review these requirements periodically and set expiration periods for instance, quarterly reviews and expiration in 12 months, followed by an annual review.

If there is a transition period during a merger/acquisition, the same process is applied. Within this period, assessments required in the following areas.

- Architecture.
- Configuration.
- Procedures.
- Best practices.

The appropriate changes and adjustments must be made and shall meet the new requirements.

Service-Level Requirements

Service level agreement works mainly as a performance measure, and it is used with key performance indicators. Organizations have the responsibility to monitor performance and they have to serve the clients within a given frame so that they meet the expected performance. This is the main purpose of service level agreements.

Among the agreements, an organization makes with vendors and service providers, Service Level Agreements (known as SLA) is extremely important. SLAs provide a guarantee of service in a timely manner, including incident responses. In other words, it serves as a guarantee of performance. There are internal and external SLAs. An organization itself

provides such agreements to their customers, and especially they provide information technology and other time-sensitive, mission-critical services. There can be external SLAs with vendors and service providers that the organization depends on. Other than SLAs, there are operating level agreements (OLA) and Underpinning Contracts (UC). No matter what the classification is, they must maximize performance while keeping the costs low.

Service Level Agreements

These are external agreements, as stated previously, in most cases — an agreement between a service provider and a client. SLA tracks the performance against commitment to the customer according to the SLA. An agreement can have one or more service tags. These tags can define rewards and penalties respectively, for meeting the goals, exceeding expectations, or addressing compliance issues that violate the agreement.

Operational Level Agreements

These are internal agreements and defined for internal users so that they can meet SLAs. Like SLAs, OLAs may contain one or more service tags. The tags can be used to track internal commitments.

Underpinning Contracts

This is a type of an agreement to track performance between a vendor and an external service provider.

If you are familiar with ITIL or ITSM, you must have a good idea about OLAs. In this case, it represents a relationship between an information technology service provider and another information technology organization. It includes operational relationships between,

- Operations Management.
- Network administration.
- Incident management.
- Support groups.

- Service desks.

These relationships are documented and secure by the service manager. The most basic OLA is also a document and works as a matter of record between relevant parties. The document includes the following parts.

- An overview.
- Responsible parties and stakeholders.
- Services and charges.
- Operating hours, response times, and escalation policies. This covers requests such as work and service requests, incident and problem management. It also includes maintenance and change management and exceptions.
- Reporting and reviewing.
- Auditing.
- Service level agreement mandates (for OLAs). OLA implementation requires precision, attention to detail, and awareness of how the OLA tallies with the SLA.





SLAs and OLAs must have realistic values, derived by analyzing and monitoring performance statistics. These performance statistics are used to derive key performance indicators. If we take a look at the structure of SLA/OLA, there can be several levels. The levels are based on the priorities of the customers and the performance requirements they need. For instance, IaaS, PaaS, and SaaS services provide several subscription levels. SLAs are used to measure performance when serving the pro or enterprise subscribers in many cases.

The basic structure of an SLA includes the following:

- A master service agreement (MSA).
- Service level agreements (SLAs) and key performance indicators (KPIs) to measure the performance using performance metrics agreed upon.

- Operational level agreements (OLAs).

When implementing an SLA, an organization must understand its capabilities and analyze the performance requirements expected by the customers. In other words, an SLA must satisfy the business requirements of the customers. Both parties must be aware of the SLA in action when the customer is served. The following is a general service level agreement followed by a web conferencing provider.

Priority	Respond within	Resolve within	Operational Hrs	Escalation email
Urgent	1 Hrs ▼	4 Hrs ▼	Business Hours ▼	
High	4 Hrs ▼	12 Hrs ▼	Business Hours ▼	
Medium	8 Hrs ▼	1 Days ▼	Business Hours ▼	
Low	1 Days ▼	3 Days ▼	Business Hours ▼	

The urgent priority is provided to the enterprise subscribers. High priority is provided to pro subscribers. Medium is provided to the customers of subscribers, and the lowest is for feedback purposes.

Chapter Thirteen

Establish and Maintain a Security Awareness, Education, and Training Program

This is the final chapter of this book, and yet one of the most important topics is discussed here. The number one success factor of any program in an organization is making awareness. Without proper knowledge and understanding of the current proceedings, any program does not make sense. Therefore, training and education become key success factors. The content must be easy to understand, engaging and comprehensive. In addition, the content must be reviewed continuously to make improvements. It must be evaluated periodically for effectiveness.

In this chapter, you will learn,

- Methods and techniques to present awareness and training.
- Periodic content reviews.
- Program effectiveness evaluation.

As previously stated, there is a weak link in any information security and risk management program. That is none other than humans. Unaware, uneducated, untrained staff and users can lead an organization to disastrous situations. Failures with compliance with the law, regulations, and standards, failures of ethical practices, mistakes, and abuse of assets are the potential actions these individuals may commit. Therefore, communication of a security program is the most crucial and important part that comes after implementing a successful security and risk management program.

The training can be started from basic awareness and develop the staff toward awareness of information security basic, awareness of risks, threats and vulnerabilities, and ethical requirements. Later they can be trained with more advanced goals such as compliance and standardization. A successful training program is always beyond text and documentation. It must be more engaging and the key players such as CEO, director board, and senior

management must involve so that they can bring inspiration and motivation throughout the program. A successful program evaluates the employee skills, train them toward professional goals beyond the basics, reward the talented and make them carry out the program to the next level.

A training program may consist of reading guides (online/offline), learning processes and procedures, watching videos, walkthroughs, learning more technical content through seminars, webinars, gaming and competitions, and certification and reward programs to assure the education as well as the motivation.

Methods and Techniques to Present Awareness and Training

There are two issues when it comes to such programs. One is the belief of the seniors or the overconfidence in other words about the workers. They may assume that users are already aware, and they should become aware of themselves, even without a successful training program present. The other is the overconfidence of employees. Many of them assume they know everything because they simply watched something related or read things in a blog or on Facebook. Both the assumptions bring chaos. Therefore, a proper evaluation of the degree of awareness is the first step. Then it can be addressed through a training program geared for the need.

The security team should have confidence in their understanding of the organizational security program, risk management, and business continuity program and they should have the ability to distribute their awareness to others. At this point, they can train the key roles in an organization such as non-technical senior management and executives. They must have a solid understanding of segments relating to their area of expertise and become aware of the program, organizational compliance, policies, standards, baselines, procedures and guidelines because they have a responsibility to educate their departments, groups, and the rest.

An awareness program requires to satisfy the following requirements to reach its goal toward success.

- The engagement of CEO and senior management is a major requirement because decisions, design, and funding must come from

the top. The design and presentation of the program are the responsibility of senior management.

- The program should display clear objectives and a vision toward success.
- It must clearly demonstrate the benefits it provides to employees and their business functions.
- The approach must be bottom-up, and it should start from basics and developed toward specific technical and business goals.
- The training program should be more engaging and live. It has to be enjoyable and a place where people share knowledge, in a friendly manner. If the program is too technical, boring, and tough; it may not go through the psychological barriers of the staff.
- Training such as workshops should provide decent challenges and competitions so that teamwork and trust can be built upon.
- There have to be tests to measure and review the outcome. It can be a specific test in a controlled environment or an ad-hoc test during work.
- The training content must be reviewed at least per three months, for instance, and update the content to gap new technological and business objectives, and changes.
- It is always better to have an in-house testing and certification program in parallel so that the staff and stakeholders can test their skills against professional examinations and obtain certification. This is the method to motivate the staff to keep their standards up and exercise continuous improvement.

Periodic Content Reviews

As stated in the previous section, the program itself has to achieve the goal, continuous improvement. Periodic content review by senior management, business executives, legal and psychological consultants within the team, or even from outside can enhance the program to shape the people and meet business objectives. The program requires certain dedicated professionals to

work on monitoring and evaluating the content continuously. Especially when there are changes, during the change management process, it must be communicated and gear the staff to adopt the changes. For instance, if an organization has to be compliant with new legislation, or if they experienced a breach and new security measures are in place, the training program has to be able to initiate new training programs and also keep the content up to date with the process.

The training content may include engaging presentations, speeches (especially from the top as those can heavily inspire and influence), video content, blog, tests, and even social networks. Social networks can be used to organize events and campaigns as they become more and more compelling. To measure the requirements such as changing content, remove obsolete content and adding new content may require approval from the boards especially when there are strategic changes and compliance requirements.

The trainers can conduct ad-hoc tests and simulations to get an idea of how effective the content is. This gives a perspective on the effectiveness of the content, what is not understood, what requires a more friendly approach, and what new changes have to be introduced. There are many technologies and tools to make this a reality.

Program Effectiveness Evaluation

Effectiveness assures the budget allocated for training is worthy and provides a good return on investment. It also stands as the performance indicator. If the program is effective, it saves costs as it leads to mitigation of risks; good business practices can increase productivity thus making the security, risk and business continuity programs successful beyond the expectation.

To measure the effectiveness, there must be an evaluation and mathematical structure. To satisfy these requirements, the seniors who manage the training program have to implement a performance measuring system. It can have key performance metrics just like the SLAs. Once the metrics are in place, they can evaluate it by running tests. If the outcome of tests indicates positive results, or acceptable results, the training program has a positive effect on staff and is effective.

For instance, the team can run ad-hoc tests, surveys, or group-based tests focusing on scamming. The outcome can be documented. Then they can deliver an awareness program on scamming followed by another series of ad-hoc tests on individuals or groups. If the vulnerability rate is sufficiently lower than the previous test (before the training program), then the training was effective. Next, they can deliver periodic evaluations and see if the rate is stable. Then they can make educated guesses about when another training is required and what has to be updated or changed.

A training program does not have to be 100% perfect. It, however, should make a positive and lasting impact and inspiration, leading the organization toward its business objectives and goals while ensuring security, compliance, risk mitigation and business continuity.

Conclusion

I hope you have gained basic to comprehensive knowledge in CISSP Domain 1 - Security and Risk Management by reading this book. This is just one step to CISSP examination and eight domains. You have just begun the journey, and therefore, I recommend you to go through all the available resources that you can grab. Do read, exercise, learn through experiments and gain work experience along with the studies if you are already an intern or a professional. At the end of this book, you should be able to think and apply your knowledge at an organizational level to shape the risk management process.

If you are getting ready for the CISSP examination, please do make a plan and learn at your phase. The CISSP certification is a remarkable achievement. Therefore, consider this as a challenge of your lifetime. It is a challenging exam that aims to test your knowledge as well as practice and experience. Once you complete all the domains, you have to register for the examination at least two months earlier. Study hard, and take your time before you register for the exam. It is always best to go through past papers, questions and use exam simulators to test your skills and expertise. If you are ready, you can find more information about the examination by following the link below.

<https://www.isc2.org/Certifications/CISSP>

If you wish to obtain the Flash Cards, you can do it by navigating to <https://enroll.isc2.org/product?catalog=CISSP-FC>

When you study, do not forget to join a CISSP study group. There are many communities and platforms to help you with this journey. In these communities, you will find much useful information, experts, technical skills, and a great community as a whole which has a common interest in information security.

If you think about more training, I would like to recommend taking a video course, workshops, and webinars. You will be able to collect an extensive amount of useful information from these. To test yourself, use practice tests

and exam simulations. You may also find past CISSP exam questions and answers on the internet.

Finally, if you are about to sit for the exam, remember, it is 3 hours long. So you must get a good rest, a good night sleep before you go. Have a good meal, take snacks, and enough hydration with you. You can consume these during a break. Do not forget to bring your registration information, printed material, your NIC, some emergency medicine, etc. It is also good if you dress comfortably and arrive early. You can leave your mobile device and other irrelevant things before you arrive. During the examination, take sufficient breaks and keep yourself energized and hydrated.

If you find this book useful, do not hesitate to leave comments or critics. I would like to hear it from you and appreciate your feedback very much!

References

- <https://www.isc2.org/Certifications/CISSP>
- <https://www.isc2.org/Certifications/Ultimate-Guides/CISSP/>
- <https://www.isc2.org/Certifications/CISSP/experience-requirements>
- <http://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=4>
- <https://learning.oreilly.com/library/view/isc2-ciissp-certified/9781119475934/c02.xhtml>
- [https://www.payscale.com/research/US/Certification=Certified_Information_Systems_Security_Professional_\(CISSP\)/Salary](https://www.payscale.com/research/US/Certification=Certified_Information_Systems_Security_Professional_(CISSP)/Salary)
- <https://www.simplilearn.com/average-annual-salary-of-a-ciissp-certified-professional-article>
- <https://www.dummies.com/programming/certification/privacy-requirements-compliance-ciissp-exam/>
- <https://www.dummies.com/programming/certification/ability-identify-threats-vulnerabilities-ciissp-exam/>
- <https://resources.infosecinstitute.com/category/certifications-training/ciissp/domains/security-and-risk-management/>

CISSP

*Simple and Effective Strategies to Learn the
Fundamentals of Information Security
Systems for CISSP Exam*

DANIEL JONES

Introduction

The book “CISSP: Simple and Effective Strategies to Learn the Fundamentals of Information Security for CISSP Exam” contains all the necessary topics and concepts that a CISSP candidate should know. These concepts have been detailed down to their fundamental levels, making them neither too complex nor too puzzling to absorb. The topics have been provisioned in such a way that each topic implements the concepts outlined in the preceding section, and each chapter is designed to make sure that the candidate has ample content to absorb, even if they are just the fundamentals.

From starting with a quick refresher of some familiar theories, to venturing towards the outer boundaries of information security ,and giving a general, yet an informative outline of encryption and decryption of message transmission over a network, the book features all the important concepts. It addresses the major difficulties a candidate faces when preparing for the CISSP exam.

Similarly, this book is designed to allow the reader to capitalize more on their time rather than going through every topic they read. It’s written to be easy to absorb and simple to understand by breaking down complex concepts to their fundamental counterparts and then gradually bringing them together again to recreate the picture of what was once a compounded concept to a comprehensible concept.

Chapter 1

Security and Risk Management

In this chapter, we will quickly refresh some fundamental concepts and guide you in changing your approach and mindset towards the CISSP Exam and your active role in the Information Security System.

Maintaining Confidentiality and Various Requirements

Confidentiality : The case in which the information is distributed among the specific people you intend to share it with. During the process of sharing or storing the data, it should be protected using appropriate measures.

Requirements for confidentiality are:

- To prevent the PII/PHI from being disclosed, it should be protected using approved algorithms.
- The sensitive fields like passwords and codes should be concealed for protection.
- A password or code must not be kept in cleartext.
- In the case of transferring information that is considered sensitive, TLS should be used for a protected transmission.
- Unsecure transfer protocols like FTP should not be used for the transmission of sensitive information.
- The sensitive information should not be stored in insecure places such as log files.

System Integrity and Availability

Integrity: It is the prevention of changing of data due to modifications of system or software. The system should perform its functions as expected.

- Harmful and malicious code injection techniques can modify the database and make it vulnerable.
- The input validation is the proper testing of input, which is a mitigation technique.
- The accuracy and reliability of the data are confirmed in Data integrity.
- CRCs (Cyclic redundancy check), message digests, checksums, Hashes, MACs.
- Internal and external consistency.

Following are some of the integrity requirements:

- The use of the input validation technique is important as it can prevent the data control language from being entered and also can be used to enforce the data types and field sizes.
- A message-digest should be available with published software so that the user can check if the software is complete and accurate.
- The subjects should not be allowed to modify the data except the case where they are given explicit permission.

Availability : The data which is required must be available for access at all times.

The Metrics used in the availability of the data are:

- MTD/RPO/RTO.
- SLAs.
- MTBF/MTTR.

Availability has the following requirements:

- It is specified in SLAs that the software in consideration should satisfy the availability requirement of 99.999%.

- The software is required to provide support of access to at least 200 users simultaneously.
- The software must be able to provide support to the process of replication and offer load balancing to the users.
- Restoration of the software's Mission Critical Functions to normal operations should be completed within 30 minutes.

Identification: The user should be identified distinctively.

Authentication: The user's claim of identity should be checked for validity.

Authorization: After authentication, the entity or user is checked for necessary permissions and privileges.

Auditing: The application or system should have any of its activity audited, which is the inspection of technical issues or breaches.

Accountability: An action performed is traced back to the subject.

Enhancing Security and Designating the Roles

1. **Senior manager:** They are in charge of planning and directing the work of the most important group. They monitor the work being done and take counteractive actions wherever necessary.
2. **Security professional:** The information security team is responsible for protecting sensitive information.
3. **Data owner:** They are accountable for the data assets and classifies the data.
4. **Data custodian:** They perform day-to-day backups and ensure the safe custody, transfer, and storage of data.
5. **User:** The end-user is ultimately required to use the product.
6. **Auditor:** They are in charge of reviewing the data to ensure the accuracy and validity of the said data sample.

Regarding the role of entities involved in the area of Control Frameworks, we will talk about some of them briefly;

COBIT/COSO - They provide the framework and goals. COSO is an acronym for The Committee of Sponsoring Organizations, and COBIT is an acronym for Control Objectives for Information and Related Technologies. Their primary function is to assist the companies in organizing and monitoring controls of financial reports.

ITIL - It provides an idea of how to achieve those goals.

Due care - The role of prudence and conducting oneself morally.

Due diligence - To exercise those activities which will facilitate others in the maintenance of “due care.”

Security Policy - It is the mandatory document that specifies the security range, which is necessary for an organization.

Standards - These are the compulsory requirements for organization security.

Baseline - The minimum security requirements for an organization are called the baselines.

Guidelines - The guidelines give the idea as to how the standards and baselines are executed. These guidelines are provided as an optional function.

Procedure - The procedure is a step-by-step file containing instructions for maintenance of integrity and accuracy of the business.

Identifying and Assessing Threats and Risks

Now that we have become familiar with the importance that information security systems hold in an organization that primarily handles digital data, we can move forward and discuss how we can effectively identify threats and assess the potential risks that they pose.

Threat Modeling

The process, in which prospective risks like malware, viruses, etc. are identified, grouped into categories, and then thoroughly analyzed, is called threat modeling.

The process of threat modeling is further classified based on the stage where the code is currently at, i.e., still under development or after being completely developed (finished product). The techniques used for such situations respectively are:

Proactive Measure : The proactive technique is used during the design and development process.

Reactive Measure : Such measures are taken after the product is completed and deployed.

The goal of threat modeling is basically to:

- a) Decrease the number of designs related to security and eliminate coding defects as much as possible.
- b) Reduce the severity of any defects that may remain after the product is completed.

Threats most commonly target the following areas in an information security system:

1. Assets: The threats focused on important and valuable assets should be identified.
2. Attackers: There is a need to identify the prospective attackers on the valuable data and what they are aiming for.
3. Software: There may be potential security risk regarding the developed or completed software which needs to be identified.

Below are some examples of popular threat models:

STRIDE Model – It is a threat model developed by Microsoft, which withholds the purpose of examining the variety of compromise concerns.

S – Spoofing

T - Tampering

R – Repudiation

I - Information Disclosure

D - Denial of Service

E - Elevation of privileges

DREAD Model – This threat model was developed to perform the function of analyzing five main questions on the basis of which a flexible rating solution is obtained. These questions are:

D - Damage potential (How heavy the damage can be if the threat attacks)

R - Reproducibility (How easy or complicated will it be for the exploit to be reproduced by the attacker)

E - Exploitability (How much work is done in launching the attack)

A - Affected users (The number of users that will be impacted by this threat)

D - Discoverability (How hard it is to discover the threat and weakness)

Risk Terminology

Asset valuation - How much value an asset has

Risk - The probability that a threat will find a vulnerable asset and exploit the valuable data.

Threat - A harmful bug that can utilize an asset and damage it.

Vulnerability - It means weakness or a lack of defense against a threat.

Exploit - Unfairly use something; Instance of compromise

Controls - These are the protective measures or mechanisms which are used to secure vulnerabilities.

Countermeasure - Reactive measure which is put to use after being deployed

Total risk - The extent of risk or threat experienced before a protection mechanism is executed.

Secondary risk - The type of risk created in response to another risk.

Residual risk - After a risk response is completed, the total amount of risk left behind is the residual risk.

Fallback plan - A backup plan in case the first method does not succeed; in other words, “Plan B.”

Workaround - It is the response that is not planned in case the usual response does not work, or an unknown risk appears.

Risk Management

After assessing the possible threats and risks through which the security of the information system can be exploited, we will now discuss key points that will help us manage the posed risk.

- Risk assessment- The assets, threats, and vulnerabilities are recognized and categorized.
 - a) Quantitative: It is focused on analyzing the time and cost-effectiveness of the risks on the projects.
 - b) Qualitative: It is focused on evaluating the likelihood and influence of the risks.
- Risk Analysis- The total value of the prospective risks is calculated. They can be calculated by the formulas of ALE (Annualized loss expectancy) and SLE (Single loss expectancy).

$$SLE = AV * EF$$

ARO = Annual rate of occurrence

$$ALE = SLE * ARO$$

- Risk mitigation- It is the response to the risks by reducing the negative effects of the threats.
- Risk monitoring- It is an ongoing process of identifying new risks and managing them because they can appear at any time.

Cost/Benefit Analysis

The countermeasure that is taken for ALE to reduce the potential loss is basically the cost/benefit analysis. Its formula is written as:

$ALE \text{ before safeguard} - ALE \text{ after implementing safeguard} - \text{Annual cost of safeguard} = \text{Value of the safeguard to company.}$

Risk Treatment: It is the process in which certain measures are selected and executed to modify the risk. The methods used to manage risk are MART

M – Mitigate

A – Accept

R – Reject

T – Transfer

Controls

Security controls are safeguards that protect assets and computer systems from risks.

They are classified as:

Control Types

- Technical
- Administrative
- Physical

Control Functions

- Preventive – The preventive measure is taken to deter attacks and protect against collusion.
- Detective – These controls locate problems within a company's working and prevent unfair dealings like a fraud.
- Corrective – Back-ups of information and system are used to restore the resources after the damage caused by an unwanted attack.

Assess Controls

They include the Control functions and following controls:

- Directive – The security policy that encourages the manifestation of required action.
- Deterrent – A warning sign that delays or discourages the attacker, e.g., Dogs.
- Compensating – It is an alternate control that is used in place of a security measure too difficult to implement.
- Recovery – These controls restore back-ups of information and system after an action is performed.

Documentation review: In this process, the information exchanged in dealings like business is read and reviewed by validating it against the standards and expectations.

Risk Management Framework

It is an organized process in which the potential risks are identified, and strategies are put together to eliminate them.

C – Categorize the information system

S – Select suitable security controls

I – Implement the selected controls

A – Assess the security controls

A – Authorize the information system

M – Monitor the performance of the security controls

Business Continuity Management (BCM)

Business Continuity Planning: The type of planning where systems related to prevention and restoration are produced to counter the potential threats and attacks.

- Business Organization Analysis – It is an analysis of the workings of a business organization to develop a plan to improve the performance.
- BCP team – A skilled team that can work together effectively in times of crisis is necessary.
- Validate BOA
- Business Impact Analysis (BIA) – The analysis that is performed to evaluate the potential effects on business operations when a threat is realized.
- Continuity Planning – The planning makes sure that the organization can continue its operations even in the event of a disaster.
- Approval and implementation – The plan is then approved after examination and implemented when necessary.
- Maintenance – The BCP should be maintained and constantly improved.

Disaster Recovery

- Critical systems
- MTD, RTO, RPO

- Offsite selection
- Recovery of critical system
- Normal systems
- Get back to the primary site

Process and Planning

- Business Organization Analysis
- BCP team selection
- Validates BOA
- Resource requirement
- A legal and regulatory requirement

Business Impact Analysis

- Identify Assets and value
- Risk Identification (Threats)
- Likelihood estimation (ARO)
- Impact Assessment (Exposure Factor)
- Resource Prioritization (Analysis)

Continuity Planning

- Strategy planning - bridges gap between BIA and Continuity planning
- Provision and process - people, buildings & infrastructure (Meat of BCP)
- Plan Approval – (Senior management support and approval: Very important)
- Plan implementation

- Training and Education

BCP Documentation

- Continuity plan goals
- Statement of importance
- Statement of priorities
- Statement of organization responsibility
- Statement of urgency and timing
- Risk assessment
- Risk acceptance/mitigation

The primary focus of this chapter is to refresh your memory of the concepts which you have come across and studied while preparing for the CISSP Exam. The preceding chapters will be focused on more detailed concepts about Information Security Systems.

Chapter 2

Telecommunication and Network Security

Data networks can be categorized into two types according to the geographical areas these networks covers. These types are Local Area Network (LAN) and Wide Area Network (WAN).

Local Area Network (LAN)

The type of data network that covers a small geographical part and operates in that limited area, such as any floor of a building or the whole building, is referred to as Local Area Network (LAN). The main function of LAN is to interconnect servers, workstations, printers, and various other devices to allow the sharing of resources such as files and e-mails. Some important characteristics of LAN are mentioned below:

- Network resources can be connected and shared among devices over a limited geographical area, which could span up to a single floor, a whole building, or a group of buildings.
- Compared to other means, LAN is both economical to set up and easier to maintain. This is because the equipment required to set up LAN is easily available, which includes servers, client workstations, printers, switches, bridges, hubs, repeaters, wireless access points (WAPs), and several security devices.
- LAN can be set up in the form of wired connections or can even be wireless. An arrangement of both wired and wireless can be used as well.
- Such network type works at high speed when compared to alternative means. For wired connections, the speed is usually 10 megabits per second (Mbps) and can also be as much as 100 Mbps or 1000 Mbps, which can also be referred to as 1 gigabit per second (Gbps). In the case of wireless networks, the speed

is typically 11 or 54 Mbps. When even higher speed is needed, as in Storage Area Networks (SANs) and high-performance data centers, then LAN with speed of 10 Gbps is also available.

When mentioning the data storage or data speed, it is important to use the correct expression for them. The data speed is referred to in bits per second as is 100 megabits per second (Mbps), while the data storage uses the term bytes such as 100 megabytes (MB). Both of the abbreviations have a small difference of just one “small b” and “capital B,” but they are different as a byte is equal to 8 bits.

LAN also has a function in two of the layers of the OSI model, referred to as the Data link layer and the Physical layer.

Wide Area Network (WAN)

Wide Area Network (WAN) is the type of data network which operates in a large geographical area and connects numerous LANs and other WANs as well. This internetwork is formed with the help of telecommunication devices. Some important characteristics of WAN are:

- Multiple LANs can be connected with each other with the help of WAN. The connections can be spread over a large geographical area such as small cities (Metropolitan Area Network MAN), regions, countries, a global corporate network, the entire planet(the internet), or even beyond that in the International Space Station, which is accomplished through satellites.
- Setting up a network like WAN is comparatively expensive as it is wide-scale. The network connections include equipment like routers, Channel service unit(CSU) and Data service unit (DSU) devices, firewalls, Virtual private networks (VPNs) concentrators, and many security devices.
- WAN connections work at low speed with the assistance of various devices and technologies. These devices include a Dial-up which performs with a speed of kilobits per second (Kbps); a Digital Subscriber Line (DSL) working with 128 Kbps or 3

Mbps speed; T-1 with a speed of 1.544 Mbps; a DS-3 of speed 45 Mbps; OC-12 and OC-255 with 622 Mbps and 13 Gbps speed respectively.

Example of WAN are mentioned below:

Internet: The most important type of WAN is the Internet, which is a world-wide or global network that interlinks public networks and establishes a connection between the whole world. It was developed by the U.S. Department of Defense (DoD) Advanced Research Projects Agency (ARPA). Connection to the internet is provided to the users and systems by means of Internet Service Providers (ISPs).

Intranet: An intranet functions as a private internet limited to an organization or company. The authorized users, such as a company's employees, can access the information available on the company network via web-based technologies of the intranet. The information contained on the network can only be accessed by users that are authorized.

Extranet: An extension of the intranet to provide limited access to the company's information to vendors, business partners, and other relevant parties. An example of this can be given through an automobile manufacturer who may use an extranet and connect to outside business partners such as parts manufacturers, distributors, and dealerships. Extranets are typically operated via the internet by using a Virtual Private Network (VPN) and other protected connections to avoid leakage of sensitive information.

OSI Reference Model

To enable a connection and interoperability between the network devices without the assistance of the manufacturer, a model was designed by the International Organization for Standardization (ISO) in 1984. This model is called the Open Systems Interconnection (OSI) Reference Model, which is simply referred to as the OSI model. This model uses a layered methodology to set up standard protocols for communication and interoperability between the network devices. The OSI model approach is useful in the way that it simplifies the complex networking problems into

functional components whose design and development are relatively easier to understand. It provides the following advantages:

- It avoids paying particular attention to the specific issues and instead focuses on the general functions of the process of communication.
- With the help of this model, the complex and compound process of the communication between the network devices is simplified into sub-layers and smaller components.
- It supports the interoperability between the layers by defining standard interfaces.
- It helps the vendors with the development process when they want to change a specific feature of a single layer. In this case, they don't have to rebuild the whole protocol stack and can just alter that specific feature.
- OSI model allows troubleshooting to become easier and more logical.

There are a total of seven different layers in the OSI model which define the data communication process between applications and systems available on a computer network. These layers are as follows:

- Application – Layer 7
- Presentation – Layer 6
- Session – Layer 5
- Transport – Layer 4
- Network – Layer 3
- Data Link – Layer 2
- Physical – Layer 1

In the OSI model, data travels starting from the highest layer, which is the application layer (layer 7), and passes downward through layer until it

reaches the lowest layer of the Physical layer (Layer 1). From the Physical layer, it is transferred across the network medium to the end node of another medium, where it travels upwards from the lowest layer to the highest. The communication of each layer is limited to their adjacent layers, which are the layers directly above or below them. The process of Data Encapsulation is used for this communication, where the protocol information from the above layer is wrapped in the data section of the layer below.

The First Layer: Physical Layer

The physical layer is comprised of physical materials such as copper wires, fiber-optic cables, and hubs. Bits are exchanged back and forth between devices via the network cabling. Physical layer deals with the mechanical, electrical, and functional requirements pertaining to the network. These requirements include the network topologies, connectors, cabling, interface types, and the function of converting bits to electrical or light signals and vice versa. The network topologies are constructed with the help of copper or fiber-optic cables.

Network Topologies

Network topologies consist of four basic and common types which are named as:

- Bus topology
- Star topology
- Ring topology
- Mesh topology

These basic types have further variations, such as the Fiber Distributed Data Interface (FDDI), star-bus, star-ring, etc.

Star

Star topology is the type of network topology in which each of the individual network devices or nodes is directly connected to a central

device called a hub, switch, or concentrator. The central hub or switch is the single point of failure or a bottleneck, which establishes a point-to-point connection with each node, and all the data communications pass through it. Due to its ideal feasibility in an environment of any size, it is the most commonly used basic topology presently. Other advantages of star topology include easy installation and maintenance, and the faults in the network as easily discovered and dealt with in isolation without affecting the rest of the network.

Mesh

The mesh topology has all of its devices or systems interconnected, which leads to the provision of many paths for the transmission of resources. In such topology, even if the link between two routers is damaged, the resources can still be transmitted between the two specific devices via other links and devices, as can be seen in the figure.

The mesh topology is used as a partial mesh in most networks only for the most critical parts of the network, such as the routers, switch, or hub, and is accomplished by the use of various Network Interface Cards (NICs) or server clustering. This is done so that the single points of failure can be eliminated and communications will not be interrupted even if one device server fails.

Ring

In a ring topology, the data is transmitted among the devices in a circular ring as the end devices are connected to each other in the form of a closed-loop. This type of topology bears a resemblance to the star topology in terms of physical appearance. Its functionality depends on the fact that the individual devices are linked with the Multistation Access Unit (MSAU/MAU).

The ring topology is commonly used in networks such as the token-ring and FDDI networks. The data communication in the ring topology is transmitted in a single direction around the ring.

Bus

The bus or linear bus topology uses a trunk or a backbone, which is a single cable to which all the end devices are connected, and this cable is terminated on both ends. Bus topologies are advantageous for use in very small networks because they are inexpensive and easy to install. But they are not feasible in large networks because of physical limitations; its backbone is a single point of failure, which means damage on any point of it will result in the failure of the entire network. Also, if a fault occurs in a large bus topology network, tracing it would be extremely difficult. Nowadays, bus networks are rarely used because they are no longer the cheapest and easiest-to-install network topology.

Cable and Connector Types

Data is transferred among various devices with the help of cables and connectors, in which the data is carried in the form of electrical or light signals. There are quite a few characteristics regarding data signaling, such as:

- Types of data signaling (Analog or digital signaling)
- Control mechanism (Asynchronous and synchronous communications)
- Classification (Baseband and broadband)

The data signals in baseband signaling are transmitted across a single channel, and this type of signaling is commonly used in LANs where twisted-pair cabling is utilized. While in broadband signaling, analog signals are transferred using multiple channels over a range of frequencies, and these signals may be in the form of voice, video, or data. In data networks, four basic types of cables are used which include coaxial, twinaxial, twisted-pair, and fiber-optic cables.

Coaxial Cable

Coaxial or coax cables were used in the early days when LAN was developed and is being brought back to use as the broadband networks are emerging. This type of cable is made up of a single core of solid copper wire, which is enclosed by a Teflon or plastic insulator, a metal foil wrap, or a braided metal shielding. The insulator or wrap is then covered by a sheath

made of plastic. Due to this construction, the coax cable is very tough, durable, and resistant to stray signals like Electromagnetic Interference (EMI) or Radio Frequency Interference (RFI) signals. The cables or satellite television receivers commonly use the coax cabling.

Coax cables can be divided into two types:

- **Thick:** This type of coax cable is referred to as RG8, RG11, or thicknet. A screw-type connector, also called the Attachment Unit Interface (AUI), is used in the Thicknet cables.
- **Thin:** This coax cable is also called the RG58 or thinnet. This thinnet cable uses a bayonet-type connector, also known as Bayonet Neill-Concelman (BNC) connector, to connect to the network devices.

Twinaxial Cable

The twinaxial or twinax cables bear a similarity with the coax cables with the exception that there are two cores of solid copper-wire in the twinax cable while there is only one core in the coax cable. The function of twinax is to transmit data at very high speed (e.g., 10 GB Ethernet) over short distances (e.g., 10 meters) at a relatively low cost. The Twinax cabling is used in networks like SANs and top-of-rack network switches, where the critical servers are linked to the high-speed cores. Some other advantageous features of Twinax cables are the lower transceiver latency, power consumption, and low bit error ratios.

Twisted-Pair Cables

The twisted-pair cables are light in weight, cheap, flexible, and easy to install and so they are the most commonly used cables in LAN these days. The telephone wire that is commonly seen is an example of a twisted-pair cable. A total of four copper-wire pairs are twisted together inside the twisted-pair cable so that the crosstalk and attenuation can be decreased, which in turn improves the transmission quality. Crosstalk is the negative interference of a signal traveling in one channel with the signal in another channel, which can result in parts of another conversation being heard over the phone. Attenuation occurs when the data wave traveling over a medium eventually loses its intensity.

Out of the ten categories of twisted-pair cables, only four are considered as the standards by the TIA/EIA. These four categories are Cat 3, Cat 5e, Cat 6, and Cat 6a, which are being used for present-day networking.

There are two types of twisted-pair cables in use, which are the unshielded twisted-pair cables (UTP) and the shielded twisted-pair cables (STP). UTP is the cable that is in common use due to being cheaper and easier to work with, while the STP is used in specific circumstances such as the need for security or noise problem. The noise problem can be caused by electric motors, microwave ovens, fluorescent lights, etc., which emit RFI and EMI. Electromagnetic emissions by an attacker are intercepted by STP as well.

In U.S. military terms, the study of electromagnetic emissions coming from devices like computers is called TEMPEST.

Fiber-Optic Cable

The most expensive yet most reliable form of data cabling is the fiber-optic cabling, and it is commonly used in the high-availability networks like FDDI and backbone networks. In these types of cables, the data is carried in the form of light signals instead of the typical electrical signals. These signals are carried by the fiber-optic cable consisting of glass core, a glass insulator, Kevlar fiber strands, and a Teflon outer sheath. The transmission speed of data on fiber-optic cables is very high and can travel long distances while being resistant to interception and interference. The cable is terminated with a connector SC-type, ST-type or LC-type)

The Ethernet terms are used to define the transmission speed and the signaling type, where the last part is less defined as it may be referring to the approximate length, the connector type, or the type and speed of the connector.

Interface Types

The first physical layer specifies the interface between the Data Terminal Equipment (DTE) and the Data Communication Equipment (DCE).

Some of the common interface standards that should be remembered for CISSP examination are:

- EIA/TIA-232
- EIA/TIA-449
- V.24. CCITT
- V.35. CCITT
- X.21bis. CCITT
- High-Speed Serial Interface (HSSI)

Networking Equipment

The networking devices or equipment such as network interface cards (NICs), Network media, repeaters, and hubs are all devices that function at the Physical layer of the OSI model.

NICs are basically devices that link the computer to the network. They are present either as an integration on the computer motherboard or installed as an adapter card (e.g., PC card). WIC (WAN interface card) is similar to the NIC and connects the router to the digital circuit. WICs may be present in the form of HWICs (High-speed WAN interface cards) or VWICs (Voice WAN interface cards).

A repeater is a simple device with its only functions being that it amplifies the incoming signal to its original intensity. It counters the problem of attenuation and enables one to extend the length of the cable segment.

A hub can be considered a central device that can link various devices of LAN, which can be servers or workstations. The passive hub is a basic type of hub in which the data are entering and exiting one or more ports is not amplified or regenerated. The active hub (multi-port repeater) is a combination of the passive hub and a repeater.

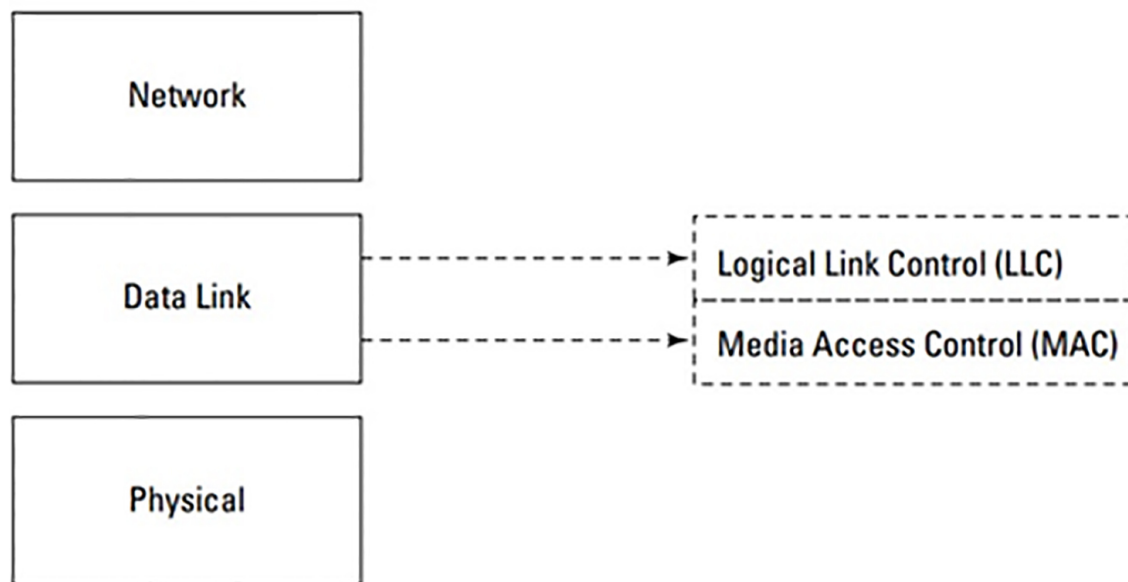
Like a hub, a switch connect many LAN devices together, but it only sends the outgoing packets to the actual destination devices instead of sending them to all the devices. The physical interface of the switch is defined at the physical layer, while its functions lie in the data link layer.

The Second Layer: Data Link Layer

The major focus and primary function of the Data Link Layer are to guarantee and make sure that a user-prompted message is sent to the intended device available on the physical network link. To elaborate this further, the working of the Data Link Layer defines the foundation of a “networking protocol,” such as the ones used in Ethernet (Quick Reminder! A networking protocol is a set of rules which two individual computers connected over a network follow to effectively communicate). In simple terms, the main job of the Data Link Layer is to:

- Intercept messages from layers that are above it and format them into frames so that they can be transmitted.
- Handle point-to-point synchronization
- Error Control
- Perform link encryption, if needed

This layer further consists of two sub-layers which are shown in the figure below:



As shown above, the two sub-layers are the LLC (Logical Link Control) and MAC (Media Access Control).

Each of these two sub-layers has their own specific jobs to perform.

Logical Link Control (LLC)

The chief functions of this sub-layer include:

1. Making use of the SSAPs (Source Service Access Points) and the DSAPs (Destination Service Access Points) to create a suitable interface for the Media Access Control sub-layer.
2. Oversee and supervise the network protocol steps through which the frames are transmitted either up to the Network Layer or down to the Physical Layer. This basically includes functions such as control, sequencing, and acknowledgment of the said frames.
3. Maintains and manages the flow control of the information along with its timing in such a way that the data being exchanged between two computers is steady. This means that if a computer that is receiving the data is not as fast as the computer sending the data, then the LLC manages the data flow so that the receiving computer is not overwhelmed.

Media Access Control (MAC)

Similar to the LLC, the Media Access Control sub-layer is also involved in framing. However, apart from that, the MAC sub-layer has the following main functions to perform:

1. **Managing Error Control:** The mechanism through which this task is done is through the use of a CRC (Cyclic Redundancy Check).
2. **Recognizing Hardware devices and MAC Addresses.** The MAC address is also known commonly as the device's unique physical identification. This address is encoded in 48-bit by the manufacturer in a way that the first 24 bits correlate to the manufacturer or vendor of the device while the last 24 bits are unique to the device.
3. **Mediates and controls the three basic types of Media Access types, which are namely, Contention, Token-passing, and**

Polling.

Protocols in Local Area Networks and the Transmission Methods

The protocols used commonly in Local Area Networks are known to be pertaining to both the Data Link and Physical Layer. Some of these common LAN protocols are explained below:

- **ARCnet:** This protocol is actually one of the oldest protocols developed and used in the early days of network communications utilizing the LAN technology. The transfer of data through the ARCnet protocol is achieved by making use of a media access method known as token-passing. The practical implementation of this method is done in a star topological system connected using the coaxial cable. The performance of this protocol is slow but predictable.
- **Ethernet:** This network protocol is probably the most familiar to the majority of the people as the go-to LAN protocol to use when connecting their PCs or Laptops to the internet through an internet router. The data transferred via this protocol to a physical local area network medium is achieved by using the CSMA/CD. The reason for using the CSMA/CD is because of the fact that they are basically designed to work for networks that observe heavy traffics. The speed of a typical Ethernet is about 10 Mbps, while a Fast Ethernet can reach transfer speeds of up to 100 Mbps, and a Gigabit Ethernet can provide transfer speeds of a whopping 1000 Mbps. This increase in speed is observed because Fast Ethernet is established over a Cat-5 twisted pair cabling or fiber optic cabling. Similar is the case for Gigabit Ethernet, i.e., it is established over either a Cat-5 or Cat-6 twisted pair cabling or a fiber optic cabling.
- **Token Ring:** This network protocol is similar to the Ethernet LAN protocol in the sense that it also is responsible for transporting data to a Physical LAN medium, but the difference is in the media access method used. Just as the name suggests, this protocol uses the token-passing media access method. The

operating speed generally observed in the token ring protocol is 4 and 16 Mbps.

- **FDDI:** This protocol stands for “Fiber Distributed Data Interface” and is tasked with transferring data to a physical LAN medium. The method used is the same as in the token ring protocol, i.e., the token-passing media access method. The difference is that the FDDI protocol is implemented in a network system that is actually a dual ring, which is, in fact, counter-rotating. In addition, it is implemented over a fiber optic cable for improved transfer speeds which go up to 100 Mbps. The reason why the FDDI protocol is different from the token ring protocol despite using the same media access methods is that in the FDDI network, all of the existing stations are basically connected to both of the dual rings. Due to this arrangement, whenever this network system experiences a network break or fault, the ring responds by wrapping back through the node which is in its immediate proximity and move to the node on the second ring.
- **ARP:** ARP is known as the Address Resolution Protocol, and its primary purpose is mapping the Network Layer IP addresses to the Media Access Control (MAC) addresses, hence the name Address Resolution Protocol. The address mapping is done by transmitting ARP query messages over the network segment. In this way, the ARP identifies the physical addresses of the devices attached to the network. Afterward, the obtained translations, which are basically IP address To MAC conversions, are then stored as a cached dynamic table on the system.
- **RARP:** RARP is known as Reverse Address Resolution Protocol. As the name of this protocol suggests, the RARP is the reciprocal of the ARP. To elaborate, the ARP maps IP addresses to MAC addresses while the RARP maps MAC addresses to IP addresses. The reason why we need such a protocol in a LAN network is because of certain machines, such as diskless computers. These machines require such a protocol

as a pre-requisite or a necessary component in discovering their IP address. Just like the ARP, the RARP transmits or relays a RARP message query, which details the system's MAC address and requests for the network to inform it of its IP address.

In short, ARP and RARP are similar to each other in the fact that they both are Second Layer protocols. At the same time, they differ in the function that ARP functions to identify the machine's physical (MAC) address from only its IP address and the RARP functions to identify the machine's network IP address from only its MAC address.

We discussed the LAN protocols and transmission methods, but there is still one aspect that needs our attention, and that is the type of data transmissions in a LAN network. The data transmissions which are found in a LAN network can be classified into three distinct types which are the following:

- 1. Unicast:** In this mode of transmission, the data packets from the source server or computer are sent to a single receiving device. This is done by employing or specifying the destination device's IP address on the network.
- 2. Multicast:** In this mode of transmission, the data packets from the source server are first copied and then sent to the different multiple receiving devices on the network. In this mode, the receiving devices are using a special multicast IP address instead of their unique IP address, and this multicast IP address is configured specifically for this purpose.
- 3. Broadcast:** In this mode of transmission, the IP address used on a destination network is another type known as a Broadcast IP address, and every device on the network receives the data packets which have been copied beforehand by the source computer or server.

Protocols in WLAN and WLAN Tech

WLAN is known as wireless LAN, and the technologies used in this network type are implemented at the lower layers of the standard reference

model of the OSI. The protocols implemented in this type of network basically defines the way the frames will be transferred (or transmitted) in a wireless medium, i.e., air. The WLAN has transmission standards known commonly as the WLAN standards, and they are outlined in the table below.

Type	Speed	Description
802.11a	54 Mbps	Operates at 5 GHz (yielding lower interference compared to 2.4Ghz)
802.11b	11 Mbps	Operates at 2.4 GHz (the first widely used protocol)
802.11g	54 Mbps	Operates at 2.4GHz (also backward compatible with the 802.11b standard)
802.11n	600 Mbps	Operates at 5 GHz or 2.4 GHz

In the early days of the WLAN network era, the encryption used was the Wired Equivalent Privacy (WEP) protocol. However, it was later seen that the practicality of this protocol was insufficient and inefficient. Hence, new encryption standards were developed, which would cover the discrepancies of the WEP protocol, and these deployed standards, which are still in use today, are the WPA and WPA2. This encryption protocol is known as WiFi Protected Access, and even the standard WPA using the protocol known as the Temporal Key Integrity Protocol (TKIP) is considered as insufficient in terms of security aspects.

Different Protocols and Technologies of WAN

WAN is known as the Wireless Area Network, and it primarily functions in the lower realms of the OSI Reference Model, more specifically, at the lower three layers and primarily at the Data Link Layer. The protocols used in WAN basically lay out the primary method by which the frames will be carried from one device to another device connected through a single data link.

The different WAN protocols are mainly classified into two categories - Point to Point Links and Circuit Switched Networks.

Point to Point Links

These are essentially links that provide a communication path which goes from the customer's network to the carrier's network and finally to some remote network. The communication path is, in fact, a WAN communication path that is pre-established. The protocols used in Point to Point Links include:

- **L2F:** This protocol is known as Layer 2 Forwarding protocol and is basically a tunneling protocol. Cisco first developed the L2F protocol, and the primary use of this protocol is to implement VPNs, specifically traffic that is using the PPP (Point to Point Protocol). However, the L2F protocol lacks in security as it does not provide any encryption or confidentiality when directing the data traffic.
- **L2TP:** This protocol is known as the Layer 2 Tunneling Protocol and is derived from the L2F protocol. Similarly, it is also a tunneling protocol (if it wasn't evident from the name). The L2TP is chiefly used for implementing VPNs. The L2TP establishes a tunneling session by using the UDP port 1701. The major difference between L2F and L2TP is that the latter is implemented along with an encryption protocol for security and privacy purposes. Hence, encryption protocols such as IPsec are deployed alongside the L2TP protocol because, on its own, the L2TP protocol does not have any kind of capability to encrypt data traffic or provide data confidentiality.
- **PPP:** This Point to Point Protocol is actually an improvisation over the SLIP protocol, and this protocol functions to primarily provide and establish R-to-R (Router to Router) and H-to-H (Host to Host) connections. Such connections by the PPP are capable of being established over synchronous or asynchronous connections. The improvements of PPP over the SLIP are evident in the areas regarding mechanisms such as built-in

security. In the modern age, the PPP protocol is more commonly used and preferred over the SLIP protocol.

- **PPTP:** The Point to Point Tunneling Protocol is the most commonly used protocol in implementing VPNs that are using PPP data traffic. This protocol, developed by the company Microsoft, has no native addition of encryption or confidentiality protocols. However, PPTP does support other encryption protocols for security, such as PAP, CHAP, and EAP.
- **SLIP:** SLIP is known as “Serial Line IP” and was primarily developed and implemented to support the TCP/IP networking of the time (such as dial-up modems) over serial lines, which were asynchronous and had low transfer speeds. In a more specific context, the SLIP protocol was developed specifically for the Berkley UNIX computers.

Circuit Switched Networks

In this type of network, the communication session which is established between the sender and receiver is actually a physical circuit path that is maintained after being established. This circuit path is then terminated at the end of each communication session. We observe the implementation of this network type commonly in the network systems of Telephone companies.

Examples of Circuit Switched Networks are:

- **xDSL:** xDSL is known as the “Digital Subscriber Line.” In this network connection, the remote customers are given high-bandwidth connectivity via their existing analog phone lines. There are different types of xDSL connectivity lines which are available today, and these are detailed in the table below:

Type	Characteristic	Description
ADSL and ADSL2	Downstream rate: 1.5 to 12 Mbps	ADSL stands for “Asynchronous Digital Subscriber Line.” ADSL is primarily designed with the focus

	Upstream rate: 0.5 to 3.5 Mbps Operating Range: Up to 14,400 ft	of providing the customer with higher bandwidths in downstream than in upstreams.
SDSL	Downstream rate: 1.544 Mbps Upstream rate: 1.544 Mbps Operating Range: Up to 10,000 ft	SDSL stands for “Single-line Digital Subscriber Line.” Unlike ADSL, SDSL is designed with the primary focus of providing high bandwidth downstream as well as upstream. This is done over a single copper twisted pair.
HDSL	Downstream rate: 1.544 Mbps Upstream rate: 1.544 Mbps Operating range: Up to 12,000 ft	HDSL stands for “High-rate Digital Subscriber Line”. The bandwidth rates are the same as SDSL; however, the difference is that it uses two copper twisted pairs and is mostly used for providing the local consumers access to T1 services.
VDSL	Downstream rate: 13 to 52 Mbps Upstream rate: 1.5 to 2.3 Mbps Operating Range: 1,000 to 4,500 ft	VDSL stands for “Very high Digital-rate Subscriber Line.” Just as the name suggests, the purpose of VDSL is to deliver very high bandwidth speeds while using a single copper twisted pair. VDSL2 delivers even faster downstream and upstream rates, both exceeding 100 Mbps.

- **DOCSIS:** This communication protocol in the circuit-switched network is known as “Data Over Cable Services Interface Specification.” DOCSIS has the capability of transmitting data over an already established (existing) cable TV system at very high speeds.

- **ISDN:** This communication protocol is known as the Integrated Services Digital Network, and the primary place of operation of an ISDN is over the analog phone lines. However, it is important to remember that these analog phone lines are already converted so that they use digital signaling. It is due to this nature of the operation line, which enables the ISDN to transmit both data traffic and voice traffic. The different types of data are transmitted through the ISDN by using separate channels. For instance, a B-channel which has been defined by the ISDN will handle information relating to data, voice, and other services. Similarly, a D-channel defined by the ISDN will only handle control and signaling information. The ISDN is further classified into two levels based on the services provided which are BRI (Basic Rate Interface) and PRI (Primary Rate Interface).

Packet-Switched Networks

In this type of network, devices are connected to a network (carrier network), and the devices share the bandwidth on the communication link through a technique known as statistical multiplexing. Compared to Circuit-switched networks, Packet-switched networks are more resistant to traffic congestions and errors. Some examples of packet-switched networks are given below:

- **ATM:** also known as “Asynchronous Transfer Mode.” ATM is a technology that is characteristic of its extremely high-speed and low-delay functioning responses. The ATM achieves this speed by using techniques such as switching and multiplexing to quickly relay information such as voice, video, or data in the form of 53-byte fixed-length cells. In addition, the processing of the information contained in the cell is done in the hardware, which further reduces the transit delay significantly. For this reason, ATM is preferable for handling uneven traffic and is deployed on fiber-optic networks.

Some other examples of packet-switched networks include **Frame Relay** , **MPLS** (Multi-Protocol Label Switching), **SONET** (Synchronous Optical Network), **SDH** (Synchronous Digital Hierarchy) and **SMDS** (Switched Multimegabit Digital Service).

Comparison Between Circuit Switching and Packet Switching

Circuit Switching	Packet Switching
Fixed Delays	Variable Delays
The network is connection-oriented	The network is not connection-oriented or simply, connectionless-oriented
Preferable for connections that are always on experiencing stable and constant data traffic along with occasional voice communications.	Preferable for network situations that experience uneven or a sudden burst of data (user) traffic. It is also preferable for data communication purposes.

In simple terms, the Packet-switching method is the preferred network type for on-demand connections that experience a burst of traffic.

Other WAN protocols are defined at the Data Link Layer. These WAN protocols are :

- **HDLC:** also known as “High-Level Data Link Control.” HDLC is basically a synchronous protocol whose primary function is to support configurations such as point-to-point and multipoint. HDLC is bit-oriented and is actually derived from SDLC. HDLC works on the data encapsulation principle, which is meant for synchronous serial links. However, the downside of this WAN protocol is that most of the vendor implementations of HDLC are, in fact, incompatible.
- **SDLC:** also known as “Synchronous Data Link Control,” SDLC is similar to the HDLC in some areas such as being bit-

oriented. However, the characteristics which differentiate SDLC from HDLC is that the former is a full-duplex serial protocol and was developed by the company “IBM.” The main purpose of this protocol was to facilitate, enable, and allow communication establishment, specifically between mainframes and remote offices. SDLC works on the principle of the polling method of media access. According to this method, polling occurs between two entities known as the primary and the secondaries. The primary is the front end of the network, while the secondaries are the remote stations of the network. The front end (or primary) basically polls the remote station (or secondaries) to decide whether a communication is needed or not.

The Networking Equipment Found in the Data Link Layer

There devices which work at the Data Link Layer as networking equipment are

1. Bridges
2. Switches
3. DTEs
4. DCEs

The Bridge

The bridge is a device that is actually a semi-intelligent repeater. Just as the name suggests, a bridge is used to connect network segments together (which may be two or more in number). The connected network segments can be similar to each other or even dissimilar; it does not affect the connecting function of the bridge. Moreover, as the bridge connects network segments together, it also simultaneously maintains an ARP cache. This ARP (Address Resolution Protocol) contains the individual MAC addresses of the devices that are on the conjoined network segments.

The Switch

The switch is a device that can be classified as intelligent because of its functioning, i.e., it routes traffic based on MAC addresses. However, the

switch differs from a typical hub in the sense that it only transmits data to a port that is identified to be connected to the MAC address of the destination.

DTE (Data Terminal Equipment)

A DTE is basically a term that is used to refer to devices that are at the user end of a user-to-network interface. DTE devices pair up and connect with DCE (Data Communication Equipment or Data Circuit-Terminating Equipment). Similar to DTE, DCE is a term used to refer to devices that are the network end of the user-to-network interface.

The Third Layer: Network Layer

The transfer of data packets between devices available on the same network or on interconnected networks (internetworks) via routing and other similar functions is accomplished in the third layer that is the Network layer. The Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP) are all known as Routing protocols that are defined in the Network Layer. The routed protocols such as Internet Protocol (IP) and Internetwork Packet Exchange (IPX) are utilized on the Network layer for the logical addressing of systems on the network. Therefore, the routed protocol messages are transmitted across a network via routing protocols.

Routing Protocols

The routing protocols included in the network layer are used by the routers to determine the most appropriate path by which they will forward the data packets to one another and form a connection with other routers on WAN. These protocols can either be categorized as a Static routing protocol or a Dynamic routing protocol.

In a static routing protocol, the administrator uses a manually configured routing entry to create and update routes. These static routes are fixed and cannot change the direction of the traffic dynamically to a different route if the original route is down, which results in the failure of the whole network. Similarly, in the case when the data traffic in the chosen route is overcrowded, the router using a static routing protocol cannot reroute the data dynamically to a lesser congested and relatively faster route. Keeping

in light the above discussion, the static routing protocol is used in small networks or limited special-case scenarios. Its advantages include low bandwidth requirements and built-in security.

In a dynamic routing protocol, the routers share information about the network with each other and determine the best path to reach a given destination. To provide efficiency, the routing table is updated timely to give the routers the current routing information for better data transmission. The dynamic routing protocol has three basic types of link-state and distance-vector for the intra-domain routing and the path-vector for the inter-domain routing.

The distance-vector protocol makes use of a simple algorithm to make routing decisions that are based on the cumulative value of distance and vector. The information on changes in topology networks is periodically shared among the neighboring routers and systems. The main problem faced by the distance-vector routing is convergence, which is the time taken for a routing table to be updated. Without the function of convergence, the routers are left uninformed of the topology changes and might end up transmitting the data packets to the wrong destination. The speed of the network reduces considerably during convergence when the information is being shared among the routers.

In a link-state protocol, every router calculates and maintains a routing table based on the entire network. These routers occasionally transmit updates regarding the neighboring connections to every other router in the network. Despite being computation-intensive, they consider various factors like reliability, cost, delay, speed, and load, and find the most effective route to a destination. Compared to the slow convergence of distance-vector protocols, the convergence of link-state is very fast occurring usually in just a few seconds—an example of the link-state protocol in the Open Shortest Path First (OSPF) protocol.

The path-vector protocol is similar to the distance-vector protocol, but it does not have the limitation of scalability related to limited hop counts. The Border Gateway Protocol (BGP) is an example of the path-vector protocol.

Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) is an example of the distance-vector protocol in which the distance factor uses the hop count routing metric. The RIP implements a hop count with the limit of 15 so that the routing loops can be avoided in which the data packets get stuck being transmitted between several routers, but this also restricts the network size that can utilize the RIP. If the hop count between the source and destination is more than 15 router nodes, then the destination is considered inaccessible. The other three mechanisms used by RIP to eliminate routing loops are:

- Split horizon
- Route poisoning
- Holddown timers

The RIP is a connectionless protocol because it uses the UDP port 520 transfer protocol. It has the disadvantages of slow convergence and deficient security, and so these limitations render it a legacy protocol, but it is still used widely because of this simplicity.

Open Shortest Path First (OSPF)

The link-state includes the Open shortest path first (OSPF) protocol, which is used in the large company networks. The routing in OSPF is operated within a single autonomous system (AS) due to which is known as an Interior Gateway Protocol (IGP). It does not use the Transfer protocol like TCP or UDP and is enclosed in the IP datagrams. Area Identifiers are used in OSPF to correspond to the IP addresses, copy them without any problems, and to determine the routers to which it should send the data packets.

Intermediate System to Intermediate System (IS-IS)

The IS-IS is also a link-state protocol used in a packet-switched network to route the data traffic. This IGP used within a single autonomous system is implemented in large networks like the service-provider backbone network.

Border Gateway Protocol (BGP)

The Border Gateway Protocol is an example of the path-vector protocol that is used for routing among multiple Autonomous Systems, and so it is referred to as an External Gateway Protocol (EGP). The large private IP networks and Internet Service Providers (ISPs) use this protocol as their core. The BGP can be referred to as External BGP (eBGP) if it is used for routing between separate Autonomous systems and internal BGP (iBGP) if it operates within a single Autonomous System.

Routed Protocols

The Network layer consists of routing protocols that are used to support the data traffic by setting up a destination for the data packets containing the routing information, which then allows these packets to be transferred within the network via routing protocols.

Internet Protocol (IP)

The information regarding the address of the data packet is available in the Internet Protocol (IP) that allows the packet to be routed. The IP makes up a part of the TCP/IP, which is a suite of communication protocols used to interconnect devices on the internet and thus is called the language of the internet.

The functions of IP include:

- The best-effort delivery of datagrams without the need to establish a connection with the recipient.
- Breaking up the datagrams and then reassembling them.

The most widely used IP is IP version 4 (IPv4), which uses a 32-bit logical IP address. This address is divided into four 8-bit parts, which are referred to as octets, and it contains two main parts, which are the network number and host number. The five address classes supported by IP addressing are listed in the table.

Some IP addresses are also used for private networks only, and these are:

- Class A which supports the address 10.0.0.0 – 10.255.255.255
- Class B address which is 172.16.0.0 – 172.31.0.0

- Class C which is 192.168.0.0 – 192.168.255.255

These private IP addresses aren't available for routing on the internet and are only for implementation on firewalls and gateways. The method of Network Address Translation (NAT) is used to hide the architecture of the network, increase security, and conserve the IP address. The functions of NAT also include converting the private IP addresses, which are non-routable into registered IP addresses in case of communication across the internet.

Another version is the IP version 6 (IPv6), where the 128-bit logical IP address is used to increase the functions of IP by providing security, support for multimedia, and backward compatibility with IPv4. IPv6 was developed so that it could be used after the IP addresses in IPv4 were used up, but the development of NAT has delayed this depletion. As a result, IPv6 is not widely used on the internet.

Internetwork Packet Exchange

The Internetwork Packet Exchange is a connectionless protocol that is used as a part of the IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) protocol unit, which is similar to the TCP/IP suite. In the beginning, it was used to route data packets across the internet in the old networks like Novell NetWare.

Other Network Layer Protocols

Apart from the protocols mentioned above, Network Layer makes use of a variety of other protocols as well. The Internet Control Message Protocol (ICMP) and Simple Key Management for Internet Protocols (SKIP) are protocols defined in the Network layer as well.

Internet Control Message Protocol (ICMP)

The ICMP checks the processing of transferred IP data packets and reports errors and various information back to the source. These error and information messages could be

- Destination Unreachable
- Time Exceeded

- Redirect
- Echo request and reply

To test if a network device is reachable or not, the utility called Packet Internet Groper (PING) borrows the function of the ICMP messages.

Simple Key Management for Internet Protocols (SKIP)

The SKIP in the Network Layer is used to send encrypted keys and data packets without the need for the establishment of a prior connection session. Due to the size of extra header information added in the encrypted packets, the SKIP becomes bandwidth-intensive.

Networking Equipment at the Network Layer

The third layer of OSI uses routers and gateways as its primary networking equipment.

Routers

The devices that receive, analyze, and forward the data packets to another network are known as routers. They link various networks and move the incoming data packets using the logical addresses only to the destination network due to which they are called intelligent devices. Routers utilize both hardware and software parts and use a variety of algorithms that route the data packets along the best path leading to the destination. The ideal path is chosen based on various factors like bandwidth, distance, cost, and delay.

Gateways

The software operating on a computer or a router creates gateways that examine the data packets, translate incompatibilities, and link different programs. The example of gateways would include the linking of an IP network to an IPX network or a Microsoft Exchange mail server to a Lotus Notes server, which will be called a mail gateway.

The Fourth Layer: Transport Layer

The major concern of the transport layer is mediating the movement of data between the different layers. For this purpose, the transport layer masks the

characteristics of lower layers, such as their functions from the upper layers in the OSI model. Apart from this, the major functions of the transport layer include:

- **Flow Control:** direct the transmission of data between the sending device and the receiving device with the main purpose of managing the influx of data that the receiving device experiences. In essence, the transport layer ensures that the receiving device is not flooded with data that it cannot process.
- **Multiplexing:** divides a physical channel into multiple logical channels, which makes it feasible for multiple devices or applications to transmit data over one physical channel (or link).
- **Virtual Circuit Management:** interacting with virtual circuits in a network and managing them in the sense to establish, maintain, and terminate the said virtual circuits.
- **Error Checking and Recovery:** incorporating the applications of multiple mechanisms to achieve the function of identifying data transmission errors and taking steps to rectify this error, for instance, issuing a request to the transmitting device to re-send or retransmit the data.

The Protocols

Like the other layers in the OSI model, the Transport layer also sports several important protocols, such as:

1. **TCP:** also known as the Transmission Control Protocol, in nature, is actually a connection-oriented protocol capable of providing reliable transport delivery of data packets across the network. In addition, this protocol is also full-duplex capable, meaning this protocol can transmit and receive data communication simultaneously. The pre-requisite for data transmission between two devices in communication using the TCP protocol is a direct connection. This direct connection is established through a three-way handshake. The main features

which are characteristic of the TCP protocol are **Connection-oriented, Reliable , Slow** .

2. **UDP:** also known as User Datagram Protocol. The nature of the UDP protocol is actually that of a connectionless protocol. Due to this, the UDP protocol is capable of providing quick and fast datagram deliveries across a network. However, this protocol is not reliable because connectionless protocols are unable to guarantee the delivery of datagrams (also known as data packets). Hence, this protocol is the most suitable for cases where data is needed to be delivered quickly, and the transferred data is not sensitive to packet loss or doesn't need to be fragmented. The most common applications of UDP include **DNS** (Domain Name System), **SNMP** (Simple Network Management Protocol), and even streaming content that can be either audio or video.
3. **SPX:** also known as Sequenced Packet Exchange, is a protocol whose primary function and concern is to guarantee the delivery of data in aged networks, specifically the older Novell Netware IPX/SPX networks. The working of this protocol includes sequencing the packets that have been transmitted, reassembling the packets which are received by the device on the network, then proceed to double-check that all the packets have been received. If some packets have not been received, the protocol proceeds to request the re-transmission of the missing packets.

Below is a table identifying the nature of the protocols discussed above.

Protocol	Layer	Type
Transmission Control Protocol (TCP)	Transport Layer (Fourth Layer)	Connection-oriented
User Datagram Protocol (UDP)	Transport Layer (Fourth Layer)	Connectionless-oriented

Internet Protocol (IP)	Network Layer (Third Layer)	Connectionless-oriented
Internetwork Packet Exchange (IPX)	Network Layer (Third Layer)	Connectionless-oriented
Sequenced Packet Exchange (SPX)	Transport Layer (Fourth Layer)	Connection-oriented

(Reference: "Introducing the Internet Protocol Suite." System Administration Guide, Volume 3)

Apart from these mentioned protocols, there is one more protocol, which is actually a security protocol.

- **SSL/TLS:** also known as Security Sockets Layer/Transport Layer Security, this protocol mainly concerned with providing security for two devices (client and a server) communicating over the internet. The security is actually session-based encryption and authentication.

The Fifth Layer: Session Layer

The major concern of the Session Layer is to:

- Establish
- Coordinate
- Terminate

Service requests or server responses (in other words, communication sessions) between networked systems. It is also important to discuss the details of what consists of a standard communication session to understand the protocols used in this layer.

A typical communication session can be divided into the following separate phases:

1. **Connection Establishment:** This is the first and foremost approach that will take place in any communication session, the initial contact between the systems that are communication.

During the communication establishment, an agreement is also made between the end devices, detailing the communication parameters and communication protocols and mode of operation to be used. There are three different modes of operation, which are:

- **Simplex Mode** : In this mode of operation, the communication path established is basically one-way. This mode is observed when a transmitter at one end and a receiver at the other end establish a communication path. For example, in an AM radio, music is broadcasted by the radio station, and the receiver can only hear the broadcast.
- **Half -Duplex Mode** : In this mode of operation, both the devices which are connected to each other are capable of communication. In other words, unlike in the Simplex mode where only one device could communicate, the Half-Duplex Mode allows both of the devices to be able to transmit and receive messages, however, not at the same time. For instance, think of a walkie-talkie, where to speak, one must press a button only after the other end of the radio stops transmitting a message.
- **Full -Duplex Mode** : Unlike the other two modes of operation, where either one device would transmit, and one would receive or both devices could receive and transmit but not at the same time, the Full-Duplex mode of operation allows both the communicating devices to transmit and receive simultaneously. For instance, think of a telephone where users can transmit and receive analog signals at the same time.

2. **Data Transfer:** Once communication has been established, data (also known as information in this case) is exchanged between the two devices at each end.

3. **Connection Release or Termination:** Once the data transfer between the communicating devices has been completed, the end devices systematically terminate the communication session.

The Protocols

Below are some of the protocols used in the Session Layer of the OSI Model.

1. **NetBIOS** : this protocol is known as the “Network Basic Input Output System.” Developed by Microsoft, the NetBIOS protocol basically enables applications running on a system to communicate over a Local Area Network. This protocol is capable of being combined with other protocols, such as TCP/IP (after combining with TCP/IP, NetBIOS becomes NBT), allowing the applications to communicate on an even larger network than LAN.
2. **NFS** : this protocol is known as the “Network File System.” Developed by the company Sun Microsystems, the NFS protocol is purposed to work with systems on which users need to access remote resources a network, which is basically a Unix-based TCP/IP network. The protocol specifically facilitates transparent user access.
3. **RPC** : this protocol is known as “Remote Procedure Call.” In essence, the RPC is basically a redirection tool that works on a client-server network.
4. **SSH/SSH-2**: this protocol is known as “Secure Shell.” This protocol is basically a secure substitute or an alternative for remote access, such as Telnet. The Secure Shell protocol basically works by establishing a tunnel, which is encrypted for security purposes, between the two devices (the client and server). In addition, the Secure Shell protocol also holds the capability to be able to authenticate the client to the server.
5. **SIP** : this protocol is known as the “Session Initiation Protocol.” SIP is commonly used in large and huge IP-based

networks for communication purposes such as establishing, managing, and terminating the established real-time communication.

The Sixth Layer: Presentation Layer

The primary functions of the presentation layer include applying coding and conversion to the data before sending it to the Application layer so that the compatibility between the data of the sender and receiver Application layer is ensured.

- **Data representation:** The use of standard formats of data in the form of image, video, or sound ensure that the application layer data can be exchanged between different system types.
- **Character conversion:** During the exchange of data between different types of systems, a standard type of character conversion structure is used.
- **Data compression:** To accurately decompress the data exchanged when it arrives at the destination, a common compression scheme should be used beforehand.
- **Data encryption:** Proper decryption of the data at the layer where it was received also needs a common or standard encryption scheme.

Some presentation layer protocols include:

- **American Standard Code for Information Interchange (ASCII):** It is referred to as a character-encoding scheme where the code is used to represent the 128 letters of the English alphabet, with each letter being assigned a number ranging from anywhere between 0 and 127.
- **Extended Binary-Coded Decimal Interchange Code (EBCDIC):** It is an eight-bit binary coding scheme for alphabetic and numeric characters that are used on IBM mainframe and mid-range computer systems.

- **Graphics Interchange Format (GIF):** The bitmap image format that supports about 256 colors and is used to create static or animated images or logos.
- **Joint Photographic Experts Group (JPEG):** It is a commonly used method of compressing digital photographs which are then stored or transmitted.

Motion Picture Experts Group: The most commonly used audio and video compression method which are then stored or transmitted.

The Seventh Layer: Application Layer

The highest layer of the OSI model is Layer 7, the Application layer. Its primary functions include dealing with features of communication associated with the network access and providing the user with an interface. Thus, the common interaction point between the user and the Application layer is the application being used.

Its responsibilities include:

- Searching for accessibility of possible associates and establishing communication with them.
- Determining the availability of necessary resources
- Making it possible for the communication to be synchronized

The software application such as Microsoft word and excel must not be mixed up with Application layer protocols which include:

Chapter 3

Security of Software Development

In this chapter, we will address the security issues that soft wares are exposed to during their development. In addition, a CISSP candidate should be knowledgeable of not only the process of software development but also the workings of malicious code that target and harm systems, applications, utilities, or even embedded systems. In this way, the security professionals will be able to supervise and instruct the developers in creating appropriate software that can combat and safeguard the potential targets of malicious codes and viruses.

Security Workings in Distributed Software

Securing the Distributed systems faced numerous problems which can be summed up into three main issues:

- **Software Integrity:** The software components of an application in a distributed system may reside on multiple systems, which are all situated in different physical locations, and different groups handle the management of these systems. The system may contain workstations numbering in hundreds, and all are required to perform with the original client software. In this case, it is a strenuous task to keep a check on these original versions of every separate component. It becomes even more difficult if separate parts of the organization or separate companies operate with different types of hardware platforms. Such an issue can be understood by the supposed situation where damage befalls one of the systems which have the newly released application installed on them, in case of which it has to rely on backups for rebuilding. An issue also arises when the new application or software does not install properly on several workstations.

- **Data Integrity:** Considering the additional help of technologies like data replication and cloud computing, that data present in a distributed system may reside in numerous physical locations simultaneously, which gives rise to problems as well. The main issue, in this case, is the fact that it is almost impossible to keep the data accurate and in sync in all these different locations. Consider a case where backup tapes were saved before upgrading an application while there is a hardware platform that operates the older version of the application. If even subtle changes are made to the application, they can prove to be bothersome.
- **Access Control:** The software components separated in a distributed system require communication via the network. This communication in the absence of proper security is quite dangerous due to the danger of hacking and threats of attack regarding sensitive information. A viable approach is to set up an authentication or access control in the network, which is used by the components to prove each other's identity and protect themselves from attackers.

The factors such as the tradeoff among offloading application logic from centralized servers and the complexity in the distributed system workings rendered the distributed systems idea not very practical. In the end, it was used just to propel the field of technology forward.

Nowadays, the development of mobile applications has proved that the method of distributed systems could make a comeback. The applications in the mobiles and tablet computers can communicate with other systems such as the application servers, database servers, and other devices.

Working with Agents in Distributed Systems

A software component making up a part of the distributed system that has a specific function is known as an agent. For example, an agent might be a system that collects the designated credit card information and builds up a merchant transaction which is delivered to the bank. The transaction is then analyzed and processed by the agent and sends an affirmative or non-

affirmative answer to the main application, which is then passed on to the customer.

Nowadays, agents are more common in the field of systems management instead of business applications. Some examples are:

- **Patch management:** The patches on a server are installed or removed with the help of an agent, whereas a central management console entirely controls the procedure.
- **Host-based intrusion detection systems (HIDSs):** If the agents detect a potential threat through searching for attempted tampering, alarm messages are sent to the central console for action against the threat.
- **Performance and capacity monitoring:** The use of resources of computers, including the CPU memory, time, and disk space, is constantly analyzed by agents.

Object-Oriented Environments

The development of object-oriented applications became a competition for the distributed systems as their foundation did not lie in the information systems; rather, it was based on objects and the concept of reusability. Its fundamental principle is based on the fact that the objects that are written can be reused many times, increasing efficiency of the development effort of an enterprise's software. It is an entirely different computing world that includes the analysis, design, programming, and databases of object-oriented applications.

In object-orientation, the workings within an object are protected, which is referred to as encapsulation of the object. During communication with each other, an object performs its specified function after it receives the message, and this process is referred to as a method.

An instance is the running of an object, while the procedure in which the instance is started is known as instantiation. Another meaning of an instance can be an object that is part of a class of objects.

- **Behavior:** It is the result produced by an object after it receives a message.
- **Class:** It is a template that defines methods and variables required to be included in a specific category of objects, according to the description of David Taylor, author of “Business Engineering with Object Technology.” Common variables and methods cover the class, whereas objects define unique characteristics. Parts of a class (subclasses) and collections of classes (superclasses) are also included in Object Oriented system.

Example of class: Coffee can be taken as a class, which can be further specified as a latte. Other types of coffees are also objects in this class, e.g., Americano, cappuccino, iced coffee, espresso, and mochaccino. The unique details for every one of these types can be linked to the methods. These methods could be either the brewing process or the purpose of its intake.

- **Class hierarchy:** The collection of objects and classes are in hierarchical, ordered or organized as a branched structure.
- **Delegation:** When a request is made to an object for an unavailable method, it delegates the message to the object having the method.
- **Encapsulation:** The components of the object are concealed or encapsulated, also called the object’s packaging.
- **Inheritance:** Several characteristics of an object are inherited from the class when the class is instantiated.
- **Instance:** It refers to a specific type of object that is included in the class as a member.
- **Message:** It is the process by which communication is established between objects. The message comprises an object’s name involved in communication, the associated method, and a few parameters. The Sender in the

communication is the object that sends the message while the receiver object acquires it.

- **Method:** It is the process of a function found in an object in the form of a code.
- **Multiple inheritance:** If an object inherits its characteristics from more than one different class, it is known as multiple inheritance.
- **Object:** The object is the most simple and basic unit used in the Object-orientation.
- **Polyinstantiation:** A new object can be created from a given object, provided the new object has different values than the existing object. This process is referred to as polyinstantiation.
- **Polymorphism:** A new object being added to the system might need to have the existing procedures in the system to be rewritten, but it is not necessary. The process of rewriting can be avoided by polymorphism, in which the details for implementation are completed with the help of a common message interface.

Databases

A database contains data from several applications that are defined, stored, and manipulated according to its mechanism. The function of the programming and command interface present in the database is to create the data, then manage and administrate it. The database management systems are present on a different server, which is physically and plausibly separate from the application server.

The Database Management Servers (DBMSs) contain the access-control method by which it protects the data provided in the database from attackers and allows access to only specified permitted users.

The most common types of databases are:

- Relational databases

- Hierarchical databases
- Object-oriented databases

Database Security

The access control contains a granularity that defines the limit of control of access and manipulation of the database, tables, rows, and field data. In a low granularity, the user is allowed access to read or read/write all the rows and fields present in a table. While in high granularity, the user can only access a limited choice of fields and rows. A lot of time of the database administrator and the security administrator is consumed in the case of high granularity as they have to supervise the maintenance of all the permissions in this access control.

The tiresome job of managing the high granularity permissions can be made less time-consuming and easier with the use of views. A view refers to a virtual table that presents the data contained in the rows and fields of one or more than one database table. The users are then given access to only these views and not the actual table, which makes dealing with the security issues easier.

Aggregation is referred to the process where numerous data items of low-sensitivity are put together in one place, causing this combination of data to become highly sensitive. This method results in many privacy and security issues. For example, the home address, date of birth, social security number, etc. don't have much importance by themselves. Still, if they are aggregated and an attacker gains access to this information, a case of identity theft follows which is quite damaging and risky.

Due to the level of sensitivity, some piece of information is kept out of reach for security purposes, but it does not stop the potential intruders from inferring. Here inference is the ability to deduce or derive something regarding the sensitive data. For instance, if there is mention of the presence of highly sensitive data in an application, the potential attackers will infer that it contains some information that is worth stealing.

Data Dictionaries

The information regarding all the fields and tables provided in an application is included in a database, which is known as the data dictionary. The data dictionary is used by DBMS, applications, and security tools to make or edit tables, manage access to sensitive information, and as a central control point to maintain the application database schemes.

Data Warehouses

A database that is specifically designed to support the day-to-day operations of the business, such as business research, planning, and decision support, is called the data warehouse.

Types of Databases

The various types of databases that were first developed approximately 40 years ago were based on the form of data architectures or the methods used by them to organize and the information.

Hierarchical Database

In a hierarchical type of database, the data is organized in a branched tree-like structure where the parent records are arranged at the top part of the database. In contrast, the child records are present in the successive layers in the hierarchy. IBM's Information Management System (IMS), first used in the 1960s, is the most popular example of the hierarchical databases, and they are still commonly used nowadays in the IBM mainframes.

Network Database

The network databases are basically the improved version of the hierarchical databases differing in their path of networking between the records. In the hierarchical database, the records are linked to each other in a simple branched structure. In contrast, in the network databases, these records are connected to other records via linking paths, which are significantly different than those of the hierarchical database paths.

Relational Database

After the development of hierarchical and network databases, the designers improved the database design even further. They finally came up with the relational database, which can be said to be the culmination of the database

design. The relationship and link between the records or data sets in the relational database have the freedom identical to a network database without the limitations of a hierarchical database. These data set relationships can be modified by the developers or administrators of the database to match the needs of the business.

The schema, including the rows, tables, and others, are used to make up the structure of the relational database. The rows in the structure are the records in the database, while the tables store these rows. Any field in the table which contains a unique value is called the primary key, which supports the function of rapid table lookups. These lookups operate through the binary searches and lookup algorithms until the specific record is found. For more quick lookups, an index is created in the table for any field.

The foreign key is considered to be one of the most powerful functions included in the relational database as it comprises of a table field that leads to a primary key in a separate table.

The stored procedures are stored directly in the relational database and provide subroutines easily accessible by the application software.

The canned statements which are called by an application in the relational database are referred to as the prepared statements or parameterized statements.

The features that aid in making the application more resilient to SQL injection attacks are the Stored procedures and the prepared statements.

Distributed Database

The distributed database got its name not from its design, but from the fact that its various components are divided into many physical locations. Its design can vary from hierarchical to network, relational, object, or any other design.

Object Database

The object database model is the type of database that contains its information in the form of objects as used in object-oriented application design, so it is considered a part of this design. The data records and their methods are included in the object system, and they also have classes (types

of data), instantiations (individual data records), inheritance, and encapsulation.

Object databases appeal to only a small, specialized group in the database management market where the dominating player is the relational database.

Database Transactions

The modification in the database in the form of addition, removal, or alteration of the data sets or records is termed as a transaction. These transactions in the applications are done through functions calls, accomplished by the API of the database management system. The fact that the management of data can be entrusted to the relational database, while the software developer focuses on the main functions of the application is considered to be an advantageous feature.

The Structured Query Language (SQL) developed in the 1970s is the most widely used computer language in a database. Its functions include performing a query on a database, updating the data, defining the database structure, and implementing access management. SQL statements are dynamically created and sent to the database management system for queries and data updates. Some commands of SQL are:

- **Select:** Particular data records are requested to be returned when a query is performed on a database.
- **Update:** Some of the fields and rows in a database table are altered and updated.
- **Insert:** New rows are inserted into the table.

It is possible to perform the statement functions altogether by grouping them in a transaction that results in database integrity. For instance, a business transaction may use the all-or-nothing update operation where either all the tables or none of them will be updated.

Locking is a method that is used to prevent collisions between programs that are trying to update the same table or row. An entire row, table, or field can be placed under locks that are managed by the database management

system. Some rules are followed if a data set is locked for a certain amount of time.

Operating Systems

Operating system (OS) is a system software containing a set of programs that are used in the management of the computer hardware and software resources and aids in the functioning of the programs of application software.

The kernel is the central component and program at the core of an operating system that carries out several activities including:

- **Process management:** When multiple programs are running simultaneously in an operating system, their initiation, execution, and termination are controlled by the kernel. The resources like hardware components are shared among the programs efficiently with the help of the kernel.
- **Memory management:** The memory is allocated to programs by the kernel, which limits the use and access of storage according to needs. The kernel also oversees the requests to increase or decrease the memory usage by the programs.
- **Interrupts:** On some occasions, when an urgent event occurs, the hardware components send an interrupt signal to the operating system. This signal received by the kernel suspends the running programs and processing for a short amount of time until the urgent task is taken care of.
- **Hardware resource management:** The computer programs running on the operating system are granted access to the memory, hard disks, adaptors like network and bus adaptors, and other such hardware components with the assistance of kernel.

The interaction between the kernel of the operating system and some specific hardware resources is managed by programs known as device drivers.

The user interface is a part of the OS, which enables the interaction and communication between a user and the computer. The two main types of the user interface are:

- **Command-line:** Some operating systems like Microsoft DOS and old UNIX use the type of user interface called the command line. In this interface, the command is typed in by the user via a keyboard while the computer receives the command and responds accordingly.
- **Graphical:** The graphical user interface is a visual way of interacting with the computer where the screen is divided into windows and controlled by a keyboard or a pointing device like a mouse or a touchpad. Linux, Android, Microsoft Windows, and Mac OS are examples of the graphical user interface.

The security functions performed by the operating systems are as follows:

- **Authentication:** For the sensitive information to be accessed by a user from a local or remote location, the OS must first identify the person. The user can gain access by providing a valid user id and password.
- **Access control:** The resources such as printers or scanners are only accessible to those users who have gained the required permission from the OS.
- **Process isolation:** The memory associated with a program cannot be approached or modified by any other process due to the limitations implemented by the OS. This way, the interference between programs can be eliminated.
- **Network communication:** Some basic protocols of the network are included as a part of the OS to establish communication between different computers
- **Filesystem access:** The permission labels associated with each file by the OS limit what the user can access in the file systems. Some specific files need the authorization of the user before

they can be accessed, and thus, this principle is used in workstations and servers for security purposes.

In addition, in being able to protect its resources and processes, a secure OS should also be able to defend itself from attackers. Only then can it succeed in protecting the system information.

Systems Development Life Cycle

The stages involved in the development of a system from an initial model to completed form is done by the help of a conceptual model called the systems/software development life cycle (SDLC). The steps of conception, implementation, support, and retirement of software are all designed within the SDLC.

The objectives of SDLC are:

- To design a system that can implement correct and secure functions.
- To do a development project that is inexpensive and not time-consuming.

The waterfall model of SDLC comprises steps progressing sequentially from conception to completion of the system in a way that is similar to the waterfall series. Each step in this model is executed successively, as depicted in the model.

Conceptual Definition

A conceptual definition is based on concepts where the system is described on a high-level but generally does not delve into specific details.

Functional Requirements

The functional requirements describe the characteristics and services that must be present in the system.

The description of functional requirements contains more details than the conceptual definition due to a lack of design information.

A test plan is devised to examine each characteristic of the functional requirement and contains details such as the procedure of each test and its expected results.

Functional Specifications

Functional specifications are described as a list of characteristics that specify the system's intended functions, services, appearance, etc. This list also contains security-related functions like authentication, authorization, availability, and confidentiality.

Design

Design is the description which is comprised of details related to the design of a system. These fine details are considered to be of the highest level.

Design Reviews

The last step of designing a system is called Design reviews, in which the final designs are examined and evaluated by a group of experts. The impossible specifications and unnecessary details are weeded out and have to be redone by the engineers until the design passes the last test.

Coding

Coding is actually the part of a system's development life cycle that most software developers prefer to jump right into it. Although it is a lot easier just to start coding right away while ignoring all the preceding steps which are the standard to be followed, it is not advisable; this would be similar to boarding an airplane, which was built even before the engineering drawings and blueprints had been produced and approved. In short, the software is at more risk of defecting with bugs and other problems. Hence, software developers need to understand and follow secure coding guidelines and practices.

Code Review

To examine the finished product of coding, code review is put into action by the engineers where they check each other's coding for any kind of mistake. This phase of testing is really important as those mistakes can be highlighted and fixed timely, which would have cost greatly in the stages of

implementation and maintenance. The errors in the coding that may result in weak security are also eliminated with the help of several tools.

Unit Test

The individual parts of a developed application or program can be examined separately in a process called unit testing. It is performed during coding to check if these parts are functioning correctly.

System Test

The system test is the test plan that was devised in the stage of functional requirements. It is carried out when all the components of the system have been assembled and need a final test for examination of functionality and security. To eliminate any possibility of vulnerability in the security of the system, the organization uses tools that perform a strict check for any errors.

Certification and Accreditation

In certification, the system is formally assessed to check if every feature is working properly, and then it is officially declared to be fully functional.

In accreditation, the system is recognized and approved by the relevant people to be put into production by selling, building, or shipping it.

Maintenance

During the time the system is being produced, complaints and requests for change arrive from the customers due to some mistakes made during the development of requirements. To solve this problem, the process of maintenance starts. Maintenance includes the processes of Change Management and Configuration management to take charge of the system and control it through new developers while the original ones are occupied with another project.

Change Management

The stakeholders review the changes made to the system before they are properly executed. This business process by which the system modifications receives formal review and approval for implementation is

called the Change management. The opinions and concerns of everyone involved are given a chance and considered for a smooth process.

The change management process is handled by the change review board, where the members of various departments are included.

Configuration Management

Configuration management deals with the process of recording the details related to the modifications made in the system. All the changes made in the software coding and various documentation are noted down and stored. The Configuration management also archives the technical details involving change, release, and each instance of the system.

Controlling the Security of Applications

In this section, we will focus our discussion on ways through which we can make the software more secure by employing different techniques, mechanisms, and characteristics.

Process Isolation

Just as the name suggests, through Process Isolation, details, and resources of a defined process are isolated from the interference of other tools and users. More specifically, a running process is prohibited from performing certain actions such as viewing or modifying the memory cache, which belongs to some other process. For example, consider that a user is working on a system, and he sees a running payroll program. Since this program's process is isolated, the user will be unable to view the allocated memory space that is being used by the program.

This service is provided natively by the currently popular Operating systems such as Mac, Windows, and Linux. This service can be performed and provided by even older Operating Systems such as RSTS/E, Kronos, and TOPS-10. Due to this, the system developer is alleviated from the task of having to build a wall around the application.

Hardware Segmentation

Just like process isolation, hardware segmentation basically refers to a practice through which functions are isolated to keep the desired hardware

platforms distinguished and separated. The goal of this entire process is to guarantee the system function's integrity and security. On a practical note, the practice and goal of hardware segmentation are to create a distance between the application developers and the production systems. Furthermore, hardware segmentation is also capable of being a divider between different applications or even environments so that none of them get in the way of each other.

Separation of Privilege

Separation of Privilege is also known as “least privilege,” which ensures that in a system, there are no individuals or objects (programs which make requests of databases) which possess more functions than they are entitled to. For instance, consider a finance application. When talking about the aspect of releasing payment to others, we come across three programs - the entity which is requesting the payment, the entity which is approving the payment, and the entity which is performing the payment. In this program, each individual has a specific role and job to perform, and hence, they are given the necessary privileges to be able to perform their approved function. However, no individual is given function exceeding their authority. This is known as the separation of privilege.

Accountability

Accountability is basically the ability of the application to detect and document any change made to the data. The record of the change made to the data extends to the application describing the event, for instance, which individual made the change, what was the change made, what was the time during which the change was made. Due to this feature, it becomes very difficult for individuals to tamper with the data without the activity being recorded and documented by the application or database.

Defense in Depth

Just as the name suggests, the Defense in Depth is a concept that revolves around the idea of using multiple security mechanisms to protect any asset. Since the security mechanisms are implemented as layers, this method is also known as “layering.” The main idea is that by using several security mechanisms, they adamantly form a protective layer around the asset,

which is to be protected. If even one of the layers presumably fails or is bypassed, then the other layers will still be functioning.

Abstraction

Abstraction is essentially a process where the user views an application from the standpoint of its functions that are of the highest level. By doing this, all of the functions that are lower level than the standpoint become abstractions. The reason they are called “abstractions” is that these lower-level functions work even without us knowing how, thus, treating them as black boxes.

Data Hiding

Just as the name suggests, the Data Hiding concept basically refers to the practice of concealing data of an object by hiding the object within another (encapsulation). By doing this, we can effectively mask and conceal the functioning details of the first object.

System High Mode

This simply refers to a system that operates at an information level that is of the highest authorization and classification. The access to this system is restricted, and only those individuals have clearance to access this system, which has an authorization of at least the same level or above the system’s information classification clearance.

Security Kernel

Security Kernel is a combined entity of several components, such as hardware, software, and firmware. The major function of a Security Kernel is to act as a mediator of access and functions between bodies such as objects and subjects. If we consider the model of protection rings, then according to this, rings which are more at a distance from the innermost ring have restricted access rights. In this protection rings model, the position of the security kernel is the innermost ring. Because of this position, the security kernel has unrestricted access to all system hardware and data resources.

Reference Monitor

The Reference Monitor is basically a component deployed and implemented by the Security Kernel of the system. The primary concern of the Reference Monitor is enforcing access controls on data and devices on the host system. The practical realization of this function is that whenever a user is detected requesting access to a file, the Reference Monitor deploys the function “Is this Person Allowed to Access This File.”

Supervisor and User Modes

Supervisor and User Modes are two different types of account privileges. In the computer systems of today, we can see that user accounts are bound by the associated privileges given to them. These privileges extend to either allowing unrestricted access and bypassing all security controls or just simply restricted access with all their requests being checked by the security controls. Supervisor Mode is also known as root privileges in certain systems (such as UNIX), Super Mode, and many other lexical terms for the same concept. Supervisor mode is advised to be used only for jobs pertaining to system administration, and user-end activities should always be run on User Mode. If a normal application is given privileged access, then it may exhibit unexpected behavior because it will bypass the system’s security mechanisms and controls.

Protecting with Antivirus Software

The use of antivirus is extensive and commonly used as standard equipment on many desktops and servers.

During the working of antivirus (AV) software, the procedure of the operating system to open and store files is interrupted, and the file content is matched with a list of virus signatures. If a match is found, the AV software immediately alerts the user of the detection of a virus via a pop-up window while preventing the virus file from being opened or saved. In an enterprise version, an alert is sent to the central monitoring console, after which the antivirus bureau takes necessary action against the virus.

Antivirus software vendors keep updating their versions, which allows the users to automatically download a new virus signature file, which then protects the systems from the latest viruses. In enterprise versions, the updated signature files are sent to every desktop system, and scans are made

timely. Updates in AV software and its signature files are checked once or twice a day.

Heuristics

Heuristics is the method by which the AV software examines certain suspicious behaviors in the system and detects the new variety of viruses before they can cause any harm. This method was developed after the number of viruses grew to almost a million, and the usual process of checking all the virus signatures became less and less efficient.

- **Conservation of space:** The problem of limited storage is not as prominent in PC hard disks as it is in lightweight devices such as smartphones, PDAs, etc. In this case, the use of heuristics reduces the need to keep a large signature file, which keeps updating as the number of viruses grows.
- **Decreased download time:** With the problem of the ever-increasing virus number, the signature files need to be downloaded and updated frequently. The time and internet capacity consumed to download these files can be saved with the use of heuristics.
- **Improved computer performance:** Instead of tediously comparing the files and messages with the large signature files to find a virus signature, it is better to employ heuristics and focus the defenses of the computer on finding any anomalous behavior.

AV Popping up Everywhere

In the present day, AV software is almost used everywhere. In addition to desktop computers, it can also be run specifically on e-mail servers to scan the attachments in e-mails for any potential viruses. The web proxy servers, file servers, and application servers all use AV software, where even firewalls and spam blocker applications are also being put into use.

The UNIX systems act as file servers and are used as a part of the information conduit between different computers, so antivirus software is used on UNIX as well to check for computer viruses.

The Perpetrators

The perpetrators often involved in the threats and attacks performed on sensitive information via viruses include people like hackers, intruders, virus writers, bot herders, and phreakers.

Hackers

Hackers are people with commendable computer skills that use their abilities to gain unauthorized access to sensitive information. These resourceful and creative people utilize their knowledge to find ways to explore the working, design, and architecture and also exploit the weaknesses in a security system.

Some responsible hackers put their abilities to use and discover vulnerabilities in any hardware or software and have them fixed so that real dangerous computer menaces will not be able to cause damage. Hackers are also hired by companies as consultants to improve their system security with their help.

Script Kiddies

The people that have no real knowledge of hacking but still acquire and make use of the programs and scripts developed by the hackers are called script kiddies. They mostly don't even know how their tools work, but they can still be harmful to systems and servers.

Virus Writers

The virus writers that are skilled and experienced can create new viruses that are quite effective and dangerous. While some virus writers are similar to script kiddies and can only make weak variations of already existing viruses with the help of templates and illegal cookbooks of viruses.

Bot Herders

Bot herders control and maintain bot armies by installing malicious software in various servers and computers to attack them. The individual can create these bot machines on his own, but mostly bot herders use software already developed by another party to create them.

Phreakers

Phreakers are referred to hackers who attack servers and systems to make use of free services. This term was originally used for people who hacked into telephone networks for the purpose of gaining free services spanning a long distance. After the security in telephone networks was reinforced, these phreakers turned to steal call cards.

Black Hats and White Hats

Black hats and white hats refer to harmful people and good people, respectively.

Chapter 4

Cryptography

In this chapter, we will focus our discussion on keeping the online information secure and safe by using cryptography. Cryptography is basically the encryption and decryption of information data so that only the receiver, which is intended to view the data, can access it, and unauthorized users cannot make sense of the information even if they obtain it.

It is very important for a CISSP candidate to have, at the very least, a good grasp on the fundamentals of cryptography. This is because the CISSP exam is known to check the candidate's proficiency in being able to efficiently apply the concepts of cryptography to the modern world problems and issues.

The Basics of Cryptography

In today's age, cryptography has entered the real of complex science rather than random encryption. In this section, we will discuss some of the cryptography basics, which include:

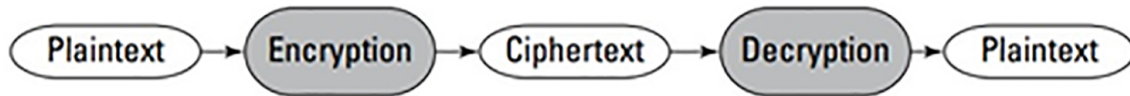
- Relevant Terms and Concepts
- The Cryptosystem components
- The Classes and types of ciphers

Plaintext and Ciphertext

Plaintext and Ciphertext both refer to the readability format of the message. While "plaintext" basically refers to the message which is simply in its original or decrypted form, a ciphertext refers to a plaintext message that has been encrypted, using cryptography, into a format (mostly scrambled and unintelligible) that is not readable until decrypted.

Encryption or Decryption

Encryption can be defined in terms of plaintext and ciphertext as the process, which simply converts a message in plaintext format into a ciphertext format. Decryption is the opposite of encryption, i.e., converting a ciphertext message into a plaintext format.



There are primarily two ways to encrypt a message on a network which are:

1. End-to-End Encryption
2. Link Encryption

End-to-End Encryption

In this type of encryption, the encryption of the data packets transmitted through a network is done at the source only once. The decryption then takes place only if the encrypted data packet reaches the decryption destination.

It is important to remember that only the data packets are encrypted and not the routing information; otherwise, the data would not be properly routed through the network.

Link Encryption

In this type of encryption, the data packets being routed through the network path are encrypted, decrypted, and then re-encrypted at every link (node). However, link encryption has a pre-requisite being that each link (node) of the routing path features separate and distinct key pairs for its upstream and downstream neighbors.

The major advantage of the link encryption, which also makes it different from End-to-End encryption, is that the entire data, and this includes the routing information, is encrypted. But as link encryption has its advantages, it also has its fair share of disadvantages which are:

- **Latency** : As we know that the data packets are encrypted and then decrypted and re-encrypted again at every node, this

creates an inevitable delay in the transmission of these data packets.

- **Inherent vulnerability** : The message using link encryption is at risk of being compromised if either the node is attacked or if the node's cache is compromised (where the message is saved).

The Cryptosystem

As the name suggests, the cryptosystem is actually a deployed or implemented system of hardware or software which is tasked with encrypting (converting the plaintext into ciphertext) and decrypting (converting the ciphertext back into plaintext) messages.

Below are some properties that are necessary for a cryptosystem to be effective and show results.

- The overall process of encryption and decryption is adamantly efficient. This efficiency extends to all of the possible keys which are housed in the keyspace of the cryptosystem.
- The usability and productivity of the cryptosystem should not be hard.
- The underlying effectiveness and security of the cryptosystem lies not in the secrecy of its algorithm but instead, in the secrecy of the crypto variables or keys used by it.

An algorithm that is kept as a secret is known as a "Restricted Algorithm," and the catch with these restricted algorithms is that they need to be hidden or concealed within the cryptosystem because, if discovered, the encrypted messages can be easily deciphered. Due to this characteristic of the algorithm, they are not commonly used as the prime factor for encrypting messages as the effectiveness of the restricted algorithm will boil down to how well it is hidden rather than the complexity and the enormous amount of variable solutions of the algorithm. Restricted Algorithms are seen to be used in applications where only minimal security is required.

Following are the basic elements on which the cryptosystem is made up:

1. **Cryptographic algorithm** : this is also known as a “cipher.” The main purpose of a cryptographic algorithm within a cryptographic system is to chronologically outline the details of the steps that the mathematical functions will take to create the ciphertext (encipher) and plaintext (decipher).
2. **Cryptovariable** : this element is also known as a “key.” Just as the name suggests, the key is a unique value that is applied to the cryptographic algorithm around which the enciphering and deciphering will be done. If the key is known, the message can be easily deciphered. Hence the robustness and effectiveness of the entire cryptosystem is largely dependent on how secure and tough the crypto variable (or the key) is.

Classes of Ciphers

The transformation of data into a cryptographic form is known as cipher. Ciphers basically operate on data resulting in either enciphering them or deciphering them. Similarly, based on the type of data on which ciphers operate, they can be classified into two categories, respectively:

1. **Block Ciphers**: The class of cipher, which chiefly operates on a single fixed block of plaintext data to convert it and produce a ciphertext corresponding to the plaintext, is known as a block cipher. The size of the block of data is typically 64 bits. Compared to stream ciphers, block ciphers are preferable when implementing ciphers in software. This is because the keys of block ciphers are much easier to manage (as using a given key on the same plaintext block will, every time, produce the same ciphertext block), and the support for block ciphers is wider.
2. **Stream Ciphers**: The class of cipher, which works in real-time and operates chiefly on a stream of data (which is continuous), is known as a stream cipher. The stream cipher works bit by bit, enciphering and deciphering the data stream, making it generally faster than a block cipher. The code required to implement it is also easier. But the problem faced when using a stream cipher is that the keys used by it are disposed of after a single use making key management immensely hectic and

difficult. If a stream cipher is used on a given plaintext (bit or byte) data, the corresponding ciphertext (bit or byte data) produced will always be different each time the original plaintext is encrypted. Hence, stream ciphers are generally preferred to be used in hardware rather than software. (A one-time pad is an example of a stream cipher).

The Different Types of Ciphers

Previously, we talked about the classes of ciphers based on the type of data on which they operate. Now, we will discuss the two different types of ciphers based on the way through which they convert plaintext into ciphertext. These two different types of ciphers are:

- 1. Substitution Ciphers:** As the name suggests, these types of ciphers transform plaintext into ciphertext by replacing the original components of the plaintext (such as the bits, characters, or character blocks) with alternate complementary components (alternate bits, characters or character blocks). Let's consider a situation where we are using a simple substitution cipher. The key (crypto variable) added to this cipher is generated by using the standard English alphabet, and this key is "modulo 26". We will now encrypt the word "BOY" by using the substitution cipher. By utilizing the math of the "modulo 26" key, three characters will be added to the plaintext message, and the result will be :

B	O	Y	PLAINTEXT
2	15	25	NUMERIC VALUE
<u>3</u>	<u>3</u>	<u>3</u>	SUBSTITUTION VALUE
5	18	2	MODULO 26 RESULT
E	R	B	CIPHERTEXT

Furthermore, substitution ciphers are classified into two categories based on the alphabets used - **monoalphabetic** (the cipher uses one alphabet to encrypt the entirety of the plaintext) and **polyalphabetic** (the cipher uses different alphabets when encrypting the bits, characters or character blocks of the plaintext).

2. Transposition Ciphers: These types of ciphers simply rearrange or systematically scramble the components (bits, characters, or character blocks) of the plaintext to produce a corresponding ciphertext. For instance, a columnar transposition cipher will rearrange a message (that is read horizontally) into columns to produce a ciphertext. Consider the following example : we have a single line of plaintext which needs to be converted into a ciphertext, this plaintext message is

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

This message will be first rearranged into nine columns (based on the number of words) :

THEQUICKB

ROWNFOXJ

UMPSOVERT

HELAZYDOG

After rearranging the message, it will be encrypted (or in this case, transposed) vertically resulting in a ciphertext:

TRMEHOPLEWSAQNOZUFVYIOEDCXROKJTGBUH

As we can see from this example, the letters used in the ciphertext are the same as the original plaintext message, and only the arrangement has been changed.

Apart from these two major types of ciphers, below is a list of some other notable ciphers:

- **Codes:** this type of cipher adds in words and phrases to the ciphertext.
- **Running ciphers:** also known as “book ciphers,” the elements used are from a book. For instance, in the “The Catcher in the Rye,” a running cipher can take page 137 as the key, and the text which is on that page is added to the modulo 26 to either encrypt or decrypt the message.
- **Vernam ciphers:** they are basically one-time pads.
- **Concealment ciphers:** ciphers that use pictures to conceal the original message.

Symmetric and Asymmetric Key Systems

Up until now, we have discussed the fundamentals of cryptosystems. In this section, we will focus on the details of the cryptographic algorithms.

Symmetric and Asymmetric key systems are basically classifications of the Cryptographic algorithms.

Symmetric Key Cryptography

The Symmetric key cryptography is also known by the terms “symmetric algorithm,” “secret key,” “single key,” and “private key cryptography” because symmetric key cryptography performs encryption and decryption of data by using one key only.

To understand Symmetric key cryptography better, let’s discuss an example where two entities (A and B) need to exchange messages by using Symmetric key cryptography. The procedure followed by these two entities would be something like this:

- Person A (sender) generates a plaintext message and then proceeds to encrypt this message by using a key that is only familiar to Person B (intended recipient).
- The encrypted ciphertext message is transmitted to Person B.

- Person B receives the message and proceeds to decrypt the ciphertext by using the same key, which was used by Person A, obtaining the original plaintext message.

Now let's bring in another person to the scenario. However, this person would harbor malicious intent as he would try to read the message without being allowed to do so. For the attacker (Person C) to read the message sent by Person A, he would first have to figure out the secret key, which was used to encrypt the message. This can be done by either using a brute-force attack or intercepting the key when the two entities (A and B) initially exchanged the message.

The Advantages and Disadvantages

Basically, this is how Symmetric key cryptography works. Although it may seem simple and secure, the symmetric system still has some major disadvantages, which are:

- **Distribution** : It is an absolute necessity that the distribution of the secret keys is secure. Otherwise, the data would be easily compromised if the secret key reaches someone who is not intended to access the data. The secure distribution of the secret keys can be ensured either by using out-of-band methods or by simply using the asymmetric systems.
- **Scalability** : No two communicating parties would have the same secret keys. Every communicating party would use a key that would be unique from the keys being used by the other parties.
- **Limited Functionality** : This is the major drawback of symmetric systems, i.e., not being able to provide authentication or non-repudiation.

While it's undeniable that the symmetric system does have some major flaws, there are still certain advantages that come with this system. Some of these advantages include:

- **Speed**: Due to their simple encryption mechanism, symmetric systems are much faster when compared to asymmetric

systems.

- **Strength** : Symmetric systems become more robust, secure, and harder to decrypt as larger and larger keys are used, such as a 128 bit, 256 bit, or even larger keys.
- **Availability** : Organizations have multiple options of algorithms they can choose from and implement in their system.

Standards Included in the Symmetric Key Algorithms

Additionally, symmetric algorithms feature several standards, such as:

- **DES**: also known as “Data Encryption Standard,” belongs to the class of a block cipher and primarily uses a 56-bit key. Furthermore, the DES algorithm is a symmetric key cipher, is composed of two elements, namely an algorithm and a key. The Algorithm itself is 64-bit while the key is 56-bit.
- **3DES**: also known as “Triple Data Encryption Standard,” is basically an extension to the life-cycle of the original DES algorithm. As we can infer from the name, the 3DES implementations involve encrypting the message, first by one key, then encrypting it again using a second key. After this, it is again encrypted by either using another third key or the first key, hence the name Triple DES. Since three separate 56-bit keys are being used, the length of the effective key is 168-bits. The work and time required to crack the Triple-DES algorithm are not only thrice that of the DES algorithm, but it is virtually impossible. But 3DES is not a holy grail; it comes with its fair share of disadvantages with the major one being its unacceptably slow speed making it incompatible with applications that need speedy throughput of huge chunks of data. Another weakness lies in its implementation through which a cryptanalyst can shrink the size of the key’s effective length down to 108-bit in a brute force attack.
- **AES**: also known as “Advanced Encryption Standard,” has its foundations based upon the Rijndael Block Cipher (has a key

length of 128, 192, and 256-bits and designed to be simple, fast and impervious to most of the known methods of attacks).

- **IDEA Cipher** : also known as the “International Data Encryption Algorithm” Cipher, is actually an evolution and improvement over the two data encryption standards, namely the PES (Proposed Encryption Standard) and IPES (Improved Proposed Encryption Standard). The IDEA cipher is classified as a block cipher due to its cryptosystem mechanics as it operates on plaintext blocks with a length of 64-bit and converting them to ciphertext by using a key whose length is 128-bit. Similar to DES, IDEA is capable of operating in four modes, each of which is distinct, and the IDEA cipher generally performs about eight rounds on sub-blocks that are 16-bit. Although the IDEA cipher is superior to RC4 and 3DES in terms of encryption prowess, however, due to the reason that it's patented, the IDEA cipher does not enjoy widespread use.

Asymmetric Key Cryptography

Asymmetric key cryptography is a type of cryptography that uses two distinct and separate keys such that one key is used for only encryption purposes. In contrast, the other key is used for decryption purposes (unlike symmetric key cryptography, which uses a single private key for both encryption and decryption purposes). Asymmetric key cryptography is also known as public-key cryptography because the keys are in such pairs that one of the keys is a public key (known by the sender and is used to encrypt the plaintext message). In contrast, the other key is a private key (known only by the intended recipient and used to decrypt the ciphertext message). Let's observe a demonstration to understand the concept of Asymmetric key cryptography better.

Consider a scenario where two people, namely Mr.A and Mr.B, wish to exchange a message between each other by using Asymmetric key cryptography. The steps taken by them to do so would be:

- First and foremost, Mr.A (the sender) proceeds to encrypt the plaintext message by using a public key, which is known by Mr.B (intended recipient).

- Once the plaintext message has been converted into ciphertext using person B's public key, the ciphertext message is transmitted to the intended recipient.
- After receiving the message, person B proceeds to decrypt the message by using a private key, which only he possesses.

Due to the use of a public key and a private key, the encrypted message becomes very secure because of the fact that even if an attacker gains access to the public key which was used to encrypt the message, only the private key can decrypt it. This means that not even the original sender who encrypted the message has the means to decrypt it. This is the major reason why we call the Asymmetric key system as a secure message as this system basically ensures the coherence of the confidentiality of the message.

Furthermore, a sender who is transmitting the encrypted plaintext message can ensure the authenticity of the message by signing the plaintext message during encryption. Let's change the above demonstration slightly to understand this concept:

- Mr.A (the sender) proceeds to encrypt the message by using Mr.B's (the intended recipient) public key, after encrypting it one time with the public key, Mr.A will now encrypt it again with a private key which is his own.
- After encryption, a ciphertext is produced, which is transmitted by Mr.A and received by Mr.B.
- After receiving the ciphertext, Mr.B will first confirm the authenticity of the message by using Mr.A's public key. After verifying its authenticity, Mr.B will now decrypt the ciphertext message using his private key.

To summarize the concept of verifying a plaintext message's authenticity, the sender signs the message with his private key, and the recipient uses his public key to confirm the received ciphertext message's authenticity.

While it may seem that asymmetric key cryptography can be cracked and taken advantage of by reversing the mathematical calculations to obtain a private key from the public key, that is certainly not the case. While it is

true that public and private keys are mathematically related to each other, it is impossible to derive a private key from a public key. This is because the asymmetric system employs the concept of one-way functions (a mathematical problem which can be computed in one direction but not in the reverse direction). To work around this characteristic of one-way functions, the Asymmetric system uses the private key (which is actually a trap door), which serves the function of resolving the reverse operation we discussed as the prominent characteristic of the one-way function.

Uses

Owing to their complexity, Asymmetric systems are preferred for uses such as:

- Key management
- Digital signatures

Furthermore, Asymmetric systems can be used in combination with Symmetric systems resulting in a hybrid system in the sense that the secret keys of the latter can be distributed securely by taking advantage of the functionality of Asymmetric systems.

Advantages and Disadvantages

The advantages of an Asymmetric system include:

- **Extended Functionality:** Compared to Symmetric systems that are capable of only providing confidentiality, Asymmetric systems feature extended functionality as they can provide both confidentiality as well as authentication.
- **Scalability:** The scalability of Asymmetric systems is infinitely better than what Symmetric systems can offer. This is because the latter requires exchange of secret keys between all the parties that are communicating while on the other hand, there is no need to exchange secret keys between the communicating parties, which not only resolves the issue of key management but it also scales in real-world practicality than Symmetric systems.

Methods of Attack

The methods used by hackers to attack cryptosystems can be classified into four major types, namely:

1. **Analytic Attacks:** the attack method in which the target of the hacker is to decrease the algorithm's complexity by using algebraic manipulation is known as an Analytic attack.
2. **Brute Force Attacks:** the attack method in which the hacker (cryptanalyst) attacks the cryptosystem, throwing all the possible key combinations at it until he comes across the right one. Hence the name brute force. The effectiveness of this attack depends on the length of the key and the speed of the attacker; however, this method is very time and resource-intensive.
3. **Implementation Attacks:** the attack method in which the hacker tries to aim the weaknesses in the cryptosystem (vulnerabilities that may be in the algorithm or protocols of the system) and exploit them to their advantage.
4. **Statistical Attacks:** this attack method is similar to an implementation attack in the sense that the hacker exploits the weakness in the protocol or algorithm of the cryptosystem in the implementation attack while, in a statistical attack, the hacker exploits a statistical weakness in the cryptosystem. This statistical weakness can be a simple lack of randomness in the key generation process.

Chapter 5

Operating in a Secure Environment

In this chapter, we will discuss the components of a computer and the resulting operations in a secure environment.

Computer Architecture

The design of a computer is discussed in computer architecture which includes:

- Hardware
- Firmware
- Software

Hardware

The physical parts of computer architecture are called hardware devices. Peripheral devices include a keyboard, mouse, printers, etc. while the main components are CPU, memory, and bus.

CPU

The Central Processing Unit (CPU) contains electronic circuits that carry out arithmetic, logic, and computing functions. It is comprised of components such as:

- **Arithmetic Logic Unit (ALU):** It carries out the logic functions consisting of numerical calculation such as addition, subtraction, multiplication, and division.
- **Bus Interface Unit (BIU):** Its primary functions include the management of data transmission between CPU and input/output devices via the bus systems.

- **Control Unit (CU):** The activities of various components during the execution of a program is coordinated by it.
- **Decode Unit:** In this component, the encoded data being received is converted into commands according to the instruction set architecture of the CPU.
- **Floating-Point Unit (FPU):** The FPU manages the larger mathematical operations based on floating-point calculations for the ALU and CU.
- **Memory Management Unit (MMU):** Provides addresses and sequence to the stored data and converts logical addressing to physical addressing.
- **Pre-fetch Unit:** It fetched the data in a slower memory to CPU registers for faster execution of the operation.
- **Protection Test Unit:** Ensures the proper implementation of all CPU functions.
- **Registers:** It temporarily stores the data, addresses, and instruction of the CPU in buffers

The fetch and execute cycle is the main operation of the CPU managed by its clock signals. In the fetch stage, the required instruction is retrieved from the memory while the execution phase operates to decode and carry out the instruction.

The CPU has four operating states:

- **Operating state:** The CPU carries out one or more instructions
- **Problem state:** In this state, the application problems are solved where only a limited subset of non-privileged instructions is involved.
- **Supervisory state:** It executes the privileged instruction accessible only by the system administrator or authorized user.

- **Wait for the state:** In this phase, the cycle is extended because the execution of an instruction is taking a long time.

The two basic computer designs are:

- **Complex-Instruction-Set Computing (CISC):** In this design, more than one operation can be carried out for only one instruction. The fetch phase of the “fetch-execute” cycle is the longest. The CISC architecture can be found in Motorola 68000 and PDP-11.
- **Reduced-Instruction-Set Computing (RISC):** The simple instructions are executed in this type of computer system where the clock signals are less in number. Both phases of the “Fetch-Execute” cycle are equal in these systems. Alpha and SPARC are examples of this design.

The microprocessors (CPU) are also classified according to functionality:

- **Multitasking:** In this process, a single processor rotates the execution of more than one task or subprograms.
- **Multiprogramming:** It takes turns to execute multiple programs in a single processor.
- **Multiprocessing:** The process of multiprocessing involves multiple processors performing numerous program executions at the same time.

The states associated with operating-system capabilities are:

- **Multistate:** It allows the use of multiple operating states like the modes of single-user and multiuser in Linux, and the Normal and Safe modes in Windows system.
- **Multiuser:** This type of operating system can identify and differentiate between different types of users, and provide shell environments, privileges, isolation, and profiles according to their identity. The privileged accounts in multiuser are susceptible to security concerns.

Bus

The bus refers to the data connections between the various devices of the computer through which signals, addresses, and data are exchanged between them. Some bus structures are:

- **Data bus:** It controls the transfer of data between various components like CPU, memory, and peripheral parts.
- **Address bus:** The addresses related to data and instructions are transferred by the address bus in between the CPU and memory.
- **Control bus:** The control bus transmits the information regarding control between the CPU and other components.

Main Memory

The main use of the Main memory includes storage of data, instructions, and programs. The two types of physical memory are:

- **Random Access Memory (RAM):** It is the kind of volatile memory whose data can be accessed and altered. RAM is present in the computer structure in the form of cache memory or primary memory. RAM can be divided into further two types.
 1. **Dynamic RAM (DRAM):** Due to capacitance decay, this type of RAM must be refreshed every two milliseconds by using multiphase clock signals.
 2. **Static RAM:** The SRAM is relatively faster than DRAM. It does not need to be constantly refreshed as it uses circuit latches, so it only needs a single-phase clock signal.
- **Read-Only Memory (ROM):** The ROM memory is Non-volatile memory where the data can be accessed directly, but it cannot be easily altered. It is included in the structure of the computer as firmware. Some types of ROM include:
 1. **Programmable ROM (PROM):** It is the type of ROM that cannot be altered once written.

2. **Erasable Programmable ROM (EPROM):** The type of ROM where the data can be erased by shining ultraviolet light onto a transparent quartz window visible on the chip.
3. **Electrically Erasable Programmable ROM (EEPROM):** It can be rewritten repeatedly with the use of high electrical voltage instead of UV light.
4. **Flash Memory:** It is used in USB drives for storage and transfer of data.

Secondary Memory

The secondary memory consists of non-volatile external devices to provide the computer with dynamic storage. The protection domain and memory addressing are the processes in memory that enhance its security.

Virtual memory addressing modes

- **Base Addressing:** This is used as a base or origin to calculate other virtual addresses.
- **Absolute Addressing:** This can act as a base address or can be used to locate without using referring to a base address.
- **Indexed Addressing:** The address is located using an index register as a reference.
- **Indirect Addressing:** This address contains in itself another address, which leads to a final location point existing in the memory.
- **Direct Addressing:** The address directly leads to the final point in the memory.

The difference between virtual memory and virtual addressing is that virtual memory is the apparent memory created by the combination of physical memory and hard-disk storage space, while virtual addressing is the specification of a location provided in the memory used by programmers and applications.

Firmware

Firmware refers to the program existing in the ROM memory and its electronic circuits.

Software

The operating system and programs running on the computer are both a part of the Software.

Operating System

An operating system controls the basic functions and workings of a computer, and other programs are also operated on this logical platform. The components of an operating system include:

- **Kernel:** It is the core component of the operating system which performs all the important tasks such as control of processes and hardware devices, and communication with external parts.
- **Device drivers:** These are used for communication between external and internal parts of the operating system as directed by the kernel.
- **Tools:** These programs work independently to provide maintenance such as filesystem repair and network testing, which can be controlled manually or automatically.

The main functions of an operating system are:

- **Process Management:** It allows the execution of various programs simultaneously.
- **Resource Management:** It manages access to resources with the help of different schemes.
- **I/O Device Management:** It establishes a connection to the external devices (input and output devices) and controls communication.
- **Memory Management:** This function manages the ROM, providing access to it, and moving processes back and forth.

- **File Management:** The operating system controls the file systems present on the devices and operations related to them.
- **Communications Management:** The communication processes on all the media and devices are controlled by it.

Virtualization

Security Architecture

The security architecture is a security design that defines the security controls and their implementation in the system architecture. It consists of a few concepts, such as:

Trusted Computing Base (TCB)

The entire collection of applications and mechanisms related to the protection that is used to implement the security policy is called Trusted Computing Base. It has a distinct boundary called the security perimeter.

Through the access control, a subject gives or denies permission to an object while this process is enforced on an object by the reference monitor.

A security kernel combines the software, firmware, and hardware into TCB, which makes use of the reference monitor process. It mediates access, prevents modification, and is verified as correct.

Operating in a Secured Environment

Open and Closed System

An open system has an independent code that can be freely accessed by anyone, and it operates according to an open standard due to which it can interoperate with different systems. The bugs and vulnerabilities can be detected and sorted out for better efficiency and development.

The code used in a closed system is not easily accessible to customers, and researchers and the proprietary components used in this system may or may not be interoperable with other systems.

Protection Rings

Protection rings are a hierarchical system architecture where the levels of interaction are arranged in the form of concentric rings with the trust level of the interaction increases with closeness to the center. The center ring 0 has the most privileges and includes the security kernel. The interaction rings farther from the center have lesser privileges. This type of architecture can be found in the MIT MULTICS operating system.

Security Modes

The security modes of operation deal with the information stored in various levels and are defined according to the classification level of information and the level of permission given to the authorized users.

- **Dedicated:** The clearance level provided by the authorized users must be able to access the highest level of information in the system. It is also important to have a valid need-to-know.
- **System High:** The user's clearance level should be able to access the highest level of information while a valid need-to-know is not needed.
- **Multilevel:** The information is processed in the classification levels of a trusted computer system. It needs an appropriate clearance level, and limitations are imposed by the system accordingly.
- **Limited Access:** For this type of mode, a security clearance is not needed, and the highest information level is Sensitive But Unclassified (SBU).

Recovery Procedures

Protecting the system and prevent vulnerabilities in the security during system hardware or software failure requires the following designs are implemented:

- **Fault-Tolerant Systems:** These systems detect and correct or avoid errors and faults, and so they can continue operating in the event of failure of any component.

- **Fail-Safe Systems:** The failure in system components results in termination of program execution to keep the system safe from compromise.
- **Fail-Soft (resilient) Systems:** In this system, when a hardware or software fails to function, the noncritical processes are dismissed as the system shifts to de-graded mode.
- **Failover system:** The failure of hardware or software causes the system to automatically move the processes to another component, such as the clustered server.

Vulnerabilities in Security Architecture

Many weaknesses and vulnerabilities might be present in a system architecture, some of which are:

- **Covert Channels:** The communication and transfer of information between processes that should not be allowed within the legitimate communication channel.
- **Rootkits:** This software collection gains access to a system or software that is illegal and operates to overthrow the system architecture. It uses various techniques to mask its existence and make it impossible for the target system to detect them.
- **Race Conditions:** The multiuser or multiprocessing systems may have some critical problems in their software code that result in the flaw of causing the output of a program to be tied to another timed event. The race condition, such as a time-of-check-to-time-of-use bug that is caused by the rare condition involving the checking of a system part and the use of the results of that check.
- **State Attacks:** The user sessions managed by web applications are used to identify users and differentiate between them. The process and algorithm by which these sessions are created must be able to resist attack and protect their session identifiers, or else the session might be taken over by the attacker who can commit fraud and monetary theft.

- **Emanations:** Sometimes, a system emits electromagnetic and acoustic energy, which can be dangerous in terms of security as these energy rays can be intercepted and used to obtain information illegally. For example, the CRT radiations from a monitor can be captured and interpreted to know what kind of data was being displayed on it. Furthermore, if a network has more than one coaxial cable that is not terminated in the cable plant, then an unrelated person can eavesdrop and obtain information.

Security Countermeasures

To make the environment and architecture of a system more protected and secure, countermeasures against the weaknesses are taken, which are listed as follows:

Defense in Depth

The security architecture defines a concept known as the defense-in-depth in which two or more than two layers of controls protect the data stored in the system from incoming attacks.

For instance, the database in a defense in depth architecture would contain several protective components where each of them has complete protection mechanisms but combined, they give a deeper and varied defense. These layers are:

- The Screening Router
- Firewall
- The system that prevents Intrusion
- Hardened Operating System
- Filtering of network access based on OS

System Hardening

The hardening of a system occurs before it is connected to the internet. In this process, the following measures are taken:

- Removal of components that are not needed.
- Removal of unneeded accounts.
- Termination of unnecessary network listening ports.
- Change of easy default passwords to complex ones.
- Execution of necessary programs at the lowest privilege, if possible.
- Installation of available security patches.

Heterogeneous Environment

The heterogeneous environment consists of various types of systems, which leads to better security advantages. The different systems will not have the same weaknesses which will make it harder to exploit its vulnerabilities while the uniform homogeneous system may have the same kind of weakness in all its similar devices and attack on one system will result in the attack of other similar systems present in the structure as well.

System Resilience

A resilient system is one that operates even under less favorable conditions. Some examples include:

- **Filter Malicious Input:** Any kind of input that may be recognized as a possible malicious or harmful attack will be instantly rejected.
- **Redundant Components:** Some redundant components like multiple network interfaces and power supplies are included with the system so that when hardware fails or malfunctions, they can be used to keep the system running.
- **Maintenance hooks:** These are undocumented features or a trapdoor in the software that is hidden and can allow the data to be exposed without the usual checks. It could be used at unusual points or when the data is to be obtained for illegal purposes.

- **Security countermeasures:** These countermeasures are prepared to eliminate the vulnerabilities in a system.
 1. Keeping the information regarding the system as hidden as possible.
 2. Provide access to the system only to the people carrying out the functions of the organization.
 3. Reducing the attacks by terminating unneeded services.
 4. Rendering access difficult via stronger authentication methods.

Security Models

Through the use of security models, the complex security mechanisms and systems are analyzed using simple concepts.

Confidentiality

Confidentiality defines the concept that only authorized users may access the information and functions, which is controlled by:

- **Access and authorization:** Only the people possessing the proper authorization related to business can access the facilities and controls.
- **Vulnerability management:** It includes processes like vulnerability elimination to patch hardening so that the system can remain protected from any possible attacks.
- **Sound System Design:** Such a design where unauthorized users are not allowed near sensitive data is called sound system design.
- **Sound data management practices:** The details of control of an organization on information use is included in the sound data management practices.

Integrity

The correct arrival of data in a system and remaining unaltered throughout its life is referred to as integrity. It rejects the efforts made by unauthorized users to change the data. Some of its characteristics are Completeness, Accuracy, Timeliness, and Validity.

The measures, as mentioned below, make sure that the data integrity is maintained and its quality is the highest possible.

- **Authorization:** The data retains integrity if it has the required qualification and authorization to be stored in a system.
- **Input Control :** It verifies the range and format of the input to check if it is in the proper standard.
- **Access Control :** It manages access and permission to alter the data.
- **Output Control :** It verifies if the output of the system is in the proper format or not.

Availability

The availability of a system is influenced by some characteristics, which are:

- **Resilient hardware design:** The presence of features in a system that ensures that the system will keep operating even in the case of failure of a component increase its availability.
- **Resilient software:** The design of the system and other components should be reliable and dependable.
- **Resilient architecture:** The redundancy in routers, firewalls, switches, and other such components in the architecture will prevent single points of failure.
- **Sound configuration management and Change management processes:** The occurrence of sudden downtimes is due to careless configuration management and Change Management practices, which results in a decrease in the availability of the

system. Hence, system management practices must be configured with care and diligence to avoid such a scenario.

Access Control Models

In these models, the access control systems and requirements are expressed in the form of theoretical or mathematical frameworks. Some common access control models are:

Bell-LaPadula

This formal confidentiality model was developed for the government and military applications, and it belongs to the category of mandatory access control systems. Its function includes managing the confidentiality of information by controlling access to it. Due to this access control model, the information does not travel from higher to lower layers for security purposes.

- **Simple security property (SS Property):** If an object has a sensitivity level that is higher than that of the subject, then it is not available to the subject as known in the “no read up” (NRU) process.
- ***-property (Star property):** If the object has a sensitivity level lower than that of the subject, then the subject cannot write information to the object as known in the “no write down” (NDU) process.

Bell-LaPadula can also act as a discretionary access control model due to the following properties:

- **Discretionary security property:** According to this property, the Access Matrix is the one that controls the permissions of access.
- **Trusted subject:** This property is the reverse of the *-property and can allow the subject to write down on the object, but it cannot change its intent.

Access Matrix

In a discretionary access control system, the access matrix provides the permission of access to the subject so that they can write or alter objects.

Take-grant

The take-grant systems offer the operations of creating, revoke, take, and grant to rights that are transferred between a subject and an object or another subject.

Biba

The Biba integrity model is a lattice-based model that makes sure that unauthorized users will not be able to make changes to the data. It includes the following properties:

- **Simple integrity property:** The object with its integrity level relatively lower, cannot be read by the subject. It is also known as “no read down.”
- ***-integrity property (Star integrity property):** If the object has a higher integrity level than the subject, then it can’t be written over by the subject.

Clark-Wilson

The Clark-Wilson model is an integrity model that provides the foundation for an integrity policy and puts forward a security framework for commercial purposes. It uses the following items and procedures to define the requirements for inputting data.

- **Unconstrained data item(UDI):** This represents the data present outside the control area whose integrity is not preserved.
- **Constrained data item (CDI):** It is the data available inside of a control area where its integrity must be protected according to the integrity policy.
- **Integrity Verification Procedures (IVP):** The validity of the CDIs is ensured through this procedure.

- **Transformation Procedures (TP):** This procedure ensures that the integrity of the CDIs is maintained.

The transactions in the Clark-Wilson model are controlled so that the internal and external data is consistent and ordered.

Information Flow

This type of access control model controls the flow of information by assigning the data with security values and class and giving them a direction during their transmission from one application or system to another. It analyzes the covert channels by examining the source of information and the path of the information flow.

Non-Interference

The primary concern of a non-interference model is to make sure that the various objects and subjects have no interaction with other objects and subjects on the same system so as not to interfere with the functioning of one another. Moreover, a non-interference model prevents the actions of subjects and objects on a system from being transparent (seen) to the other subjects and objects.

Evaluation Criteria

The purpose of the evaluation criteria is to provide us with a standard through which we can quantify the security level of the network or system. In this section, we will discuss three major types of evaluation criteria:

1. Trusted Computer System Evaluation Criteria (TCSEC)
2. Trusted Network Interpretation (TNI)
3. European Information Technology Security Evaluation Criteria (ITSEC)

Trusted Computer System Evaluation Criteria (TCSEC)

The TCSEC criteria are also known as “Orange Book.” The reason for this terminology is because of the history this evaluation criterion has, i.e., the TCSEC criteria were first developed for the U.S Department of Defense and was a part of the Rainbow series. The TSCEC was developed by the

institute “National Computer Security Center” way back in the early days of computers in 1983. With its implementation based upon the Bell-LaPuda model, the main objectives of the TSCEC criteria were to:

- **Measurement** : The first objective is to layout a metric standard through which it becomes feasible to evaluate the relative trust levels between computer systems.
- **Guidance** : The second objective is to highlight a standard to be followed by vendors according to which they build their computer systems, all while keeping the security requirements in mind to be qualified for a trust level.
- **Acquisition** : The third objective is to highlight a standard for the customers according to which they can specify acquisition requirements and, by doing so, find the computer systems that are fulfilling these requirements.

In the TCSEC evaluation criteria, security protection is divided into four major classes and sub-classes, detailed further in the table below.

Class	Name	Sample Requirements
D	Minimal Protection	Reserved for systems that fail evaluation.
C1	Discretionary Protection (DAC)	The system doesn't need to distinguish between individual users and types of access.
C2	Controlled access protection (DAC)	The system must distinguish between individual users and types of access; object reuse security features required.
B1	Labeled security protection (MAC)	Sensitivity labels required for all subjects and storage objects.
B2	Structured	Sensitivity labels required for all

	Protection (MAC)	subjects and objects; trusted path requirements.
B3	Security Domains (MAC)	Access control lists (ACLs) are specifically required; the system must protect against covert channels.
A1	Verified Design (MAC)	Formal Top-Level Specification (FTLS) required; configuration management procedures must be enforced throughout the entire system life cycle.
Beyond A1		Self-protection and reference monitors are implemented in the Trusted Computing Base (TCB). TCB verified to source-code level.

(According to DOD 5200.28-STD "Department of Defense Trusted Computer System Evaluation Criteria," 1985)

Although it is not necessary to be knowledgeable of all the requirements for each level of the TCSEC while preparing for the CISSP exam, it is still necessary to know the levels at which the DAC and MAC are implemented in. In addition, the following concepts are also important to understand and remember:

- Relative trust levels of the TCSEC classes.
- Relative trust levels of the TCSEC sub-classes.

Below are some of the prominent limitations of the TCSEC (Orange Book) :

1. Although the Orange Book takes care of issues such as confidentiality, it does not address the availability and integrity issues.

2. The Orange Book is not compatible (or even applicable) to the majority of the commercial systems.
3. The major emphasis of the Orange Book is on securing the system from any unauthorized access, even though the fact that the statistical evidence details the primary cause of security violations to be inside access.
4. The Orange Book is simply not designed to have the capability of addressing networking issues.

Trusted Network Interpretation (TNI)

In the preceding section, we briefly mentioned the Rainbow Series and how the TCSEC is actually a part of the Rainbow Series. Well, the Trusted Network Interpretation is also a part of that same Rainbow Series, and the primary concern of this evaluation criteria is to resolve issues in trusted computer and communication network systems such as confidentiality and integrity. Trusted Network Interpretation is also commonly referred to as “Red Book” within the Rainbow Series, just as how TCSEC is referred to as “Orange Book.”

The Trusted Network Interpretation evaluation criteria are divided into two parts, as detailed below:

1. The first section of the TNI is basically a guideline that extends the functions of system protection standards, which were initially defined by the Orange Book (TCSEC).
2. The second section of the TNI introduces and details some extra security features. These new security features include transmission security, communications integrity, and protection from DDoS (denial of service).

European Information Technology Security Evaluation Criteria (ITSEC)

The ITSEC (European Information Technology Security Evaluation Criteria) was initially developed in the later stages of the 1980s, a little after the advent of the TCSEC criteria. Similar to TNI, the ITSEC evaluation

criteria address the same issues that the Orange Book wasn't capable of, i.e., issues pertaining to integrity, confidentiality, and availability were addressed by the ITSEC and not only that, ITSEC does this by evaluating the whole system as well. This was later termed as "Target of Evaluation."

While the ITSEC evaluation criteria chiefly evaluate **functionality** and **assurance**, however, this is done separately, and this evaluation is further divided into classes and levels, respectively (ten functionality classes and seven assurance levels). For further details of this evaluation done by the ITSEC, refer to the table below:

Functionality (F) Class	Assurance (E) Level	Description
NA	E0	Equivalent to TCSEC Level D
F-C1	E1	Equivalent to TCSEC Level C1
F-C2	E2	Equivalent to TCSEC Level C2
F-B1	E3	Equivalent to TCSEC Level B1
F-B2	E4	Equivalent to TCSEC Level B2
F-B3	E5	Equivalent to TCSEC Level B3
F-B3	E6	Equivalent to TCSEC Level A1
F-IN	NA	TOEs with high integrity requirements
F-AV	NA	TOEs with high availability requirements
F-DI	NA	TOEs with high integrity requirements during data communication
F-DC	NA	TOEs with high confidentiality requirements during data communication
F-DX	NA	Networks with high confidentiality and integrity

	Requirements
--	--------------

(Reference: <https://www.pearsonitcertification.com/articles/article.aspx?p=1998558&seqNum=5>)

Chapter 6

Business Continuity Planning and Disaster Recovery Planning

This chapter steers our focus chiefly on two types of plans, namely:

- Business Continuity Planning (BCP)
- Disaster Recovery Planning (DRP)

In an organization, both BCP and DRP are essential and very crucial in helping the organization to bounce back from a loss whenever a disaster comes their way. In short, it is essential for business organizations to have an active Business Continuity Plan and a Disaster Recovery Plan so that they easily continue and recover the business operations whenever a calamity or disaster strikes them. Hence, in this chapter, we will be exploring the fundamentals of this domain.

Setting Up a Business Continuity Plan

Setting up a BCP includes the following steps:

1. Identifying the Elements of a Business Continuity Plan
2. Developing the Business Continuity Plan
3. Implementing the Business Continuity Plan
4. Maintaining the Business Continuity Plan

In this section, we will discuss these four steps towards setting up a proper BCP.

Identifying the Elements of a BCP

Before we can proceed to put a Business Continuity Plan into action, we must first assess and identify the components which serve two purposes.

They are handling the continuance of the business organization's critical functions, and also encompassing all the supporting functions and resources correlating to these critical functions.

Following are main components of a BCP:

- **Emergency Response:** they are basically teams that respond to emergency situations while following written procedures and checklists to maintain the functionality of the business's critical functions. The purpose of a written procedure is very simple. After a disaster, it is not ensured that the people whose job is to perform the critical functions are available. As such, their replacements will need to substitute for them, and there may come a case where these people are not familiar with the task; hence a written procedure will greatly help them. Moreover, in a disaster, the situation can become quite chaotic, and a written guideline of procedures can direct the team's focus and resources towards performing these critical functions (similar to the "break the glass" instruction during emergencies).
- **Damage Assessment:** this usually involves the assistance of experts (specifically the ones who assess damages to buildings, special pieces of equipment, and machinery) that perform an inspection of the organization's premises and give an assessment of the damage as the aftermath of a disaster. Furthermore, a damage assessment can be divided into different stages depending on the nature of the disaster, for instance, a preliminary assessment may just be a quick overview of the situation while the following damage assessment may be a detailed and in-depth assessment of the destruction. The purpose of a damage assessment is to provide an analyzed view of the situation in which whether the organization can utilize the building, equipment, or machinery that was affected or if these items need to be repaired or if they have become utterly useless and need to be replaced.
- **Personnel Safety:** it is very crucial to distinguish the priorities and values during a disaster, and accordingly, the safety and

well-being of the organization's personnel should be the utmost priority, ahead of any and every item.

- **Personnel Notification:** every business organization should have an apt and effective provision of notifying every personnel regarding an outbreak of a disaster. It is due to the fact that not every person immediately notices every disaster, and this aspect is even more evident when communication infrastructures are compromised in a disaster. Hence an organization must have key provisions through which they can notify all of their personnel of the current situation and keep the chaos and disorganization to a minimum while carrying out proper counter-measures.
- **Backups and Off-site Storage:** data is a very important asset for any business organization, and since it is a very sensitive and volatile asset, it is very important to keep proper backups for all the important data. Any fault in the hardware or software could corrupt the data and fatally damage the organization's functioning. It is advised to perform data backups every day and keep another separate back-up somewhere secure away from the main organization's building, ensuring that if a disaster hits the main site and the computers storing important data are compromised. Off-site storage will be able to replace this loss of data effectively. In short, the major purpose of an off-site data storage backups is to basically ensure that in the event of a disaster and major data loss in the primary data centers of the organization, then there is up-to-date back-up data available to minimize the losses.
- **Utilities:** in the case of power failures or power outages, an organization should have a back-up power source to keep the critical machinery and equipment running. For this purpose, an uninterruptable power supply (UPS) can act as a good option for power outages that last for a few hours. During prolonged periods such as a day or two, the organization should have a plan for fuel replenishment for its running generators.

- **Logistics and Supplies:** the BCP team should assess the essential components which are needed to maintain the proper working of the critical functions. After figuring out the most important aspects which are needed to sustain the critical functions, the team needs to take every disaster situation in consideration when planning countermeasures. For instance, if an organization's critical functions depend on a just-in-time shipment, but, due to an earthquake, the shipment is delayed or is unable to reach the organization, then there should be other alternatives through which these materials can be acquired.
- **Data Process Continuity Plan:** in this digital age, one of the most vital facilities which are now emphasized accordingly in business organizations is none other than data facilities such as data processing sites. There are seven major types of data processing types which are namely:
 1. **Cold Site :** Cold sites are basically vacant rooms that are set up with environmental facilities. However, a cold site does not have any computing equipment, hence making it a very inexpensive option for an organization. But, it is important to take note that since no computing equipment is set-up when the time comes for the organization to assume a workload, then it will take time for the setup to be completed.
 2. **Warm Site :** Warm sites are basically just cold sites, with the difference being that warm sites are preemptively equipped with the necessary computing equipment and communication links. However, for a warm site to assume operations such as production, the computers in this data processing site must be first loaded with the required business data and application software.
 3. **Hot Site :** Hot sites are essentially a data processing site which is fully equipped with the proper equipment (the computers used are the same as the production system).

This site is synced with the active main production system computers so that all application changes, operating system changes, and patches are synced; even the business transactions are synced to the Hot site by means of mirroring or transaction replication. Furthermore, the operating staff stationed at the Hot site are trained and familiar with the site's functioning making it possible for Hot sites to take over production operations only at a moment's notice if required to. Hot sites are very effective; however, the funds required to set them up and manage them are very expensive.

4. **Reciprocal Site** : A Reciprocal site is basically a site that is shared by two organizations under an agreement. This agreement to share an organization's own data center and pledge its availability is known as "reciprocal agreement" and it comes into effect when a disaster befalls any of the organizations who have signed this agreement.
5. **Multiple Data Centers** : Just as the name suggests, big organizations which have the funds and capital to invest, use multiple data centers (regional data centers that are far apart from each other) for their daily operations. The purpose of this is to steer away from the trouble of arranging other types of sites (hot, cold, or warm sites) and bringing the concept of "divided we stand" into effect.

In summary, the most effective in terms of recovery and readiness is a hot site; however, a lot of funds and effort are required to set it up and manage it.

Developing the Business Continuity Plan

Developing a Business Continuity Plan is arguably the hardest part of setting up a BCP because this phase involves formulating strategies for each

critical business function. The process of formulating and developing such strategies is also known as “Continuity Strategy.”

Strategizing to Make the BCP a Success

An important step of working towards developing a Continuity Strategy is, first of all, strategizing towards ensuring that the BCP turns out to be a success. For that, a successful and effective Continuity Strategy is required. The following guidelines emphasize some of the most important aspects one should be aware of during this phase of the project:

- **Call things as they are:** this means that if you’re involved in developing the Continuity Strategy for the BCP, then you should set aside your biases and politics and give calls based on their actual importance. The priority is to keep the business afloat even before a disaster befalls the organization.
- **Build Small Teams of Experts:** smaller teams with trained professionals are vastly better than big teams with novices because this not only makes teamwork more prominent, and smaller teams are easier to manage. Teams comprising of experts who excel in their respective fields will not only analyze critical business functions more accurately, but they will also show better results.
- **Brainstorming:** brainstorming is never a bad practice. Often times, some mediocre ideas lead to better ideas, and this can eventually lead to another excellent idea.
- **Result Sharing between Teams:** holding sharing sessions of highlights that each team has observed over the past few weeks can not only generate good ideas. It can also improve the overall effort that each team has put in so far and promote more productivity.
- **Discourage Competition:** competition among teams should be discouraged and abhorred because this will lead to inevitable failure. Unity, teamwork, and the desire for success should be mutual among the personnel of the organization to succeed in formulating an effective Continuity Strategy.

- **Retain a BCP Expert:** a BCP expert who has experience in formulating successful BCP plans and continuity strategy can boost the productivity of your teams immensely.

Simplifying Large or Complex Critical Functions

Most of the time, some critical functions are either just too large or just very complex to analyze in one go. In such cases, breaking down these functions into smaller, more comprehensible and easy to analyze can play a big role in making the BCP a success. A typical complex critical business function can be broken down into smaller components such as:

- **People** : identify the important people that play a critical role or are considered as a critical sub-function to the main function. These are the people who are needed to maintain the proper functioning of the organization.
- **Facilities** : figure out the contingency plan in case the primary facilities of the organization are not available for use and from where can the organization gain access to the necessary facilities to resume their functions.
- **Technology** : identify all the electronic, hardware, software, and computer (including networking) equipment that support the critical business function. Afterward, consider what other components or equipment are capable of supporting the same critical function if any one or all of the original supporting elements become unavailable.
- **Miscellaneous** : identify all the other elements, equipment, components, services, and supplies that support the critical functions.

After breaking down a complex business function into smaller corresponding elements, each element is assigned to a specific individual within a team. It then becomes necessary for the team members and individuals of other groups to meet up frequently to make sure that the strategies devised by each group and individual can come together form a complete, cohesive whole. In short, integrating the individual strategy

pieces into a complete Continuity Strategy is very important after breaking down a complex function.

Documenting the Strategy

The next part of developing a Business Continuity Plan after strategizing a Continuity strategy is to document every small detail of it (every minute detail documented in chronological order, step- by-step). Documenting the details of a continuity strategy for each critical function is a very important task due to the fact that it helps people and personnel of a business organization perform the tasks demanded of them with minimal chances of mistakes. In other words, the individuals developing the continuity plans and strategies may not be the same people who are carrying out these plans and strategies. They can be either unavailable or have their roles swapped during a disaster; hence a documented strategy can help remedy this situation to quite an extent.

Implementing the Business Continuity Plan

Although it can be considered quite the milestone for an organization that has developed and documented a Business Continuity Plan after carefully reviewing and editing it (and placing it into the three-ring binders), the job is still incomplete. The BCP needs to be tested, announced, and socialized, implemented, and maintained.

Securing Senior Management Approval

The importance of senior management's approval lies in the fact that when they personally and publicly approve the Business Continuity Plan within the business organization, then all the employees and personnel of the organization are given an idea of the importance of such an emergency planning. In short, when the BCP has been documented and reviewed by the stakeholders, the next approval required is from senior management, and their approval involved announcing the BCP publicly inside the business organization to make it official.

Promoting Organizational Awareness

Once a Business Continuity Plan has been announced publicly, the next step is to make sure that every working individual of the organization

understands their role in this plan. To achieve this awareness, one method is to establish training camps for a large number of people who are required to be present in the case a disaster does strike. Hence, all of the employees and personnel should know and understand the Business Continuity Plan.

Maintaining the Plan

Once a Business Continuity Plan has been fully developed and implemented, the next job is for the BCP team leader to make sure that, if any details need changing or editing, they are done. He should be aware of the environmental changes and other factors that are directly related to the Business Continuity Plan and keep track of how it affects the plan and maintain the BCP accordingly.

Setting Up a Disaster Recovery Plan

A BCP and DRP have certain elements in common such as both of these plans:

- Have common roots
- Require assembly of project teams
- Require executive support and sponsorship
- Identify critical business functions

Although both Business Continuity Planning and Disaster Recovery Planning go hand-in-hand with each other, this is where the similarities between these two come to an end. In the succeeding topics of this section, we will talk about how a business organization can develop a Disaster Recovery Plan.

Developing a Disaster Recovery Plan

The main difference between a BCP and a DRP is that a Business Continuity Plan is to keep the business functions operating, while a Disaster Recovery Plan is to restore the facilities that have been damaged in the disaster. As such, it is working towards restoring the original locations so that the critical business functions can resume operation in their main site.

Preparing for Emergency Response

Responding to emergency situations is the job of the emergency response team. These teams are required to be prepared and ready for any and every possible scenario and hence, to assemble such a team, it is needed to give them specialized training so that they are capable of tackling situations such as:

- Water damage
- Smoke damage
- Structural damage
- Flooding
- Hazardous materials

Not only is it necessary for the emergency response teams to be familiar with the procedure when dealing with such situations, but the teams should also be knowledgeable and know every detail about all the facilities in the organization. For this purpose, every type of response should be documented so that the responding teams can know how to respond to each situation and are kept up-to-date with any changes and updates in the facilities.

Furthermore, two major activities come under the situation of responding to emergencies, and they are **salvage** and **recovery**.

Salvage

The major concern and purpose of the salvage team are to restore the functionality of the damaged facilities back to their original conditions. The process of restoration includes:

- **Damage Assessment** : Examining the facilities thoroughly and assessing the extent and nature of the damage received by them. In most cases, experts such as structural engineers are tasked with performing such assessments for the organization.
- **Salvage Assets** : Taking out and removing the remaining assets of the organizations - this includes items such as computer

equipment, records, furniture, inventory, etc.

- **Cleaning** : After salvaging the assets, the next activity is cleaning the facility to clear out and diminish damages such as smoke damage, water damage, debris, etc. In most cases, companies that are professionals in doing such jobs are hired.
- **Restoring** : Once the assets have been salvaged and the facilities have been cleaned, the next plan of action is to perform complete repairs where necessary and bring the facilities up to operational readiness as they were before the disaster struck the business organization. Once done, the facility is now ready to resume performing its business functions normally.

In short, the primary concern of the salvage team is to repair and restore the facility and get it up and running again.

Recovery

Recovery is directing the BCP team to equip the alternate facility sites with the required supplies and deal with the logistics and coordination of this process so that the main operational functions of the business can be run from there.

Notifying the Personnel

Similar to the Business Continuity Plan, the Disaster Recovery Planning should include proper communication links and provisions to notify the working personnel of the organization of the facilities which have been affected and are now closed. Moreover, additional work instructions can also be relayed through this communication channel in emergency disaster situations.

Facilitating External Communications

Facilitating the external communications during a disaster basically includes the same steps and provisions taken by the BCP team. In essence, there is no real difference between the information and logistical planning for external communication equipped by the BCP team and the DRP team.

Maintaining Physical and Logical Security

Although it's not frequent, there are situations where maintaining physical security for the business organization becomes crucial in the aftermath of a disaster because there are chances of heathens looting and vandalizing the organization amidst all the chaos. To avoid this, the organization should be capable of deploying additional security guards to maintain the security of its assets until law and order are restored. Moreover, this physical security does not simply extend towards the assets of the organization, but it also covers the well-being and safety of the personnel working there.

Now comes the part of reinforcing the logical security. By logical security, meaning the protection of data and information from unauthorized access. For such purposes, the security controls which have deployed and implemented in the main systems of the organization should be applied to the recovery systems as-well to keep the vulnerable data secure. Such security controls include

1. Access controls
2. Authorization
3. Audit logging
4. Intrusion detection
5. Firewalls
6. Encryption of data
7. Backup
8. Physical access controls
9. Environmental controls
10. Personnel controls (performing background checks etc.)

In short, since the information being processed, used, and stored on recovery systems is basically the same information that would be on the

main production system of the organization. Hence there should be no compromise in implementing the security controls, and the same security controls used on the main systems should be applied to the recovery systems.

Conclusion

Throughout this book, we have journeyed through the fundamentals of some of the key concepts which are crucial to have an understanding of for the CISSP exam. Whilst the major focus of the exam is on topics related to Information Security and Networking, we have also discussed the important business planning. These include Business Continuity Planning and Disaster Recovery Planning, designed to help the candidate gather some practical information regarding a professional organization's inner workings and security channels. This book purposely leaves out some very complex and difficult to understand concepts and topics and focuses solely on presenting those fundamental ideas and concepts that a candidate should be knowledgeable of at any cost when appearing for the CISSP exam. The book stays true to its purpose of highlighting key topics that are seemingly too compounded and complex to understand by breaking it down to its fundamentals and then, after gaining a clear understanding of the fundamentals, present the concept once again but this time, easy to comprehend and understand.

In short, the book has covered a variety of topics all purposed to boost the success rate of the CISSP candidate by keeping the concepts down to their fundamentals, making them easier to understand and relatively simple to absorb.

CISSP

*A Comprehensive Guide
of Advanced Methods to Learn the CISSP
CBK Reference*

DANIEL JONES

Introduction

CISSP is the world's most renowned, premier, and most accepted cybersecurity certification offered by (ISC)². CISSP stands for Certified Information Systems Security Practitioner. In 1994 CISSP was launched, and it opened a path to standardized, recognized common body of knowledge for information security practitioners.

(ISC)²

Formed in 1989, (ISC)² is the world's leading and the largest, non-profit IT security organization. As with any industry information security knowledge and competency required a solid standardization as well as vendor neutrality. Hence, the foundation of "International Information Systems Security Certification Consortium" or, in short (ISC)², addressed these issues significantly.

(ISC)² currently offers a wide range of security certification paths such as CISSP, SSCP, CCSP, CAP, CSSLP, and HCISPP. It has the largest community of information security professionals where the brightest and vibrant minds congregate. CISSP is one of the paths you could take to join the membership with attractive perks. You can find out more by visiting their site from <https://www.isc2.org/>

Foundation of CISSP and Current Standing

CISSP was officially launched in 1994, and it provides solid assurance through the ever-evolving nature of information technology. In 2003, NSA (National Security Agency, Department of Defense, USA), adopted it as the baseline to form the Information System Security Engineer Professional (ISSEP) program. This is one of the concentrations of CISSP.

Other industry and tech giants firmly accept CISSP as the most comprehensive and acclaimed certification. A member of the (ISC)² is known to have many benefits, perks, and unparalleled recognition. For instance, CISSP stands the most required certification on LinkedIn. CISSP is also the first to meet the ISO/IEC Standard 17024.

CISSP is available in 160 nations, and 142000+ currently holds the certification.

Job Prospects

Among the Information and Communication Technology field, there are certain high-risk and high-reward carriers. The information security field is on the top of this list. It is widely respected and rewarded. With the ever-emerging technological advancements and the ever-growing security threats, information security carrier has become a uniquely challenging and highly paid profession.

A CISSP holder remains top of this ladder with adequate skills, and respect among the community. Therefore, it is a path toward a rewarding carrier and provides a boost to an existing carrier. The certification also provides many more benefits such as,

- A robust foundation.
- Carrier advancements.
- High profile knowledge and skills with vendor neutrality
- Training opportunities and advancements
- Extremely high paygrades.
- A vivid community of professionals with top-level skills

Let us look at the current job prospects. A CISSP holder is a perfect match with the following roles.

- Chief Information Officer
- Director of Security
- Information Technology Directors
- Information Security Managers
- Network Security Professionals
- System Engineers
- Security Auditors and Consultants

Salary Prospects:

- According to the industry researches and surveys, the average salary in the U.S.A. is \$131,030.

Industry Prospects:

- The demand for information security professionals is expected to grow by 18% from 2014 to 2024.
- There is a higher demand in the defense sector, finance sector, and the professional service sector. Also, healthy growth is expected in sectors such as healthcare and retail.

Thinking About CISSP Certification?

CISSP is not just a do it and leave it kind of certification. In fact, it is a multi-disciplinary security career path for those who admire world-class recognition, the best of its class professional practices, and practice information security as a lifestyle. From an organizational perspective, CISSP practitioners can architect, implement, administer, and maintain a strong, robust, and competitive information security strategy. In reality, practical implementation of such is a crucial and cumbersome task, yet once implemented, it acts as the defense shield of the entire organizational operations. This is one of the most critical business requirements. CISSP is introduced as a solution and a bridge between business and information security gaps. Therefore, this certification is an outstanding proof of critical skills, knowledge, and intelligence required to address these requirements.

CISSP is not just a theoretical approach to information security practices. Through the learning curve, you must be able to maintain the knowledge and practical skills, and you must prove your qualifications to become a successful CISSP practitioner. In other words, you are not granted certification and acceptance until you prove the practical skills in real-world engagements.

In this book, you are prepared for the theoretical part; in other words, the common body of knowledge (CBK). What is CBK? As you may already aware, the seriousness of responsibilities as an information security professional is unmatched. To achieve these crucial challenges and mission-critical goals of the industry, you need to have an in-depth understanding of the information security components that forms the comprehensive

framework known as the common body of knowledge. The CBK includes eight domains and relevant skills, techniques, and best practices. After, it is arranged so that the reader gains both comprehensive and competitive knowledge once studied.

It does not matter if you are new to the information security field the book is a step by step guide letting you learn from your pace and master each domain. In this book, the chapters are divided into smaller chunks of knowledge so that you can absorb and memorize better. Each chapter includes examples, graphics, and tips that you can use to understand, memorize, and recall the information with ease. Therefore, even for a starter, the books will be a useful guide.

How to Use this Book

CISSP is one of the most comprehensive, widely accepted, dominant, mature, and vendor-neutral professional certifications. Such a place has its perks and challenges. Your responsibility to keep your commitment, dedication, and practices to conquer it. Other vendor-neutral certification paths lead to the same goal. If the selection is CISSP, you have already accepted it and is a great choice.

In truth, CISSP is not for everyone as it requires you to ultimately develop the highest competency through knowledge, skills, and techniques. Practicing daily while facing higher-level challenges requires a deep focus and understanding. That requires your internal skills polished sharply. To address these requirements through the CBK realms, you need to have a robust starting point.

The intension of this book is to provide you a solid understanding of fundamentals. Without knowing the basics, it is difficult to perceive the vast level of information that you are going to concentrate on through the CISSP journey. In fact, the book starts with the basics, but it does not stop there. It takes you to more advanced topics once you are ready. In other words, it provides A-Z knowledge in all the eight realms, nothing less.

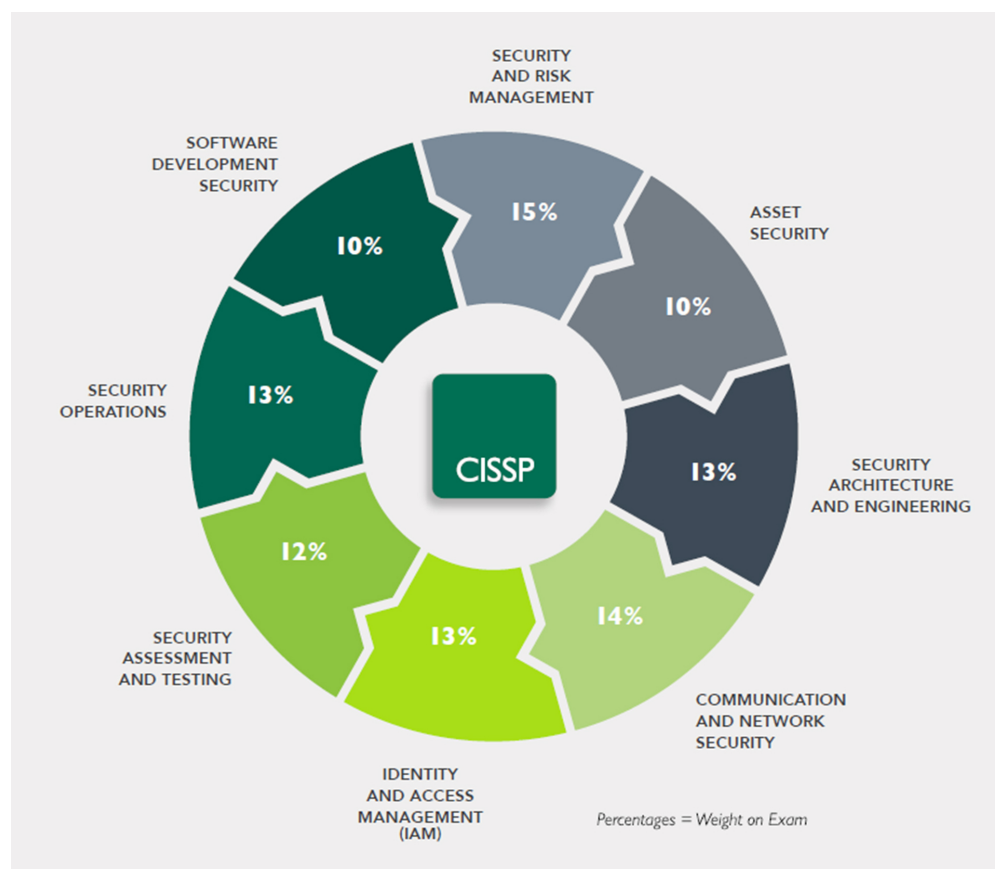
The book includes highlighted areas where you need more focus, and it helps you to keep short notes. Each section includes additional tips and relevant examples to help grasp the knowledge. While reading this book,

you are advised to keep short notes, use (ISC)², and other resources, take part in relevant webinars, workshops, and other activities to get more hands-on and to get more familiar. It is effective to build stories, mind maps, charts, and graphical representations so that you can easily recall the important study areas. Applying critical thinking is required while scaling your information store in your mind. To pass the examination and become a CISSP practitioner, key success factors are reading and understanding, applied knowledge, critical thinking, and experience. Therefore, you need to pay special attention and focus on these factors as well.

CISSP Domains, Learning Options, and Examination

CISSP Domains

CISSP Common Body Knowledge comprises of eight domains. Each domain is a critical step toward achieving a specific security goal. Therefore, the students are critically evaluated for their expertise in every domain. Let's look at the eight domains below.



CISSP 8 domains and weight. Image credit: (ISC)²

More on CISSP

- CISSP examination is available in 8 languages at 882 locations in 114 countries.
- English examination is now computer-based (from December 18, 2017). This is known as Computerized Adaptive Testing (CAT). The number of questions can be from 100 to 150. You have to complete the test within 3 hours.
- Non-English examinations are still conducted as linear and a fixed form examination.
- The examination is available in many other languages, including Brazilian, French, German, Japanese, Korean, Portuguese, Spanish, Simplified Chinese, and a suitable language for visually impaired.
- There will be 250 questions, unlike in the CAT, and is 6 hours long.
- The passing score is 700.

Learning Options

There are four major options if you are willing to learn CISSP from scratch.

- Classroom-based.
- Online, instructor-led.
- Online, self-paced.
- Onsite.

The first option is classroom-based training, like any other program. This is more common among students who prefer more guidance, attention, and community. It allows the students to work with the instructor directly. The trainer is often an (ISC)² professional or an authorized partner institution. The classroom can be discussion-based, and students receive well-

structured, official courseware. Training will take three to five days, eight hours per day. It includes real-world case studies, examples, and scenarios.

The next option is more suitable for the same student category with travel difficulties or a busy schedule. In fact, online or virtual classrooms are the best in contrast to all the other options. It is highly cost-effective, reduced pollution, and saves time. When this option is selected, (ISC)² courseware is available for 60 days. Also, an authorized instructor is available to help you. The course is available as a weekday or weekend course (part-time). Finally, there is also a dedicated examination scheduling assistant.

The next option is the popular one above all at present. This method is more suitable for people who are geographically dispersed. In nature, this is similar to the virtual classroom option. However, there will be no live instructor. Instead, there will be a curriculum, engaging course content, HD video lessons created by the instructors. This also turns on portability.

If you select (ISC)², you will get access to flashcards, examination simulators, and interactive games and are available for 120 days. With this option, however, there is a catch. That is, you have a large selection of training providers other than (ISC)² and authorized partners. Not all the institutions are authorized by CISSP, and there can be a wide range of selections when it comes to the diverse material and technique they use.

For organizations, there is the “Onsite” training option. This is similar to classroom-based training. With this option, (ISC)² provides an examination schedule assistant for you.

If you are planning to purchase books, there are excellent written material that specifically focuses on the CISSP curriculum, specific domains, exam preps, and many more. You can find the study resources at <https://www.isc2.org/Training/Self-Study-Resources>

Preparing for the Examination

Preparing for the CISSP examination is also something you need to plan carefully. CISSP content is wide, full of broad and complex study areas. In addition to the classroom or self-paced study, you need to focus on exam readiness. You will be able to find high-quality, CISSP model questions and

exam simulations. Flashcards and podcasts also help significantly. But the CISSP examination is not just about what you have learned.

The following factors may disqualify you from (ISC)² certifications due to lack of the highest ethics and professional caliber.

- If you have been convicted of felony or court-martial in the military.
- If you have been involved in publicly identified hacking criminals or being one of them.
- If you have had a professional license, membership, registration, or certification revoke, or disciplined by an organization/government agency.
- If you have been using aliases or pseudonyms.

If you think you are qualified, it's time to register for the examination. You must do this at least two months earlier. You can find more information at <https://www.isc2.org/Certifications/CISSP> .

I also recommend you join appropriate CISSP study groups. There are many groups on the internet. WhatsApp is the most popular option nowadays.

Steps to Register for the Examination

1. Pearson VUE is the exclusive, global administrator of all (ISC)² examinations. Therefore, you need to create an account at <http://www.pearsonvue.com/isc2/>
2. Select the appropriate (ISC)² exam.
3. Schedule your exam and venue.

More information is available at <https://www.isc2.org/Register-for-Exam>

On the Day of the Examination

Finally, when the exam day is near, you need to prepare for the long day. Remember, the CAT is 3 hours long. If you take the non-English option, it

can be 6 hours long. I will list some helpful steps here so that you can properly get ready.

- Few days before the examination, have a good rest, and release your stresses.
- Before the day of the exam, have a good night's sleep.
- Prepare your registration information, printed materials, NIC, and other relevant documents before you sleep. You may also need to include emergency medicine.
- Before you go to the examination center, have a proper meal.
- Dress comfortably.
- Bring snacks and enough hydration.
- Leave your mobile and other irrelevant things outside.
- During the examination, take sufficient breaks and keep yourself energized. Drink enough water/drinks to keep you hydrated.

I hope these tips will be useful when you face the CISSP examination as, for me, it was a challenge of a lifetime.

Chapter 1

Domain 1 - Security and Risk Management

If you don't invest in risk management, it does not matter what business you're in; it is a risky business – **Gary Cohn** (*Former Director of the United States National Economic Council*)

Risk can be thought of as exposure to something dangerous, harmful, or even a loss. In fact, the exposure has an adverse impact because the exposed object has a value. Furthermore, the risk is the potential toward a loss. If strategically managed, it can either allow the continuation of the task or action, or else, it may result in a high reward (high-risk, high reward). In reality, any action may have a potential risk; however, if unknown, the degree of the risk is significant (if unplanned and/or unexpected). For instance, if you invest your income on something, if there is a risk associated with it, you may lose part of the whole of the original investment.

Oxford English Dictionary defines the risk as to the “(Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility.” According to the Cambridge English Dictionary, it is “the possibility of something bad happening.” International Organization for Standardization defines risk as to the “effect of uncertainty on objectives.” There are other definitions as well, but all the definitions point to a common set of characteristics such as potential, probability, uncertainty, and loss.

Does risk always cause a bad effect? No. Risk is everywhere. When you invest in something, you also invest in the inherited risk. For instance, if you risk your life to find a cure for an uncontrollable disease and if you can find a cure later, it is worth the risk. Another example would be lending money to a trustworthy person/company. In any cases mentioned above, however, things may change, and unless you are prepared for it, it has the potential to damage your investment.

If you are running a business, as you understand, every action you perform has an associated risk factor. It is of utmost importance that you identify, quantify, and assess the risks and make a strategy to prevent, mitigate, or reduce the potential damage from a risk. If the damage is unavoidable, you must also plan to recover with minimal effort and expenses. Finally, risk can be identified as the main source of adverse impact. Such impacts deeply affect organizations and their stakeholders. This is why a corporate strategy is required to manage risk and ensure business continuity.

What are the potentials, which in turn generate a risk? A risk can emerge from vulnerability or a threat. These can be associated with operations, with the system that is responsible for the operation and the operating environment.

The Role of Information and Risk

Information and communication technologies have become a core part of the business operations in this digital era. Many small to large scale companies implement, control, monitor, and maintain their operations with one or more integrated information technology solutions. Large corporations like banking operations, institutes involving scientific explorations, healthcare heavily relies on current and future technologies. In most cases, these are tiered, and more than one layer depends on other layers. Therefore, each independent system and collaboration have to deal with multiple risk factors. For instance, these systems work with information. Information can have multiple levels depending on the importance. A company has to depend on the underlying systems to store and utilize the available information, transfer information, and destroy obsolete information. In each scenario, users have to depend on multiple underlying systems and sometimes foreign systems. In this case, a company may have neither the visibility (transparency) nor control on these foreign systems. Hence, this may lead to disclose or expose sensitive information putting the company, stakeholders, and the entire operation into jeopardy.

The Risk from Other Sources

There can be multiple factors governing present and future risks. In this case, risk can be a financial loss or any other type of loss, including

reputation, loss of lives, or stolen information or assets disclosing sensitive information to unauthorized parties.

If we take an example operation such as a supply-chain, many associated risks are not related to information. Some of these can be avoided or cannot, while others cannot, but it is possible to reduce the impact. Let's look at some of the potential risks that can damage a supply-chain.

- Economic instability.
- Political changes.
- Natural disasters such as extreme weather. These are also called catastrophes.
- Environmental risks, for instance, waste disposal, and related laws.
- Supplier consistency.
- Data validity, integrity, and quality.
- Connectivity – communication failures mainly due to information technology operation failures (i.e., infrastructure, operations, integration, software failures). For instance, a DDoS attack can cause critical availability and communication issues.
- Transport issues.

When considering this example, there are multiple risks, and it is not just about information technology. You, as a security professional, may indeed involve in information security assurance programs. Still, you need to manage all these risks if you are part of the business continuity and risk management operation.

Risk as a Term

There are many terms when it comes to risk. It is better to unpack the risk and get familiar with these terms first.

- Risk behavior: behavior that may lead to a negative outcome. This is mainly used in the health industry.

- Risk condition: Conditions that may cause a risk.
- Risk exposure: Risk by being exposed to a dangerous condition.
- Risk factors: Individual attributes that contribute to risks.

Risk, Threat, and Vulnerability

In the information security field, most of the time, you will hear these three terms. There is a lot of confusion and some interchangeability. This is something you have to clarify to understand (perceive) the basic concepts.

Threats

A threat itself is a negative event. It can definitely lead to a negative outcome. In fact, the negative outcome can be damage to or loss of an asset. The following examples describe various threats.

- A fire in your headquarters that hosts the datacenter.
- A flood hitting the headquarters.
- An attempt to steal information by a hacktivist.
- Accidental deletion of a partition that hosts your client data.
- An employee attempting to sell a corporate secret to a rival.

As you see with these examples, these threats are probable.

Threat Agents

A threat agent is the one initializing the threat scenario. For instance, a flood is caused by nature. It is, therefore, the threat agent. Other examples of threat agents from the previous examples are faulty wiring, hacktivists, careless users, and insiders with malicious intent or dissatisfaction.

Vulnerabilities

A vulnerability is either a known yet patched weakness or a weakness that has not been found yet. In either case, a vulnerability makes a threat possible. A threat agent can use the vulnerability to attack, steal, or damage the asset. The vulnerability can also make a threat significant. A list of common vulnerabilities is listed below.

- Lack of access control.
- Failure to check authorization.
- Failure to audit actions.
- Failure to encrypt data in motion and data at rest.
- Cross-site Scripting.
- SQL Injection.
- Cleartext passwords.

Exploitation

A vulnerability can be used to cause a threat. This act is known as exploitation. Therefore, exploiting a vulnerability is the main intension of the threat agent.

Risk?

Risk and threat are often confused and used interchangeably. However, a threat is not exactly the risk. In fact, the risk is a combination of threat probability and its impact (potential loss). Therefore, we can generate the following formula.

$$\text{Risk} = \text{Threat Probability} * \text{Impact}$$

Let's look at another example.

- Among the top 10 vulnerabilities classified by Open Web Application Security Project (OWASP), "Injection" is on the top of the list. OWASP top ten vulnerabilities are <https://owasp.org/www-project-top-ten/>
- The most significant threat that injection (i.e., SQL injection) enables is information stealing.
- Here, the threat actor can be someone who wishes to gain information to prove something or who is financially motivated.
- If exploited and stolen valuable data such as user account passwords, for instance, it causes a significant financial cost,

including reputation loss, loss of assets, and even litigation.

- What is the probability of the attack? Injections are not difficult to perform against poorly secured databases; for instance, a poorly coded front-end may allow unexpected inputs leading to possible exploitation. Database-driven websites are often open to the internet, and therefore, the probability is higher given the above facts. Therefore, the risk here is significant. Hence, we can classify this vulnerability as a high-risk.

It is also important to identify what a zero-day vulnerability is. It is something not identified by the manufacturer, maker, coder, or testers. If there is an open vulnerability, it is a zero-day vulnerability. Once identified by a threat actor, exploited, and gets successful, it is called a zero-day exploit.

Risk can also be defined as,

$$\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Cost}$$

Here, we can identify a new term, cost. There are three costs concerning the impact of the risk and the expenses a company has a deal with to recover from the impact. The three costs are,

- Hard costs: Repair or replacement cost raised by the damaged assets. In addition, quantifiable resources such as work hours and IT staff are also included.
- Semi-hard costs: The impact (loss) during the downtime.
- Soft costs: Reputation, public relations, and end-user productivity.

Now when we look at the formula carefully, if you reduce the threats by fixing the vulnerabilities and keep the cost as lower as possible, the risk becomes almost 0. Is it for real?

There may be certain vulnerabilities that can be patched once and for all. But the threats may remain the same. In addition, no matter how efficient and effective a security program is, there is always a door for vulnerabilities. Therefore, we use the word “mitigation” when it comes to risks. Most risk can be mitigated rather than prevented forever.

For instance, is it possible to predict an extreme natural disaster to 100%? Our technologies are not that miraculous. There may be tools and techniques to assess possible risks, however. This identification is the absolute key to a successful risk mitigation strategy. This entire operation is known as **risk management** . It creates a formidable strategy and tactics to identify, qualify/quantify, asses, mitigate, prevent, and recover from a future or a current impact, including disasters (catastrophic events). Disaster recovery is an integral part of the risk management itself. As a process,

- Identifying threats and vulnerabilities,
- Performing risk assessments,
- Building risk responses,
- Setting up controls and countermeasures,
- Evaluation and reviews
- Making improvements from lessons learned.

In the next chapters, we will be discussing the entire risk management process and current frameworks that you can utilize to create your risk management program, including disaster recovery and business continuity strategy.

1.1 Understand and Apply Concepts of Confidentiality, Integrity, and Availability

One of the main foundation topics of information security is none other than confidentiality, integrity, and availability, in short, the CIA (not the Central Intelligence Agency) or AIC. These three are also pillars of information security.

As a CISSP student, you must have a good understanding of what these terms are and what they do together. For instance, this concept helpful in developing and maintaining security policies and countermeasures.

Confidentiality

Confidentiality is thought to be the main aspect of information security by most people, even though it is not the actual utilization. In previous sections, you were introduced to assets such as data or information. Data or

information a company owns and maintains have critical importance. The importance requires implementing limited transparency and authorization to access, modify, transfer, and erase.

You also learned about threats and vulnerabilities. Information theft is the top priority of most cyber-attacks and crimes. In a successful attempt, data may be stolen, modified/alterd, or corrupted. By looking at these events, it is possible to understand what characteristics must be concerned when protecting the object (data). If one can gain access or “authenticate” and gain further access to the object via “authorization” for this person, confidentiality is zero. In addition, he/she is capable of altering data that may violate “Integrity” constraints. Such an act can raise availability issues (i.e., if data is lost, corrupted, or modified or even erased).

Confidentiality works as a safeguard. In fact, it ensures and controls the level of disclosure against unauthorized parties. By unauthorized parties, it does not mean hiding something from everyone ensures confidentiality. Instead, it must be available for the appropriate parties, and each level should know what they need to know. If the “need to know” requirement is zero for a party, they must not be able to access such information.

Now there is the question about the method that we need to use to build this list of appropriate parties, their role, and responsibility. This process is known as “data or information classification.” Information classification is a broad topic. However, you can always start from a simple starting point. You can ask questions like “how data can be classified?” and a “what is the simplest criterion?”

With any classifier, there are key factors.

- Value: What is the value of the information?
- Clearance: Which person or group(s) should have clearance?
- Impact: What is the impact if it gets disclosed?

The value of the information also defines the risk factors.

Based on the answers to the above three factors, it is possible to construct a classification table. After, the table is filled, by assigning values to each cell

and calculating the final value. Once it is complete, you can determine the clearance level, group, safeguards, countermeasures, and regulations.

When implementing information classification and clearance, you can utilize two basic principles. Those are,

- Need to Know principle: For instance, if a tech support manager is utilized to do his task “A.” Then he needs access to the set of data “B.” He attempts to access B while the adjacent files “C” and “D.” With a need to know, he should not be able to access C and D but “D is
- Least privilege principle: Once access is allowed, there has to be a measure to control the set of common resources. In this way, the user has basic privileges over the object so that he/she can perform only the work required.

To safeguard confidentiality physically, there are many tools and techniques. Some of these are,

- Implementation of secure physical environments.
- Authentication systems using humans, devices, and software.
- Passwords
- Two or multi-factor authentication.
- Encryption.

Data or information has the following three states.

- Data in use.
- Data in motion.
- Data at rest.

At each stage, this data must be protected. To do so, we use a technique known as encryption. There are many encryption techniques, such as private and public key encryption, hashing, and certifications. Since encryption can be applied to each state, it is the main technique used.

Next, we will look into the threats to confidentiality.

The main threat to confidentiality is disclosure. The list below includes some instances when data confidentiality is compromised.

- Data theft – loss of sensitive or confidential information.
- Malware attacks
- Faulty configuration – i.e., an issue with website configuration allowing leakage.
- Human error: Keeping a password written on the desk and everywhere.

Integrity

In the next stage, a privileged user who has enough access to data can modify the changes. The data must remain original and free of unnecessary alternations. This is what integrity ensures.

If we are to define integrity, it is the assurance of accuracy, trustworthiness, and consistency of information during the lifecycle of data. Data integrity ensures that no unauthorized modifications occurred. This does not necessarily mean an authorized party cannot alter the data. This is addressed through a different concept (later in the lesson).

To ensure integrity, implementing user access controls (i.e., authentication), setting necessary permissions (i.e., object-level), and authorization is required. Version control is another technique. Such techniques also prevent human errors and discourage malicious intent.

Threats to Integrity

- Data corruption (at rest, in transit).
- Storage failures.
- Server crashes.
- Any other physical damages.
- Not validating user input.

- Not backing up data.
- Not auditing object level, system-level, and user-level actions appropriately.

Integrity can be enabled by implementing confidentiality through encryption. But you cannot ensure integrity with the use of encryption. It is not straightforward. Encryption is a key component of confidentiality. However, certain problems deviate encryption and confidentiality from integrity. For instance, encryption pre-handshakes, overhead may use cleartext. Some network protocols also separate these from each other.

There is a way to ensure integrity by using a cryptographic hash function. This technique is known as the **Digital Signature**. This will be discussed during the encryption lesson.

Availability

Availability is the last pillar in the CIA triad. Now you are aware of confidentiality and integrity. However, if the data is not accessible at some point, does it matter? In other words, the data is confidential, and integrity is kept, but what happens if it is not available?

There are a few requirements for data. It must be available, must be available when required (without delay), and available without any compromise or corruption.

There are many threats to availability, and these are uncontrollable in contrast to the other two. Some of these are listed below.

- Natural disasters, causing dysfunction and losing premises.
- Political incidents.
- Network failures, congestion, excessive load leading to outages.
- Hardware failures and overloading.
- Software faults causing malfunctions.
- Security incidents such as exploitations, intrusions, distributed denial of service attacks (DDoS).

Now, as you have seen, each component in the CIA triad has its associated risks. Therefore, it is imperative that appropriate measures and monitoring are established, kept track of, maintained, and reviewed. The establishment must be started from implementing an appropriate security strategy initiated by the top levels in the organizational hierarchy (i.e., CEO, directors).

To mitigate the risks of losing business continuity, many organizations develop strategies to establish routing checks, maintenance, fault tolerance through redundancy and other techniques, load balancing, scattering, or dispersing critical functional units from each other and some other techniques. Each of these countermeasures must be tested, verified, and regularly simulated to keep the readiness. In an IT strategy, you should include all the tactics such as strict security control and authentication, proper authorization, fail-over clustering, load-balancing, monitoring and redundancy, adherence to standardization and compliance, compliance with national policies, and regulation. Hence, during a disaster, you can quickly recover from, and prevent if possible, mitigate and detect otherwise while minimizing the downtime. For instance, if you own a data center, in addition to these measures, redundant datacenter points (at least two) are vital to keeping the ongoing operation running.

1.2 Evaluate and Apply Security Governance Principles

Before going into the evaluation and application of security governance principles, you should be familiar with certain terms. Let's start with "principles."

A principle is neither a rule nor a law. It is neither a protocol nor a practice. Hence, it is not a specific standard. Then what is a principle? The principle is a fundamental truth. Therefore, it serves as the foundation of a truth-based system. For the safeguard of information, security governance is practiced. To plan, implement, and exercise information security, these principles can be used. Best of all, these principles, such as good corporate principles have evolved for decades.

In a corporate environment, there is often a well-defined set of governance principles. In fact, such corporations were flexible enough to adapt to address the ever-changing requirements. In other words, fluidity is required to construct and evolve with such a framework.

Why is there a need for such corporate security governance principles or a framework? A company or an organization formulates business goals, strategies, and policies such that the company can reach its mission through achievements. To maintain the competency, the business operation must be executed with precision and control. To do so, policymakers have to evaluate the current standings and then enhance the institutional governance frameworks, including legal and regulatory frameworks. While doing so, the overall business strategy of the company should be maintained such that it can fulfill corporate responsibilities, business goals, maintain economic efficiency, and financial stability. In reality, a well-structured organization with properly formulated security governance principles can ensure sustainability through its solid strategy. In fact, the main intension of the utilization of such principles is this ultimate objective.

If we take a look at good governance principles those are,

- Adhere to national laws, regulations, and compliances.
- Adhere to corporate responsibility and accountability.
- Business continuity and sustainability through risk management and disaster recovery.
- Ethical conduct.
- Equity and equality stance.
- Financial transparency.
- Valuing cultural diversity.
- Fluidity and flexibility.
- Rights and responsibilities.

In the next section, we will be looking into how an organizational hierarchy initiates, engages with the development, and how other parties contribute this bottom-up approach so that a successful corporate information security and risk management strategy is implemented and maintained.

1. The chairperson or the CEO is responsible for initiating and laying out the first step toward a short and long-term and sustainable corporate strategy. He/she must have a clear idea of past, present, and future obstacles and risks through analyzing

the operational history of the organization. If it is a starting up an organization, it is possible to evaluate the peers and compare it with its own strategic business implementation.

2. Next, with the senior management, the head of the corporation or the board start the initial planning process while allocating the necessary resources. It may establish a specific committee to govern the process (let's name this as "X"). Together they also review the current business plan, current financial stance, past and present risks, and how it was able to mitigate such risks so far.
3. Next, with the oversight of the X, managers start to develop the initial draft and evaluate the implementation possibilities thorough analysis, including a feasibility study. The main objectives of this development are business growth and sustainability while maintaining security and standards.
4. In the next stage, the management produces financial statements both accurately and failed. This is a critical step as it reveals the actual financial state. Such statements must have been disclosed to the stakeholders and relevant parties on time to maintain transparency. These statements greatly help investors to analyze the business soundness, financial prospects, and the associated risks.
5. The next process is the auditing process. An audit committee and the X oversee the annual audit process. In this case, it is the internal financial auditing and control. This is extended to oversee the compliance and risk management processes. To ensure accuracy and unbiased auditing, an external party will be involved in the later stages.
6. X plays a key role in corporate governance. It requires shaping the board with diverse figures so that they can be utilized in a critical stage (in the light of the need).
7. A compensation committee plays the next important role, which is rewarding. Rewarding is a high-end motivational

factor. As a matter of fact, the board establishes a philosophy so that the company can award the organizational hierarchy for achieving business objectives, goals, performance, thus ensuring the active contribution both physically and mentally.

8. Another important step in the long-term value creation. This is mainly performed through meetings and engagements with long-term shareholders so that the underlying issues be identified and resolved. Shareholders who take part in corporate decision making and changes in the strategies are encouraged to disclose relevant identifying information for accountability. This is a critical step in ensuring the long-term interests of the company at present or in the future.

Although it is a long and cumbersome section, it is actual footage of the corporate governance principle as a step by step procedure. As with many organizations, information and communications assets and technologies play a critical role, and therefore, an integrated and incorporated strategy is a must.

Alignment of security function to business strategy, goals, mission, and objectives

If you properly understood how the overall information security initiative and strategies are formulated, funded, resourced, and carried out, you should see the important characteristics outlined. The role of the information security is not just to sit here in a corner and look at something to see if it does something and then report to someone. The real requirement arises with the planning of business strategy itself as it is possible to identify and document all the risks a business had or has to go through.

In the actual business planning process, the board or committee or the top of the hierarchy with the collaboration of the management concentrates on the vision and the mission objective of the organization, business goals, objectives toward each goal until it reaches the ultimate goal. To prevent or mitigate the risks associated with information and ICT assets, their functions and dependencies must be clearly identified and streamlined with these objectives, goals, missions, and the overall business strategy.

In simple terms, for the entire framework to function properly, the relationship of the business elements to information security must be understood. When this is clear, it is much easier to allocate organizational resources and budget to the initiatives. Hence, the outcome is more efficient and effective with properly formulated and aligned overall security strategy, including risk management.

Mission, Goals, and Objectives

The term mission was made popular during space projects. If you remember the mission to the moon, it may give you a clear image of what a mission really is. As with the lunar project, with every business, there is a mission. This mission is described in the mission statement (you would have seen these statements in the official websites owned by businesses).

The objectives here can be thought of as milestones to reach a specific goal while the mission statement describes the actual, overall goal. In other words, when you accomplish all the specific goals, you arrive at the overall goal and the accomplishment. Then one can say, “mission complete!”

When laying out a security strategy for a business, the architects must have a clear understanding of the mission, goals, and objectives. If this is not properly understood, it is difficult to align with strategy flexibly. Thus it loses the scalability and eventually leading to failures in one way or another.

Governance Committees

This topic was formally introduced in the previous example of governance principles. It was firm on the idea that information security is a top-down approach. The head of the organization, the board of directors, and senior management engage with the strategic decisions and policy formations. To address different areas and requirements, there have to be one or more committees to govern the entire process. This also paves the path to address compliance and regulatory issues.

The executive levels must have transparency to the overall security strategies and the operation. They should also take part and contribute to the implementation and review. Function-wise, In the actual process, the teams

must meet so that they can review the existing strategy, incidents, request for changes, approve the changes, and address the new requirements.

These activities enforce the effectiveness and efficiency of the security management process while pushing it forward. The biggest hidden risk to the security program is the budgeting concerns. If failed to prove the effectiveness and efficiency, there will be serious questions if the program worth the cost. Therefore, committees must be functioning while keeping the organizational business and security goals in their minds.

Organizational Processes (e.g., acquisitions, divestitures, governance committees)

Acquisitions and Divestitures

Acquisitions and divestitures are part of any business. In reality, medium to large organizations often goes through this path, either being acquirer or being acquired. None of these are straightforward and easy procedures.

Why does a business acquire other businesses? Any business, to remain sustainable, must elevate competitiveness. In addition, it should maintain agility and focus to compete efficiently. In this process, larger organizations tend to acquire or purchase smaller organizations if they seem fit. In other cases, smaller companies tend to sell themselves to become more reputed, popular, or secure.

At present, many acquisitions occur when there is a need for advancements and to integrate innovative and bleeding-edge technologies. However, there is a significant level of challenge. That is to adopt different business strategies, objectives, and goals with the current one. This includes possible risks, as well. Furthermore, the information that the mother company will open to the newly acquired and the risks associated with this is another concern. Another is the information security risks the new company brings together. Therefore, modern acquisitions have become a complex process. This is true for any case, such as a merger, acquisition, and even divestiture.

During acquisitions, multiple concerns arrive at the table. For instance, there are multiple security considerations. Any existing organization employs different security and risk management strategies (or they may not have in the worst-case scenario), even a committee and their structural

approach. It may have its executives, strategies, policies, and procedures. Therefore, the information security operation can be significantly different in contrast to the acquiring company.

With any acquisition, there is an associated risk. The company getting acquired, for instance, may use different management and monitoring systems, incident management procedures, disclosing information to certain parties, including third parties, utilize transborder technologies, and so on. Therefore, the operation may violate the existing compliance and regulations followed by the acquiring company. In addition, certain stakeholders, suppliers, and other core parties may bring trust issues, thus raising policy violations.

Therefore, it must go through careful planning, execution, monitoring, and auditing process. The existing security framework of the acquiring company has to be more flexible so that it will make ease of the acquired company. And, some reforms may be required and must be negotiated.

Here is a list of security concerns.

- The difference in strategies under different authorities.
- Different policies, procedures, and processes.
- Risk and loopholes.
- Lack of utilization of solid and trusted frameworks.
- Devices and people with undesired states bringing threats through vulnerabilities.

The following functionality areas must be compared and synchronized with the acquiring company.

- Risk management, operations management, incident management.
- Security management and monitoring.
- Auditing.
- Stakeholder impacts and third-party involvements.

When a company is splitting to two or even more, it is a similar process. However, the reforms require to focus more on dividing, changing, reforming, and even forming new entirely. There may be changes applied or

reforms to the vision, missions, objectives, and strategies. In addition, there may be new regulations and compliance requirements. Above all, the divided portion will have new leadership and strategic changes, initiatives and obsoletions, and budgetary concerns. Everything may have an impact on how the information security strategy is should be carried out.

Organizational Roles and Responsibilities

In an organization, task delegation, responsibility, and accountability flow from top to bottom. To manage specific tasks, there must be specific categories so that the responsibility can be delegated. These are called “roles.” When it is about designing a strategy to assure security through risk management and disaster recovery, each role has a certain responsibility so that his/her/their tasks contribute to enforcing security while mitigating the risks. This responsibility structure is critical to business continuity.

There are many internal roles as well as external parties such as suppliers, stakeholders, and consultants. When implementing a security strategy, the organization’s head, directors, and executive-level management have the ultimate responsibility for proper initialization and shaping. They must demonstrate a strong allegiance with this security program. Especially the executives are responsible for multiple functions. We may call this wearing multiple hats.

Managers are responsible for implementing a proper security strategy. They are also responsible for laws, regulations, and even mandates. To implement, develop, and communicate the implementation, this role requires specific and vibrant skills, expertise, and leadership qualities. Therefore, they have to always have room for education, recognition, rewarding, and penalties.

The employees have the responsibility above all. They should understand it is here for their safety, so they have to understand, honor, trust, and adhere to the security framework. To do so, they should be provided with proper guidance and awareness about policies, procedures, baselines, guidelines, penalties, and also legislation, mandates, compliance, rules, and regulations (as required).

Learning, understanding, and complying with the security program, each role contributes positively hence prevent security issues through due care. Due care and due diligence will be introduced later.

Security Control Frameworks (SCF)

Many organizations face significant business challenges trading locally and internationally. Doing so, they have to stay compliant with a mixture of industry-specific, state-mandated, and international cybersecurity laws and regulations. Organizations often adopt a security control framework to aid in these compliance efforts.

Most of the time, an SCF is adopted by most security institutions such as banking and finance. In contrast, healthcare and medical organizations were the opposite, according to a survey conducted by Tenable. If you are interested, you can read more here: <https://www.tenable.com/whitepapers/trends-in-security-framework-adoption>

These frameworks must be able to provide comparisons against industry benchmarks and a comparison against the framework. If there is no ability to measure success, then it is not the best framework you should be looking for.

The following security control frameworks are the most popular and most dominant.

- CIS (Critical Security Controls)
- COBIT (Control Objectives for Information Technology).
- COSO (Committee of Sponsoring Organizations of the Treadway Commission).
- HITRUST (Health Information Trust Alliance).
- ISO 27000 standards.
- ITIL (Information Technology Infrastructure Library)
- NIST (US National Institute of Standards and Technology).

- OCTAVE framework (Operationally Critical Threat, Asset, and Vulnerability Evaluation).
- PCI-DSS (Payment Card Industry Data Security Standard).

In a different section, we will be looking deeper into some of the most influential security frameworks.

There are four types of controls in SCFs. Those are,

- Preventive
- Deterrent
- Detective
- Corrective

In addition, there are another two called “compensative” and “assessment” as well.

Preventing Controls

Preventive frameworks are the frontline defense. These are enforced physically and through training. Some examples of preventive frameworks are,

- Awareness training
- Biometrics
- Data classification
- Encryption
- Firewalls
- Intrusion Prevention Systems (IPS)
- Security cameras
- Security personal
- Security policies
- Smart cards
- Strong authentication

Deterrent Controls

This can be thought of as the second line of security controls. The intention is to discourage malicious attempts by deploying appropriate countermeasures. In addition, if someone attempts to bypass or overrule, there is a consequence. Some examples would be,

- Cameras
- Dogs
- Guards
- Fences
- Warning signs

Detective Controls

These controls have the sole intention of detection. This is the next line of defense if someone or something can breach the preventive and deterrent measures. These are effective when there is an incident (now) or after an incident. Some detective frameworks operate in real-time, and some are not.

- Auditing (non-real time) and logging
- CCTV cameras (real-time)
- Intrusion Detection Systems (IDS systems, real-time or non-real time) including certain antivirus and internet security programs
- Guards
- Motion detectors

Corrective Controls

The last one of our line-ups is corrective controls. It is responsible for fixing, recovering, and restoring the system, device, or environment. For instance, restoring an operating system to a last-known-good state, restoring a failed RAID system, or recovering part of a database server. The controls include,

- Antivirus
- Bugfixes, patches and other updates

- Backing up and recovery

Compensative control is an alternative control. These are deployed when there is a practical issue with the deployment – either too difficult or impractical. It focuses on the following areas.

- Administrative
- Directive
- Logical
- Physical

A few examples of these types of controls are encryption, logging, and segregation of controls. Framework-wise, PCI-DSS is a framework with which such controls can be deployed.

Due Care/Due Diligence

Due care, by the name implies, is the understanding of and adherence to the governance principles your organizations must have in order to understand and get ready to face the risks. In simpler terms, due care is correcting something at the very moment. Therefore, we can call it D(ue) C(are) or DC, and it is the same as “Do Correct!”

Due diligence moves one step ahead. This process attempts to understand why a correction needed in the first place. That means, it investigates on detecting the reason behind an incident. Same as due care, DD here can be used to remember the meaning of this, that is, “Do Detect!”

If we compare these two, DC is to implement something right that can perform the mitigation – do the right thing. DD makes sure that the right thing was done correctly. It also tries to determine if it requires repetitions – steps to do the right thing are within the risk parameters and is accurate.

If you followed so far, you should notice that due diligence always comes first. In fact, due diligence is about collecting the facts during the management process. That is to “know.” Due care comes in action as a matter of fact and is to “do.” Also, it is good to notice that due diligence is a long-term process.

In an organization, due diligence must start from the top and approach the bottom. Due care, on the other hand, goes the other way.

If we take some examples, due diligence is the issuance of policies, standards, baselines, guidelines, and procedures, while due care is the application of these. Another is monitoring intrusions coming from outside to an internal network and is due care. Implementing perimeter security as a result of an initiative of the top-level personal is due diligence.

If we take a more relevant example, due care is making sure you are providing an adequate level of training to your employees about information security steps, such as how to use safety practices (i.e., using strong passwords, lock screens, apply updates). To make sure the steps and the entire strategy is correct and sound, we learned how we could use security frameworks such as COBIT or ISO 27001. This is due diligence.

1.3 Determine Compliance Requirements

Staying in compliance is above all the requirements when it comes to the quality and standard of business operations. It is another word for “betterment.” There are many national-level laws, regulations, mandates, transborder laws, standards, and specific compliance frameworks and an organization to provide a guarantee of safety, must adhere to one or more legal or compliance frameworks.

If an organization is failed to comply or failed in an audit later, the consequences can be severe. The worst-case scenario is the termination of the business and a serious amount of fine. As a CISSP student, your knowledge in this area must be sharp above all.

Contractual, Legal, Industry Standards, and Regulatory Requirements

In this section, you must understand that an organization must follow the legal requirements (local) such as acts, compliance policies, and mandates with clinical precision. These can be adopted as an integral part of the business operation by following a proper framework. Just like the security control frameworks, there are multiple frameworks implemented in different countries. There are global and regionally accepted compliance acts or policies. Some examples are,

- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley Act (SOX)

You must also remember that code of conduct and professional ethics is also part of this system; thus, assures the compliance will be properly followed. Hence, these activities will ensure safety and security in the organization while setting examples of lawful operations.

Let's also have a brief look at how laws came to existence.

There are two widely known legal systems at present.

- Common law system
- Civil law system

Commons laws follow a newer legal system based on new concepts. In fact, constitutions allow judicial decisions to provision the statutes. For instance, in the American legal system, there are three branches. Those are administrative law, civil law, and criminal law.

Almost all the civil laws had been derived from the Roman law system. In truth, these laws are from legislative enactments. It is common to see these laws in the nations those once were colonies of Europe.

To learn more about these two systems, you can get to <https://ppp.worldbank.org/public-private-partnership/legislation-regulation/framework-assessment/legal-systems/common-vs-civil-law>

There are laws pertaining to privacy, civil, and criminal activities. In the world, the classifications would be civil, criminal, internal, natural, and public. In addition, there are religion-based laws such as Sharia.

Any organization must have a legal framework, a qualified staff to set it up and maintain – including information security professionals, and an audit committee. This set up assures the legality of the business, thus prevents from intentionally/mistakenly committing criminal or offensive activities.

Above all, this is requiring to identify internal offenders and bring to justice.

Privacy Requirements

Privacy has a unique importance to many people. With the evolution of societies, social conduct, ethics, and morality, privacy became more and more important. As you see here, it is a sociological concept. Privacy must not be used as another term for confidentiality. Privacy is about personal identification. The definition says it is about personally identifiable information or PII. On the contrary, confidentiality is an attribute of an asset or piece of information.

Privacy is a critical component to assure nowadays as the organizations get to know PIIs of millions, and they can either sell it or disclose the information (parts) with any party they wish. Therefore, globally, and locally, governments and other governing bodies started to make legislations and acts so that the customers are protected from privacy violations. As privacy can be stolen, used to impersonate, commit a crime, and protecting privacy is vital.

However, with the growth of criminal activities, there is a need for sharing information with the government as well. Most corporations are obliged to do so by other acts. This also raises concerns about privacy and raises questions such as if there is true privacy.

The arrival of messengers and social networks raises many concerns. For instance, Facebook was seriously questioned for its privacy policy. They opened private information of the users to third parties. This is also the case with Google. Although they may not allow third-parties to obtain specific information, they will be able to identify patterns and vectors. For this reason, they were pushed to ensure privacy and are obliged to provide information on how they share PII and privacy options to configure or prevent sharing information. If you have seen the privacy policy pages made for websites, you should be able to understand why they have to keep transparency.

There are two types of personal information. Those are,

- Personal Identifiable Information (PII)

- Sensitive Personal Information (SPI)

There are multiple global, regional, and national laws to protect this information. A well-known example is the General Data Protection Rule (GDPR) established by the European Union. Similar examples are ISO 27001 and PCI-DSS.

Therefore, the protection of privacy must play a key role in an information governance strategy. It must be a holistic approach. Why? For instance, someone's privacy can be protected until the person commits a crime. In such cases, to identify a criminal, a government may request a bank to disclose the information of the criminal. This helps the law and enforcement to track the criminal. But if the person is not a criminal, it may violate his rights to privacy. Since it is such a sensitive matter, a holistic approach is essential together with confidentiality and compliance.

To place proactive measures on collecting, preserving, and enforcing the choices of the customers, how and when their personal information is collected, processed, stored, and shared (or likelihood) must be made transparent, and an organization must ensure the safety of such information. Since an organization is a collection of many teams such as human resource, financial, legal, information technology, etc. the implementation and exercise of the safeguards is a collaborative approach. It is no longer, though, as an atomistic process like in the past.

1.4 Understand Legal and Regulatory Issues that pertain to Information Security in a Global Context

Information technology can be categorized into personal, local (national), regional and universal (or global), In this chapter, we are going to look at the legal and regulatory issues pertaining to information security in a universal context.

Cybercrime and Data Breaches

What is cybercrime? Cybercrime can be defined as criminal conduct carried out by employing a computer and/or internet. The motives behind cybercrime are similar to the general criminal activities, but it has other motives. The main motives can be,

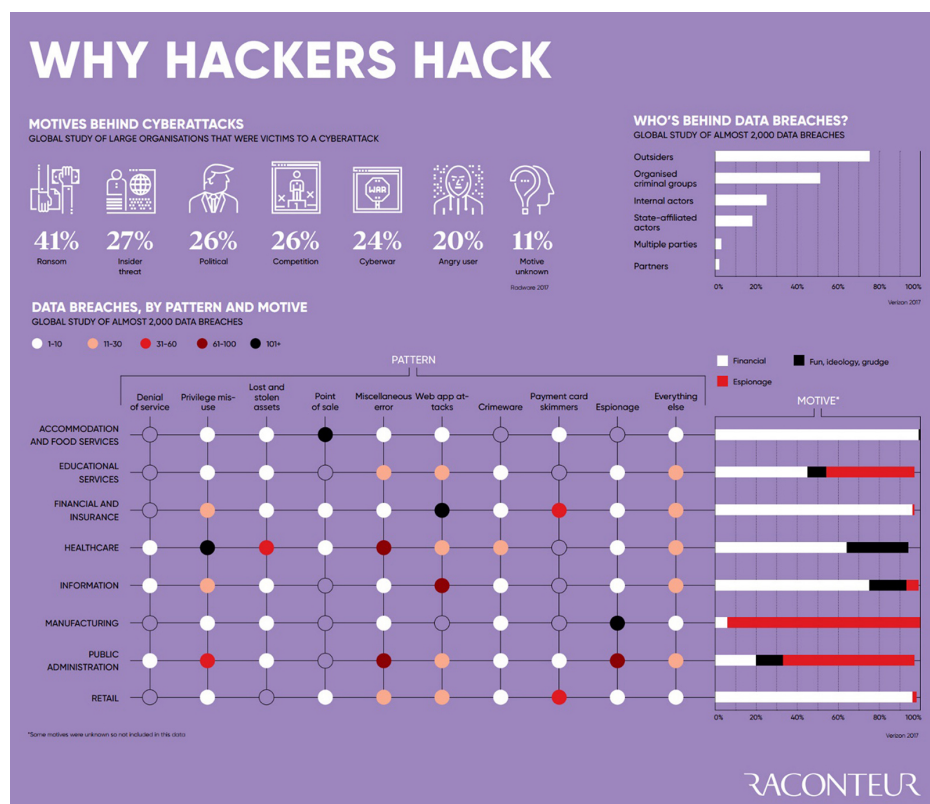
- Financial: This is the main motive. Information stealing/theft is highly profitable. For instance, if you steal a database of usernames and passwords or credit card information, it is profitable. Another importance is that an attacker can find interested parties to sell certain information, such as business secrets. For instance, an organization may have one or more competitors, and they are willing to destabilize it. Most financial crimes occur through insider threats and actors. Others are competitive and objective attacks. Healthcare businesses are also a target.
- Competition: Among manufacturers, there are interests in trade secrets and many other assets. These types of attacks focus on intellectual properties. Through this, a competitor can gain competitive intelligence.
- Ideological/Emotional: A competitor or any other party who has a motive to deny service to your customers by sabotaging systems or devices and reputation. For instance, a frustrated former employee may involve in such attacks. Fun, Ideologies, and Grudges are collectively categorized into one as *FIG*.
- Political/Religious: Cybercrime is rapidly utilized to achieve political ends by state actors. Some interests would be manipulating elections, attack and shut down power stations, distribute ransomware for blackmailing purposes, and is a growing threat to all organizations. Political espionage is a term we use it to describe these types of attacks.
- Prestige or Curiosity: Some criminals just enjoy finding and exploiting weaknesses. Sometimes it is due to the public interests or in others due to grudges. Later these findings can be used by the to gain financial or political gain.

According to an infographic released by Raconteur (<https://www.raconteur.net/>) in 2017, the following important facts and statistics can be found.

Types of cybercrime include the following.

- Botnet operations

- Child pornography and other illegal and lethal acts
- DDoS operations
- Fraud
- Hacking
- Identity theft
- Malware distribution and malvertising
- Piracy
- Ransomware distribution and cyberstalking and bullying
- Scamming including phishing
- Social engineering
- Spamming



According to a data breach investigation report released by Verizon in 2019, the following trends can be observed.

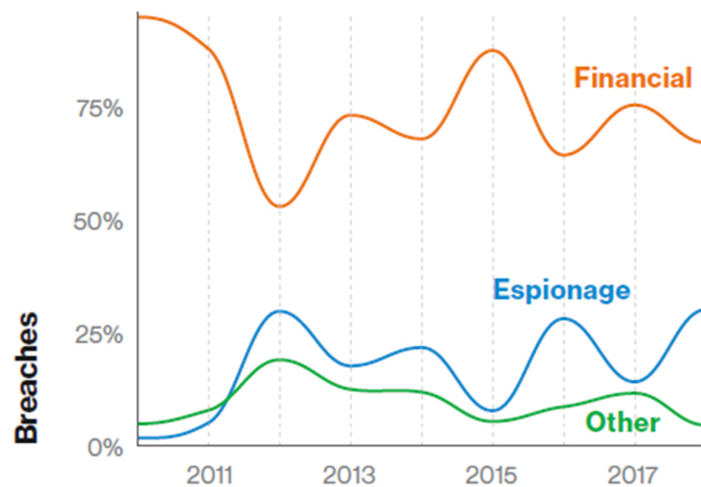


Figure 7. Threat actor motives in breaches over time

When the organizations spread their wings through a nation or beyond borders, the risk is growing, and there is a possibility to experience any one of these crimes during the lifecycle. Therefore, it is important to become familiar with different legal systems, both local and global. Different nations and regions exercise different laws, legislations, mandates, and policies. Due diligence is the key player here to address the requirement proactively.

To protect both individual and organizational data, mitigate breaches, and take legal steps, many nations implement and enforce legal requirements. For instance, California S.B. 1386 is an example of an amendment to the civil code related to privacy. From a more global perspective, the U.S. Health Information Technology for Economic and Clinical Health Act (HITECH) act motivates the creation of Electronic Health Records (EHR), improve security and privacy. The General Data Protection Regulation in the European Union introduced mandatory requirements relating to privacy.

Licensing and Intellectual Property Requirements

To understand the intellectual properties, let's look at the following diagram.

<div>Trade Secrets</div> <div>Protect secret or confidential information.</div>	<div>Trademarks</div> <div>Protect brands. Example: Samsung trademark and logo.</div>
<div>Copyrights</div> <div>Protects the authors (authorship). Examples: Books, Movies</div>	<div>Patents</div> <div>Protects an invention or a special functional or an ornamental design.</div>

There can be others such as database designs, industrial designs, and other newer categories that require similar protection.

A license agreement, on the other hand, is a signed agreement or a contract between a buyer and the seller. For instance, software vendors sell a license to use their software for some time or the lifetimes. A good example is Microsoft Windows licensing. The requirements and terms are subject to change, given the country or region. For instance, Windows has specific licensing requirements in the countries under the European Union. It is a noteworthy feature of some licenses that they have the ability to be redistributed or reused.

Import/Export Controls

Imported goods and services may have a significant risk imposed on an organization's CIA triad as well as on privacy and the overall governance. This is why strict legal requirements stand to safeguard the nation and the buyers. If an imported object does not meet the requirements, it will be, therefore, prevented, controlled, quarantined, and even destroyed safely. For instance, many countries set forth restrictions on importing mobile phones and communication equipment as these can be used to track, hijack, or steal private information. These standards must be strictly adhered to by logistic services as well.

If the object is a piece of software or a software technology such as encryption and cryptographic products, some export laws are governing the restrictions. There are laws, for instance, in China and the Middle East to prevent VPN technologies. In fact, the danger a VPN can impose is significant as the underlying infrastructure is not transparent, and it can include *transborder dataflows* . Therefore, there is a possibility even for state-backed information theft.

If an organization depends on services such as VPN, cloud, and virtual services (IaaS, PaaS, SaaS, and other), there are country-specific laws, regional laws, and regulations on how it must meet the compliance requirements as well as privacy requirements. Failing to do so can result in a fatal impact on a business. Therefore, planning for risks, threats, and business continuity involves a thorough understanding of this context.

Transborder Dataflow

As stated in the previous section, there are multiple instances when organizational data resides in multiple places rather than in a single country. When data is beyond the borders of a country and its legislative framework, there are significant concerns on data privacy and security as there are different laws and safety concerns as they fall under different protocols. With the ever-growing internet-based VPN technologies, Cloud-based networks, and virtual computing, there is great exposure and a risk to security and privacy, not just organization-wise but to national security as well.

Since there is a requirement on a framework that regulates and mitigates risks, certain countries had established their own set of frameworks. A good

example is the EU-US Privacy Shield Framework. Previously, the U.S. Department of Defense (DoD) and the European Union formed such an agreement. This was known as the Safe Harbor act. The European Commission Directive enforced this requirement on Data Protection on countries that held data of European citizens. In 2015, a European court overturned the agreement. It stated that only the twenty-eight European nations (European Union) have the sole responsibility of determining how to collect online information and related data. The gap was later bridged with a new directive in 2016. This agreement is known as the EU-US Privacy Shield Framework.

Crime Prevention Acts and Laws in the U.S.

- Electronic Communications Privacy Act (1986)
- Computer Security Act (1987)
- Federal Sentencing Guidelines (1991)
- Economic Espionage Act (1996)
- Child Pornography Prevention Act (1996)
- Patriot Act (2001)
- Sarbanes-Oxley Act (SOX, 2002)
- Federal Information Systems Management Act (FISMA, 2002)
- CAN-SPAM Act (2003)
- Identity Theft and Assumption Deterrent Act (2003)

European Acts

- Directive 95/46/EC on the protection of personal data (1995)
- Safe Harbor Act (1998) between Europe and the U.S.
- The Council of Europe's Convention on Cybercrime (2001)
- EU-US Privacy Shield Framework (2016)

Privacy

Privacy was introduced in a previous chapter. According to many definitions, privacy comprises of two main components. Those are data protection and appropriate use and handling of data.

There are several major legislations established for privacy protection in the U.S. Those are,

- Federal Privacy Act (1974)
- Health Information Technology for Economic and Clinical Health (HITECH 2009)
- Gramm-Leach-Bliley Financial Services Modernization Act

In Europe,

- U.K. Data Protection Act (1998)
- General Data Protection Regulation (GDPR)

1.5 Understand, Adhere To and Promote Professional Ethics

In this section, we will be looking into what ethics are and the two types of ethical conduct that you must understand and adhere to as a CISSP practitioner as well as the other, which is local to your organization.

Ethics are a set of moral principles that govern a person's behavior. This is one of the most critical parts or a pillar of information security as it provides the moral foundation to the security strategy. Without following ethics, no one will truly adhere to the strategy.

If we look into a bit of history of computer ethics, it is originated in the 1940s with Norbert Wiener, an MIT professor. This was delved deeper into his second book, *The Human Use of Human Beings* . After a few months in the same year, the world's first computer crime was committed. Unfortunately, there was no law to punish the criminal. In 1973, the Association of Computing Machinery (ACM) adopted the code of ethics, and Donn Parker led the development. In the invention of the term, computer ethics was invented by a medical researcher and a teacher, Walter Maner, as he found out ethical decisions are difficult when there are computers added.

During 1978, the Rights to Financial Privacy act limited the government's ability to search bank records. The U.S. Congress adopted it. People like Terrell Bynum, Kames Moor, and Deborah Johnson and others contributed to the ethics by publishing important guidelines. In 1988, the Computer Matching and Privacy act were adopted by the U.S. government, and the purpose was to restrict them from identifying debtors. In 1992, ACM adopted personal responsibilities to its act through 24 statements, and it is known as the ACM code of Ethics and Professional Conduct.

Ethics comes from a Greek word *ethos* . The meaning resembles the characters (good conduct) of an individual as well as a community. In moral philosophy, ethics are the following though the process.

- Making good choices in your life
- Maintaining rights and responsibilities
- Making moral decisions
- Making a good judgment between right or wrong

There are four types of ethics. Those are,

- Applied ethics: Covers areas such as capital punishment, rights of other species, and ethics during wars.
- Meta-ethics: Deals with the nature of moral judgment
- Normative ethics: Moral judgment.

(ISC)² Code of Professional Ethics Cannons

(ISC)² firmly believes that the security professionals who are certified by (ISC)² must earn and maintain the privileges. As a result, all (ISC)² certified professionals must fully commit to supporting (ISC)² code of ethics. Failing to do so may result in a revocation of the certificate. In other words, the code is a condition of the certificate.

There are four major and mandatory canons in the code. Let's look at them.

- Protection: Protect society and its common good. Through the act, earn public trust and confidence. Also, protect the infrastructure,

which is another critical step.

- Honesty: You have to act honorably. It means you act honestly, justly, and responsibly while honoring the legal frameworks.
- Principles: Provide competent and diligent service.
- Profession: Go through the ladder while protecting the profession.

To learn more, visit <https://www.isc2.org/Ethics>

Organizational Code of Ethics

As stated previously, an organization must maintain a code of ethics and good conduct so that it can enforce and assure the employees are adhering to and honor the information security and any other business strategies. This also brings empathy to the plate. As a matter of fact, they have to follow it, protect it, and reveal the people who would not follow. Therefore, the code of ethics for them can be thought of as principles. As a security professional, your role is adhering to these principles, educate and encourage others to do so, and inspire the teams and the entire organization. Hence, good conduct displays as a strong moral character of the organization to others, including stakeholders, suppliers, third parties, and customers. In turn, this motivates customers to depend on the principles and built better relationships. This entire flow is essential to do good business.

Also, strong ethics in corporate conduct gain trust among peers during government contracts and secures trust in other regions as well. As you understand, many information security incidents occur due to bad ethics. Therefore, by following the principles, you can be among the people who build your actions and thoughts upon a strong code of conduct.

Ethics, as you noticed here, requires leaders and role models. Therefore, senior management and executives have the main responsibility of making a culture so that others can adopt without a problem. Many employees may arrive from diverse cultures and work together to form an organizational culture. Therefore, integrating ethics into this culture is not a difficult task if you plan well. However, it may not work with just by example. In psychology, people are motivated through rewards. Therefore, a proper rewarding program ensures strength and sustainability.

Let's look at the key components of the code of ethics.

- Values: Organizational moral values such as honesty, integrity, and fairness – the humane perspectives
- Principles
- Personal responsibility: Responsibility and accountability
- Management support: One of the critical steps of the ethical regulation program is the initialization at the top and flow from start to bottom. It must be strengthened further through a rewarding program.
- Compliance: Organizational code of ethics can significantly influence and assure compliance standards.

Basic procedures for creating a code of ethics

- Review current standards and stance of ethical conduct by analyzing the past and present interactions
- Review business documents and policies applied to multiple areas such as onboarding, use of personal devices and taking off hours, etc.
- Analyze ethical dilemmas encountered
- Implementation
- Review process: Every employee and stakeholder must be involved.
- Address workplace issues (i.e., romance, relationships, grudges)
- Appoint roles, responsibilities, and utilize role models.
- Review for the legality through the legal department
- Finalize and publish
- Monitor and review

1.6 Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines

We are now moving from the initialization phase of the security framework/strategy to the implementation phase. It is better to revisit the previous sections if you haven't followed it properly.

When moving into the development, distribution, and communicating (awareness training), it becomes a responsibility of the management. The normal procedure would be to start with architecting a security framework or using an existing one as the aid. The formation of security policies can be initiated at this point. The policy requires the oversight of the head/chairperson/CEO, and they need to approve it. Once they pass it to motion, an appropriate board needs to approve and do review regularly.

An information security policy works as a definition as well as a description of how an organization should safeguard and exercise security principles and practices (for instance, how due care and due diligence is exercised). In other words, how an organization is intending to safeguard its assets and values. Consider the security policy as the first step toward a well-structured and organized security architecture.

If this is the first step, the next step is none other than setting standards or standardization. You can think of the standards as rules, in fact, mandatory rules. The policy will be developed upon these rules.

In the next stage, there is a need for guidelines. What would you do with guidelines? You follow the guidelines. What sort of a guideline is required here? To implement or develop policy, standard, or anything, you need to have a structured set of instructions to follow. This is the purpose of guidelines. However, another set of guidelines will be used to guide the employees, customers, and stakeholders through the security program.

Finally, by following the standards and guidelines, the management team will create procedures. Now, if we move back to the policies, a policy does not have specific. It simply describes the goals. Therefore, a policy is neither standard nor a guideline. Since it is not specific, it isn't a procedure of control. Above all, you need to keep in mind that a policy does not describe the implementation details or specifics. It is the responsibility of

procedures. Finally, a policy, as previously stated a definition. It helps to define what is to be protected and how to ensure proper control through the implementation and development. Here, the term *control* means what and how to protect and what restrictions will be set forth. This is essential to ensure the proper selection of products and follow best practices, for instance.

Standards

Standards are important when you arrive at the implementation stage. Standards shape the security framework and procedures. In fact, a standard aid in decision making such as when purchasing hardware such as servers, software to help business decisions, and when purchasing any other technology.

Organizations select specific standards (a few) and move forward with it. If an asset or a process does not have a specific standard, it may end up with having no standard (may become vulnerable or facing interoperability issues). The importance of a standard is the guarantee that the selected works in your environment, and it adheres to industry specifics, remain within the regulations and compliance.

If we take a simple example, a policy requires an organization to have multi-factor authentication. And then, the organization decides to use smart cards. They select a specific standard by consulting the security analyst and understanding the policy requirements. Their long-term goal is interoperability. Interoperability is a characteristic of a product or a system. With it, a system's interfaces are completely understood, and able to work with any other product or a system seamlessly. By following a standard, they can ensure the interoperability as well as the security during the entire operation.

Procedures

Procedures directly control the development. As stated earlier, it is a set of step-by-step instructions on how to implement security policies. Hence, procedures are mandatory. It is also important to document these procedures to troubleshoot, reverse engineer, to follow whenever needed and to make

necessary upgrades to. Therefore, well-written procedural documents save significant time and money.

The following examples are of procedures touching various areas of an organization.

- Access control
- Administrative
- Auditing
- Configuration
- Security monitoring
- Incident response

Guidelines

Guidelines are instructions providing information and guidance. Although these are not mandatory instructions, do a major task of carrying knowledge. It is a critical method of communication for making awareness. Therefore, it is an efficient method of carrying information, warnings, regulations, prohibition, penalties, and ethics as well, thus making awareness. For instance, a guideline can be set to teach how a person should follow best practices, i.e., safeguarding passwords.

Baselines

A baseline is actually a benchmark, and it can be thought of as ground zero. It is, in other words, a minimal level of security concerning CISSP that is necessary to meet a policy requirement. It can be adapted so that business requirements including business policies, compliances, standards, and other areas. For instance, a firewall has a baseline configuration. A server has a baseline configuration. It is provided to meet a set of standardized minimum requirements. A baseline also ensures the basic requirements, i.e., protection.

To create a baseline, you have to create a written policy, in this case, a security policy. For instance, if it is a Windows group policy created through a security policy initiative, once it is determined, the administrators

will use different methods to deploy it. Once it is configured, the baseline can be stored or backed up for future use. These baselines will be compared when provisioning new systems.

It is also important to notice that an organization often uses one baseline per product or a configuration. There are also specific tools to create baselines. Another important role of a baseline is the ability to compare advanced configuration against it. This is also useful in benchmarking.

1.7 Identify, Analyze, and Prioritize Business Continuity (BC) Requirements

Business continuity is the utmost consideration of a business entity. Continuity matters when there are financial or any other issues affecting the business environment. This does not, however, mean that business continuity is not a concern when there are no current risks, threats, or ongoing issues. That is because future risks, zero-day threats are things you cannot be certain not to occur.

In simple terms, business continuity is sustaining critical operations even in the worst-case scenario. Business continuity goes hand in hand with disaster recovery. If there is a risk, there is a need for planning for business continuity. If the risk affects the organization, it must recover from the damages. This is when disaster recovery comes into play.

Therefore, when we talk about business continuity, we also talk about disaster recovery. In fact, business continuity and disaster recovery require a holistic management approach. If we breakdown the process here, the team responsible for business continuity planning (this usually is also initiated by the top of an organization and controlled through a board) creates a framework so that they can identify potential threats. Then it is possible to build resiliency. Once they identify and document potential threats and vulnerabilities (through analysis), it is possible to respond to events effectively while safeguarding the interests of the organization's stakeholders. Their interests would be brand, reputation, or value.

We can also through the disaster recovery process (DRP) as the implementation level while the business continuity process (BCP) is a planning stage. The other difference is that the DRP is highly technical. For

instance, we ask questions like what if our web firewall fails at the perimeter? How can we recover it? That is clearly about the DRP. If it is about BCP, we may ask questions like what if an earthquake destroys our headquarters? That prediction and response require more of a planning stage.

Develop and Document Scope and Plan

- During this process, the management request approval from the head of the organization by creating a business case
- The head has to approve it to take it to the next stage of development
- Formulate the plan collaboratively by business and technical teams together
- At this stage, there will be a business continuity policy statement (BCPS) followed by a Business Impact Analysis (BIA).
- Once the process gets past this stage, the rest of the development occurs.

Business continuity and disaster recovery require planning. Therefore, the planning process comprises the following important stages.

1. Project planning.
2. Business Impact Analysis (BIA).
3. Recovery strategy - formulation.
4. Planning the process, designing, and developing.
5. Implementation.
6. Reviewing and testing.
7. Maintenance and monitoring.

Now, if we take a look at the BCP and DRP, we can identify the steps of the holistic approach that was mentioned before. There are two parts.

1. Business Continuity Process. This includes,
 - a. Policies and strategies.
 - b. Risk management.
 - c. Planning.
2. Validation of the implementation.
 - a. The recovery process for Information Technology.
 - b. Alternatives (i.e., sites).
 - c. Keeping onsite and offsite backups. Replication is another important part.

Note: There are several backup sites that you need to become aware of. Those are,

- Hot site: This type of site remains up and running continuously. It can be configured in a branch office often. Alternatively, it can be configured in a cloud or a data center. It must be available immediately upon a recovery event. In addition, it must be far away from the main site.
- Warm site: This is a cheaper option to a host site and is unable to perform an immediate recovery upon an event. Even though this is true, it also comprises power, network, servers, phones, and other resources.
- Cold site: This is the cheapest option and takes more time to perform a recovery.

Business Impact Analysis (BIA)

Business Continuity Planning Process

Although planning is a thorough and lengthy process, the following main stages can be understood.

1. Identifying potential compliance requirements.

2. Documentation of the identified requirements.
3. Identify and document potential risks, threats, and vulnerabilities.
4. BIA process.
5. Prioritize resources such as processes, systems, and units according to the criticality of each resource.
6. Next, determine the resumption procedures.
7. Delegate the tasks and responsibilities.
8. Document everything and create procedures and guidelines.
9. Bring awareness through training programs.
- 10.

Review the process.

Steps for Performing a BIA

BIA is a complex process, and therefore, having a basic knowledge will help you during the real-world scenarios. Let's get familiar with terms first.

Maximum Tolerable Downtime or MTD : For how long a company can survive without a broken component, a lost function, or even a major loss? This maximum duration is the MTD.

Recovery Point Objective or RPO : How far can you go back and recover from? To what point can it be recovered? This is the RPO.

Recovery Time Objective : Time that is required to recover from a failure.

With this understanding, let's look at the step-by-step BIA process.

1. Select the data sources (i.e., individuals) to gather data. Tools such as questionnaires can be used in this stage.
2. Use qualitative and quantitative approaches and techniques to collect data.
3. Identify critical business functions.

4. Identify the dependent objects on those functions.
5. Calculate the MTDs.
6. Identify potential threats and vulnerabilities.
7. Assess the risk and make the necessary calculations to identify and clarify the findings.
8. Document all the findings and create the final report.
9. Submit the report to management.

In parallel, run the following steps.

1. Run tests and verify the completeness of the gathered data.
2. Determine the recovery time.
3. If unable to recover, determine the alternatives.
4. Calculate the potential costs.

Once you complete the BIA process, you can go ahead with the business continuity process outlined below.

1. Develop the planned recovery strategy and procedures.
2. Plan development.
3. Testing and reviews (i.e., exercises).

Example Scenario: This is a real-world example of the BIA process.

1. Develop a set of questionnaires, as stated before.
2. Train the responsible person on how to conduct and complete a BIA. It is possible to train the person through workshops or any other method.
3. Collect the BIA forms.
4. Perform a review.

5. As the final stage, validate data through follow-ups and interviews.

Once this is complete, you can move to the next stage.

Recovery Strategy

In the next stage, the planning and implementation of the recovery process occur.

1. Since the BIA is already performed, it is the time to identify and document the resource requirements.
2. Perform a gap analysis. This will determine the gaps between the current capabilities against the recovery requirements.
3. Next, explore and walk through the strategy and obtain the approval from the management.
4. Implement and finalize.

Plan Development

In this phase, the following activities are executed.

1. Development of the framework.
2. Forming the teams and assigning roles and responsibilities.
3. Planning for relocation.
4. Compilation of business continuity and disaster recovery procedures.
5. Documenting the procedures.
6. Validation of the plan.
7. Obtaining management approval.

Testing and Trials

The most important part of this entire process is to develop a realistic combat strategy. Therefore, this is the most vital stage of all. This includes,

1. Determining test requirements and maintenance requirements.
2. Plan testing procedures and exercises.
3. Provide training continuously.
4. Conduct orientation exercises.
5. Execute the tests and document the findings into a comprehensive report.
6. Through lessons learned, revise, and update the business continuity strategy, process, procedures, and all.

In this section, you have learned how you can develop realistic business continuity and disaster recovery strategy. Assessing the strategy and updating the strategy are important tasks. In addition, regular checking up of measures and training exercises are critical for successful mitigation and recovery.

1.8 Contribute To and Enforce Personnel Security Policies and Procedures

People are unarguably the weakest entity in a security plan. They bring realistic and significant risks by knowing or unknowing or being careless. Any user of a system can cause catastrophic damage to the assets and information. There are intelligent attacks, like social engineering and phishing. There are more sophisticated attacks like viruses, remote control, ransomware, and other disclosures. In addition, there can be impersonations. And sometimes, due to grudges and personal reasons, there can be insider threats such as man-in-the-middle attacks, information exposure or theft, and even terrorist activities. To reduce all these risks, the security policy must have policies set, procedures documented, and ready.

Candidate Screening in Hiring

This is one of the most important parts of hiring an employee, among others. The candidate must face different background checks such as identity checks, clean records against criminal activities (criminal records), recommendations, and social media activities. In addition, he must be

validated against his activities, education, certification, past jobs and performance, medical status, and whatever is necessary. Finally, a person can be background-checked through external referees. In such cases, an employer has to confirm who the referee is (identity) and if the person is a relation to the candidate. If the candidate successfully ends with a clean record, it is possible to put him in a probation period.

Employment Agreements and Policies

Employee agreement is one of the most important documents when it comes to the hiring process. Most employers, as well as candidates, do not handle this process well. Upon hiring a candidate, he signs an agreement or a contract with an organization. Once the person signs it, he is bound to protect it during work and even when he/she is not at work, but when he/she is using company assets.

An agreement defines job roles, duties, and responsibilities, accountability, wages, onboarding, termination, rewards, and penalties. Code of conduct and accountability sections are followed by a section where an employee agrees with the penalties and consequences if he/she fails to adhere to.

The agreement must also clearly disclose the actions the organization takes when there is something wrong. This reduces the potential grudges and justifies the systematic approach. And, it should include how the termination and clearance work so that the employee does not have to feel negativity during a termination process and how the organization can get its assets returned.

Onboarding and Termination Process

Onboarding is a process that starts from the first contact of the candidate, and it continues after the hiring process until the employee is well-established within the organization. This is important for the rest of the crew but mostly for the employee psychologically and technically. This also helps the newbie to learn the culture, get oriented with the duties and responsibilities through job orientation, become familiar with the business and security strategies, and become friendlier with each other.

This also reduced many risks that a new person might bring or conduct willingly or unwillingly. If the process is clear, easier to grasp, logical

(makes sense), and structured the employee will feel part of the organization and psychologically bound to protect the code of conduct, be responsible, accountable, and feel safe (this is one of the difficult yet most important goals).

Termination is a process that every employee may have to go through at least once in a lifetime. It is not an easy part of the management as well. There are general terminations due to willful leaves, the end of a contract period, reaching the age limit, and so on. There can be other more stressful situations like the removal of an employee due to cost-cutting, due to seizure of operations, due to misconduct by an employee or simply because there are better alternatives. These instances are sensitive and require careful execution.

Therefore, to simplify and streamline the process, there must be clear policies and well-documented procedures.

The below is a list of required Screening activities.

- Pre-employment screening
- Screening for criminal activities
- Screening for a sex offense
- Drug screening
- Tracing Social Security Number
- Credit history
- Compensation claim history

Termination Process in brief

- Collect and record the details
- Request the resignation letter (or receive it)
- Notifying the human resource department
- Notify the system administrators

- Termination of account both non-digital and digital
- Asset revoking checklist
- Revoke the company assets and mark the checklist
- Revoke access to all assets and mark the checklist
- Validate the received assets
- Request benefit status letter from HR and receive it
- Review any signed agreement
- Release the final payment including any additional payment
- If required, perform an exit interview, and obtain written permissions for references
- Update the information
- Close the profile
- Farewell party

Vendor, Consultant, and Contractor Agreements and Controls

A vendor can be a supplier, a manufacturer, or a similar entity. A consultant is most probably an outsider who provides external services such as auditing, guiding, contract work, and advice. A contractor is a party which/who is willing to perform a business task or multiple tasks for an organization for a period of time. For instance, a contract worker will work for two years in an organization, and he/she should know when to start and when to stop according to a clear agreement.

The risk here is that when you open your organization to these parties, you also open part or full business operation in your organization. Therefore, vendor selection, reputation, and compliance they adhere to must be carefully looked into, and adequate safeguards and restrictions must be set.

Most of the time, when an organization hires a consultant, he/she will be given a dedicated computer and connectivity to internal systems and data with specific limitations, of course. However, a consultant works with

multiple organizations. Therefore, they have to have clean records and appropriate monitoring. It is also worth considering the possibilities of making mistakes, the potential of accidental data loss, corruption, MitM attacks, and information stealing.

This is also true for the vendors. A screening and compliance check must be conducted. If there are any specific vendor-developed applications and other components are available, these have to be tested thoroughly. Through the agreements, it is possible to signify the limits and borders.

Compliance Policy Requirements

You already have good knowledge about compliances and how to integrate into corporate practices. In this case, the users must be informed, trained, and tested to verify their understanding and adherence to compliance policies. There has to be a knowledgebase of self-guidance as well as seminars, workshops, and other training sessions. By doing so, the risks are greatly reduced through knowledge and awareness.

Privacy Policy Requirements

You were already introduced with entities such as Personal Identifiable Information or PII in a previous section. An organization maintains both the internal and external PI Information. Therefore, such information must be heavily guarded against both internal risks and external ones. To safeguard such information, the least privilege and need to know principles are handy tools.

Any process or a person who has access to PII must be monitored and audited. By doing so, the level of trustworthiness of the organization can be identified.

Finally, these requirements and policies must be well-documented and transparent. The document should describe what type of information is at risk, what information is covered, and to whom it is applied.

1.9 Understand and Apply Risk Management Concepts

Risk management is the process of determining, assessing, and responding to risks. These risks can be present, future, or potential risks. Risks arise

due to threats and vulnerabilities. There can be other risks and risk factors. The risk management process comprises prevention and mitigation. To do so, a properly established and proven strategy is a must.

Identify Threats and Vulnerabilities

If you recall what you have learned so far, you already have the definitions in your mind. A vulnerability is an exploitable weakness. When there is a vulnerability, there is a degree of risk that a threat may emerge and exploit the vulnerability. There can be many vulnerabilities; some are easier to detect, but some are hidden. Sometimes subject matter experts find these vulnerabilities and disclose to responsible parties. Most others may find an exploit and gain advantage through it. They are threat actors.

What are the controls? These are the mechanisms or techniques used to reduce, restrain, or regulate existing or future vulnerabilities. You already learned the controls, and those are preventive, detective, deterrent, and corrective controls.

Risk Assessment/Analysis

Assessment of Risks

Risk assessment is the first step toward risk management. It is vital that an organization determine the vulnerabilities and how vulnerabilities can become threats. If a threat agent can exploit a vulnerability, there is a magnitude of the impact. This impact must be identified through the risk assessment procedure.

There are a few techniques to assess risks. Those are,

- Qualitative risk assessment: In a qualitative analysis, an event or a regulatory control is studied. By studying, we can arrive at an understanding of the quality of its implementation. The important thing to understand here is that a decision has been made about the impact on the organization if the control is not in place. The probability of the need for user control is also known. This excels at providing the risk assessor information about how well (the degree) the control is implemented at this moment. In this method, a scale can be utilized. Using such methods of risk assessment, it is possible to evaluate based on a specific standard or guidance.

- Quantitative risk assessment: In this method, available and verifiable data is used to produce numerical value. This is then used to predict the probability of risk.
- Hybrid (qualitative and quantitative) risk assessment: This approach is a mixed version of both qualitative and quantitative methods.

Performing a Quantitative Assessment

As you are aware, this assessment deals with numbers. In other words, numbers, and dollar amounts. In this process, costs are assigned to the elements of risk assessment, to threats found, and to the assets. The following elements are included in this process.

- Asset value
- Impact
- Threat frequency
- Effectiveness of safeguards
- Costs of safeguards
- Probability
- Uncertainty

The catch with this method is that you cannot realistically determine or apply cost values to some elements. In such cases, the qualitative method is applied. Now let's look at the process of quantitative assessment.

1. Estimating the potential loss: In this process, the Single Loss Expectancy (SLE) is calculated. The formula is $SLE \times Asset\ Value - Exposure\ Factor$. Here, the items to consider are theft of assets, physical destruction, information theft, loss of data, and the threats which might cause delays in processing. The exposure factor is the percentage of damage a realized threat can cause.

2. Annual Rate of Occurrence (ARO): This answers the question, “how many times is expected to happen per specific duration?”
3. Annual Loss of Expectancy (ALE): The final step helps to calculate the magnitude of the risk. It is calculated as $ALE \times SLE = ARO$.

Do not forget to include all the associated costs such as cost of repair, cost of replacement, and reload, the value of the equipment or lost data, and loss of productivity.

Performing a Qualitative Assessment

In this method, no numbers and dollar amounts are in use. Instead, it depends on scenarios. As you understand, it is difficult or impossible to assign values to certain assets. Hence, an absolute quantitative analysis is not possible. On the other hand, an absolute qualitative assessment is possible.

It is possible to rank the losses based on a scale, for instance, as low, medium, and high. A low risk can be thought of as a minor and short-term loss, while a medium can result in a moderate level of damage to the organization, including repair costs. High risk can result in catastrophic losses such as losing reputation, legal actions followed by a fine, or a loss of a significant amount of revenue.

The catch with this approach is you cannot realistically communicate the values.

There are some techniques to perform qualitative assessments such as FRAP (Facilitated Risk Assessment Process) and Delphi.

Risk Response

To respond to risk, there must be a systematic approach. Four main actions can be taken. Those are,

- Risk mitigation: Risk cannot be prevented all the time. Minimizing effort is the best approach.

- Risk assignment: Assigning or placement of risk is the process of assigning or transferring the cost of a loss a risk represents to another entity. This can be another organization, a vendor, or a similar entity. Some examples are outsourcing and insurances.
- Risk acceptance: This is the normal procedure of facing the risk.
- Risk rejection: Risk rejection is the process of ignoring that risk is not present. This can lead to dangerous outcomes, but some organizations would prefer this path.

Countermeasure Selection and Implementation

The implementation and placement of countermeasures or controls or safeguards is a critical step in risk mitigation. These controls can be physical (humans, hardware, fences, dogs, or CCTV) or logical (software, such as firewalls) or even hybrid (hardware firewalls with other software functions).

If we take a simple example of password security, you can set to prevent reversible password encryption, using names and common words, enhance the strength by increasing the number of characters and different character requirements. In addition, you can enable two or multi-factor authentication.

There are many countermeasures for each component, point, and perimeter. The selection must go through a proper evaluation procedure, and the team must know how to configure, install, manage, and maintain the countermeasures and controls.

Applicable Types of Controls

There are several types of controls, and you were introduced to the controls previously. Those are,

- Preventive controls
- Detective controls
- Corrective controls
- Deterrent controls

- Recovery controls: These are for recovery purposes. In fact, there can be many instances, such as general information loss, hardware fault, corruption, information stealing, physical damage, and any other disaster. The controls would be backup and recovery procedures, disks, network-attached storage, storage area networks, clustering, disk arrays (RAID types), and software.
- Compensative controls

Security Control Assessment (SCA)

A security assessment is a key component of the security strategy. It is important because if you do not periodically assess it, you are unable to detect flaws, required changes - updates/upgrades/retirements/obsoletions, vulnerabilities, and budgetary concerns.

You can use certain tools to conduct an SCA. For instance, NIST SCA aids in performing a comprehensive SCA. For more information refer NIST Special Publication 800-53 <https://csrc.nist.gov/Projects/risk-management/Security-Assessment>).

Monitoring and Measurement

Monitoring is a critical step toward a successful security program. It is important to keep an eye on the implementation and deployment and optimize it to reach maximum performance and precision. This step assures sustainability as it helps to mitigate future and unknown threats continuously. This process must be designated, and there must be a dedicated team.

Let's take an example to understand why it is important. You set up a perimeter firewall and think everything will be under control. Eventually, the firewall receives various types of scans, and it logs the attempts. However, you are not paying attention, and you do not set up a proper alerting procedure. In the end, after a period of reconnaissance, an attacker finds an exploit, launches a successful attack, and breach the perimeter.

As you see here, you were unaware of the vulnerability because you thought this was a one-time setup. You did not patch and update the firewall. In addition, you did not set up a monitoring program and forgot to

set up an alerting system to alert the responsible parties upon an incident. Furthermore, you may not have implemented a backup and recovery process if someone breaches. All of these failures point to one thing, weak security practices.

Therefore, a proper monitoring system with alerting, properly configured thresholds, automatic locking down features, and a timely updating/patching program is required to tackle these situations. Another important action is to secure the logs. If you wish to trace any incidents, you need the logs. Therefore, securing and backing up logs are important parts, especially if log rotation occurs. Periodic reviews and auditing of the logs will help to find the incidents, future threats, and vulnerabilities. It is quite important to keep your contact with the vendor and its information so that you can timely update and patch the assets.

In a general organizational environment, reviewing and measuring processes are conducted per week. During the reviewing process, the following key areas will be focused.

- Number of occurrences
- Nature of the occurrences, both success, and failure
- Duration
- Affected assets
- Impact
- Involved parties and location

Asset Valuation

Asset valuation plays an important role in the risk management process. In any organization, the management must be aware of types of assets, both intangible and tangible, as well as the values. There are several methods utilized in asset valuation.

- Cost method: This method is based on the original price of the asset when it was purchased.

- Market value method: This is based on the value when an asset is sold in the open market. If the asset is not available in the market, there are two additional methods. Those are,
 - o Replacement value: If an asset similar to this can be bought, based on that, the value is calculated.
 - o Net realizable value: The selling price of the asset (if it can be sold), deducted by the expenditure.
- Average cost method: Total cost of goods available for sale divided by the units available. When the valuation cannot be distinguished, this is a good approach to use.
- Base-stock method: Any organization maintains a certain amount of stocks. Hence, this is based on the value of such a base-stock.

Reporting

Reports and alerts play a key role as it is stressed several times previously. It helps to prioritize the requirements and needs. This brings the ability to properly utilize the assets, controls, countermeasures, proactive management of security issues, and safeguards the organizational assets, including information.

When reporting, it is important to keep in mind that the report must reflect the risk posture of an organization. Upon preparing a report, you must follow a standard. It requires clarifying, and sometimes you cannot be too technical. The report must make sense, in other words, to all the parties. You should also consider the requirements set by current acts, mandates, regulations, and whatever standards or compliance requirements available within your organization.

Continuously Improvement

This stresses the need for continuous improvement to keep the risk management and recovery strategy updated and free of flaws. In other words, this is an incremental process, and it is possible to apply it to any level or function in an organization.

To aid in this process, you can use the ISO/IEC 27000 family. It provides requirements for a comprehensive Information Security Management System (ISMS) in the clauses 5.1, 5.2, 6.1, 6.2, 9.1, 9.3, 10.1, and 10.2.

Risk Frameworks

You need some aid for establishing proper and precise risk assessment, resolution, and monitoring strategy so that the outcome is a solid risk management process. This is where you need to utilize a risk framework. There are many risk frameworks already developed and available. The most outstanding and accepted risk frameworks are,

- NIST Risk Assessment Framework: Visit <https://www.nist.gov/document/vickienistriskmanagementframeworkoverview-hpcpdf> for more information.
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE): Visit <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473> for more information. There are two versions, version 2.0 for the enterprise and the OCTAVE-S v1.0 for small and medium businesses.
- ISO 27005:2008. More information is available at <https://www.iso.org/standard/42107.html>
- The Risk IT framework by the Information Systems Audit and Control Association (ISACA). Visit <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx> for more information.

1.10 Understand and Apply Threat Modeling Concepts and Methodologies

Threat modeling is a technique utilized to identify and quantify threats such that threats can be communicated and prioritized. This concept is used extensively in the software development process.

Threat modeling techniques focus on one of the following areas.

- Attacker
- Asset
- Software

Some of the widely accepted and popular threat modeling methods are as follows.

- Process for Attack Simulation and Threat Analysis (PASTA) is a risk-centric modeling technique.
- Spoofing Identity, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (STRIDE), invented and adopted by Microsoft. For more information, visit <https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling>
- Visual, Agile, and Simple Threat (VAST) is another threat modeling framework based on a platform known as *ThreatModeler* . For more information, visit <https://threatmodeler.com/>, <https://threatmodeler.com/threat-modeling-methodologies-vast/>

Also, you could also use OCTAVE, CVSS by NIST, LINDDUN, and many others. The tool selection depends on the requirement, ease, and the scenario.

In addition to these tools and techniques, you can use certain other tools, such as threat rating systems. This is to rate and give a weight to each threat so it can be used in modeling to understand better. Damage, Reproducibility, Exploitability, Affected Users, Discoverability (DREAD) by Microsoft is an example. As you may have guessed, it can be used for qualitative risk analysis. Also, remember that the STRIDE/DREAD aggregated model is also a very useful modeling method.

Let's also look at threat modeling steps to break down and understand.

1. Identification phase
2. Describing the architecture

3. Breaking down the processes
4. Classifying threats
5. Categorizing threats
6. Rating the threats

1.11 Apply Risk-Based Management Concepts to the Supply Chain

Once we develop a comprehensive risk management program, it is possible to apply it to many business functions and components. In this scenario, it is applied to the supply management areas. An organization may have to work with external parties such as suppliers, contractors, transportation and logistics services, and many others. To successfully reduce risks and recover during any kind of outage, you must apply the risk-based management concepts to this area as it brings many risks, including threats and outages. The same concept can be applied upon acquisitions and mergers. If you have been following so far, you should have also guessed that this is a scenario where due diligence is exercised.

Risk Associated with Hardware, Software, and Services

In this section, we will be looking at the risks associated with these assets other than the live-ware or humans. All the new and existing hardware, software, and even services expand the risk surface of an organization. Unless properly determined and managed through the risk framework, these components impose extensive threats to the survival of the operation. In addition, it may bring interoperability and integration difficulties and compliance failures.

When purchasing hardware, there are many things to evaluate so that you can ensure the safety and security. The vendors must be able to continuously support the hardware maintenance by supplying patches, updates, and possible guides on security. When it comes to integration, you must also consider the risks it may bring.

Software, on the other hand, brings even more risks as unlike a device, it brings code and layers of security issues. For instance, there can be flaws in

the component level, modular level, compilation level, and so on. Some architectural support may also bring issues. In addition, when you use different features, it may also bring risks, mainly revealing internal information such as IPs to remote servers and customer data as well, especially if you consider cloud-based software. Those bring even more risks to internet-based threats. Furthermore, compliance requirements may also impose certain restrictions upon such selections.

The services include a more complex matrix. Service may mean more human involvement apart from software services. For instance, an internet service provider provides multiple internet-based services to many organizations. Therefore, it is the main information highway for outside activities as well as for customers who depend on the services provided by an organization. Although ISPs provide service level agreements and security, the services an organization provides outside, and the assets used to access the internet must be protected from internet threats such as viruses, trojan horses, ransomware, scams, phishing, sniffing and all kind of attacks including DDoS.

Third-Party Assessment and Monitoring

No organization can live without third parties as the supply chain is something a single entity can sustain individually. Among many considerations, to safeguard internal assets and shared information, non-disclosure agreements, agreements on security and privacy, and any service level agreements (SLAs) must be reviewed by the organization's head and the board of approval. Upon the review process, the organizational goals, compliant request, security architecture, and standards can be compared.

Minimum Security Requirements

For each component, that first into the organization's business should have a set of minimum-security requirements. This serves as a baseline. Upon this, required safeguards can be built and must be communicated to other parties. Ultimately, it aids in closing security gaps, the ability to determine new requirements, detect/resolve vulnerabilities, and deploy necessary controls.

Once the security requirements are derived, it must be reviewed continuously, at least at the functional level. A full annual review is also required. In addition, upon an acquisition or a merger, there is a need for change management. A transition period is required in this scenario. During the transition period, things such as security policies, procedures and practices, compliance requirements, and regulatory requirements must be carefully considered.

Service-Level Agreement Requirements

A service level agreement or an SLA is mainly a measure of service excellence in terms of quality and performance. It is used together with performance metrics and key performance indicators (KPI). For an organization, servicing clients on time or within an acceptable time frame is critically important. Therefore, many organizations that provide services have SLAs implemented, and when they offer services, the clients and the provider agrees upon terms.

For instance, an organization may provide a cloud service to its customers. They have to offer one or a set of SLAs depending on the subscription level. Here is an example,

- Responding to urgent calls/tickets within 15 minutes for premium subscribers by an account manager.
- Responding to high importance tickets within 1 hour. Instant chat support for these customers.
- Responding to non-critical issues within 24 hours. These are often handled through tickets.

An organization may have such agreements with the ones they depend on, for instance, an internet service provider or a cloud service provider. Upon purchasing such services, an organization must look through the service level agreements as well as the performance track records. SLA is a guarantee of service in terms of timely response and recovery. For mission-critical services, such dependencies may cause vital blows on businesses if those external or third-party providers do not honor the SLAs. Such risks exist, and an organization must avoid it as much as possible.

There are other agreements, such as the following.

- Operating Level Agreements (OLA): These are internal service level agreements defined for internal users. OLAs comprise of service tags just like SLAs and are used to track internal performance.
- Underpinning Contracts (UC): This measures the performance between a vendor and a service provider (external).

Service management is part of an organization, especially if the organization provides some sort of service. If you have studied ITSM or ITIL, you are introduced to OLAs and SLAs in depth. OLAs often include,

- Service desk
- Support groups
- Systems administration
- Operations management
- Incident management

A basic structure of an SLA includes,

- A master service agreement, also known as the MSA
- SLA and KPI
- One or more OLAs

1.12 Establish and Maintain a Security Awareness, Education, and Training Program

In any organization, the weakest link is not a device or software but users, the employees. Therefore, a well-structured training program initiated by the head of the organization is a critical success factor. Awareness issues and lack of skills or technical knowledge may lead employees to make mistakes, dissatisfaction, overestimation, and carelessness. Managing this is another critical part of risk management.

Methods and Techniques to Present Awareness and Training

The most crucial part of a training program initiative is to make a belief in this. In many instances, heads of the organization do not believe in a proper training program. They overestimate their skills and do not care if employees do not have a proper understanding. Instead, they believe in other teams, such as the IT administration, to make all the arrangements. This is where the program is likely to fail.

At the first stage, the relevant skills professionals, with or without consultants, draft and finalize the security program. The board and management team responsible for the program must have a thorough understanding of the program, and they must meet the required skills and competencies through education and certification.

The next stage is making awareness and communicates the relevant information to the other departments and managers, especially non-technical people. This is a high-level training program that focuses on orientation. Once this is achieved, they can build their competencies and communicate the knowledge, techniques, and practices to their teams. Here is a set of steps to handle this program comprehensively.

1. Head of the organization and the senior management discuss and agree on what they should deliver and communicate to the lower levels.
2. The training program is designed, and the senior management actively engages with the entire program.
3. The program is presented and delivers clear perspectives and how it benefits business in the long and short-term.
4. The demonstrations must communicate how this is beneficial to the sustainability and how it helps the employees, with clarity.
5. The program must aim for ground-up progress.
6. To make it interesting, presentation techniques including graphics, storytelling, appealing visuals, multimedia, and digitalized environments such as conferencing tools and remote capabilities can be used to save time and space.

7. The training program should be enjoyable and engaging.
8. During the program, there has to be a way of testing awareness and knowledge.
9. Regular exercises (without letting them know) can reveal the truth.
10.
Continuously update the program and content.
11.
Periodic training.
12.
Internal assessment and learning center establishment for people who would like to learn more and get certifications.

Another important aspect of training is the ability to utilize peers, vendors, consultants, and institutes, for instance, (ISC)².

Periodic Content Reviews

Training content and material must be updated as the technologies change, get updated, replaced, security issues, and content get updated daily, new vulnerabilities and threats can emerge.

Again, the content must be easier to grasp for non-technical people. As mentioned earlier, the content must be engaging and hands-on. It is also possible to organize such training programs, workshops, webinars, and all through social networks. Collaboration tools such as Microsoft Office 365 brings new heights to training.

Program Effectiveness Evaluation

To measure the effectiveness of the program, there has to be an evaluation criterion. For instance, it is possible to implement performance metrics. Then upon training and after the training, you can create periodic testing so that the employees can be tested for the level of awareness. For instance,

you can attempt to phish the users through various methods, and if the success rate is lower than the previous tests, then there is positive progress.

Chapter 2

Domain 2 - Asset Security

What is an asset? An asset represents an object owned by an organization. It also has a certain value to the organization. An asset can be a person, a piece of information or data, a building, a device, or a deed. We have already looked into assets in the previous chapter. This chapter focuses on safeguarding the assets. In fact, it is about safeguarding the data or information as these are the most valuable assets. Information security is the main focus of successful security, and it is also the responsibility of a CISSP certified professional.

Before going into the safeguarding techniques, it is better to define what data is. Data is the building block of information, the bits, and pieces of scattered knowledge. Data has different states. It can be at rest, moving, being transformed, and being used. When combined data create meaningful information.

Data also has a lifecycle. It is formed, stored, used, transformed, archived, and removed. During the entire lifecycle, an organization must safeguard the information by applying the CIA practices and through the security strategy. However, data can have different meanings in an organization. Some data can be critically important, some may be sensitive to some departments or roles, and some may be informative. You have to determine the level of criticality and priority when safeguarding data. To achieve this, we use the technique known as the *data classification*.

2.1 Identify and Classify Information and Assets

Data Classification

Data must be identified, categorized, and tagged so that the data and information can be opened to a specific party. To identify the categorized data, you have to do the tagging, and it is known as Labeling.

The other objective of data classification is to delegate the responsibility of the data to roles. Other roles cannot access the data unless the guardian releases the key. This is known as *clearance* . Only the party who intended to access data will be the only one to see it.

If someone requires having data access, they have to go through the *access approval* process. To safeguard data, we apply two principles. One is *need-to-know* . This means the user's knowledge is limited to what he/she should know but nothing beyond that. The other is called the *least privilege* . This means the person gets the least authorization to perform anything on data.

If someone requires access to data that is not designated to him, he needs to be granted access. Upon grant, the user must be communicated the sensitivity level of the data and how he/she should protect it and the limitations put on the data. To track and audit what they do, they have to go through the authentication, authorization, and accounting processes. This is also known as the triple-A (AAA). To provide the necessary access to perform a job, the least privilege can be exercised.

Many countries follow government legislation and act when implementing a classification procedure. In the U.S., the executive order 12356 is applied to national security information. Upon classifying, de-classifying, and safeguarding information, this can be applied. In different countries, there are different procedures.

Data Classification Considerations

- Data security
- Access rights
- Data encryption
- Data retention
- Data disposal
- Data usage,
- Regulations and compliance requirements.

Labeling

Let's look into the different types of labeling.

- Top secret: This is the highest level of security applied to government and military information. Exposing such data can do grave damage to the nation.
- Secret: This is the next classification. For an organization, leaked information at this level can cause massive damage and loss of reputation.
- Confidential: If leaked, it may damage up to a certain level to an organization or the country.
- Sensitive but Unclassified: This data can affect people if it gets leaked. For instance, a person's medical condition can cause personal losses and social issues.
- For Office Use Only
- Unclassified

Asset Classification

In this section, the focus is on data assets and physical assets. Asset classification is also used in information security, although it is more used in accounting.

2.2 Determine and Maintain Information and Asset Ownership

The data owner is the person who is designated to manage, maintain, and safeguard the asset. This is also true for data. To safeguard data, there must be an owner, and he/she must be responsible and accountable for what happens to data. Data owners should also take part in classifying data, apply rules and regulations, permission and authorization, clearance, safeguard, retention, and dispose of data and devices.

2.3 Protect Privacy

To manage privacy, data is assigned to and maintained by several roles, and you must be familiar with these roles and how they maintain data.

- Mission Owners: Has the ultimate responsibility to initiate, fund, and establish a proper security program to safeguard data.
- Data owner: Data owners are usually data managers. Among their responsibilities, data classification, labeling, retention, backup/recovery, and disposal remain the most important.
- Data custodian: A custodian is a person who has delegated responsibilities. For instance, a data owner may appoint a data custodian to backup data according to a routine. Some system-level custodians maintain systems by applying updates and patches.
- System Owner: As the name implies, this role is responsible for managing and maintaining the systems that hold data. Server managers, network, and system administrators play this role on multiple occasions.
- Users: People who use and modify data. This does not mean they are not responsible. In fact, they have the most responsibilities as they may expose, corrupt, or delete data. In this case, they have to follow the guidelines through training.

Data Controllers and Data Processors

A Data Controller, according to the European Commission, is the one that “determines the purposes for which and the means by which personal data is processed. So, if your company/organization decides ‘why’ and ‘how’ the personal data should be processed, it is the data controller. Employees processing personal data within your organization do so to fulfill your tasks as a data controller.”

The Data processor, on the other hand, manages the data on behalf of the data controller. The definition provided by the European Union says, “The data processor processes personal data only on behalf of the controller. The data processor is usually a third-party external to the company. However, in the case of groups of undertakings, one undertaking may act as a processor for another undertaking.”

A data controller becomes a data processor considering a different dataset. This is the meaning of the “However, in the case of groups of undertakings,

one undertaking may act as a processor for another undertaking.”

A joint data controller, according to the European Union’s definition is, “Your company/organization is a joint controller when together with one or more organizations it jointly determines ‘why’ and ‘how’ personal data should be processed. Joint controllers must enter into an arrangement setting out their respective responsibilities for complying with the GDPR rules. The main aspects of the arrangement must be communicated to the individuals whose data is being processed.”

Data Remanence

Data storage can pose a significant threat as traditional methods may not entirely remove the data when deleted. This is true for magnetic tapes and disks. With the new technologies, there are ways to recover data even from the new storage technologies. Therefore, data remanence can cause data exposure. The technology lot (RAM, ROM, Flash, Magnetic, SSD, etc.) multiplies the threat.

Destroying Data

As you are aware of the data exposure when you simply erase and dump the storage, you have to understand how to destroy the data and assets when required properly. Use the following methods to destroy data and devices.

- **Overwrite:** Data overwriting is a popular method of destroying data. This is often applied to magnetic disks. By overwriting the existing data by ones or zeros in multiple rounds, data can be properly erased, and each pass closes the recoverability to zero.
- **Degaussing:** Only applied to the magnetic disks, the method destroys data as well as the disk. In fact, the device is exposed to a strong magnetic field.
- **Destroy Physical destruction of the devices.** This is usually (but not always if not done properly) the best method.
- **Shred:** This is applied to magnetic tapes, paper data, plastic devices. It is also similar to the destroy method.

Collection Limitation

This is a bit tricky but a significantly important method. This simply means you do not store what is unnecessary. It saves time, space, and money altogether. For instance, an organization does not require a significant amount of personal data from the employees. If someone is collecting such data, they must security storage, security communicate, and securely transfer the data while being transparent about what is collected. Current laws and regulations force the data collectors (i.e., websites) to obtain approval from the users as soon as they land on their sites.

2.4 Ensure Appropriate Asset Retention

Retention or archival of data also imposes a certain amount of risks. Any organization has to keep old data in need of the future. However, the data at rest does not impose a threat like moving or modifying it. The main risk here is two-fold. If the data is stored in offline storage, there may be a physical threat from device-itself (e.g., degradation), people, and the environment. If the data is stored online (for instance, Amazon Glacier) still it is offline. Still, when it is online, there is a risk in the transfer as well as there must be a guarantee that data controller and custodians do not alter or expose data. It is also vulnerable to impersonation and other types of attacks.

Therefore, the retention vectors must be carefully selected. For instance, due to longer periods of retention, the technologies used may eventually get obsoleted. When this occurs, the data must be loaded to new devices, and it must be cost-effective. Some obsolete devices may corrupt data. Therefore, an occasional routine is required to validate data.

In any case, routine checks, recovery trials, and checks on physical devices (if an organization maintains) are required. When storing the devices, the area must follow standards and compliance requirements. Physical degradation can be managed through well-constructed rooms with controlled HVAC setups. Resistance to fire and environmental disasters are also significant considerations.

2.5 Determine Data Security Controls

Understand the Data States

Before going into data security controls, you must have a solid understanding of data states. Let's look at the different states that data can exist.

- Data at rest: Data is stored and not being used
- Data in motion: Data is being retrieved, transferred, or transmitted
- Data in use: Any operation or action on data such as modifications and saving

Scoping and Tailoring

By scoping, the controls that are within or without the scope are determined. This is known as selecting the standards. Tailoring means the mounting (re-orientation, implementation, and development) the controls to fit the requirements.

NIST - Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication (SP) 800-53 Revision 4 provides an excellent guideline for scoping and tailoring. It is summarized below.

- By following the initial security control baseline, identify and designate common controls
- Determining and applying to scope
- Selection of compensation controls
- Assigning values to organizational security control parameters (these are defined within the organization)
- Provide additional controls to the baseline (enhancements)
- Providing specification of information to implement the controls

Standard Selection

This is a documentation process of selecting the standards for the organization-specific technologies or architectures that will be selected. This serves as a baseline to start building on top of it. In this process, the focus mainly remains on the technology selection rather than a vendor selection. Since the selection caters to the need regardless of the different teams or individuals, it caters to the need for new teams and individuals as well. Hence, it provides scalability and sustainability.

There are widely accepted frameworks to select. Some of these are already introduced in previous sections.

- OCTAVE
- ISO 17999 and 27000 standards
- COBIT
- PCI-DSS

Data Protection Methods

Appropriate data protection methods and technologies must be utilized to protect the data at each stage. Let's look at this in detail.

- Data at rest: Data at rest is the data that is not being used or transferred. There is an integrated memory protection build with many operating systems nowadays to stop memory hijacking and leaking. When it comes to storage, there are additional security configurations such as encryption, permissions to access the storage and authorization information, and physical controls to limit access to hot storage and archives. WORM storage is also a storage medium (e.g., CD-R), and it has built-in integrity protection, although it does not provide confidentiality (you have to use other means).
- Data in transit (or in motion): Data is either in transit in the computer's circuitry when in use or in the network circuitry when transferred or access through remote means. Such data has the most threats. There are many protection mechanisms like TLS, certificates, public-key encryption, and many others. When it comes to remote access through VPN and RDS technologies, there are many security additions, including public-key encryption and relevant VPN technologies. Also, firewalls and other mechanisms must be installed in perimeters and the remote devices. Remediation is another technique that can prevent remote devices from accessing the internet network unless secure.
- Data in use: To protect live data, there are many operating system level mechanisms to protect the working memory. Security mechanisms like not security, tamper protection modules, kernel,

and user address space, process isolation, hardware segmentation, virtual memory protection, buffer protection, cache protection, and extended protection through antivirus and internet security.

Along with these protections, preserving logs and auditing reveal any threat and attack attempts to the operating system and memory. Analyzing logs and configuring alerts can proactively prevent and detect the incidents.

2.6 Establish Information and Asset Handling Requirements

Handling assets require classification and labeling. Appropriate labeling can be applied to disks, tapes, and archives significantly help to categorize the devices. This method can be applied to any other data storage devices such as disks, removable drives, CD/DVD, external hardware assets, and even file cabinets.

Storage areas must have appropriate security and classification. It has to be applied to the roles, and they must have proper clearance and access mechanisms in place. The access levels can be controlled through labeling, locking mechanisms, authentication and biometrics, and any relevant controls.

As stated earlier, the destruction of data is the final step of this process. This is already covered in a previous section.

Chapter 3

Domain 3 - Security Architecture and Engineering

3.1 Implement and Manage Engineering Processes using Secure Design Principles

In this domain, we will be looking at the engineering perspective of security architecture. This domain is highly technical in contrast to other domains.

Following a secure design, the principle is essential to lay a foundation from the ground up whenever you design and develop strategies, assets such as software and other digital tools.

To stay within the security boundary from the start, an organization must follow standards and guidelines made available by governments, security associations, and relevant bodies. This process assures risk mitigation while preventing interoperability issues, compliance issues, and functionality issues.

The following is a list summarizing the engineering process.

- Forming design ideas and concepts
- Collecting and documenting the requirements
- Feasibility study and specification of requirements
- System design
- Implementation phase
- Testing: Tests will be started at the component level and expand to modular tests. The next stage would be unit tests – alpha and beta tests followed by user experience studies. Finally, there will be a full test followed by scenario tests, simulations, and acceptance tests. In general, the developer will be using a development platform

and a testing platform dedicated to the engineering tasks. This also ensures that the main production system remains untouched.

- Deployment
- Training
- Maintenance and support including change management

3.2 Understand the Fundamental Concepts of Security Models

A security model works as a blueprint, and it enables the possibilities of addressing security gaps by initializing security boundaries. CISSP students should be familiar with the existing security models, their pros, and cons and how to implement if required.

Bell LaPadula (BLP) Model

Bell LaPadula model follows a state-machine model. It is a linear non-discretionary model. Later it was formalized as part of the multi-level security policy (MLS) - U.S. department of defense. This model addresses confidentiality. It has the following features.

This model assures no-read-up and no-write-down actions. Sounds like Greek? Let's clarify.

- No-read-up (reading down): A subject with lower-level clearance is prevented reading upper objects which require higher clearance
- No-write-down: A subject with higher clearance cannot write (attach or pass) security objects to lower levels

The model guarantees security integrity by the following security measures

- Get access: Before obtaining access to read, append or execute an object, a protocol must be used
- Release access: Once the action is performed, releases the access
- Give access: An object creator allows an action performed on his creation

- Rescind access: This is revoking access after giving access to an object (the opposite of the give access)
- Create object: A protocol allows the creator to activate an object
- Delete object: The opposite of the create object
- Change security level (below the current level)

One problem with the BLP model is the missing write-up controls. Hence, it requires the collaboration of other models.

Biba Model

This model addresses the gaps introduced with the BLP model. In fact, it assures no-read-down and no-write-up. In this case, a subject with higher-level clearance cannot read from lower integrity security objects. In addition, a lower level subject cannot write to objects which require higher integrity.

Clark-Wilson Model is another model, and the main focus of this model is integrity, but we are not going to look into this model in depth.

3.3 Select Controls Based Upon Systems Security Requirements

This section of the lesson focuses on selecting the controls by following a specific standard. Let's look at an example.

Common Criteria for Information technology Security Evaluation (A.K.A CC or Common Criteria) is an ISO/IEC 15408 international standard. This standard was brought upon so that it can unify the goals. The following order standards are integrated into this standard. Those are,

- Information Technology Security Evaluation Criteria (ITSEC)
- Trusted Computer System Evaluation Criteria (TCSEC) – A.K.A. the Orange book, part of the rainbow series
- Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)

Let's look at the CC process in detail.

- Common criteria cannot be applied to hardware as well as software
- The target of the evaluation (ToE) must be selected first
- A PP or protection profile is a specific set of features that are required to stay in compliance with the common criteria. Vendors may provide protection profiles with certain exclusion
- A security target or an ST identifies the security properties concerning the target of evaluation
- The entire evaluation process assesses the confidence level

Common criteria focus on the assurance of security requirements. To do so, it defines seven levels of evaluation assurance.

1. EAL1: Functionally tested
2. EAL2: Structurally tested
3. EAL3: Methodically tested and checked
4. EAL4: Methodically Designed, Tested and Reviewed
5. EAL5: Semi-Formally Designed and Tested
6. EAL6: Semi-Formally Verified Design and Tested
7. EAL7: Formally Verified and Tested

Carnegie Mellon University develops this, and the full document is available at <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=298707/>

3.4 Understand Security Capabilities of Information Systems (e.g., Memory Protection, Trusted Platform Module (TPM), Encryption/Decryption)

In this section, hardware security controls are being looked into, such as memory protection, Trusted Platform Module, and encryption. In other words, these are hardware.

First, we have to become familiar with some concepts used in the design.

- Abstraction: Abstraction is a method of hiding unnecessary components. This helps to reduce risks. For instance, when you do a write operation to a file in your computer, you do not know which stacks are being used.
- Layering: Separates modules into tiers. This works together with abstraction.
- Security domains: These domains classify and limits the access level. In other words, each domain is a classification. The concept is widely applied to hardware. For instance, there is a model known as the *ring model* . It separates the Kernel mode and the user mode in an operating system, whether it is virtualized or not.

Protecting the Working Memory

Computer memory (read-write or random-access memory) is utilized by the kernel, the operating system as well as the software processes. There are reserved memory locations only the kernel can access. Some are reserved for the operating system itself. Hijacking processes or memory leaks can occur if a software program or even an operating system component does not behave as expected. For instance, if a program is attempting to access a memory location that is not assigned to it, the software or the operating system may crash. Eventually, this becomes an exploit. The following security steps are available with multiple operating systems.

- Hardware Segmentation: This is the segmentation of the hardware assets according to the importance during memory allocation.
- Process isolation: Isolating process memory such as virtual memory, encapsulation, and multiplexing, and so on.

Even though the operating systems run on top of our hardware, and even the organization's assets such as servers and workstations. In addition, nowadays, the most popular component is a smartphone. It may also bring threats to the organization unless controlled and applied standards.

Another popular option is virtualization. In this case, the hypervisor must be protected. There are two types of hypervisors.

- Type 1: The operating system level virtualization (VMware ESXi)
- Type 2: These services run on the operating system, such as VMWare, workstations, and other local goods.

Trusted Platform Module (TPM)

This module is a small chip integrated into a computer motherboard. Its sole responsibility is securing and assisting cryptographic operations. The chip can generate random numbers, cryptographic objects, and other security operations. Windows platform offers a service called BitLocker. It can utilize the TPM for maximum security. With this, it is easier to encrypt/decrypt the entire hard disk. It is a useful tool to protect confidentiality. There are many instances where TPM is used to provide security and tamper protection.

Interfaces

An interface is a connection between 2 pieces of electronic devices or between a human and a computing device. For instance, in a client-server operation, when a human wants to connect to the server, an interface is used. A simple example is a network interface card. It is an interface between the motherboard and the user. Another is the email client interface.

Interfaces also need to have security built-in, and the following list comprises them.

- Encryption: This is mostly applied to client-server systems. End to end encryption is used to communicate from a client to server and vis versa to prevent multiple attacks. Many web and mobile-based applications use encryption to protect user interactions. If the security is questionable, then there are VPN technologies providing end to end encryption, for instance, IPSec, SSTP technologies. Remote desktop protocols also provide the same level of control.
- Fault tolerance: Fault tolerance is the resistance to faults and the ability to recover/proceed when there is a fault condition. In this case, a well-structured standby and backup systems are used.

- Message signing: This ensures authenticity and non-repudiation.

3.5 Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements

Client-Based Systems

Client-based systems can be the most vulnerable as the client endpoints are used and managed by the end-users. A client system can be a computer or a hand-held device. Since most of the devices are connected to the internet at some point, they are quite vulnerable.

Many users are unaware of security practices. Among the things they do, the following objects widen the attack space.

- Operating system and kernel vulnerabilities
- Missing updates
- Running decommissioned software
- Installing multiple, unnecessary software
- Potentially unwanted applications
- Adware
- Malware

Most of these issues arise due to the lack of knowledge and awareness. In some cases, the lack of technicality is another issue. Even if the devices are protected, the users are also susceptible to social engineering and psychological attacks. Therefore, the top-level consideration of a security program must be client protection and privacy. In addition to corporate protection protecting the individual clients must be protected, remediated before connecting to the internal networks, and protect remote users using policies. For internet protection, a commercial internet security suite can be installed. Most of the time, organizations purchase complete enterprise suites to fulfill the requirements.

Server-Based Systems

Internal servers are protected within the premises if proper internal access controls and monitoring are set. In addition, accepted standards must be followed when designing the server rooms and upon placements. Backup power, fire extinguishers, sensors, and emergency controls protect servers from physical threats. Servers are also vulnerable to insider threats from people.

Therefore, following proper standards and procedures ensure the physical and logical safety. In a high-security environment (military and other similar organizations), custom Linux/Unix based operating systems are used to implement security baselines, They also implement custom security configurations (i.e., access controls such as discretionary controls), layer access controls and authentication procedures, end-point protection with layered firewall systems and sophisticated technologies, to prevent DDoS attacks on servers that accept internet-based clients.

There are a huge number of threats that may compromise the servers if they are not properly updated and audited for security holes. These can be internal vulnerabilities, known exploits, internet-based reconnaissance attacks, and many others. Furthermore, client devices may also distribute threats if those are not properly screened.

Web servers and database servers can also be targeted often. There are sophisticated technologies to monitor incoming traffics to identify attack patterns. Some of these units or software utilizes artificial intelligence for decision making. In addition to these threats, legitimate or non-legitimate incoming traffic can overload the servers. Load balancing units are present to manage the loads and redirect if necessary or even stop accepting requests upon an incident.

Some networks use IPS/IDS/Honeypot solution to provide internet-based attacks.

Databases

Databases are the most vulnerable services as they hold all the valuable data. For an attacker, this is the price on most occasions. A database may contain mission-critical data, Personal Identifiable Information (PII),

customer information, passwords, and many other critical such as payment information/credit card information.

Operating systems also include databases. For instance, the credentials database in Windows, known as SAM (Security Accounts Manager), is a popular choice of attackers. However, it is not easy to breach such instances, but you have to make sure it is protected. SQL injection attack is the number one threat to a database. Mainly design flaws cause such vulnerabilities. There are many tools available to scan the databases and web sites to determine if there are vulnerabilities.

Cryptographic System

Cryptography is the study on the techniques used to hide original information by mathematically producing random code. The hiding process is known as encryption, and revealing it is known as decryption. A cryptographic system can be implemented in-house. Or else, there are many external products to implement a system. However, there are vulnerabilities to these techniques and systems.

- Even though cryptographic services are enabled, the applications depending on this may have vulnerabilities.
- The encryption key must remain strong (in length), and it must be kept secret. For symmetric key, it must be at least 256 bits long. However, the recommended length is 2048 bits. The encryption algorithm is also important. Some algorithms may have been expired or exploited.
- Another important fact is the protocol used. For instance, there are security protocols such as SSL, TLS, SSH, IPsec, and so on. Some of these may be deprecated, while others developed stronger.

Industry Control Systems (ICS)

A good example of an Industrial Control System is SCADA. SCADA stands for *Supervisory Control and Data Acquisition*. It can be deployed in an organization within a specific grid. Within this grid, there will be systems, devices, and software. Some of these systems pose a significant risk as the systems are older and use obsolete technologies. Such systems

control national-level systems, and a sophisticated attack can take down the entire operation.

In the history of attacks on ICS systems, Stuxnet is a vital and most successful penetration of all time. This virus targeted the ICS systems in Iran's nuclear power plants. Another famous malware attack is Duqu.

ICS systems often operate along with the powerline communication systems, and in such instances, it becomes another risk. This is why these systems require the highest level of safeguarding.

Cloud-Based Systems

There are several types of cloud-based architectures. Those are,

- Public cloud: Organizations outsource the infrastructure for multiple benefits. The benefits include maintenance cost, ease of integration, high availability, and especially leverage economies of scale.
- Private cloud: This is the on-premise version of the cloud.
- Infrastructure as a Service (IaaS): IaaS service providers provide infrastructure level services and provisioning. They provide networking services, storage, processing, memory, and other features, including computing and elastic services. Amazon AWS is a good example.
- Platform as a Service (PaaS): At this level, support for application development and hosting are provided as a service. The underlying infrastructure is not manageable, unlike in IaaS. It is taken care of by the service provider. An example would be Google App Engine.
- Software as a Service (SaaS): These are cloud-based application services such as Microsoft 365, Google Apps, etc.
- Desktop as a Service (DaaS): DaaS is a new type of service that provides remote VDI capabilities through the cloud (VDI stands for Virtual Desktop Infrastructure).

- Hybrid: Multiple hybrid services emerged on top of these well-known service architectures.

The service providers manage Cloud-based systems except for when you purchase an IaaS solution and manage your boxes. Service providers manage security and privacy while providing methods to maintain availability and load management schemes. If an organization depends on IaaS, they have the responsibility to safeguard the infrastructure by themselves, by adding necessary firewalls, DDoS protection, and other available means.

When it comes to outsourcing the complete infrastructure, you have to face a risk. You cannot entirely depend on remote means. For instance, when an internet backbone is damaged, you will not have a way to survive. Therefore, when selecting the cloud, an organization must consider another backup site. Alternatively, to keep the cloud as a backup. However, for archiving purposes, it is more promising.

In any cloud-based environment, authentication, authorization, and accounting facilities are available. With these facilities, it is possible to layout proper and strong confidentiality, integrity, and non-repudiation features. For instance, Amazon AWS provides Identity and Access Management (IAM) features. In addition, it provides all types of network safeguards.

Whenever you fully manage a cloud component on your own, you are responsible for the security. For instance, if you run a web server, you have to scan it for vulnerabilities, keep a backup, implement load balancing, DDoS protection, malware protection, follow secure coding practices, and safeguard the backend services. There are many industry tools to attempt to exploit your servers, run vulnerability scans, and security baselines.

If you are managing cloud-based database systems, you must establish proper safeguard mechanisms, validation of data, prevent injection attacks, and keep proper backup and recovery systems.

Finally, certain organizations must follow compliance and regulatory requirements (e.g., HIPAA or PCI-DSS). In such cases, they have a responsibility to meet these requirements by working with service providers

and establishing proper security policies. In addition, these organizations can hire consultants and experts to guide them through the process. Another consideration is the service migration. In such cases, there must be trained and technically sustainable professionals within the organization. They can hire consultants to train and assist with their migration process. Nowadays, service providers provide consultancy services with their service offerings.

Databases

You are aware that data and information are the most valuable assets for an organization. Internal databases, as well as databases that accept queries from web servers, are highly vulnerable to attacks. Most of the time, the databases get weakened due to lack of security planning, lack of proper roles and permissions, lack of auditing, lack of data validation, lack of vulnerability scanning and assurance, and lack of reviewing the backups. These areas must be implemented and reviewed periodically.

Backing up a database is a critical step in any operation. The backups must be validated periodically and to keep offsite backups is highly encouraged. An offsite backup can be in a different geographical location or in the cloud.

Distributed Systems

Nowadays, many internet-based systems are distributed across borders. With distributed systems, there are not only risks from environmental facts and the internet but also due to transborder data flow. There are many services, such as cloud-based services, file-sharing services, and web services. We discussed the security considerations and legal issues with these systems in previous sections.

Internet of Things (IoT)

IoT is an emerging and interesting area of applied information technology. However, this is an area that is extremely difficult to layout a unified security approach. There are many devices engineered by different vendors, and even home-made products by enthusiasts available. For instance, there are many products developed with Raspberry Pi. Few examples of IoT devices are wearables, health monitors, home management systems, home

security and industrial surveillance systems, home appliances, powerline communication systems, vehicle control systems, and payment systems.

The problem with many devices is the lack of security considerations from ground up. Some of these devices do not get periodic patches, bug fixes, security awareness, and a lack of authentication and authorization procedures. The main culprit is the incapability of access management and cryptography. This brings a huge risk, and this is why IoT is not for every organization. A critical evaluation is required if an organization is really willing to utilize such systems into the organization. Furthermore, if it is difficult to manage through the existing policies, it must be discouraged.

3.6 Assess and Mitigate Vulnerabilities in Web-Based Systems

Web-Based Systems

A web-based system is simply any application, service, or even a device that depends on web technologies. Some of these systems are browser-based, while some are software applications, including mobile apps. In addition, some systems depend on either a client-server architecture or a multi-tier architecture.

Any of these systems carry risk, including widening the attack surface. Most browser-based systems are validated by the browser vendors, just like the validation of mobile apps by the app store vendor. However, given the number of applications or extensions, it is practically difficult. The best method is to utilize only the required and validate its operating in a sandbox. In addition, the developers must be contacted and queried to understand security architecture and baselines.

Web Servers

Web server is a standard server or a workstation that runs a web server. A server-based architecture may use single or multi-tier architecture. As stated in the previous sections, web servers must be properly evaluated, and safeguards must be in place. Code review is another important thing. In addition, validation of user inputs, cross-site scripting vulnerabilities, and others must be determined.

Web servers must have code and malware scanning mechanisms. It should also be able to handle excessive loads, prevent fake requests, DDoS attacks, and infrastructure failures. We will be looking at the various threats to web servers in the next section. An end-point security system can combat these threats.

If you are familiar with the Open Web Application Security Project (OWASP), you may have a better idea of what web protection means and how critical it is. To understand it, let's have a look at the *top ten* threats they compile each year after a significant amount of study. Full information can be found at <https://owasp.org/www-project-top-ten/>

The top ten vulnerabilities are as follows.

- Injection
- Broken authentication
- Sensitive data exposure
- XML external entities (XXE)
- Broken access control
- Security misconfiguration
- Cross-site scripting (XSS)
- Insecure deserialization
- Using components with known vulnerabilities
- Insufficient logging and monitoring

End-Point Security

Endpoint security is a matter of unified security management approach. An endpoint is a device that is capable of accessing the internal network remotely. Endpoints can be the weakest links of a system as stressed in several sections. Therefore, an organization should carefully consider how their approach protects endpoints. A unified approach of an organization is establishing internal security, remediation (to ensure a system is up to date,

free of infection, and not compromised), encryption, and endpoint protection. There are many single and unified approaches to protect the entire system from risks and vulnerabilities.

3.7 Assess and Mitigate Vulnerabilities in Mobile Systems

Mobile devices are slowly replacing the computer and laptop era at a significant rate. The mobility, ease of operation, long battery life, and new generation mobile network technologies highly facilitate the use of mobile devices, especially when employees are on the move. Many organizations allow the *Bring Your Own Device* (BYOD) concept. The challenge here is the different hardware platforms, different operating systems, different software repositories, versioning, and security flaws. Recently, the atmosphere is changing. The developers are concentrating on one or two main platforms, follow standard procedures when assembling hardware, and even a unified security approach. Now there are capabilities to apply policies regardless of the platform.

Mobile devices may include many vulnerabilities as users tend to install many apps and services knowingly and unknowingly. Furthermore, Google and iTunes stores continuously remove rogue apps from the stores.

On the plus side, there are multiple security capabilities more than a computer, such as biometrics, sensors, multi-factor authentication, remote security, theft protection, remote control, and recovery procedures. With all these features and locked down administration (root) account, if used properly, mobile devices can beat computers in many ways. In reality, there are different use-cases, and users are more prone to entertainment. These issues open space for attackers.

These devices can hold payment information, and it also calls for threats from the internet. Specific compliance requirements have to be met before allowing mobile devices to operate organizational accounts.

3.8 Assess and Mitigate Vulnerabilities in Embedded Devices

Many electronic devices include the capability to use networking and connectivity. Such devices pose a significant threat as these devices hardly focus on security and privacy. There are many electronic devices in the

organization, such as printers, scanners, networking devices, IoT devices, robotic and AI units, and so on. When integrating these into your organization, you have to properly evaluate the design, identify the flaws, set up proper and restrictive access, and limit them to specific roles. Why embedded devices pose a significant threat?

- Embedded devices communicate with developer networks. The intention is to send crash reports, debug logs, and user experience. Such ports welcome attackers and should be filtered or blocked.
- Wi-Fi Protected Setup (WPS) is a connectivity method of many devices. By default, routers also provide these capabilities (factory settings). These services must be disabled as a rogue device can also gain access and sniff the networks through these gateways.
- IoT is the next generation. These devices are incapable of cryptographic operations and access management. Therefore, simply IoT is not for every organization.

3.9 Apply Cryptography

Cryptographic Life Cycle (e.g., key management, algorithm selection)

Cryptography deals with numbers, computational power, and complexity to ensure a piece of data is hidden from unauthorized parties. However, it does not ensure integrity unless you use a unified approach with the digital signature.

The strength of cryptographic functions depends on the secret, key length, and space. No matter how the algorithms evolve, the computational power evolves even more rapidly. This raises mathematicians' eyebrows as there are various methods and computational power as there are multi-core, multi-threading processors and Nvidia CUDA like GPU cores. There are multiple approaches to crack cryptographic keys, at least theoretically. The biggest threat to the cryptographic key is the vulnerabilities in its algorithms.

You have to avoid using weak cryptographic algorithms. There is a standard known as Federal Information Processing Standards or FIPS. It is developed by NIST in accordance with FISMA act. Following the

standards, you have to avoid vulnerable algorithms (legacy or deprecated) and weak keys lengths. Even though this may be true, there are certain restrictions on using certain key lengths depending on the type of the organization.

Cryptographic Methods

Symmetric key cryptography: The main difference between symmetric and asymmetric key encryption is the use of a single key. The same key is used to encrypt and decrypt in the symmetric approach. In this case, you will need to have a longer key to ensure safety. And you must have a secure way to distribute the key with the other party.

Asymmetric key algorithms cryptography: This follows the public key encryption approach. In this method, there are two keys involved. One is the private key or the secret key, just like in the symmetric approach. The other is a public key, and anyone can access it and use it (it is for the public).

Let's look at an example scenario. You will also learn the benefits of the asymmetric approach and how to ensure confidentiality, authenticity, and non-repudiation.

1. When someone wants to send you a secure message (confidential), he can encrypt the message with your public key.
2. You have the private key. You and only you have access to it. This message can be viewed only when you decrypt it using your private key.

This does not, however, ensure authenticity and integrity. To do this, you will use a technique known as Digital Signature.

1. To ensure the person who sends the message is the actual person, he encrypts the previously encrypted message with his private key.
2. This is attached then send to the recipient. In some cases, it will be sent as a separate message along with the original message.

3. You have to use his and only his public key to decrypt this.
Since it is his public key, you know that the person is authentic.

In symmetric-key approach, this code is known as *Message Authentication Code (MAC)* . Then again, the key sharing can be difficult, and it must not have been leaked. Therefore, MAC does not assure non-repudiation while the digital signature does.

As you must have understood, digital signature assures integrity, authentication, and non-repudiation while encryption assures confidentiality.

In this section, we will also be looking at Public Key Infrastructure (PKI) in brief. It has the following components.

- A root certificate authority (RCA) server with a possible backup (both will be offline in most cases)
- A set of subordinate servers with backups
- A set of issuing CA servers including backups
- A set of policy CA servers
- Revocation list facilitation

There is a chain of trust, starting from the root server. A root level certificate ensures the chain of trust, and it is visible in the issued certificates. For a computer or a digital device to trust the root CA, the certificate authority must be trusted by the vendor and multiple parties. This is critical if the CA is a public one (internet-based).

If you have analyzed your computer's certificate store, you will find a default list of trusted root certification authorities and intermediate certification authorities. You will see the names of popular and leading certificate service providers such as VeriSign, DigiCert, etc. You may see the Microsoft Tamper Protection Root certificate as well if you are using Windows.

A PKI must have certificate policies. In addition, it must have a *Certificate Policy Statement (CPS)* . CPS statement announces how the PKI will use

identities, how it stores the keys, and how certificates are used.

Certificates expire and must be renewed periodically. A PKI should facilitate the requirements. Above all, it must revoke such certificates, and a revocation list must be publicly available.

Key Management Practices

- Creation and distribution: As this process is secret, the information exchanged must be secure, and it must be kept between the two systems. The key can be exported with or without a private key. But if you export it with the private key, you must at least password-protect the file.
- Protection and custody: The keys must be safeguard by using a password or any other method. If it is a high priority/top-secret requirement, split custody can be used. You only own one part of the access key, and you need to aggregate the other part of the key owned by another to unlock it.
- Key rotation: It is important to rotate their keys in specific time intervals.
- Destruction of keys: Key expiration and revocation must be handled specifically to avoid security issues and possible fraudulent activities. The revocation list must be publicly accessible.
- Escrow: This method is used when a third-party should be able to access the key. In this approach, the keys required to encrypt/decrypt are held in escrow.
- Backup and recovery: This is the most important part of the encryption process. You must keep the private key or symmetric key safe. In certain cases, legislation may also require access to the private key. Nowadays, many PKI service providers offer backup methodologies.

Digital Signature

This is already introduced to you in a previous section.

Non-Repudiation

Non-repudiation is the assurance of non-deniability. For instance, a person who sends a message cannot later state that he or she did not send it. The challenge here is that it is not possible to assure whether the private key is stolen or not.

Integrity

This is already discussed in the previous section. Integrity can be assured by hashing, message authentication code in symmetric cryptography, and digital signature in asymmetric cryptography.

Understand Methods of Cryptanalytic Attacks

There are techniques and mathematical approaches or scenarios to crack cryptographic algorithms and encryption.

1. Cipher-only text: In this scenario, the attackers are aware of the algorithm and ciphertext to be decode.
2. Known plaintext: An attacker is aware of the first, and he possesses one or more plaintext-ciphertext pairs generated with the secret key.
3. Chosen plaintext: An attacker knows the encryption algorithm used, ciphertext, and a selected plaintext together with the ciphertext generated using the secret key.
4. Chosen ciphertext: This is similar to the 3rd except for ciphertext being selected by the attacker together with the decrypted plaintext generated using the key.
5. Chosen text: Selected plaintext and ciphertext combination.

Digital Rights Management

A right can be, though, as an allowed stated and also a privilege. In the human world, favor is human rights. A digital environment it becomes digital rights. Rights, in this case, can be applied to objects. It requires classification. The object access must require authorization, clearance, and permissions to execute certain actions on it. In addition, it should provide

methods to share or distribute rights. Finally, a right can be granted as well as revoked. If an object is shared externally, there must be two versions of rights and must be managed separately.

There are many digital rights management tools and techniques in the enterprise. These suites allow you to perform the aforementioned actions. The rights will be protected by using certificates, encryption, and other possible methods.

3.10 Apply Security Principles to Site and Facility Design

In this section, we will be looking into facility design. The design of facilities, buildings, server rooms, data centers, network operation centers, cabling closets, HVAC, and so on.

If you have followed so far, the design of these facilities requires engineering techniques and careful architectural development to safeguard the entities. From land selection, there must be a plan for risk management. Land location and position are important to avoid any environmental risks. For security purposes, taking advantage of natural properties is essential. For instance, for a secret facility, it is important to consider urban camouflage. This will stop making unnecessary attraction. If the land provides natural surveillance, it is another advantage. If you have ever been to an ancient castle, you must have seen how the construction is protected by surveillance and natural surroundings.

It is also important to consider territorial control when you secure already constructed areas and partitions. In most cases, there will be restricted areas in facilities, data centers, server rooms, etc. To access these facilities, one must have proper clearance and a pass. It is possible to use signs, cameras, and others to keep the people who do not have clearance away.

One of the most important considerations is access control. In fact, it is above all the other considerations. Facility entrance can be guarded with fences, walls, security guards, dogs, CCTV, and whatever is necessary. When designing access zones, parking spaces, standoff distance, lighting, warehouse access safeguards, and controls have to be selected carefully, implemented, tested, and documented.

If you are looking into the reasons why, it has to become clear that the overall goal is deterrence and mitigate disasters (e.g., environmental impacts).

When considering natural disasters, you should have a specific plan to keep the operations running. To meet these requirements, you have to keep backup sites at a safe distance. A previous chapter introduced hot, warm, and cold sites. These continuity options assist greatly in light of a catastrophic event.

There are approaches, guidelines, and mandates to follow when constructing specific facilities such as healthcare facilities, hospitals, laboratories, nuclear, and other research facilities.

Crime Prevention through Environmental Design (CPTED) provides a multi-disciplinary approach to reduce crime through urban environmental design and management. The main goal is to deter offenders, reduce chances of criminal acts, and to reduce the fear of crime. For more, visit <http://www.cpted.net/>

3.11 Implement Site and Facility Security Controls

In this section, we are looking at the internal facility operations, security, and risk mitigation.

Wiring Closets/Intermediate Distribution Facilities

Information technology infrastructure is laid out when constructing a facility (in the internal construction stages). There will be multiple cables, wires, and enclosures coming from everywhere. All the wires or the endpoints will be placed in a casing or a room. There are several threats to these wires. If they are visible on the floor, employees can damage them. If there is a risk of fire due to heat sources, it can damage the wires. If the network cables are near powerlines, there can be interference. Above all, if the cables are insecure and visible to the people, anyone can launch a Man in the Middle (MitM) attack. Therefore, the closets must be restricted to a specific team of technicians. To safeguard access, they can be issued a pass with fingerprint or other biometric control.

Server Rooms/Data Centers

An in-house server room and a data center which houses multiple hardware equipment, including server racks, require highly specific and secure design principles. You have to follow specific environmental requirements, internal design considerations, multiple compliance requirements, and sometimes obtain legal clearance.

It must be designed in a place where natural disasters (potentials) are minimal. The external safeguards must be in place. To access it, there must be a specific, documented protocol. The clearance levels must be defined along with the design. Biometric access controls are a must in this scenario.

The internal rooms must be designed to control moisture, heat, air, and dust. It must employ sensors to prevent electrical surges, overheating and fire, wetness, and static electricity. There are sophisticated and state-of-the-art controls to use with the design, including intelligent HVAC controls.

A thorough monitoring scheme is required within and outside of the facility entrance. Even when the technicians get clearance, the activities must be audited accordingly.

In addition to these requirements, continuous power supply and generators for backup power are required. The circuitry should filter surges and lightning attacks.

Media Storage Facilities/Evidence Storage

The media storage facility is a sophisticated area in a server room. It may include additional monitoring systems. However, it may be accessed more frequently. Therefore, the same considerations for controls exist.

Restricted Work Area

A restricted work area is an area reserved for mission-critical operations. In some cases, people may or may not work there. Some examples would be a server room, network operations control area (NoC), a vault, or a laboratory. More monitoring and access control are required in this case. Also, auditing is required to safeguard assets from internal attacks.

Utilities and HVAC

As stated in the previous section, heat, ventilation, air-conditioning are important environmental controls. It creates a precise atmosphere for critical hardware to operate, people to work, and facilities to meet its required conditions (e.g., laboratories).

These systems are critical when it comes to dangerous operations such as nuclear power plants. In such cases, state of the art technologies and clinical precision is required to keep the temperature, ventilation (heat control) and coolants under controls.

In a server room, you must have humidity control to avoid corrosion, ventilation, and air-conditioning to keep the air, dust, and temperature controlled.

In any of these cases, you must also consider backup power to power the operation or shut it down in time if HVAC loses electricity. In all the cases, these devices and controls must be monitored and reacted within a given time frame.

Environmental Issues

As stressed in multiple chapters, the environment, and natural disasters are part of human life. It is out of our control, and we must have plans to recover from such an incident. This is why the selection of land and surroundings is important. Appropriate considerations must be taken on the following.

- Natural disasters like floods, forest fires, volcanic eruptions, and other similar issues.
- Fire can cause damages to entire sites. Depending on the type of fire, or the source of fire, appropriate controls such as fire extinguishers and appropriate water supplies must be in place. Depending on the risk, there can be more than one type of fire extinguishers in place.
- There can be extreme weather conditions such as heavy rains, floods, hurricanes, tornados, and lightning.

- Special consideration must be taken from the design and construction of the facilities to bear the impact of events such as earthquakes. It is possible to combat physical damages by proper architectural designs and construction strategies.

Fire Prevention, Detection, and Suppression

In this section, we will look at some fire prevention, detection, and suppression controls and methods that have to be placed in facilities.

To prevent a fire, the first step is design considerations. When designing the facilities, proper analysis and documentation are required on used materials, power lines, power outlets, air conditioning, and ventilation areas, fire-sensitive entities, exit points, and critical points where fire suppression might be difficult.

In the next stage, during the design, fireproof material, techniques, and possible prevention controls must be applied. For instance, certain materials can be used for walls to resist fire during an incident.

In the next stage, it is possible to set up technologies to detect and report a fire and related incidents. This assists both in preventing as well as detecting fire. There are fire sensors, temperature/heat monitors and sensors, alarms, and cameras that can be used holistically to prevent and detect fire. These units work together in preventing, quickly detecting, and reporting incidents. The main goal here in an incident is to contain the fire and limit it to a specific, small, yet manageable area and to prevent affecting the sensitive areas.

There are many fire suppression technologies. An organization must utilize more than one method if the facility and assets have different reactions to fire. For instance, you can suppress a general fire with water, but if it is oil, then you have to select a different suppressor. The following types can be placed in areas where there is quick access.

- Water
- Gas suppressors such as FM200 is ideal for datacenters
- Foam-based suppressors

- Halon-based suppressors
- Water-mist
- Sand

Chapter 4

Domain 4 - Communication and Network Security

Everything is interconnected, and this is why you have to have a complete section to address this in the CISSP studies as the biggest threats arrive through the networks. For the students who are familiar with or have a network or system administration background, this chapter will be a quick study. However, if you are not familiar with certain technologies, it is time to follow a quick course. In this chapter, the concepts are made simpler so that you can grasp even if you possess a little knowledge.

4.1 Implement Secure Design Principles in Network Architecture

Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models

The networking architecture was built upon two major models. These are the building blocks of the communication networks that exist at present. The models are,

- OSI model
- TCP/IP model

The ISO/IEC 7498 is the conceptual model. It is, in fact, the standard model. It provides a seven-layer architecture to establish communication between two computers or devices in a networking environment. This model intended to simplify and ease understanding.

Later, a simpler version of the ISO layer was introduced and is known as the TCP/IP model. This model paved the interconnectedness through the internet. This is used with almost every internetworking as well as external networking designs.

Let's look at a comparison to understand each model. Next to the layers of these models, the relevant protocols are listed.

TCP/IP	OSI Model	Protocols
Application Layer	Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP, POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
	Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
	Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP, UDP
Internet Layer	Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Link Layer	Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
	Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi

IP – Internet Protocol Networking

Internet protocol is, in fact, the foundation of interconnected network communication and addressing. The protocol facilitates the communication of other protocols.

Let's look at the characteristics of IP. It is a *connectionless protocol*. This means it does not require prior arrangements. It is also called a *stateless protocol* as there is no way of telling when a conversation started. To achieve reliable communication, it works with the transport layer protocol TCP. TCP, in fact, a connection-oriented, reliable protocol. The reliability is achieved by using sequence numbering of packets, and error correction, and buffering.

The other transport layer protocol is the Universal Datagram Protocol. It is also a connectionless protocol. The IP protocol can work together with this as well. Since it does not require specific actions and connection orientation, it is fast.

At the moment, the 32-bit IP address scheme is consumed. It was known as TCP/IP version 4. The newer version is version 6, and it has an address space of 128-bits.

Another important concept you need to be aware of is the socket. When two devices communicate, for instance, they form two sockets. A protocol has a designated port number. There are several port identifications. Those are,

- Well-known ports/system ports: 0 – 1023 ports are reserved for well-known system services
- Registered Ports: IANA reserves 1024 to 49151, and upon request, it can be reserved.
- Private and uncommon ports: Ports from 49152–65535 can be used to connect to well-known ports and to do any development work.

Implications of Multilayer Protocols

There are different types of protocols. Some of these are single layer protocols, while others being multiplayer protocols. A multilayer protocol uses more than one TCP/IP or OSI layer. For instance, Asynchronous Transport Mode or ATM switching technique used by telecommunication service providers utilizes this approach. In fact, ATM uses three layers to operate. It utilizes these layers simultaneously. To use three layers together, it uses *encapsulation*. The data from the upper layer is encapsulated when the lower layers handle it. It also appends a header to the encapsulated data, or a header and a trailer. ATM is used in Synchronous Optical Networking (SONET). SONET is used to transfer extensive amounts of high priority data such as voice and videos over long-distance networks.

Converged Protocols

In this concept, there is a merging of two protocols. In most cases, it is a proprietary protocol and a standard protocol. This is a huge advantage as it removes the requirement for infrastructure changes and upgrades. Especially when catering multimedia needs, this is highly cost-effective. In reality, securing, scaling, and managing such is easier than implementing a proprietary network. However, combining multiple technologies and protocols bring security concerns. Then again, utilizing the existing security features in protocols, it is not impossible to derive a unified approach.

Some examples of converged protocols are,

- Fiber Channel over Ethernet (FCoE)
- iSCSI
- MPLS
- SIP (used in VoIP operations)

Software-Defined Networks

Software-defined networks emerged with the arrival of virtualization and cloud networking services. It replicates the physical networks and works with more precision in some cases. SDNs are designed to tackle issues such as budgetary concerns, adaptability issues, flexibility, scalability by adding more dynamic nature and ease. Let's look at some features of an SDN.

- Agility: It provides abstract control from forwarding. This gives administrators a huge benefit by allowing them to adjust the traffic flow to meet the dynamic requirements dynamically.
- Centralized Management: In SDN controls, centralized network intelligence that maintains a global view of networks. In other words, it appears as a network switch to application and policy engineers.
- Programmability: SDNs are directly programmable. The reason is the decoupling from the forwarding functions.
- Openness and Vendor Neutrality
- Programmatic Configuration: This is the very nature of the SDNs and is why it became this popular. It allows network professionals to configure, manage, optimize, and secure resources dynamically or via automation.

Wireless Networks

Wired networks were once the primary networking medium, but nowadays, wireless networks evolved into challenging and, in some cases, more promising in contrast to wired networks. In this mobile device era, wireless networking and wireless broadband networks are the available options for handheld devices. In parallel to broadband services, wireless services move

rapidly forward by expanding its capabilities. A wireless network follows the IEEE 802.11 standard. For more information, visit http://www.ieee802.org/11/Reports/802.11_Timelines.htm

Wireless Security Protocols

There are multiple wireless security protocols, and a CISSP student should have field knowledge of these so that the best out of the lot can be integrated into the security strategy.

- **Wired Equivalent Privacy:** WEP is a legacy and deprecated security protocol and was the standard protocol used in the past. It was forced to eliminate due to the security weaknesses in it. The WPA family of standards replaced it. WEP utilized RC4 for confidentiality and CRC-32 checksum to assure integrity. There were other versions such as 64, 128, and 256 but WEP keys. Eventually, a method was developed to find WEP keys through cryptanalysis.
- **Wi-Fi Protected Access (WPA):** This standard utilizes the Temporal Key Integrity Protocol (TKIP). It generates a 128-bit key per packet. It also offers packet integrity checks. Regrettably, WPA inherited a weakness found in WEP, allowing it to be spoofed and reinjection attacks.
- **WPA version 2:** Unlike WEP or WPA, WPA2 provides strong security and encryption support to ensure confidentiality. It supports Advanced Encryption Standard (AES), and if the client is unsupported, it provides TKIP support. For general use, you can specify a pre-shared key, but it is not recommended in an enterprise setup. In such scenarios, it supports certificate-based authentication mechanisms.
- **WPA version 3:** This is the future of the WPA2 standard and the successor to it. WPA 3 uses the latest security methods, removes the obsolete, and requires the use of *Protected Management Frames (PMF)*. It also offers natural password selection, ease of use, and forwards secrecy even after a password compromise. The enterprise features include authenticated encryption (256-bit), key derivation

and confirmation (HMAC-SHA384), Key establishment, and authentication (ECHD, ECDSA with the 384-bit elliptic curve) and Robust management frame protection (BIP-GMAC-256).

For more information, visit <https://www.wi-fi.org/discover-wi-fi/security>.

In addition to these protocols, wireless security mechanisms integrate certificate infrastructures and certificates and other protocols such as TLS and IPSec. In some organizations, Wi-Fi Protected Setup or WPS is used. Due to the vulnerabilities and risks associated with it, it must be discouraged.

4.2 Secure Network Components

A computer network is the building block of communication in any organization. Network components are part of the networking backbone, and to build the security from the ground up, those components must be secure.

Operation of Hardware

To build a network, a set of components is integrated. We will look at these devices and peripherals, including detectors, monitors, and load-balancers.

- Concentrators and Multiplexors: These devices are used to aggregate or multiplex different digital signals. FDDI is an example
- Modems and Hubs: Modems were used in the past to convert between analog to digital and vis versa. A hub is used to construct certain networks or to implement certain topologies. For instance, a ring or star topology. These are mechanical devices with no decision-making abilities or intelligence. In addition, a hub is a single collision domain, and it is neither reliable nor secure.
- Layer-two Devices: These devices operate in the OSI layer two. As you already know, this is the data link layer. Both switches and bridges operate in this layer. For bridge networking, the architectural similarity is required between two devices, for instance. It is also unable to prevent attacks that may occur in the local segment. In contrast, the switch is more efficient, and above

all, it divides the collision domain and assigns it to ports. In addition, a switch features a port- security mechanism, authentication, VLANs, and more.

- Layer-three devices: These layers operate above the data link layer. Therefore, you can expect more intelligent and decision-making devices. Layer 3 units offer a collaboration of different devices. It allows these devices to interconnect as well as to collaborate. A router and a layer three switch are the best examples. Layer 3 devices provide excellent security features, configuration, and control. For instance, you can get devices that provide advanced authentication technologies, firewall features, support for certificate services, and so on.
- Firewalls: A firewall is the main player when it comes to network security. In an enterprise environment, firewalls operate in a tiered architecture. It acts mainly as a packet filter while it can make intelligent decisions about packet forwarding. A firewall utilizes two methods. One is static filtering, and the other is stateful inspection. The second is advantageous as it makes the decisions based on the context.

Transmission Media

There are many transmission media utilized to fulfill different scenarios. The following lists the available transmission media.

- Twister pair
- Shielded twisted pair (STP)
- Unshielded twisted pair (UTP)
- Coaxial cables
- Fiber optics
- Microwave
- Powerline communication

Twisted cables are laid out through different areas in a building. In such cases, the cables may end up or go through unexpected areas. If this is the case, a Man-in-the-Middle attack (tapping) is most likely to occur. Without proper shielding, copper cables are prone to interference and radiation. Therefore, the cables must be laid out carefully.

Copper cables are prone to similar issues. For instance, Coaxial cables are bulky, not easy to operate. Just like the twisted cables, these are susceptible to tapping yet fewer interferences. Due to the shielding, it may protect against fire but not in certain cases.

Fiber connection is the most secure and untappable media. It also offers an extensive bandwidth no matter if the cable is single or multi-mode. Multi-mode has a lack of bandwidth, but both single and multiple models are managed properly.

Network Access Control (NAC) Devices

As the name implies, network access control is similar to a watchdog guarding the perimeters, and these devices may provide physical and logical controls.

- Firewalls: This is already discussed in a different section.
- Intrusion Prevention Systems/Intrusion Detection Systems/Honeypots: An IDS system is a control that can detect live threats or threats that exploited the assets. IPS, on the other hand, attempts to prevent attacks before they occur. However, IPS devices or controls provide real-time updates and alerts. A honeypot is a virtualized network, and it exists in a simulator. The simulator can be configured to open ports and express weaknesses so that the attackers can be misled. It serves the purpose of prevention as well as to collect attack vectors.
- Proxy/Reverse proxy: A forward proxy intercepts traffic from the internal network and screen certain information to the outside parties. For instance, PII information. It is also able to filter traffic. In contrast, a reverse proxy intercepts incoming traffic. At this point, it can provide load-balancing, caching, and attack mitigation.

End-Point Security

We have discussed more on end-point security in previous chapters. To protect end-point devices. Among the technical safeguards, applying security policies with auditing, rights management, mitigation and remediation networks, remote access protection, secure VPN or RDS services, unified internet security suites, host-based firewalls are the top considerations.

The next is best practices. Employees may not have enough technical awareness about an organization's security strategy and technical areas. They must be educated through training and exercises. Building a robust knowledge base for them is another success factor. In addition to these, there are corporate-managed activities and restrictions such as,

- Automated updates and patch management
- Devices restrictions such as prevention of bringing removable devices in/out and applying media policies
- Restricting applications and administration capabilities

Content Distribution Networks

A content distribution network or a CDN, in short, is placed to distribute bandwidth-consuming content without delays to end users in different geographical locations. In other words, it greatly enhances user experience. It saves the download/upload delays and saves time. Good examples would be Cloudflare CDN and Amazon CloudFront.

There are ways to pollute the caches, and there must be appropriate restrictions set. For instance, it provides data protection through Identity and Access Management, restricting access to the original content by other means, compliance and monitoring, DDoS mitigation field-level encryption, and many more features to protect the users.

Physical Devices

If logical security is the top concern, what about physical security? Just like the network security practices, physical security is also a top concern. In fact, it is, above all, in most cases. To protect physical devices within the

organization, appropriate measures such as logical and physical monitoring, sensors, and cameras can be placed. Strict access control mechanisms (keycards, codes, biometrics) and scanning are useful methods in high-security areas to avoid physical damages, theft, and unauthorized access.

Many devices include physical locks nowadays to prevent stealing devices, and upon such instance, the device will be locked. Apart from devices such as computers, mobile devices such as laptops, smartphones, and others are highly vulnerable to theft. These devices must be protected with all the available features such as encryption, password protection, screen locks, hard drive locks, remote access, and management, including remote wipe and policies that can be used to limit unauthorized access.

4.3 Implement Secure Communication Channels According to Design

In this section, we will look into secure communication methods to be used in an organization to protect the data in motion.

- Data communication: A secure communication channel is either an internal channel or an external tunnel with which secure communication can occur. If this communication occurs internally, there must be separate channels to keep communication channels secure. The best example is a Virtual LAN or a VLAN in short. VLANs offer excellent protection and security while securing the communication between the intended parties. Apart from internal communication, external communication can be protected by using protocols such as IPSec and TLS.
- Multimedia collaboration: The workplace isn't limited to text and voice activities any longer. Instead, there are hundreds of collaboration tools that can be utilized during daily operations. In fact, many activities use text, voice, video, and shared resources to perform work, contact stakeholders, for training and public events. Web conferencing and webinars are powerful ways to learn and communicate. Many collaboratives tools are providing such capabilities to organizations, schools, campuses, and other institutions. Among these tools, Microsoft 365, ERP tools such as SAP, Adobe Connect, Google Apps, Cisco WebEx, Freshworks

(helpdesk), Slack, Skype, virtual meetings, virtual classroom solutions, and other web conferencing tools are available. When using these applications, you must ensure that these provide secure communication, infrastructure security, and compliance. For instance, a conferencing tool, “Zoom,” is criticized for not being secure in the early 2020s. The WebRTC and other tools may still require developments in security areas. Protocols such as RTMP can be made secure through custom implementations.

- Remote Access: There are many protocols to facilitate secure access to your organization remotely. These are SSH, VPN technologies, Remote Desktop Services (RDS), Remote Desktop Protocol, VNC, and others. The selection must focus on end to end encryption, infrastructure safeguards, and compliance requirements. In addition, transborder restrictions must be considered. Many of these tools support certificate services and can be utilized to protect communication through TSL and other means. RADIUS and other services can be used to authenticate users through certificates and other mechanisms.
- In addition, each authenticated computer or a device must go through a remediation network to assure the compatibility and security.
When it comes to virtual infrastructures such as Virtual Desktop Infrastructures, Hypervisors, and other products offered by vendors such as VMWare and Microsoft, there are specific considerations to security. These infrastructures and VDIs must have appropriate security services running to protect the sessions. In addition, these services require failover setups to ensure accessibility.
- Voice and Video: Voice and videos make engagement and bring success to businesses. Nowadays, technical and non-technical organizations heavily utilized collaboration tools and third-party tools to connect to customers, stakeholders as well as to handle internal communication, meetings, and training. As stated previously, these are priority services (QoS or quality of service) and require extensive bandwidths. In most cases, these are delivered through special tunnels and special infrastructure (on the internet).

Among the tools, Instant Messengers are at the top. Some examples are Skype, WhatsApp, IMO, Viber, and there are other enterprise tools like Microsoft Teams, Skype for enterprise, Adobe Connect, Cisco WebEx, and many other collaborative, virtual conferencing/webinars/classrooms. These services provide end to end encryption in most cases and privacy services. But when integrating, the engineering of end to end encryption, privacy and regulations must be met. Some countries do not allow these tools, and as a security practitioner, you must be aware of these issues.

Chapter 5

Domain 5 - Identity and Access Management (IAM)

I AM, or Identity and Access Management, is one giant pillar of information security apart from the CIA triad. In this chapter, we will be looking into the areas of authentication, authorization, and accounting. It is actually the essence of user management and controls.

You already have a good understanding of the CIA triad at this point. The other important pillar is Identity, Authentication, Authorization, and Accounting. In short, it is “IAAA.” You can also call this “I triple-A.” AAA triad or triple-A is the predecessor of IAAA.

What is Authentication?

Authentication is the first line of defense in access control. Most IT and Non-IT people are familiar with some sort of an authentication mechanism. For instance, everyone uses smartphones. When someone sets up the smartphone for first use, he/she have to create an account and sign in. For instance, an Apple or a Google account. Then when the operating system requires you to prove this is you or in technical terms *to prove your identity* and allows you to change something, the first step is the challenge for a password. This is the basic requirement of authentication. It is a way of knowing that this is the authentic/original user. And it prevents others from accessing it. This is also true when you log into your personal computer or a laptop (unless, of course, you have not configured a password, which isn't the best practice). When you are at work, or when you sign in to Facebook or LinkedIn, you have to go through the authentication process. Therefore, it is simply the identity verification process.

Using a password for authentication is the traditional method. Unfortunately, using something you know is dangerous because people are neither good at remembering things like passwords, nor do they avoid sharing passwords. Therefore, moving forward, the traditional

authentication mechanisms were replaced with two or multi-factor authentication. However, the developers are aware of the inability to keep hundreds of passwords in a person's mind. This is why they have introduced mechanisms such as *Single Sign-On (SSO)*. This method is used when a user is required to sign into different parts of the software or applications hosted by the same application.

A simple example would be attending a webinar through your training partner. In every case, you log into your training partner's member areas. Then you click a link to access a webinar or training via live stream. In this case, the webinar is hosted by a third-party. You are not challenged to provide a password here and taken into the virtual room because you have already authenticated once.

There are three authentication mechanisms used either singly or in combination to provide stronger authentication. Those are,

- Something you know: A password, a pin code
- Something you have: A smartcard, a token. You withdraw money from the ATMs in this manner
- Something you are: This is something you are born with, for instance, your fingerprints, retina, or face.

What is Authorization?

Once you get approval to access an asset through the authentication procedure, your rights, and permissions to perform actions on this object must be determined. This is where authorization comes into play. In simple terms, this is the *process of verifying what you have access to*. In the early days, protocols such as *Lightweight Directory Access Protocol (LDAP)* were used to provide authorization in the enterprise, but there are many new protocols and versatile methods. In addition, it is now possible to authorize users based on location and other dynamic properties.

What is Accounting?

Accounting or accountability will be revisited later in this chapter.

5.1 Control Physical and Logical Access to Assets

Information

Information derived from user data is the most valuable asset for a business. In previous chapters, the requirement for safeguarding information is stressed. To protect the information an organization owns, the IAAA principle is the best approach as it verifies identity, let's one prove it in different means, verifies what you have access to, and your action is accounted for.

The challenge here is implementing the appropriate strategy, policies, procedures, and guidelines to authenticate and authorize users or customers properly. Although authentication is more of a straightforward method, authorization is much more complex as it requires calculations. In both cases, databases will be utilized to keep the information stored.

Systems

A system can be either a hardware device, interfaces like an operating system, or a service. Another difference between a system is being virtual or non-virtual. There are many scenarios and use cases with system access. For instance, there must be a separation of customers and internal users if they access the same database. However, the management in the internal environment is not a difficult task as services are fitting local, intranet, extranet, and internet scenarios. For instance, federation services are used to manage external access using an SSO approach. In most cases, these services are centrally managed and monitored.

As access mechanisms, an organization can use system-level username/password and multifactor authentication techniques, or biometrics integrated. Modern systems provide these features, so it is just a matter of integration. When advanced methods are required, user and system level certificates can be utilized as smartcards or with access tokens. For remote access, RADIUS technologies can be used. To separate logical boundaries, in the enterprise mechanisms like VLANs and *Organizational Units (OUs)* will be utilized. This makes the implementation of authorization easier.

Devices

A device is a physical system. In previous chapters, we have discussed how to protect physical assets. In this section, we will be looking at how the IAAA principle can protect the devices. Mainly any operating system provides single or multi-factor authentication such as a one-time password (OTP) or biometrics such as fingerprints or facial recognition. With mobile devices, there are many other options, including screen lock patterns, and so on.

In an organization, access must be restricted to authorized personal and restrict them only to the devices they need to do their job (minimal requirements). Devices have built-in mechanisms to authenticate and authorize users. Also, many devices support tamper protection, encryption, and locking mechanisms to protect authorized users and to prevent unauthorized access.

Facilities

A facility can be protected from unauthorized access at the entrance points and closing alternative entrances such as unprotected ventilators. At the main desk, they can verify their identities (swipe cards and or fingerprint readers). After this step, when they require more clearance to different areas, they can use another biometric device or the same (e.g., biometrics) to authenticate when required.

5.2 Manage Identification and Authentication of People, Devices, and Services

In this section, we will be looking at the protocols and implementation of authentication practically.

Identity Management Implementation

Lightweight Directory Access Protocol (LDAP)

LDAP is an ancient service that operates in an enterprise network. It allows services to authorize and share information in a standard form. LDAP can store information about computers, users, and groups. For instance, LDAP is used in Linux and Windows environments, and Microsoft Active Directory service uses LDAP and Kerberos for authentication. In this method, Kerberos handles the authentication, and LDAP manages the

authorization. In addition, LDAP supports encryption and is a strong feature. Currently, LDAP is used in Microsoft, Unix, and Linux environments.

Kerberos

The name Kerberos comes from a Greek myth. In this myth, Kerberos is a three-headed dog, and it guards the gates to hell. Sounds scary? It is used as a safeguard, and there is nothing to worry about. And, who developed the protocol, Hades? Actually, it is a team of researchers at the Massachusetts Institute of Technology (MIT).

Kerberos is extensively used in the Windows environment by the operating system. It is also utilized with the network file stream (NFS), for instance, in Sun operating system environments. Kerberos is a ticket-based, symmetric authentication protocol. The Kerberos process is somewhat difficult to understand as it is complex. If we breakdown the process,

1. John is log in to a Windows client, and he is requested to input the username and password. When Kohn enters the details, Kerberos uses a one-way hash function to generate a secret key. John's ID is sent to the Authentication Server (AS) at the Kerberos Key Distribution Center (KDC) to obtain an authentication ticket (Ticket Granting Ticket).
2. Then, KDC compares the details and confirms the existence of the user in the database. Then it sends back an encrypted *Ticket Granting Ticket (TGT)* .
3. The TGT is encrypted using the secret key of the *Ticket Granting Service (TGS)* .
4. The client stores the TGT. When it expires, the client's session manager will request another.
5. Now, John is requesting access to a principle such as a server. When this occurs, the client sends the TGT (active, nonexpired) to the TGS with the Service Principle Name (SPN).
6. Then the KDC verifies the authorization information.

7. If John has clearance, TGS sends a valid session key for the specific service object.
8. Finally, the client sends this key to the required service. The service confirms the authorization and grants the access (server, in this case).

RAS

RAS stands for Remote Access Service, and it is the legacy ISDN and serial option for remote access and telephony services. It used Point to Point tunneling protocol (PPP) to encapsulate IP packets. RAS can utilize protocols such as PAP/CHAP and EAP.

RADIUS

Remote Authentication Dial-in User Service or, in short, RADIUS is an opensource client-server protocol that operates in the application layer. It facilitates a unified solution to perform the triple-A functions. Protocol-wise, it utilizes UDP for communication, but UDP, as you know, is a connectionless protocol.

RADIUS is utilized to fulfill remote access authentication requirements such as VPNs and Remote Access Services (RAS). As the initial step, the client sends authentication information to the computer, and it sends the details to the remote server after encrypting it. Then the RADIUS server does the rest.

The most important thing when it comes to such authentication strategies, there must be a network access controller servers (NAC) and appropriate policies set through them to prevent any unauthorized attempts. Furthermore, it supports multiple security protocols from the lowest to the highest enterprise-grade security protocols (i.e., EAP and certificate-based authentication). In addition, it can authenticate devices as well.

TACACS

TACACS stands for Terminal Access Controller Access Control System. United States Military services develop it. It is, in fact, a stronger service when it comes to remote authentication. It is used by military services as well. TACACS+ is an enhanced version of it.

It provides triple-A services just like RADIUS, but it has its strengths. Among the strengths, the support for almost every authentication protocol is outstanding.

TACACS is a highly flexible and widely used remote authentication service, and TACACS+ supports dynamic passwords. This is the strongest feature of it, and this facilitates it to be used as a central authentication management center. Therefore, it is also used with other device authentication services such as firewalls and routers.

DIAMETER

This is the next generation RADIUS protocol. If you find a relationship with diameter and radius, you guessed correct. In mathematics, a diameter = $2 \times \text{radius}$. Unlike RADIUS, diameter depends on TCP to provide reliable communication. It also uses the Stream Control Transmission Protocol (SCTP). In addition, it utilizes TLS or IPsec to provide encrypted communication with transport layer security.

SESAME

SESAME stands for *Secure European System and Applications in a Multi-vendor Environment*. This is similar to Kerberos as it also uses a ticketing system, but advanced in many ways. As a matter of fact, it provides support for both symmetric and asymmetric encryption standards for ticket and key distribution. Since it uses public-key encryption, it is used to secure communication between domains. To achieve this, it utilizes a Privilege Attribute Server (PAS) on both sides and installs two Privilege Attribute Certificates (PAC) to provide authentication. Regrettably, due to security weaknesses, it had not gained popularity.

Single/Multi-Factor Authentication

Single-factor authentication is the traditional method that depended on a single password. Moving forward, the single mechanism evolved into many flavors and stronger versions, from passphrases to biometrics and smart cards.

In a previous section, you were introduced to multiple factors used to authenticate users. Those are, what you know, what you have, and what you are. If you are familiar with online transactions, you know how your bank

sends you a *one-time password (OTP)* after you enter the credit card and PIN. This is a combination of multiple factors. There are two types of OTPs, and those are,

- HTOP: HMAC-based one-time password uses a shared secret and a counter that increments. There is a display in the device to show you the counter.
- TTOP: Time-based one-time password uses a shared secret with the time of the day. Time synchronization must occur.

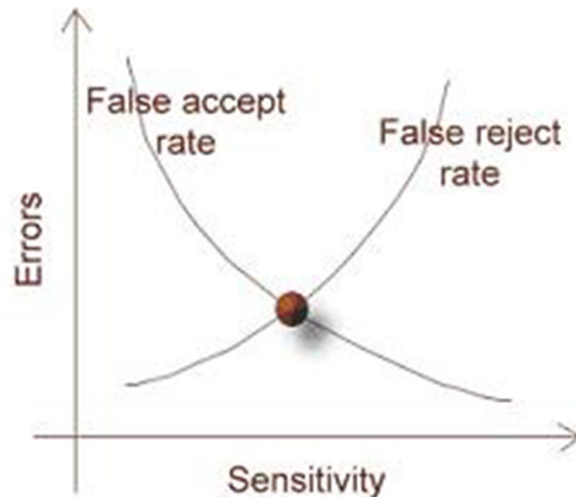
There are newer methods to generate these codes. For instance, Google Authenticator generates code, and those are one-time passwords.

In an enterprise network, there will be more sophisticated methods. Let's look at the details.

- Facial scans
- Fingerprint scans
- Iris scans
- Hand-geometry
- Keyboard dynamics
- Signature dynamics
- Retina scans

With biometrics, there is, however, a catch. The following factor may affect the certainty of the results.

- False Acceptance Rate (FAR): The possibility of a successful authentication attempt while it must be rejected
- False Rejection Rate (FRR): The possibility of rejection when it is a legitimate request
- Crossover Error Rate (CER): The sensitivity must be increased until you reach an acceptable crossover error rate between FAR and FRR. The following illustration provides you an idea.



Accountability

Accountability is an important requirement in the triple-A principle. It assures the ability to track user actions on any secure object or an asset. Accountability is generally assured through event and activity logs and auditing.

Auditing is a critical part of the evaluation process for a person's honesty and commitment. Any user can act vulnerably and willingly to compromise the assets. Therefore, configuring log collection is vital. In addition, it should be kept safe. In military environments, logging servers cannot be read by most systems. It is a one-way communication process. Also, the logs must be backed up.

At specific intervals, each user, including management, must take mandatory vacations. During this period, it is possible to audit his actions and activities.

Session Management

A session is simply an established channel for communication and other remote activities between a server (not necessarily a hardware server) and the requester. In web-based technologies, this is used extensively. When you request a webpage, your browser creates a session between it and the server. Also, mechanisms like RDS, RDP, VPN, and SSH use the sessions.

The sessions are managed through a variety of techniques, including web cookies, tokens, and other mechanisms. To make a session secure, the implementor of the client must provide support for encryption and other standards.

The sessions have their own states. When a session is idle, it may disconnect to save system resources. For instance, the TCP protocol maintains states. However, a session can be stolen, and it is a major disadvantage. For instance, someone can use a token or a browser cookie to gain access. Therefore, internal security integrations must exist with these services. For instance, session expiration can be used to prevent issues.

Registration and Proofing of Identity

Registration occurs only when there is a new activity or management tasks. However, enrolling new users is a regular process in the enterprise and businesses. Registration with government bodies also provides proof and validity of identity, just like when companies hire employees. Government IDs such as the national identity card, SSN, Driving License, and passwords are such documents.

Registration is a straightforward process. However, when enrolling new users, for instance, to an email application, a new user has to provide more details such as security questions to ensure you are what you claim to be during the account recovery. In addition, proper identity can provide accountability and non-repudiation.

Federated Identity Management (FIM)

Having multiple identities is confusing and a pain. Therefore, a federated solution is required to maintain a single and valid identity. Besides, if there are multiple identities, people may make mistakes, or someone else may use it to impersonate. When two organizations (or multiple organizations) share authentication and authorization information, this is the best solution to utilize. Federated identities can be shared between two trusted domains, for instance. This removes the burden of having to manage multiple identities. This also facilitates Single Sign-on (SSO) implementations.

IAM brings more features into this, such as identity brokers. The broker is a service provider between two or more parties. The identity broker provides

authentication or access control services in this case. It provides a single set of credentials, SSO, compliance management, and kills overheads. An identity broker includes the following.

- An Identity provider
- Resident identity provider
- Federation provider
- Federated identity provider
- Resident authorization server

What are Inbound and Outbound Identities?

Inbound identity facilitates external parties to access internal services and applications through the organization's boundaries. Outbound identity provides an assertion to become consumed by another identity broker.

Single Sign-On

This is explained in multiple chapters. All the FIM systems utilize the SSO approach, although these two are not synonymous. In truth, not all SSO implementations are FIMs. For instance, Kerberos is the Windows authentication protocol. It provides SSO service (integrated Windows authentication) but is not an FIM.

Security Assertion Markup Language (SAML)

SAML is another popular web SSO provider. It has the following components.

- A principle: A user
- An identity provider
- A service: A service requested by the user

SAML v3.0 provides one-way and two-way trust, and it can be either transitive or non-transitive.

Oauth

This is another popular authentication standard providing authorization services to *Application Programming Interfaces (APIs)* . When you configure your email for the first time, it may have asked for you to use the contacts of another. This is an example of Oauth operation. This, however, does not offer its encryption standard but depends on TLS. Oauth has the following components.

- A client application
- A resource owner
- A resource server
- An authorization server

OpenID

OpenID is a great way of avoiding many IDs and passwords on the web. It provides granular control over what you are sharing with different sites. When you authenticate, you provide the password only to the broker, and the other sites never get to read your password. These features made OpenID a de-facto standard.

Credentials Management Systems

A CMS provisions the credential requirements by individual and identity management systems such as LDAP, and also creates accounts. Therefore, it plays either a single role or a unified role in an IAM solution. Such systems are available in the cloud as well as for on-premise use.

A CMS is highly useful to ensure secure access in complex business environments. In such environments, the creation and management of users and especially securing them is a tedious task. In addition, the government regulations on privacy and security require demonstrative ability to validate identities.

CMS systems are the main target of attackers as a leak allows penetration to the entire organization and also allows people to impersonate. Therefore, to mitigate such issues, Hardware Security Models (HSMs) can be utilized. Encryption and token signing make these systems much stronger and allows to meet performance criteria.

5.3 Integrated Identity as a Third-Party Service

You have come across IaaS, PaaS, SaaS, and DaaS. There is a new generation in addition to these four. It is the *Identity and Access Management as a Service (IDaaS)* . These third-party services pose a significant threat. Such systems can be installed on-premise or use cloud-based services. Significant consideration must be put on identity lifecycle management, provisioning, governance, triple-A principle, and privilege access.

On-Premise

In this case, the services are integrated into the existing services. Third-party systems can be integrated, for instance, to provide authentication services. For instance, Microsoft Active Directory can be integrated with a third-party SSO solution. However, the risk can be greater due to exposure of sensitive information. Therefore, proper evaluation is a critical step.

In the Cloud

If you rely on cloud services, you have two flavors. One is the federation path in which you are federating an on-premise system to the cloud. The other is the use of already crafter third-party service. For instance, Amazon IAM, Google IAM, and Azure are dependable options. These systems provide some advantages like the vendor managing the infrastructure and security, time savings, scalability, no or less cost, multiple features, and excellent performance. Among the drawbacks, the inability to manage and see the underlying infrastructure, extra-cost options, lack of support for legacy systems, and lack of competency level is at the top.

Federated Services

This is introduced and discussed in a previous section.

5.4 Implement and Manage Authorization Mechanisms

In this section, you will learn more about access control models and mechanisms.

Role-Based Access Control (RBAC)

RBAC is the most popular access control method and is widely used in many organizations. This model provides much more convenience in contrast to other models, as it is not difficult to match the business functions with roles and responsibilities. Then it is just a matter of applying policies.

RBAC is non-discretionary access control. In other words, it has static boundaries and coarse grain access control. It facilitates management ease and strong protection while reducing the administrator overhead. In addition, it provides ease of delegation and control, compliance, and efficiency. An example would be Microsoft Active Directory users, groups, and principles. Microsoft Exchange servers utilize a similar model.

Rule-Based Access Control (RuBAC)

As the name implies, the method uses a set of rules. These rules are used to simplify and automated access control and security management. A firewall is a good example of this type of system. Modern firewalls and routers incorporate this model to filter packets, make intelligent decisions, and apply necessary actions. Apart from these systems, *Network Access Control (NAC)* software also utilizes similar models.

An example: Joe is a remote user accessing internal systems through a remote desktop protocol. He is allowed to access if only if his static IP matches the specific IPs in a list. It is similar to an '*If, Then*' logic. If he is using a different IP, then he is denied.

Mandatory Access Control (MAC)

MAC is a popular approach in places where the highest security is required. In such environments, it is difficult to use discretionary access controls. For instance, an owner cannot determine or control object access. When there is a need for classification and labeling, MAC is the best option. MAC provides specific or atomic level access control from scratch. It supports inheritable permissions as well.

As you may have understood to implement MAC, there must be a customized operating system. However, the practical implementation of MAC models is not as convenient as other models. It brings much more overhead, clearance issues, expenses, limitations, and a lack of user-friendliness.

Discretionary Access Control (DAC)

DAC is something many users are familiar with. You may have worked with files in an organizational environment. In Linux or Windows or even other platforms, you can control files you own and control read, write, and execute permissions, including shared permissions. Within your folders, you can manage your ownership and controls. This relieves additional administration overhead and ease of management for everyone. This model provides much more convenience in terms of clarity, transparency, and manageability. The main risk of this approach comes with the inheritable permissions. This is something an attacker can gain more control upon successful exploitation. Therefore, it is required to either disable inheritance organization-wide or apply other alternatives.

Attribute-Based Access Control (ABAC)

An entity in an organization such as a device or a system has characteristics. These characteristics can be recognized as attributes. If there is a given scenario, for instance, an information security project, you can find a set of attributes related to it. Then you can build rules upon these attributes. If and only if a subject's access request matches his/her attributes, then only he/she can be granted access. In this case, if RuBAC is utilized, there will be complexities. Instead, it is possible to create more specific rule-based control on top of it.

The challenge with this approach is to select simpler and clear sets. Otherwise, the users may have to wait for hours until a match is found. Therefore, complexity must be minimal.

5.5 Manage the Identity and Access Provisioning Lifecycle

Now you are aware of the most important parts of access control. Each asset or entity in an organization such as users, services, or devices has to go through a lifecycle of access management.

If we take an example, the human resource department in your organization hires employees. They join at a certain point, their clearance and access are provisioned and communicated, they have to go through different scenarios during the employment lifecycle, and their access-related parameters may change as they grow. For instance, if someone is promoted, the clearance,

surrendering old access control assets, and obtaining proper ones are the required steps, and they need assistance through the process.

They have to take mandatory vacations and other means necessary to facilitate auditing in many cases, and they have to surrender certain access levels. When they quit the job or complete the required work of his/her carrier life, they leave the organization. They surrender access to the organization when they do so. This lifecycle requires planning, implementing, provisioning, administering, and assisting.

Provisioning and De-Provisioning

Provisioning is the first step of providing access, for instance, preparing and creating a user account. De-provisioning is the process of taking the assets back and terminate the user account. Keeping stale accounts is a vulnerability. Keeping reserved accounts is also a dangerous practice unless the administration can safeguard it properly.

To manage these processes during the lifecycle, there has to be a checklist that includes security guidelines. Each step must be validated before moving on to the next. It should also have a clear guideline along with it.

User Access Review

This concept has been introduced in previous chapters. This is none other than the logging and tracing to audit the user activities. The audit process must be handled by senior management with the help of supervisors. This process also verifies the need-to-know and least privilege (minimum necessary). Here, the restrictions should have been already enforced through policies.

During the review, the team will assess the ethical conduct, best practices, and guidelines in contrast to a documented baseline, which should have been communicated to the user through training. If someone violates any access rights and performed illegal action knowingly or unknowingly, they have to go through a disciplinary process and training. If a severe violation is found, the access will be suspended until further notice, and the assets will be acquired and halt the access.

System Account Access Review

The use of reserved system accounts must be audited. Some of these accounts may have super permissions. This is opening the attack space very much. Therefore, an attacker can gain access to the system through vulnerable ports and exploitable services. Periodically review of these systems, activities, and if any privileged user abusing the account is the best way to ensure the safety of such accounts.

Apart from that, there are methods provided by the operating system to safeguard system accounts. Sometimes creating these accounts require complex work, but, in most cases, it is simplified. It also provides facilities to restrict the actions of the accounts.

Chapter 6

Domain 6 - Security Assessment and Testing

Security assessment and testing is the process of validating the entire security program, including the strategy, policies, procedures, and every critical component. In this section, you will learn the assessment strategies, testing process, techniques, and procedures.

6.1 Design and Validate Assessment, Test, and Audit Strategies

We have gone through the introductory topics about the auditing process. Any organization in their security plan must have a proper assessment strategy, testing procedures, and audit strategy to ensure the efficiency and effectiveness as well as the accuracy of them. This may reveal the gaps and holes in the previous and current plans, add security guidelines to prevent future failures, and reveal the actual security stance of an organization.

Auditing must evolve with the security strategy and policies as it is an integral component. Therefore, it must be audited timely. The following outlines a list of strategies to employ.

Internal Strategy

An internal strategy is developed in parallel to the internal security program. It is, in fact, aligned to the business objectives, functions, and security requirements. Depending on the size, structure, and operation, the strategy can be a complex one. In addition, tests and auditing may occur more frequently. When developing the strategy, common interests and stakeholder requirements should be considered. While doing so, compliance and regulatory requirements must be satisfied.

External Strategy

In this process, an organization is assessed to determine how an organization follows its security policies, regulations, and compliance.

Third-Party Strategies

When there is a requirement to assess the current design, testing framework, and the overall strategy neutrally, a third-party strategy should be utilized. This is critical because it realistically assesses how internal and external auditing are effective and efficient.

Now let's have a look at the steps you have to take to conduct an assessment.

1. Assess the requirements
2. Assess the situation(s)
3. Document the review
4. Identify the risks and vulnerabilities using appropriate scanning methodologies
5. Performing the analysis
6. Reporting to the head and the relevant teams

6.2 Conducting Security Control Tests

This is the stage that occurs after the assessment. The tests comprise both physical as well as logical tests.

Vulnerability Assessment

What is vulnerability? This is something you already know at this point. Testing for vulnerabilities and exploits are required. This must be performed against all the devices, software services, and the operating system as well as on users. During the assessment, it is possible to identify vulnerabilities, determine the impact and priority. Once the risk is identified, the vulnerabilities must be fixed through the risk mitigation procedures. Once this is complete, it is possible to take preventive measures and update the controls.

A vulnerability assessment is highly technical and also a logical process. For instance, physical security is assessed by looking at different perspectives.

Penetration Testing

This is the technical part of the assessment process. In this process, an individual, an internal team of professionals, or a third-party (a white hat hacker, for instance) is trying to penetrate the organization assets such as the internal network, servers, and possible exploits. If vulnerabilities exist, this exercise reveals them. There are a lot of sophisticated tools, such as scripts, software, and exploit kits are available.

There are several stages of a successful penetration test.

- Reconnaissance
- Enumeration
- Mapping the vulnerabilities
- Exploitation
- Maintaining the access
- Clearing the tracks

One or more scenarios from the following list will be executed during the process.

- Application layer tests
- Network layer tests
- Client-side testing
- Internal testing (insider threat)
- Social engineering
- Blind testing: The attacker knows the name of the target. The security team is also aware of the upcoming attempt
- Double-blind testing: Similar to blind testing but the team does not know of the upcoming attempt
- Targeted testing: Both the security team and the external parties are aware of the test and collaborate.

Log Reviews

This is stressed as important in multiple chapters. Many operating systems, device manufacturers, and software developers support logging features. Even though this is true, reviewing logs and backing up processes are two critical requirements. During the review, any unusual patterns or series of patterns reveal attack attempts both successful and failed. Therefore, it is important to enabling logging both success and failure events. From applications to the object level, logging is used.

There is another important thing about logs. Logs can be traced to track the origin of the attack attempts. Therefore, it is important in litigation. To safeguard logs, enforcing simplex communication is a great option. You can also use write-once media to safeguard logs further.

Synthetic Transactions

This concentrates on testing system-level performance and security.

Code Review and Testing

Code review is a critical part of software engineering and development. Code reviews and tests can reveal hidden security issues, gaps, and loops and helps to patch vulnerabilities. A proper patch management program is critical to ensure security, thus reducing the attack surface.

Misuse Case Testing

In software development, there can be issues with the process flow, scenarios, and logic. Erroneous code opens opportunities to launch successful exploitations and seize operations. Also, this causes password theft, privilege escalations, and memory leaks. Proper reviews and possible automatic tools can prevent these issues.

Fuzz Testing

Fuzz testing is a quality assurance technique. It can discover coding issues, security vulnerabilities, and other issues in an application. Fuzz forces a massive amount of data aiming to crash the system. Such applications are known as *fuzzers* . These applications uncover even more serious vulnerabilities that open the possibilities of DDoS attacks, buffer overflow attacks, cross-site scripting, and database injections.

Test Coverage Analysis

This section focuses on types of tests used in software development, security analysis, malware analysis, and so on.

- Automated tests
- Dynamic tests which monitor systems during the tests
- Functional tests executed to validate the functionality, stability, and reliability
- Manual tests
- Negative tests focus on invalid and unexpected inputs
- Static tests with which the system is not monitored during the tests
- Whitebox/Blackbox tests focus on two scenarios. In Whitebox testing, the tester knows about the structure and the processes. In Blackbox testing, it is the entire opposite when the tester does not know anything. It is similar to a hacking attempt. However, this does not reveal any internal vulnerabilities.
- Gray-box testing is a scenario when a tester has certain knowledge about the system and is more like a regular user. It also replicates an insider threat or a MitM attack. This is the best option to reveal both the internal and external issues.

Interface Testing

You were introduced to the concept of interfaces. Another testing scenario is the test of interfaces. This is extremely important because it can affect more than one party. For instance, a network interface card can damage the motherboard as well as causing issues to the connected device and, of course, data. These tests are structured and mostly automated. Proper documentation is required during the tests as it is required during the integration tests. The following test cases are used.

- Application Programming Interface tests (API tests)
- User Interface Tests

- Physical Interface Tests

6.3 Collect Security Process Data

Security systems, processing, and tests create a vast amount of data. For instance, systems such as Security Information and Event Management (SIEM) can process such data. Such data comprises of electronic (digital) data and paper records. Organizations set forth such processes to ensure confidentiality, integrity, and availability. Maintaining the reports in a consistent manner is required. An organization, therefore, must perform vulnerability assessments and account reviews often. In parallel, the overall process must be documented. It is possible to use spreadsheets to collect data.

Account Management

Account management and security are critical steps in any security strategy. An organization must maintain proper and consistent procedures to maintain, secure, and audit the accounts as these are used to access the systems and other valuable assets. To manage other accounts such as vendor accounts, there has to be a parallel yet a different procedure. In both cases, activities such as creation, expiration, login activities, and other attributes must be collected. In addition, physical access records must be maintained. A combination of activities can be utilized to grant and deny access.

Management Review and Approval

Initiatives and reviews at the management level (sometimes including the head and security committee or board) are key success factors of any security strategy. It is possible to collect process data through the Administrators and other teams. Management has a responsibility to delegate the task by approving the techniques to use and doing periodic checks on the person or a team. The following key activities can be observed.

- Reviewal of the most recent security incidents
- Reviewing and ratifying changes to policies
- Reviewing and ratifying major changes to the business process

- Reviewing risk indicators and key metrics
- Reviewing the budget

Key Performance and Risk Indicators

Key performance indicators or in short KPIs and Key Risk Indicators or short KRIs are the indications of performance and risks. Risk indicators are used to calculate the risks associated with accounts, processes, and other activities. On the other hand, KPIs measure the success of a process and its affection to the regular operations in an organization. A selection criterion for KRIs is listed below.

- Incident Response: Incidents reveal weaknesses, gaps, and mismatches that the organization's security or business strategy needs to address. A recurring issue indicates a trend of a potential weakness being mishandled or exploited. The key risk indicators here are dwell-time, the time required to rectify the issue, and resolve the issue.
- Logging and Monitoring: Type of events, number of occurrences, and severities. Here, the KRI focuses on the start time of the event and the time it took the analyst to realize it.
- Vulnerability Management Metrics: Performing scans, identifying the vulnerabilities, and release patches. The KRI focuses on public awareness and the time required to release a fix.

Backup Verification Data

You are already aware of how important to safeguard the data through backups. The backed-up data has a lifecycle – backing up, verification, restoring, efficiency. In this case, it is possible to delegate the authority to a trustworthy partner. The integrity of the data must be assured.

Training and Awareness

You are already aware of the importance of making awareness and training. There are three major components of an effective program, and the following table discusses the importance.

	Awareness	Training	Education
Purpose	Provides a basic idea about security and how to incorporate	Teaches how to react or respond to threats and incidents intelligently	The organizational perspective and exercise on security, why and how it responds
Level	Basic	Intermediate	Advanced
Outcome	Identifying and responding to general threats and vulnerabilities proactively	Constructing an effective response	Understanding the business and security objectives, safeguards, and continuous improvements
Learning Methods	Multimedia, web, newsletters, informal training, etc.	Formal training with hands-on	Theoretical knowledge and skill developed through multimedia collaboration (e.g., webinars), formal training, related-work, research, and engagement
Assessment	Basic tests	Application-level	Architectural level
Impact	Short/limited	Moderate	Higher and long-term

Disaster Recovery and Business Continuity (DR and BC in short)

You are revisiting the areas of DR and BC. In this case, it is about collecting data and proper documentation. For instance, if your organization takes backups, yet they do not label the backups correctly, there is no purpose of it. The best practice is to document the strategy, labels, and purpose. Maintaining a standard is also important. For instance, when utilizing

multiple vendors, these should be documented with appropriate mentioning. In addition, any available automation must be documented.

Another important part is the application of the strategy. When to use what, in other words. This is important as recovery scenarios do not occur often. But the procedures must be accessible, clear, and concise.

In the security assessment and testing, disaster recovery and business continuity go hand to hand; each depends on the other. But when recovery is in process, business functions must be able to continue up to a satisfactory level. The following areas will be focused on during the process.

- Recovery environment
- Recovery of data
- Disaster recovery procedures
- Data integrity
- Versioning

To implement and maintain effective aids are available such as the Information Security Continuous Monitoring (ISCM) available with NIST SP 800-137 strategy. It aids in implementing and maintaining a highly systematic monitoring and management program to suit dynamic requirements.

6.4 Analyze Test Output and Generate Reports

Collecting and maintaining logs is no longer a difficult process. There are many tools, including operating system support to collect logs, analyze data, and represent data through understandable reports. Meaningful information is the key to understanding the problems. The key indicators must provide statistical information with accuracy. The correct interpretation can uncover outstanding issues, performance issues, and outdated measures.

The reporting often requires multiple reports to be aggregated. In this scenario, one report can be highly technical, targeting a specific audience.

However, a non-technical manager, for instance, would not be able to interpret it with clarity. Therefore, instead of sending more technical or specific reports to other parties, it is possible to convert it into meaningful KRIs and use appropriate business metrics to convey the messages.

To make sense, the security team that is responsible for reporting must have better tools and equipment. This is the key to evolve the security strategy and program while obtaining clearance for budget allocations by proving the security program is worthy and moving in the right direction. This successful communication can bring more staff and expertise to enhance the current security program.

Regarding reporting, an organization can follow existing standards. For instance, *Statement on Standards for Attestation Engagements (SSEA18)* auditing standard proposes several reports known as *Service Organization Control (SoC)* reports. The standard was developed and is maintained by the *American Institute of Certified Public Accountants (AICPA)*. The following list comprises the existing report types.

- SoC1 Type1: An attestation of control at a service-organization at a specific point of time or within a timeframe
- SoC2 Type2: This is the same as the SoC1 Type1, but the minimum timeframe is more than six months
- SoC2: This report is for service organizations relevant to *Trust Service Principles* such as CIA triad, privacy, and processing
- SoC3: These reports are also known as WebTrust and SysTrust. The reports can be freely distributed and report whether the entity has met the Trust Service criteria or not. If there is a lack of information, a Type II SoC must be performed. Like SoC2, it can be issued on one or more Trust Principles.

To find more about SSEA18, visit <https://www.ssae-16.com/>

6.5 Conduct or Facilitate Security Audits

At this point, you are aware of what and how auditing proceeds. Auditing is examining and a measuring procedure focusing on both systems and

business processes. This is one of the critically needed assessments that reveal information on how well the processes are planned (strategies), utilized (exercised), and how effective they are.

The main requirement of a successful audit has a zero bias. This is the only path to obtain accurate results. To achieve this, an organization utilizes third-party consultants or a specific team of individuals who are not part of the ongoing business.

Audits measure the aforementioned points against the policies, standards, regulations, compliance, legal contracts, and any other existing laws an organization adhere to.

There are certain types of audits such as,

- Process audits which measure conformance of an operation or a method against pre-determined standards or instructions
- Product audits which measure conformance on specific products, hardware, or software
- System audits which are conducted on a management system

If we take a different approach, depending on the interrelationships and the relevant parties, it can be classified as,

- The internal or first-party audit which is performed by utilizing an internal team to measure conformance of internal standards, methods, and procedures against external standards
- The external or second-party audit which is performed by a customer or on behalf of a customer against a service provider
- A Third-party audit is the most unbiased. It assesses the validity of both internal and external audits and performs specific audits on selected areas in-depth. A successful audit results certification, approval of the license, registration, recognition and if failed, a penalty issues by a third-party by a lawsuit

Difference between Performance Audits, Compliance and Conformance Audits

What is a Follow-Up Audit?

A follow-up audit is an important part of the auditing process for a specific reason. If an organization thinks, “Yes, we have performed a successful audit, found issues, suggested corrective, reactive, and proactive measures, and now we are safe,” there is a problem with that logic. How do you assess if the suggestions and decisions are correctly updated and employed? This is where the follow-up audit comes. It can verify if the corrective actions have been taken and how effective those are.

The following list outlines the major steps of an auditing process.

- Preparation: Visiting the prerequisites and audit compliance by clients, lead auditor, an auditing team including the program manager
- Performance: The data collection phase (“fieldwork”)
- Reporting: The report generation and communication phase
- Follow up and Closure

An important clause from ISO 19011 (clause 6.6) is "The audit is completed when all the planned audit activities have been carried out, or otherwise agreed with the audit client."

Finally, an important difference between compliance and a comprehensive security strategy must be identified. An organization can follow compliance standards and stay compliant. But is this enough? Is it the best approach? If you had a thought like this, then that is a BIG NO! Compliance is compliance, and it isn't security. If an organization has an idea that compliance fulfills all the security needs, that is poor thinking. Both should go hand-in-hand to initiate and operate successful security, business continuity, and disaster recovery plan.

Chapter 7

Domain 7 - Security Operations

This domain focuses on the operational perspective of information security. The sections have a more practical approach rather than theoretical. In other words, this section moves toward operations from planning and designing.

7.1 Understanding and Support Investigations

Evidence Collection and Handling

When do we need to collect evidence, and why? For instance, if someone steals something from you, or when an organization steals the intellectual property of a user without knowing when an attacker enters and steals credit card information from a computer. There are many examples, and the answer to “when” is upon detection of an incident. The answer to “why” is that we need evidence to prove the incident and who behind it was. This evidence can be presented to a court in litigation and take legal actions and fine from the responsible person or entity.

If a digital crime occurs in your organization, there must be a strict policy and guidelines to hand such events as the evidence can be lost, and if it happens, there will be no way to take action against it. These issues are handled through the organization’s *incident response* strategy. There must be specific, trained professionals to handle these events. The policies and procedures must have clear guidelines and should focus on key business areas. Furthermore, it has to be communicated, trained, and rehearsed.

The techniques and tools used in the evidence collection, and the evidence collection procedure itself, depends on the nature of the incident. There can be multiple scenarios and different types of evidence. For instance, there can be physical, logical, behavioral, and logical evidence. Regardless of the type, safeguarding the collected evidence is a must. When this is recorded, there must be records on who is responsible for safekeeping the evidence and where it is kept. This responsibility can be delegated as well. This

process is known as the *chain of custody* (answers to what, when, where, who and how) . This ensures both accountability and protection.

Upon physical investigations, for instance, when an insider threat is revealed, relevant business units involved in the proceeding. Departments such as human resources have answers to certain questions. These inquiries must be well-documented.

There are four major types of evidence.

- Demonstrative evidence: Things like diagrams and charts
- Documentary evidence: These are the textual evidence
- Real evidence: These are tangible evidence such as weapons
- Testimonials: Testimonies from the witnesses

Unlike physical assets, it is difficult or impossible to seize digital assets in some cases. Any organization must have to go through common laws and regulations to seize and obtain the assets. While doing so, maintaining professionalism and ethics are important practices. From country to country, different laws are governing the procedures of seizure and retrieval. Upon criminal activities, law enforcement can take relevant assets to their custody. In any case, the evidence and the chain of custody must match.

The next task is analysis. It is a highly sensitive task. Digital and other forensic investigations require highly professional and experienced individuals or a team of individuals.

When the data found concerning the incident as evidence, when it is at rest, it must be stored in a secure facility. During transportation, the responsible teams must be accountable and reliable. Furthermore, these storage facilities must be free of contamination and hazardous material.

In the next and the final stage, the collected evidence will be presented at court in certain cases under careful supervision from either the internal law officers such as lawyers or by using an external law firm. If the physical assets can be returned to the owners, it will be ordered by the court. However, if these are to be destroyed, the court will apply to do so.

Reporting and Documentation

There are two types of internal reports. Those are non-technical reports for a non-technical audience and the technical reports for the technical-savvy audience.

Investigative Techniques

There has to be a technique to determine whether a crime was committed or not. A legal framework is required to initialize the data collection procedure. The legal department sets the framework, and other parties will follow accordingly. Collected data must be preserved until presented as evidence in a proceeding. It must be intelligent enough to make sense, raise rational arguments, and make a good impact.

During an investigation, the actions, and the activities such as collection, preserving, analyzing procedures occur. There will be multiple parties involved. Their collective analysis can determine what evidence can be presented, for instance, during a court hearing and also to determine the root cause (motives) behind the incident. The following list outlines the stages that can be observed during an investigation.

- Utilizing proven scientific methodologies
- Data collection and preservation
- Data validation
- Identification
- Analysis
- Data interpretation
- Documentation of the reports
- Presentation

This is a high-level view of the aforementioned stages.

The next section discusses the forensic tools and the main categories of them.

1. Digital forensic (hardware): This analysis focuses on computer and hardware devices. There are four processes involved here,

such as identification preservation, recovery, and investigation. The investigators will follow the standard procedures.

2. Live forensics: Performing real-time analysis on a platform, processes, memory, files, history, networking, and keystrokes. However, live forensics can affect the performance of the system being investigated.
3. Memory forensics: If there is no evidence found in static storage devices, it is the time to move to memory and volatile devices.
4. Mobile forensics: Mobile forensics focuses on mobile devices, platforms, applications, and the role of them in criminal activity.
5. Software forensics: In this process, the legitimate use of the software is traced, especially if something was stolen. For instance, if a software license is abused, it is a violation of intellectual property rights.

7.2 Understanding Requirements for Investigation Types

Administrative

The intension of administrative investigations is to collect and report relevant information to appropriate authorities. Once reported, the relevant authorities can carry the investigations further. Swift actions will be taken upon revealing the responsible parties. These investigations are often tied to the human resource department.

Criminal

As you may already figure, these investigations occur when there is a criminal incident. This is a difficult scenario, and the organization must work with law enforcement. Therefore, the collected evidence is also used in litigations. Since the evidence is highly sensitive, it must be ready to be presented to the authorities. Unless the court decides, so a person or a party is not guilty. Therefore, the relevant procedures must follow standards and

guidelines set forth by law enforcement while maintaining the chain of custody.

Civil

An example of a civil case is a violation of intellectual property rights. These cases are not as difficult as the previous one, and the responsible party may have to pay a fine in most cases.

Regulatory

If an organization violates a regulation, relevant authorities will launch an investigation against it. Infringement, violation of agreements, and compliance issues are example cases. In these situations, organizations must comply and provide all the necessary evidence and details without either hiding or destroying them.

Industry Standards

Many organizations adhere to specific standards. Hence, these investigations reveal if an organization follows the standards and procedures as expected.

7.3 Conduct Logging and Monitoring Activities

Intrusion Detection and Prevention

As you are already aware, intrusion detection and prevention are strategies, techniques, and controls that help either in detecting passive attacks or preventing active attacks. There are three types of intrusion detection systems.

- Host-based Intrusion Detection Systems (HIDS): HIDS can monitor internal and external network interfaces hosted by a system.
- Network-based Intrusion Prevention Systems (NIDS): This is the most popular type of intrusion detection system. It is a network scanner capable of listening to network activity. NIDS is widely used with antivirus, internet security, and firewall software and hardware.

- **Wireless Intrusion Detection Systems:** Unlike wired networks, wireless networks are more open and, therefore, more susceptible to attacks. This is because the network cannot be contained by physical means. These controls are capable of detecting intrusions on wireless networks in the organization.

In addition to the aforementioned systems, there are perimeter intrusion detection systems (PIDS in short), and virtualization intrusion prevention systems (VMIDS in short).

Now you have a better understanding of the available IDS systems. How do these systems detect an intrusion attempt? There are several methods that you need to be aware of.

Signature-Based

In this technique, a static signature file is used to match the patterns against it. The challenge here is a significant one. That is the effort required to keep the signature file updated. Furthermore, this technique cannot reveal zero-day vulnerabilities.

Anomaly-Based

This technique is used to monitor variations or deviations of network patterns and compare against a baseline. The advantage of this method is that you do not need a signature file. However, there is a downside. It may report multiple false-positive identifications. This may cause panic and interruptions to regular operations. These systems are capable of learning the patterns and improve.

Behavior-Based/Heuristic-Based

This approach uses a criterion to study the patterns, behaviors, or actions. The technique looks for specific strings, commands, and instructions that would not be used with regular applications. To determine the impact, the technique uses a weight-based method.

Reputation-Based

As the name implies, the detection occurs based on the reputation. This is commonly used in operating systems. It can identify and prevent malicious

websites, apps, and IP addresses. You may have come across this when installing software in Windows and when you install repositories in Linux.

Intrusion Prevention

Intrusion Prevention Systems or (IPS) are live and active systems, unlike IDS. Such systems actively monitor specific or all the network activities (network activities), and most of the time, such systems do stealth operations. IPS systems perform deep investigations and proactively detect attempts by following certain methods. Furthermore, IPS devices are capable of actively alerting and reporting to administrators. There are several types of IPS techniques similar to the IDS. Those are,

- Signature-based
- Anomaly-based
- Policy-based: The technique uses policies to determine violations

Secure Information and Event Management (SIEM)

SIEM was introduced to you in a previous pattern. In an organization, every security system generates vast amounts of data across multiple systems and saves loads of data. Systems such as SIEM provides centralized log management. This is a major requirement of large-scale enterprises. SIEM provides the following capabilities.

- Forensic reporting of security incidents
- Altering the analysis if a certain set of rules is matched

The following list outlines the SIEM process.

- Collecting data from different resources
- Normalize and aggregate data
- Data analysis: Uncovering of new and prevailing threats are identified
- Reporting

Continuous Monitoring

We have revisited the importance of continuous monitoring and logging. Logs help us to identify potential attacks, detect the attacks, and prevent the possibilities. Many malicious attempts, exploitations, or intrusions can trigger log generation. At this point, powerful monitoring solutions are available as enterprise solutions. Certain SIEM solutions offer the same service.

What are the main tasks of a monitoring system?

- Scanning and contrasting to the baseline, identifying, and prioritizing vulnerabilities
- Inventorying the assets
- Maintaining competitive threat intelligence
- Compliance and device audits
- Alerting and report generation
- Patches and updates

Egress Monitoring

This technique is used to filter and prevent sensitive data from leaving the organizational network boundaries. This is also known as *extrusion detection*. It is important because

- Data leak prevention
- Filtering malicious data from within the organization

To monitor such an information egress system uses the following.

- Data Loss Prevention (DLP)
- Egress Traffic Enforcement Policy
- Firewall rules
- Watermarks
- Stenography

7.4 Secure Provision Resources

To execute a constant business operation, the security stance must be the same. Provisioning and de-provisioning are two vital integrations to this setup. For instance, if you deploy a new application in your computer network, there can be positive as well as negative outcomes. Among the negative impacts, having an open vulnerability can lead to a great risk.

The provisioning and de-provisioning process integrates security planning, assessment, and analysis.

Asset Inventory

Inventorying existing assets is a critical step. Every asset got a specific lifecycle.

During this process, you perform inventory, track the records, and the rest of the components. Keeping a healthy inventory saves costs.

Change Management

Change management is part of the dynamic nature of the business. The adaptation process must be flexible enough to adjust the security requirements, adopt new technologies, and stay consistent. Since change management is a critical process where feasibilities are calculated, peer-reviewed, and documented since this requires the approval of the head and the relevant teams.

Configuration Management

Configuration must be standardized to assist in change management and business continuity. These configurations must be tested and backed up. Upon such requirements, a configuration management system with a Configuration Management Database (CMDB) can be used to maintain present and past data.

7.5 Understand and Apply Foundational Security Operation Concepts

Need-to-Know and Least Privilege

What is a need, and what is a want? Need is a requirement to perform something or to acquire something to fulfill a requirement. Want is a desire. To prevent information stealing and leakage and misuse, an organization must start providing access by following these two principles.

Least privilege is closely related to need-to-know, but the two are different. For instance, an employee needs to have minimal access to a certain amount of information. Then you could say he/she needs to know this to perform his/her job. Then it is possible to implement the least privilege from providing a computer with network access to perform the job while providing the minimum necessary access to data. When provided access, he/she should be able to perform the job without a problem. In terms of permissions, the baseline has to be “*deny all*.” From this point, the user can be provided minimum necessary.

Aggregation is used to unify pieces in the RBAC approach. Furthermore, transitive trust can be provided. For instance, when you create a domain in a Windows environment, it provides transitive trusts with lower-level domains. A user may receive the same level of access. However, this poses a danger as the aforementioned principles are broken.

Separation of Duties and Responsibilities

Separation of duties is required as overpowered roles can lead to chaos. For instance, in a Windows enterprise network, there is a super admin role known as the enterprise admin. This is a very dangerous role as if someone uses it often, and if an attacker gains access, he/she will be able to take full control. On the other hand, even without an attacker, the user may become a single point of failure as he is the primary authority. The power level may lead him to misuse or abuse enterprise assets.

Splitting the duties and delegation is always required to reduce power, reduce stress, and maintain accountability. In a military environment, splitting the duties can be observed. For instance, to launch a security countermeasure, a key is used to activate it. However, there can be two or more keys distributed among several people, and they have to put the key at the same time and turn.

Privilege Account Management

Privilege accounts have to be used during enterprise operations. For instance, there are multiple admin roles distributed among a few admins, or sometimes an individual gets the responsibility. To prevent information leakage, abuse, and mistakes, these accounts must be monitored closely. To do so, auditing actions must be enabled on the platform. Automated monitoring systems can also monitor and report such activities.

Job Rotation

Job rotation is required to shift the power and status of a job role. When people get familiar with a role, he/she starts acting carelessly and in an authoritative manner. This is a psychological issue. To make sure responsibility and accountability, job rotation is the solution. It breaks the thought of becoming an owner of a role. Besides, if multiple people are aware of how to perform a single task, it removes bottlenecks and offers competitive advantages. The concept is also used in cross-training in organizations. The advantages are continuous learning and improvement.

Information Lifecycle

The information lifecycle can be divided into the following phases.

- Formal planning on collecting, managing, maintaining, and securing information
- Creating, collecting, capturing, or receiving information
- Storing information while maintaining continuity and recovery
- Securing information or data at rest, data-in-transit, and data in use
- Using data in a secure environment such as sharing while the organization follows policies, standards, and compliance
- Retain and disposal information (archiving or disposing of information)

Service Level Agreements (SLA)

This topic will be widely covered in a different chapter. An SLA guarantees standard in response time and quality of response. It is, in fact, a quantified

statement. An SLA is agreed upon provisioning. Once signed between a service provider and a customer, or between an organization and a service provider, the uptimes and incident response time must adhere to the agreements.

For instance, assume an organization guarantees a 99.9 uptime, and a response time for an urgent priority case is 10 minutes. If the case is a high priority but not urgent, it is followed up within 30 minutes. However, if the uptime moves below 99.9, the service quality is hit. To resolve such issues, redundancy, fault tolerance, load balancing, clustering, and firewalling can be deployed. The response time and follow up times must adhere to the agreement.

To measure and calculate the response times, the following parameters are used.

- Available hours
- Average and peak users including concurrent users
- Escalation procedures
- General response time
- Incident response time
- Meantime between failures (MTBF)
- Meantime to restore services (MTRS)

In addition, internal SLAs such as *OLAs (Operational-Level Agreement)* and *Underpinning Contracts* must follow similar standards. To measure performance and efficiency, *Key Performance Indicators (KPI)* and *metrics* can be used.

7.6 Apply Resource Protection Techniques

In this section, the focus is on the applied protection techniques. There are many assets to safeguard owned by an organization. It can be hardware/firmware, communication devices such as routers, switches firewalls, other peripherals, and operating systems. There are many types of

confidential and non-confidential data, such as operating system data, configuration, and audit data. Furthermore, there are storage systems such as DAS, SAN, NAS, and traditional backup media such as tapes, cartridges, and external devices. Operating systems and virtualization requirements are also there. Appropriate scanning, access controls, good coding practices, good storage practices, patching, and updating can secure these assets.

Hardware and Software Assets Management

To manage assets, there must be an inventory to identify the available units and target scans and other actions, such as updates. There are many general and sophisticated tools to build an inventory of assets and create an architecture to manage and secure each component.

7.7 Conduct Incident Management

Proactiveness

Proactiveness is essential in business continuity and disaster recovery. Identifying, analyzing, and reviewing the past, present, and future threats is the first step to reach proactiveness. To ensure it is moving forward, a well-documented and rehearsed management policy, procedures, and guidelines are required. Training is also an essential part of building proactiveness.

Detection

Any incident management process starts when something is detected. It is the first phase of the incident management lifecycle. For instance, an anomaly in a log, an attempt of breach reported by a firewall, a possible malware found by an antivirus suite, an alert from a remediation network about a remote worker's obsolete device can trigger the sensors. A sensor can be a software sensor or a hardware sensor. Most cases that these systems detect are not real-time. Therefore, a passive approach may be required. During the analysis, the team must get an idea of the magnitude and priority of the impact.

Response

As soon as an issue is detected, a response team must start an investigation. They have to verify whether there was an incident or not in the first place

(to avoid false alarms). If the breach or the attempt is real-time, the affected systems must remain online. Then a team member must be able to report to the relevant parties and isolate the assets (quarantine) as soon as possible. For this, there must be a proper escalation procedure.

Mitigation

Most threats cannot be detected within a specific period of time unless there are controls in place. With the prevention controls, it is possible to prevent issues before occurring. In reality, it is difficult to prevent all the potentials. However, it is possible to minimize the impact and prevent a recurring event. This is known as mitigation. Isolation and quarantine are the main parts of the mitigation procedure.

Reporting

At this stage, the appropriate level of communication and reporting occurs. It is a critical requirement as every stakeholder should know about the incident, and an acceptable level of transparency must be maintained with the customers. By reporting timely, it is possible to get the resource pools.

Recovery

At this stage, if recovery is required, relevant controls have to be utilized to perform a recovery while the business is operated at a minimum level.

Remediation

Remediation is improving and re-enforcing existing systems, verifying and applying up to date security measures, placing additional safeguards, and making the systems in-line with the business continuity process. Many operating systems support remediation. For instance, the Windows server environment supports creating a fully operational remediation network for remote users.

Lessons Learned

The last stage of the overall process is reviewing the entire lifecycle of the incident. During the study, the effectiveness of controls and required improvement and enhancements to the remediation will be discussed. This

is the heartbeat of incident management as it is the very stage that shapes the efficiency and effectiveness of the incident management process.

7.8 Operate and Maintain Detective and Preventive Measures

Firewalls

A firewall is an alpha at the perimeter, and its main responsibility is to defend the internal network from incoming attacks. A firewall can sit in a perimeter and a demilitarized zone or even in the distribution layer in a tiered architecture. Furthermore, firewall appliances are deployed to mitigate DDoS and other sophisticated attacks. This is also true when it comes to cloud operations. Web Application Firewalls are capable of preventing DDoS and similar attacks.

For end-point protection, organizations deploy host-based internet security suites. These include built-in firewalls. Also, it is possible to install a host-based firewall application. In reality, operating systems provide built-in, basic firewalls.

IDS/IPS

Intrusion detection and prevention systems are being revisited. IDS systems are also available with host-based antivirus and internet security applications. Intrusion prevention systems, including honeypots, can significantly mitigate incoming threats. A honeypot is a simulation of an imitated enterprise network. It is a deviation and a monitoring system to get a better idea of attacks and to set up mitigation techniques and remedies.

White/Blacklisting

This is another useful method of preventing unnecessary contacts. For instance, a router can blacklist IP blacklist, an email server can blacklist the spam addresses, and host-based antiviruses can blacklist certain applications.

Security Services Provided by Third Parties

Third-party applications are a common approach to security practices. However, you should do an in-depth review and understand the gravity of the appliance or application or service they provide in terms of information

security, business continuity, and disaster recovery. The following list outlines the existing services. Some of these services providers provide artificial intelligence services, audits, and forensic capabilities.

- Cloud-based malware detection
- DDoS prevention
- Managed Service Providers (MSS): An outsourced MSS performs in-depth monitoring, evaluation, and analysis on organizational assets to detect and mitigate issues. MSS services also accept incident management cases.
- Spam filtering
- SIEM
- Web filtering

Sandboxing

Sandboxing is heavily utilized in software testing in the software engineering area. A sandboxed environment is an isolated test area such as an isolated network segment, simulated environment, or even a virtual environment. Segmentation and containment are the key outcomes. For instance, there are sandbox tools available with malware protection suites.

Honeypots/Honeynets

A honeypot is a simulation of an imitated enterprise network. It is a deviation and a monitoring system to get a better idea of attacks and to set up mitigation techniques and remedies. Honeypots operate in either an aggressive mode or using a slow move so that it can inspect packets. Furthermore, a honeypot can maintain stealth mode. A honeynet is either single or multiple instances of virtual simulation that deceives the attacker.

Antimalware

Malware or malicious intents through applications or activities can be mitigated with the use of antimalware remedies. The malware attempts to break operation and disrupt, destroy, or steal information. Antimalware suite can break its abilities using the signature-based technique. If this fails,

some utilities move to a heuristic approach. AI and machine learning empower antimalware software as it can make decisions faster and intelligently.

7.9 Implement and Support Patch and Vulnerability Management

Vulnerability and patch management are similar but somewhat different in its focus. A vulnerability is a weakness in security. On the other hand, patching is addressing security issues as well as fixing other problems found in current versions of the software. The following practices will be used in patch management.

- Reputed software products are capable of the automatic patch and vulnerability management, and they will have a resilience
- Centralized patch management, e.g., Microsoft Windows Update Service (WSUS)
- Reviewing the patch compliance report to find out the failed devices
- Testing the patches before releasing

Vulnerabilities arise due to weaknesses in coding practices, integration issues, lack of security built-into the application/device, misconfiguration, missing updates, lack of patch management, use of obsolete platforms, and depending on weak security implementations. If an attacker finds out an undisclosed security flaw, it is called a “zero-day vulnerability.” In such cases, there must be proactive countermeasures set to prevent the issues.

7.10 Understanding and Participating in Change Management

Change management is a much-needed process in every business and part of a solid business strategy. Changes are frequent in the current business, given the dynamic nature of businesses and services. Flexibility is an important aspect of a sustainable business. Hence, scalability also depends on flexibility. The following list outlines the change management process.

- Identifying the change: This is the first phase of the change management process. A request for change arises due to multiple reasons including enhancements, obsoletions, objectives, incidents and so on
- Designing the change
- Review the design and plans: The solution has to be tested as well during this stage
- Change request: At this stage, a change request is submitted to obtain approval from a committee, board, or the head of the organization. The request includes when and why it is planned to carry out, how it impacted, how it is going to change, test results, implementation or deployment plans and recovery procedures
- Notifying the responsible parties
- Implement/development/deployment
- Review

7.11 Implement Recovery Strategies

Backup Storage Strategies

A backup strategy is another critical component of business continuity and disaster recovery. Hence it is a major component in the security strategy. A backup plan must answer what an organization should back up, when and how it is backed up or archived, where it is stored (on-premise, offsite, or cloud), and how quickly it can recover. A parallel security plan is required to protect the backups from physical damages, misplacements, stealing, and integrity violations.

A good retention policy is required to reduce storage costs significantly. During the process, the data must be archived but not destroyed. To add more security, an organization can decide to store them in a high-security facility that is situated away from the organization premises. Furthermore, there are cloud services that offer intelligent backup and archival strategies. For instance, Amazon S3 and Glacier provide multiple options.

Recovery Site Strategies

For data centers and other sites, it is common to have one fully operational site or a few and at least one or more recovery sites known as *warm sites* and some *cold* sites. A cold site is an area with a facility and equipment, but it is not configured or arranged yet to become fully operational. Replication and snapshots are essential parts of synchronization between the *hot site* (main site) and warm sites. Backing up is important (offsite), as it is helpful to restart the operation at a cold site whenever needed.

Multiple Processing Sites

Having multiple sites is the best option an organization can achieve. Unless a man-made catastrophe, there is less chance of getting all the main sites to seize the functionality. With technological advancements, running multiple hot sites is no longer a difficult task. Therefore, site resiliency is an achievable goal. With lightning-fast networking infrastructures, it is possible to synchronize among the hot sites. This makes the ability to run three or more sites together and even geographically separated. The vendors get to offer backup-free technologies at present. An organization can have a public cloud vendor if they are unable to operate more than one site on their own.

System Resilience, High Availability, Quality of Service (QoS), and Fault Tolerance

System Resilience

Building resilience takes away bottlenecks. In other words, it eliminates a single point of failure. By design, redundancy, and fault tolerance can be incorporated into the architectural, physical, and logical design. Once it is up, it can withstand failures and recover faster. This makes the uptime (availability) constant with minimal downtimes. Hot-standby and cold systems are placed to restore the operation, for instance.

High Availability

Resilience is about fast recovery and minimal downtime, while high availability is the uptime. When multiple redundant systems can recover faster, allow users to use the system almost all the time, the operation can guarantee the service quality. High availability mechanisms are required to

tackle the issues. For instance, high availability clusters are an option available with web and database services. The resources are pooled as a single or multiple clusters. Even when one node fails, the rest can serve the clients without a problem while engineers have the time to fix the underlying issue.

Quality of Service (QoS)

QoS means prioritized traffic and quotas. This is used mainly to prioritize real-time data such as media streams. In fact, media streams should receive the highest priority as live video and audio must travel as quickly as possible in contrast to textual data. While media streams receive a higher priority, gaming, peer-to-peer, and web traffic receives lower priorities.

Fault Tolerance

You have introduced to fault tolerance in multiple chapters. It is the ability to withstand physical, hardware, or software failures. If devices fail, you should have a way to fix it while another is operational. The truth is fault tolerance itself cannot withstand the issue without the help of high availability and redundancy. This is a holistic approach.

To make a server fault-tolerant, it is possible to have multiple motherboards, processors, memory modules, storage with clustering, hot-standby hardware, and hot-pluggable/hot-swappable capabilities.

7.12 Implement Disaster Recovery Process

Once the Disaster recovery strategy is planned, it must be implemented technically and tested for justification of capabilities. Then it has to be tuned as required. This is a continuous process. This section goes through technical and other requirements (components) that are required to operate a successful DR program.

Response

The first thing about the response is the ability to understand the situation, impact, and ability to craft a response while minimizing the downtime. The process is highly restrictive in terms of time. To foresee the issue and proactively respond, the appropriate level of active and passive monitoring,

a staff analyzing active/passive situations, and a well-established monitoring/login/auditing procedure must be there.

Personal

In any organization, it is the best practice to have a dedicated person or a team assigned to DR tasks. They are responsible for planning, designing, budgeting, implementing, testing, exercising, training, and reviewing the entire program with the supervision from the head, a board of directors, or a committee. The team is also responsible for assigning agents to monitor the health of the operation. They must also establish backup communication methods to deliver urgent and critical information to the seniors and to customers as well.

Communications

To operate the disaster recovery program successfully, two vital components must be there. One is resourcefulness, and the other is timely communication. The second may become difficult in certain situations. For instance, upon a natural disaster such as earthquakes, floods, storms, tsunamis, and during battles/wars/civil issues. To combat these situations, well-established strategy is vital. The team must equip what is available and form a grid to communicate with the team and then possibly with the highest seats. Furthermore, the team should communicate with its business peers and key stakeholders. They should also inform the general public about the situation when required.

Assessment

At this stage, the team can establish communication between relevant parties, and incorporate technologies to assess the impact, magnitude, failures, and build a complete understanding.

Restoration

This is where the team is put to the test, especially in terms of technicality. In fact, the recovery process is set in motion as soon as the team completes the assessment stage. For instance, if the hot site fails, the operation must be transferred or migrated to the warm sites. In parallel, the recovery process is started, and fixing the existing issues is underway in the hot site. During the

process, the team must consider the safety of the operation of the failovers. Having more than one failover is promising to avoid critical failures (bottleneck) when a failover also fails to serve the requirements. This assures redundancy, resilience, load balancing, and availability.

Training and Awareness

No matter how technical, state-of-the-art a disaster recovery plan, if the staff or employees are not trained, lack of awareness and skills, the program is highly likely to fail. For instance, if the employees, stakeholders, and even the general public are unaware of certain procedures during recovery, there are unable to cope with the situation. This is why prior training is a critical success factor. The familiarity with the procedures makes the recovery program highly efficient. Readiness of, resources, financial and technical areas play key roles in a successful recovery operation.

7.13 Disaster Recovery Plans (DRP)

Read-Through/Tabletop

The team responsible for the DRP and other response teams meet read through the plan, measure the resources, and time constraints. If everything is in line, they agree that the plan is realistic. However, if it does not meet the criteria, it has to be redesigned and reviewed until it meets the constraints. If you can spot the key take here, it is none other than proper change management.

Walkthroughs

A walkthrough is a tour or an engaging demonstration. It can also be a simulation. Whatever the method is, internal teams and possible outside parties (i.e., consultants) should perform it and look for possible gaps, omissions, and flaws.

Simulation

A situation can be simulated to get a better idea, experience, and perspective. It also facilitates creating mathematical models to calculate the resources, measure the impacts, and also train through simulated rehearsals.

Parallel

This is another exercise performed on different platforms and facilities. To perform such scenario-based testing, there are built-in solutions as well as third-party solutions. The intension of this process is to test the plan while minimizing the disruption on infrastructure and other operations (you do not have to put your infrastructure and operations to test all the time).

Full Interruption

This a real simulation of a disaster situation followed by response and recovery. In fact, this is the closest you can get to a real situation. However, such exercises require high costs, time, downtime, and effort. On the other hand, without performing at least one of these tests, it is not possible to obtain a verification of the clinical precision of the existing strategy.

7.14 Participate in Business Continuity Planning and Exercises

Business continuity (BC) is the essence of every security, disaster planning, and recovery strategy. In fact, this is a holistic approach taken to assure the continuity, expansion, and scalability of the business operation to meet the organizational goals while succeeding in its mission. Regardless of the magnitude of disaster, challenges and obstacles arise day by day due to competition, uncertainty, political stance, currency issues, and other various dynamics. Mitigating each impact is one step closer to achieving the business goals. Therefore, sensitive and careful planning is necessary to tackle more prevailing issues other than the high-impact disasters which may occur less frequently.

During the planning process, the teams must identify the mission-critical business processes and financial requirements. To accurately find the impacts, the team can use *Business Impact Analysis (BIA)* .

In the next phase, it is required to review the existing technologies and vendor support. Once these stages complete, it is essential to establish failover communication procedures to use during critical situations. This was discussed in the previous section.

In reality, business continuity is not a single process handled by a team or an individual. It is a collaborative effort with the assistance of local

authorities, vendors, service providers, law enforcement, fire department, agencies, partners, and the general public.

7.15 Implement and Manage Physical Security

Perimeter Security Controls

A perimeter is a boundary where an organization's territory begins. Perimeter security is a philosophy of establishing functional apparatus at the perimeter (perimeter of a facility and a network, for instance) to safeguard its assets and data.

The main component of this is access control. Physical security such as fences, guards, signs, sensors, video surveillance, and barriers can be installed to deter and discourage unauthorized activities. Authorized people can go through the perimeter security by proving their identities and security challenges (for instance, biometrics provide credible validation).

Proper monitoring is a critical process to ensure the integrity of the setup. For instance, if an entrance door is suddenly not closing properly, there is a chance that the door got tampered with. If a sentry camera is off, it is a sign of physical damage. Another instance is when someone is using an access card but fail to access certain areas where he/she has no or less clearance. These things happen during the day to day operations, and therefore, careful monitoring is essential.

If someone loses access card that he or she used to go through the perimeter, he or she must immediately inform the authorities. The security team must be able to revoke access and issue a different access card to the person to avoid intrusions.

Monitoring systems can be automated and configured to report or alert the responsible individuals or the team. However, it is not possible to depend on a fully automated monitoring system without human intervention.

Internal Security Controls

Internal security controls safeguard internal physical assets and facilities. For instance, there can be highly restricted areas and highly operational-sensitive areas such as server rooms, wiring closets, file cabinets, archives,

or even passages where there is minimal monitoring. Furthermore, securing office spaces, desks, and cabinets can contribute.

Another important procedure to consider is the escorting of visitors. Visitors must be properly identified, walked through, monitored during their visits, and escort properly. When utilizing consultants, it is important to provide the minimum necessary and revoke access as soon as they finish the task.

7.16 Address Personal Safety and Security Concerns

Travel

Traveling is part of the daily routine of many individuals. It can be between two suburban areas, two cities, two nations, or even through different regions. When traveling, a person has to utilize multiple infrastructures, wireless communication methods, through different communities, different facilities, and has to stay in different locations. Each step increases risks, specifically on information and assets.

Even though there are government law enforcements, policies, regulations are there, the nature and dynamics of the new area can be entirely friendly or can be worse. Along with it, there are different legal actions, penalties, fines. In addition, there can be different compliance and regulation requirements, and some can be highly restrictive. Therefore, prior understanding, education, and awareness can be highly valuable.

During travel, one has to understand government restrictions if he or she carries communication devices and information. Since the person has to depend on foreign infrastructure, it is highly important to utilize all the security measures. That includes device and data encryption, anti-theft mechanisms, use of secure VPNs, avoiding transborder restrictions, avoiding or securing wireless communication (for instance, public Wi-Fi) and limit carrying sensitive information with him or her.

Before traveling, someone must be appointed or delegated to carry out security and other critical tasks. In the meantime, it is a good practice to back up the devices and data before start traveling. When using public transportation and taxi services, one must make sure to avoid important devices from getting stolen. Furthermore, contact with local authorities

must be maintained to mitigate critical and sudden situations such as theft, crime, and local conflicts.

Security Training and Awareness

This section is a revisit on the same topic but to have a different perspective. Different organizations may require different security strategies, as they may have to mitigate different types of risks. Therefore, training and awareness can be different. Therefore, a customized program that is aligned with business functions, objectives, missions, and requirements must be prepared.

During the training, employees should be able to start from the basics and best practices. The start point must be attitudes and behaviors. Information leakage prevention is one of the main targets of the awareness program. For instance, general behaviors such as carrying external devices and related activities, for instance, and the relative disadvantages and regulations, can be effectively conveyed during such activities.

The training programs must be engaging. Many types of multimedia and interactive tools can be used to deliver the message. Furthermore, a definitive, timely, updated knowledgebase can be highly advantageous.

Emergency Management

This is another area of consideration when planning for business continuity and disaster recovery. For instance, upon a sudden situation such as a terrorist attack, a high impact earthquake or a category four storm can bring panic and chaos. The organizations must have contact with authorities to manage the situation proactively. For instance, an organization should have an awareness of the natural activities near the facility they own. During an incident, the organization must be able to cope with the situation while maintaining proper communication, uplifting psychological health, collaborating with authorities, planning for recoveries (e.g., recover or relocate the employees during an incident) and notify all the relevant parties (transparency) about the management activities and the potentials.

There are many tools from a simple SMS service to mega social media services that one can use for remote communication. Mobile services may be unaffected during certain situations. There can be different situations

beyond the expectations, and the disaster recovery planning process must be proactive and flexible for adaptation and improvisation.

Duress

This is another rare but important situation that you need to become aware of. Duress is a special incident where a person is being forced to coerce an action against his or her will. The most common example is a thief pointing a gun at the head of a security guard or a manager in a bank and forcing to open a vault. Another one would be an attempt to blackmail an employee by threatening that the blackmailer has some highly personal assets in his custody. These situations are extremely delicate.

The training program should focus on these situations to provide realistic countermeasures and how to cope with such situations without getting harmed and harming others. This is similar to conflict handling.

There must be arrangements when such a situation is upon the organization itself. For instance, there can be secret cameras, secret triggers to alert authorities, and so on. It is also important to educate the employees to avoid attempting any heroic attempts. Instead, it is possible to calm the situation and people until the help is received. In such situations, panic and trauma can be devastating. However, with adequate training, one can cope with the internals to avoid making things worse. If an individual or a set of individuals have gone passed such situations, the recovery plan must have appropriate medical and psychological readiness to assist and aid such people while compensating them. The main intension here is to equip the employees and set effective countermeasures to manage situations intelligently without getting jeopardized.

Chapter 8

Domain 8 - Software Development Security

Even though you may not have experience in the software development field, any organization may have a team of developers. In some cases, internal teams may involve in integrating software and developing plugins or extensions. Sometimes it has to cope with purchasing decisions. In any case, the practice and understanding of the software development theories, models, practices, and understanding are very much needed in the dynamic nature of businesses.

When you make purchasing decisions, assessments you perform cannot just focus on the performance but security as well. Each design flaw can add more vulnerabilities, thus widening the attack space. If a design flaw causes a permanent failure, you may lose your valuable data, operating time, and money to replace it. The impact can be significant as it affects availability. If devices or software causes temporary instabilities, then you may have to rely on backing up and restoring frequently. This also significantly impact the operation.

If the organization is developing software, then the security is at the highest importance. Each stage in the software development lifecycle must be carefully planned to go through a security assessment, testing, and verification. Each release must be tested for bugs and security holes. There has to be a proper patch management program and made available to the users.

In addition to these concerns, if an organization merges or splits, the entities must redefine or assure security, governance, and control.

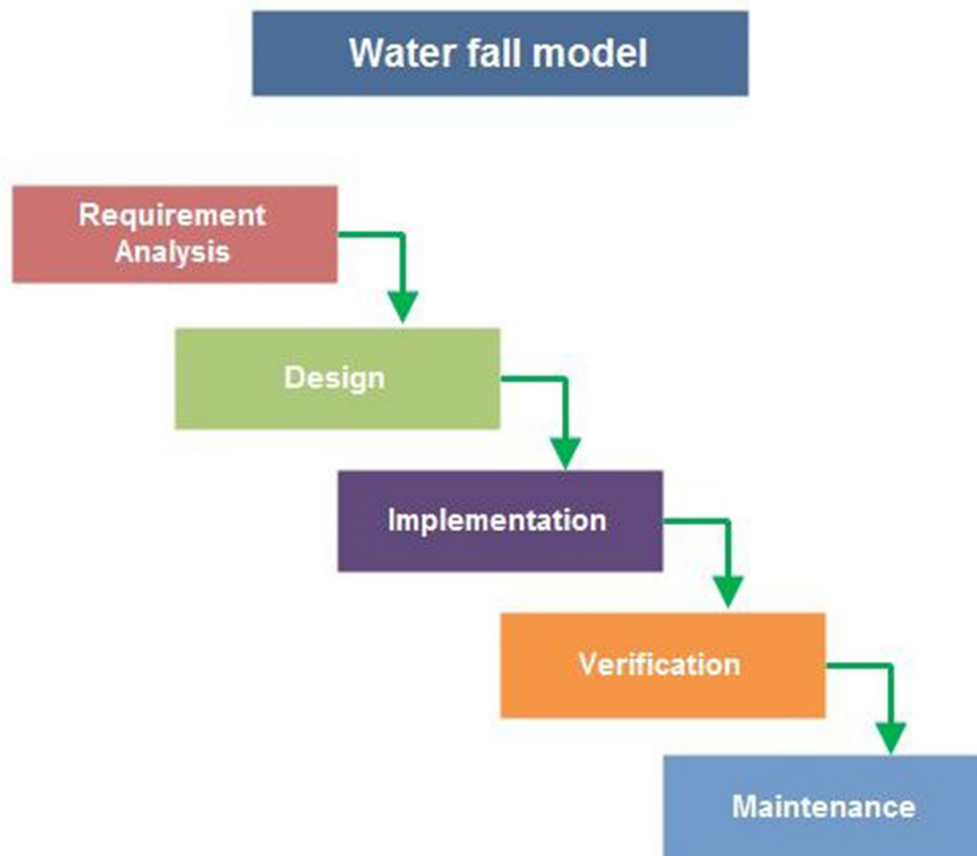
8.1 Understand and Integrate Security Throughout the Software Development Lifecycle (SDLC)

Development Methodologies

In this section, you are introduced to the previous, current, and future methods and disciplines of software development. Each model is geared to suit specific scenarios and criteria. A suitable one has to be selected. Each model has its strengths and weaknesses.

The Waterfall Model

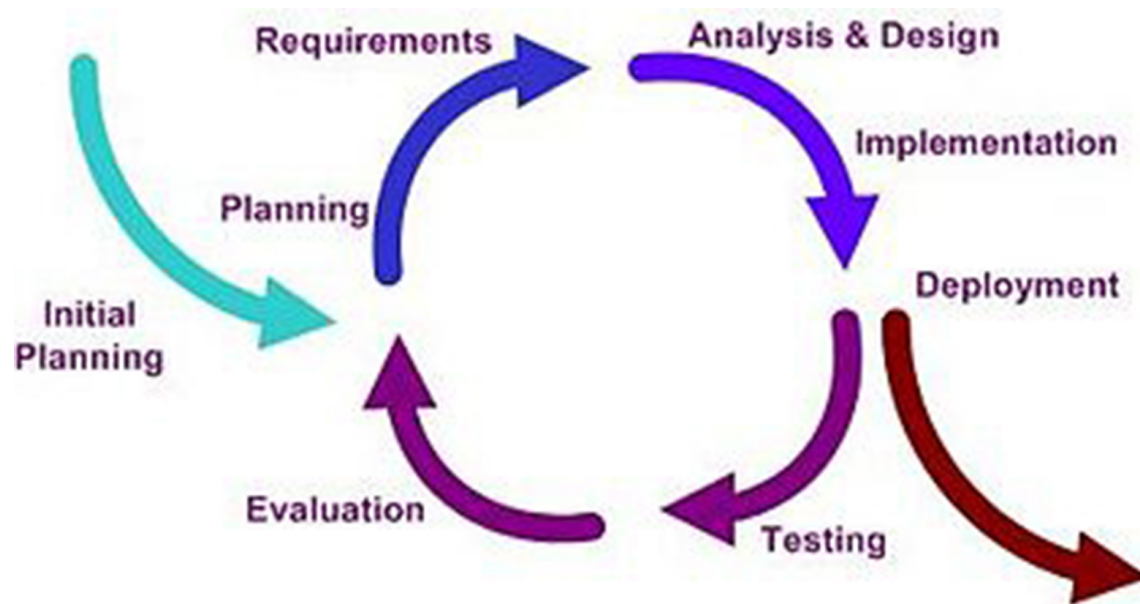
This model is one of the founding and traditional development models. Due to the flexibility issues, it was not the favorite at present. The main problem with this model is the requirement to have all the system requirements defined at the start. When the process ends, the outcome has to be tested. Then the next requirements are assigned and reset the process. As the structure is rigid, it fails to address the flexibility requirements. Military organizations may still use this as it can assure security.



Waterfall Model

Iterative Model

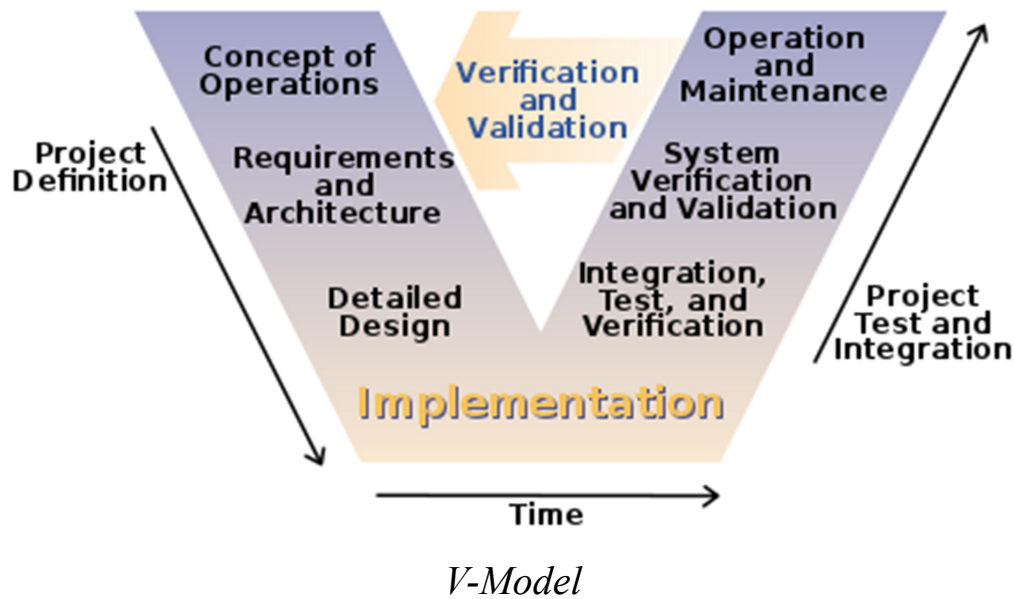
This is a modified version of the waterfall model. It had taken the waterfall model and divided it into mini-projects or cycles. By this, it eliminates having a complete requirement definition. This model is also an increment model and is similar to the agile model in some ways – there is no customer involvement in this model.



Iterative Model

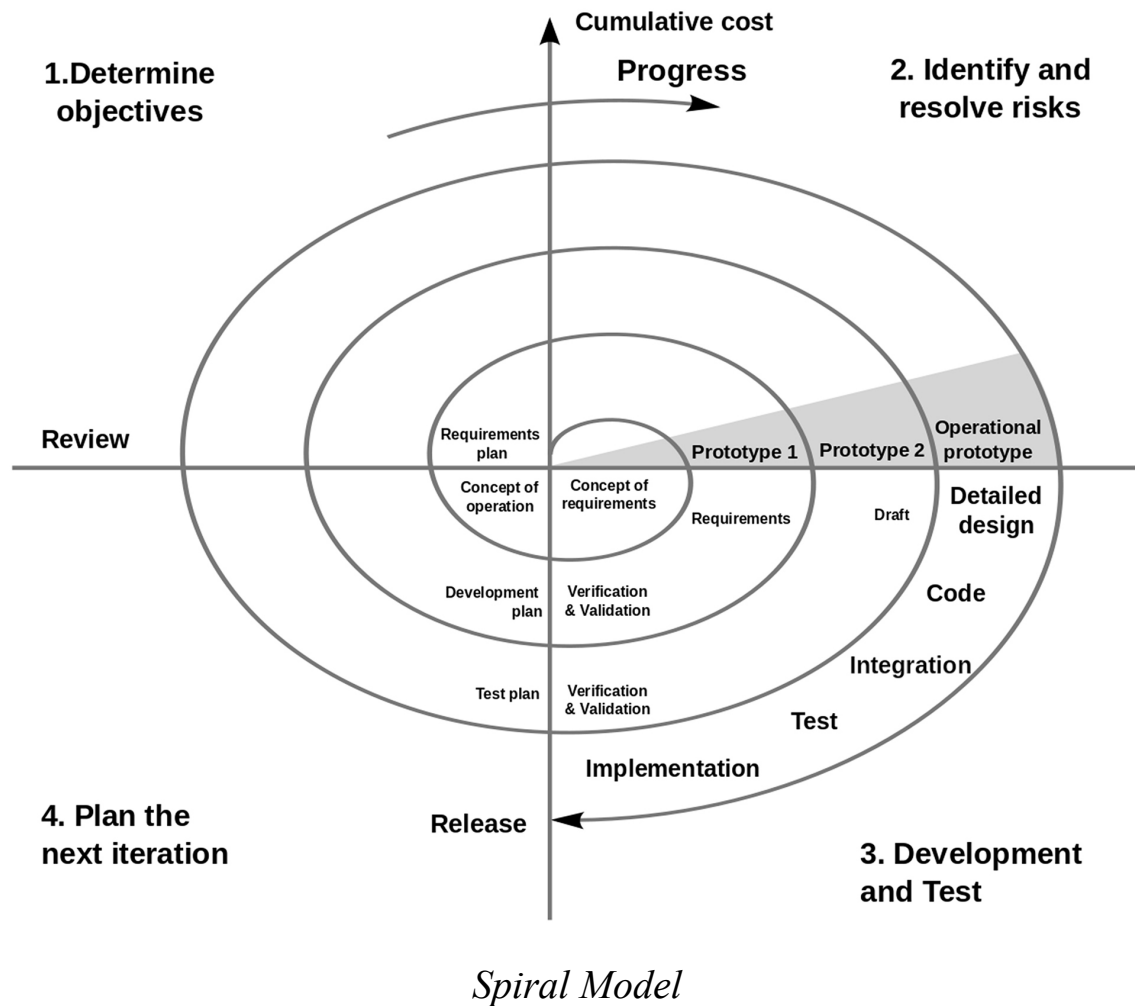
V-Model

This model also evolved from the traditional waterfall model. It pays special focus on operation and maintenance. The main difference here is the flow, which moves upward after the implementation phase.



Spiral Model

The spiral model moves away from the traditional approaches. It is an advanced model helping the developers to utilize multiple SDLC models together, forming a collaboration. As you may notice, it is a combination of the waterfall and the iterative models. The main problem with this model is the inability to know when to move to the next phase. The concept of a prototype is started with this model. A prototype is a working model to demonstrate a basic or a specific function of the project.



Lean Model

This is also a modified version of the waterfall model to greatly enhance flexibility, speed, and iterative development while reducing waste. In fact, it reduced the waste of effort and time. The seven lean principles are,

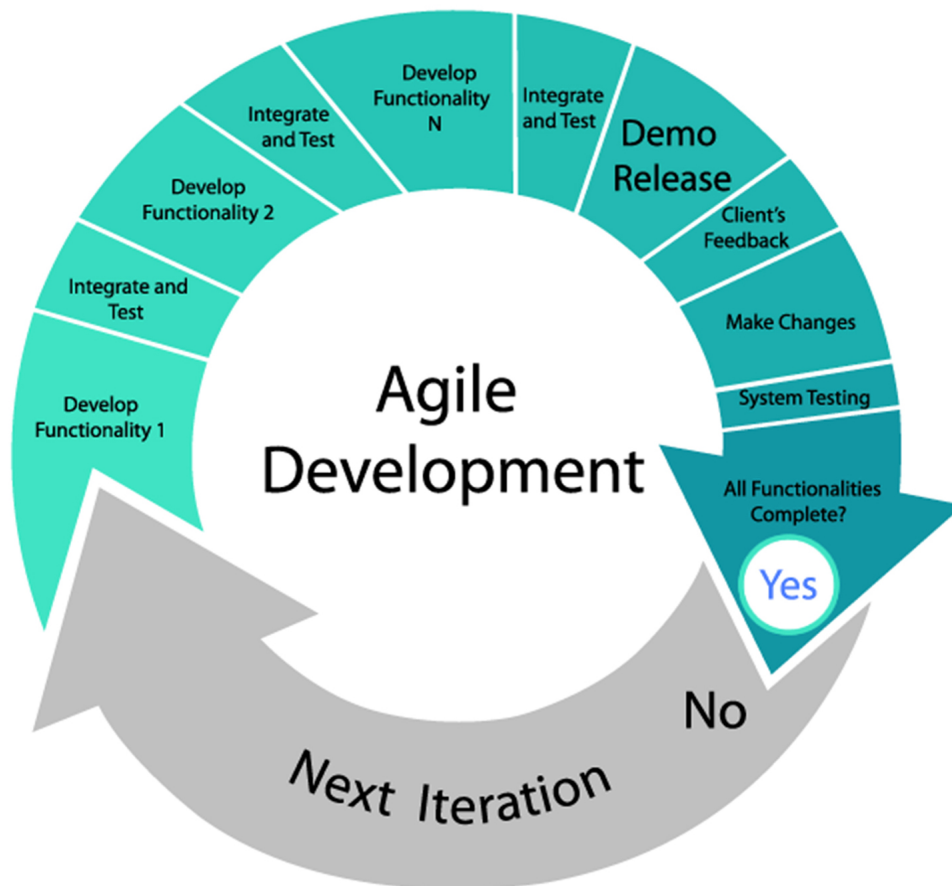
- Waste elimination
- Amplification of learning
- Deciding as late as possible
- Deliver as soon as possible

- Team empowerment
- Integrity
- Seeing the whole

Agile Model

The agile model is similar to the previous model. It can also be thought of as the opposite of the waterfall model. This model was there for a long time, but at present, it has become the main driving force of software development. It has the following phases.

1. Collecting all the requirements
2. Analysis
3. Design
4. Coding
5. Unit testing
6. Feedback - after reviewing with the client and taking the feedback and develop new requirements if necessary, or else release the final product

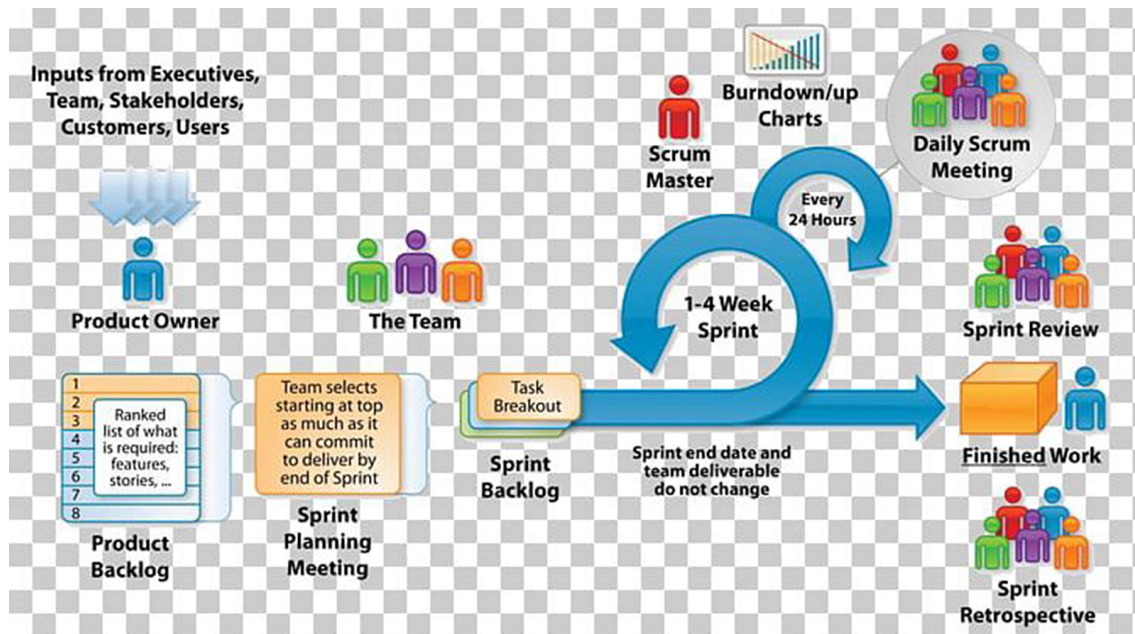


Agile Development

Scrum Model

Scrum is another agile process framework. It focuses on delivering the business value in minimal time. With this model, the most important feature is the ability to work with changing requirements. It does not expect to have all the requirements at the start of the project. It helps the team to learn and evolve as the project progresses.

Scrum can be applied to any type of teamwork and can be thought of, as a process management framework and a subset of the agile model. The main targets of this framework are accountability, teamwork, and repetitive progress.



Scrum

Prototyping

You were briefed on prototyping in the spiral model. However, in this model, prototypes will be used. Prototypes are not required to function perfectly. It should demonstrate the basic functionalities and make sense to the customer. Once approved, the SDLC continues. This is best-suited for emerging or bleeding-edge technologies so that it can be demonstrated as a prototype.

DevOps

DevOps is a new kind of a new era of software development as it is not exactly following an SDLC path that you are aware of. DevOps emerged in two trends. Those are agile and lean practices. It emphasizes the value of collaboration between the developers and operations teams in all stages. The changes are more fluid, while the risks are reduced.

Application Lifecycle Management

This is a broad concept of integrating the SDLC, DevOps, Portfolio Management, and the Service desk.

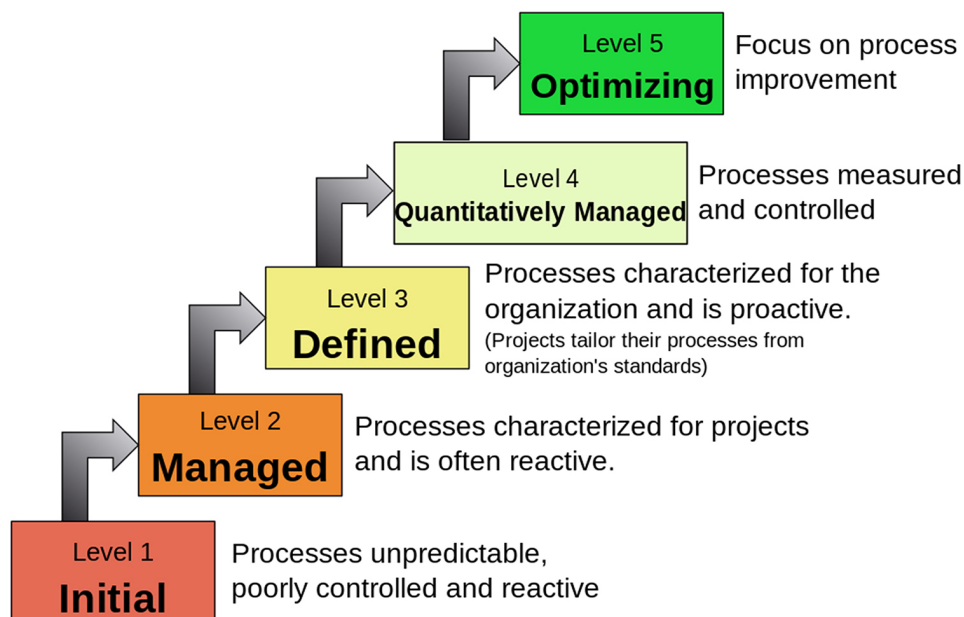
Maturity Models

These models are reference models of maturity practices. An example would be the Capability Maturity Model (CMM). This model brings proactivity by bringing more reliability and predictability. It also enhances scheduling and quality management to reduce potential defects.

CMM does not define the processes. Instead, it is a collection of best practices. The successor of the CMM model is the Capability Maturity Model Integration (CMMI). This greatly optimizes the development process.

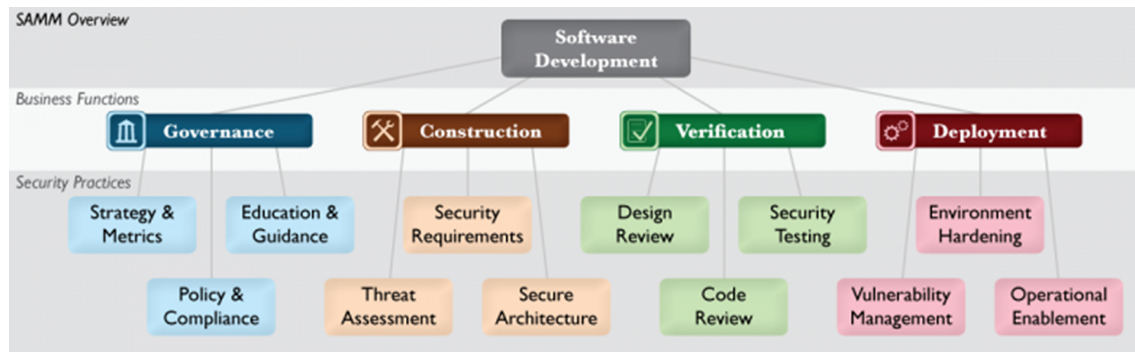
CMMI has broken down organizational maturity into five levels. The last level is the *optimizing* level. Reaching this level is the main goal of CMMI. Once it is reached, an organization can focus on maintaining it and improving it continuously. The five maturity levels are as follows.

Characteristics of the Maturity levels



Software Assurance Maturity Model (SAMM)

SAMM is an opensource model developed as a tool to assist in implementing a software security strategy. It is also known as the OpenSAMM and is part of OWASP.



OWASP SAMM Model

OpenSAMM Maturity Levels

1. Level 0: Unfulfilled practices
2. Level 1: Initial understanding – ad-hoc provisioning
3. Level 2: Enhancing efficiency and effectiveness
4. Level 3: Comprehensive mastery

Operation and Maintenance

The operation and maintenance phase is the last phase of the SDLC. It comprises activities such as support, updating/upgrading, and maintaining the quality of the product.

Change Management

Change management is a common practice in the field of software development. The dynamic nature of the business, as well as hardware, operating systems, and other technologies, raise rapid change requirements. This is where a change management strategy is required. A well-planned, documented, and the revised plan is crucial to managing the changes while

eliminating the disruptions to planned development, testing, and release activities.

Change management requires a feasibility assessment before initiating. In this study, the team should focus on the current stance, current capabilities, risk, and security. Since there will be a specific timeframe, the planning must incorporate a feasible schedule.

Integrated Product Team

In a development environment, multiple teams are collaborating to deliver a high-quality product in an appropriate timeframe. Such teams have specific roles to play, and communication and collaboration in a time-sensitive manner are vital to the project. You were introduced to DevOps and the application management lifecycle, agile, and scrum. All these models and frameworks aid the integration of product teams.

8.2 Identify and Apply Security Controls in Development Environments

In this section, we will be looking at code protection, code repositories, and intellectual property rights. Additionally, safeguarding the development environment with a multilayer risk mitigation strategy is discussed.

Security of the Software Environment

A complete organization development environment comprises of development platforms and integrated development environments (IDEs), application and web servers, and databases. There may be other instances where the involvement is hardware and robotics. This entire operation has areas to secure and ensure code security is intact.

Security Weaknesses and Vulnerabilities at the Source-Code Level

In reality, this is the most important part of all. Most of the vulnerabilities and exploits occur due to poor coding practices and integration. There are specific guidelines to write secure code. If the code is not handled before the modular level, you are creating and carrying vulnerabilities. This is also the same when it comes to web coding and database access. Lack of input validation is another common mistake. Therefore, reviewing the code and

eliminating the issues assures quality from the ground up. Otherwise, if you start to patch, it can be difficult even to find where to look for.

Configuration Management as an Aspect of Secure Coding

Configuration management is another aspect of software lifecycle management. Configuration stores can be managed together through version controlling and a central repository. There must be proper documentation to keep the configurations and changes recorded.

Security of Code Repositories

Code repositories can be the main target of an attacker to poison the software. Therefore, the internal repositories must stay isolated from the internet. Separate repositories can be managed to perform the development and release. The integrity of the code is the main goal of safeguarding the repositories. When an organization hires outside parties, extra precautions must be taken. If remote development is happening, the developers and engineers must utilize enterprise-grade VPN, RDS, or SSH protocols to connect to the office and collaborate.

Security of Application Programming Interface (API)

APIs interconnect or integrate third-party systems to the internal systems. API integration is another crucial aspect of software development. To handle security issues with APIs, different security concepts exist, such as provisioned services. The following methods exist.

- Authentication and authorization
- Encryption and digital signature
- Tokens
- Quotas and throttling
- API gateways – i.e., payment gateways
- Vulnerability practices

There are guidelines specifically for the REST and SOAP APIs. These guidelines must be followed to eliminate the potentials during the integration process. API security comprises the API key, authentication (ID and key), and *OpenID Connect (OIDC)* .

8.3 Assess the Effectiveness of Software Security

Continuous assessment is the key to reveal the existing issues and to tighten the security program. It can validate the effectiveness of the controls. Therefore, applying routine checks is important.

Auditing and Logging of Changes

In multiple sections in the book, it is stressed that auditing is a critical requirement in revealing the hidden issues. Changes in a dynamic environment must be logged accurately. When changes are implemented and rolled out, there must be a process to measure the next stages. This is when the auditing comes handy. Most of the changes cannot be made on the fly. It must be recorded, studied, implement if possible or reduce if necessary, and follow up. The logging procedures let the team keep track of the issue and follow up timely.

Risk Analysis and Mitigation

As with any other field, the software engineering area also encounters risks. Taking risks is necessary during development. In fact, it must be identified, handled, and a release must fix the issue by applying proven mitigation techniques. You are already aware of the risk management and business continuity, and therefore, you must apply the same to identify and mitigate these risks as well.

8.4 Assess Security Impact of Acquired Software

To assess the security impact of acquired software, an organization has to perform an analysis. Either when developing or acquiring software, this is the requirement. Acquired software can bring vulnerabilities otherwise.

Even though there are secure development practices, unless an organization reaches the maturity level, it may not be able to adapt and practice it effectively. For instance, the methodologies developed by fewer maturity firms, in most cases, become counterproductive against more mature firms. These results may deviate the developers from attending the real security issue. Therefore, depending on the maturity level, there are several approaches identified as productive.

1. This method is suitable for organizations with less development expertise. They could simply use binary analysis or other basic tools to detect the vulnerabilities. Such analysis results in revealing flaws. It brings a certain level of security. However, these tools may not often understand the software they can. Also, it is not tuned to the codebase. Therefore, applying this to a software developed by an organization that follows a secure development process is not optimal.
2. In this method, software developed by applying a secure development process focuses on security artifacts from the product. The organization develops it to be able to assess their maturity. The artifacts will be public documentation on its secure development process, its vulnerability response, and guides to secure configuration and operation.
3. Relying on developer conformance - ISO/IEC 27034 series or IEC/ISA-62443.

8.5 Define and Apply Secure Coding Guidelines and Standards

This is the final chapter of the 8th domain and also the last chapter in this book. This chapter discusses technical approaches to applied security in coding.

Code security in the past was considered a procedure that occurs later in the process. This is, however, an outdated concept. An organization must be able to establish proper security in coding practices to ensure the SDLC stays healthy and reputable. There are tools and techniques for developers to ensure coding security. However, traditional code review is also important to reveal some as certain vulnerabilities cannot be found through automated tests.

Security Weaknesses and Vulnerabilities at the Source-Code Level

A security-minded developer always follows guidelines, standards, and procedures to establish a set of best practices and an overall strategy to secure the code. For instance, modular level tests reveal possible security gaps. Tools such as Static Application Security Testing (SAST) aid code

analyzing procedures to find security flaws. A good example is the SAST tools provided by OWASP. It can find buffer overflows, injections, and XSS vulnerabilities. Furthermore, these tools can be integrated with multiple development platforms. However, these tools have certain false-positive rates, and therefore, a layered approach is required, including manual code inspection.

There are other new approaches, such as Interactive Application Security Testing (IAST). It is an enhanced version of SAST. The advantages of IAST tools are the ability to seamlessly integrate with new platforms and environments, faster processing, and highly accurate results.

Security of Application Programming Interfaces (APIs)

APIs are also vulnerable and prone to security threats. One of the most common is a perimeter attack. These are logical attacks. For instance, if there is a weakness in data validation, an attacker can gain the advantage. Therefore, data validation is an important mitigation technique.

The next possible attack type is the attack on the API key. A stolen key can result in identity attacks. Therefore, it must be secure as well as prevent leakages. Furthermore, attacks may occur when communication occurs between two devices. This is a crucial step to mitigate MitM attacks by enforcing the use of transport layer security and certificates.

At present, there are many security platforms such as Apigee by Google, API Connect by IBM, 3Scale by Red Hat, Amazon API Gateway, Azure API by Microsoft, SAP API Management, and others. These are the top-level and secure enterprise gateway examples. You may also use integration platforms such as Zapier.

Finally, we will be looking at some secure coding practices that an organization can use.

- Cryptography and encryption
- Communication security
- Code - best practices including compiler logging and debugging
- Database security - best practices

- Error handling and logging with auditing
- File handling – best practices
- Information protection – safeguarding practices
- Installer security
- Memory management and security
- Secure authentication and access control
- System-level security

For more information on best practices on coding and web, please visit https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide

Conclusion

You just completed all the eight domains in the CISSP CBK. I hope you have found relevant and appealing content, practical guidance, resources, and enhance your knowledge and competency. I also advise you to obtain all the possible resources to gain knowledge. This book is intended to get you ready to gain adequate knowledge in CISSP CBK competitively. In the end, you should be able to apply your knowledge in your daily tasks as a professional and get yourself ready for the examination.

If you are willing to sit for the examination, you must have a proper plan. As a start, register at least two months before and during the period, use your off days as much as possible, and study as hard as you can.

There are many CISSP study groups that you can find on the internet. Nowadays, there are many WhatsApp groups that you can join and share your knowledge and find answers to difficult questions. Furthermore, there are many other publications, video training and guides, security blogs, Facebook groups, exam simulations, past-papers, and many other resources that you can utilize to pass your examinations. Attending seminars and workshops will be another great way to gain knowledge. Nowadays, there are webinars rather than traditional seminars in which you can participate effortlessly.

Doing past paper questions and exam simulations are highly important. Since you get a limited time, you need to adjust your speed and thinking patterns.

On the day before the examination, spend a relaxing day, and have a good night's sleep. Before going to the exam center, have a good meal as the examination is either 3 hours or more depending on the method you selected. You should bring drinks and snacks along with your identity card, registration information, and don't forget to add emergency medicine to your list. Do not take mobile devices and any written pieces with you by any means. During the exam, take enough breaks and keep yourself hydrated and nourished.

If you find the book useful, I would love to hear your feedback. No matter whether you have critics or suggestions, it will help motivationally as well as technically to improve the content and style.

I wish you the best of luck in your CISSP path.

If you are willing to find Flashcards, you can obtain it from <https://enroll.isc2.org/product?catalog=CISSP-FC>

All the relevant information about the examination can be found by visiting <https://www.isc2.org/Certifications/CISSP>