(ISC)²

Chapter 1 Resource

Security Principles

Chapter Summary

In this chapter, we covered security principles, starting with concepts of information assurance. We highlighted the CIA triad as the primary components of information assurance. The "C" stands for confidentiality; we must protect the data that needs protection and prevent access to unauthorized individuals. The "I" represents integrity; we must ensure the data has not been altered in an unauthorized manner. The "A" symbolizes availability; we must make sure data is accessible to authorized users when and where it is needed, and in the form and format that is required. We also discussed the importance of privacy, authentication, non-repudiation, and authorization.

You explored the safeguards and countermeasures prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information. By applying risk management, we were able to assess and prioritize the risks (asset vulnerabilities that can be exploited by threats) to an organization. An organization can decide whether to accept the risk (ignoring the risks and continuing risky activities), avoid the risk (ceasing the risky activity to remove the likelihood that an event will occur), mitigate the risk (taking action to prevent or reduce the impact of an event), or transfer the risk (passing risk to a third party).

You then learned about three types of security controls: physical, technical and administrative. They act as safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information. The implementation of security controls should reduce risk, hopefully to an acceptable level. Physical controls address process-based security needs using physical hardware devices, such as a badge reader, architectural features of buildings and facilities, and specific security actions taken by people. Technical controls (also called logical controls) are security controls that computer systems and networks directly implement. Administrative controls (also known as managerial controls) are directives, guidelines or advisories aimed at the people within the organization.

You were then introduced to organizational security roles and governance, the policies and procedures that shape organizational management and drive decision-making. As discussed, we typically derive procedures from policies, policies from standards, standards from regulations. Regulations are commonly issued in the form of laws, usually from government (not to be confused with governance) and typically carry financial penalties for noncompliance. Standards are often used by governance teams to provide a framework to introduce policies and procedures in support of regulations. Policies are put in place by organizational governance, such as executive management, to provide guidance in all activities to ensure that the organization supports industry standards and regulations. Procedures are the detailed steps to complete a task that support departmental or organizational policies.

Finally, we covered the (ISC)² Code of Ethics, which members of the organization commit to fully support. Bottom line, we must act legally and ethically in the field of cybersecurity.

Module Names

Module 1: Understand the Security Concepts of Information Assurance

Module 2: Understand the Risk Management Process

Module 3: Understand Security Controls

Module 4: Understand Governance Elements

Module 5: Understand (ISC)² Code of Ethics

Chapter to Domain Mapping

Module Number	Module Title	Domains
1	Understand the Security Concepts of Information Assurance	1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5, 1.1.6
2	Understand the Risk Management Process	1.2.1, 1.2.2,
3	Understand Security Controls	1.3.1, 1.3.2, 1.3.3
4	Understand Governance Elements	1.5.1, 1.5.2, 1.5.3, 1.5.4
5	Understand (ISC)² Code of Ethics	1.4.1

Learning Objectives

After completing this chapter, the participant will be able to:

- Discuss the foundational concepts of cybersecurity principles.
- Recognize foundational security concepts of information assurance.
- Define risk management terminology and summarize the process.
- Relate risk management to personal or professional practices.
- Classify types of security controls.
- Distinguish between policies, procedures, standards, regulations and laws.
- Demonstrate the relationship among governance elements.
- Analyze appropriate outcomes according to the canons of the (ISC)² Code of Ethics when given examples.
- Practice the terminology and review security principles.

Chapter Takeaways

Module 1: Understand the Security Concepts of Information Assurance

CIA Triad:

- Confidentiality: Protect the data that needs protection and prevent access to unauthorized individuals.
- Integrity: Ensure the data has not been altered in an unauthorized manner.
- Availability: Ensure data is accessible to authorized users when and where it is needed, and in the form and format that is required.

Module 2: Understand the Risk Management Process

In the context of cybersecurity, typical threat actors include the following:

- Insiders (either deliberately, by simple human error, or by gross incompetence)
- Outside individuals or informal groups (either planned or opportunistic, discovering vulnerability)
- Formal entities that are nonpolitical (such as business competitors and cybercriminals)
- Formal entities that are political (such as terrorists, nation-states, and hacktivists)
- Intelligence or information gatherers (could be any of the above).
- Technology (such as free-running bots and artificial intelligence, which could be part of any of the above)

Risk Identification:

- Identify risk to communicate it clearly.
- Employees at all levels of the organization are responsible for identifying risk.
- Identify risk to protect against it.

Risk Assessment:

- The process of identifying, estimating and prioritizing risks to an organization's:
  - Operations (including its mission, functions, image and reputation)
  - Assets
  - Individuals
  - Other organizations
  - Even the nation
- Should result in aligning (or associating) each identified risk resulting from the operation of an information system with the goals, objectives, assets or processes

Risk Treatment:

- Accept the risk—Risk acceptance is taking no action to reduce the likelihood of a risk occurring.
- Avoid the risk—Risk avoidance is the decision to attempt to eliminate the risk entirely.
- Reduce (mitigate) the risk—Risk mitigation is the most common type of risk management and includes taking actions to prevent or reduce the possibility of a risk event or its impact.
- Transfer or share the risk—Risk transference is the practice of passing the risk to another party, who will accept the financial impact of the harm resulting from a risk being realized in exchange for payment.

Chapter Takeaways

Module 3: Understand Security Controls

Security Controls:

- Physical controls: physical hardware devices, such as a badge reader, architectural features of buildings and facilities that address process-based security needs.
- Technical controls (also called logical controls): security controls that computer systems and networks directly implement.
- Administrative controls (also known as managerial controls): directives, guidelines or advisories aimed at the people within the organization.

Module 4: Understand Governance Elements

Governance Elements:

- Procedures: the detailed steps to complete a task that support departmental or organizational policies.
- Policies: put in place by organizational governance, such as executive management, to provide guidance to all activities to ensure that the organization supports industry standards and regulations.
- Standards: often used by governance teams to provide a framework to introduce policies and procedures in support of regulations.
- Regulations: commonly issued in the form of laws, usually from government (not to be confused with governance) and typically carry financial penalties for non-compliance.

Module 5: Understand (ISC)² Code of Ethics

(ISC)² Code of Ethics Preamble:

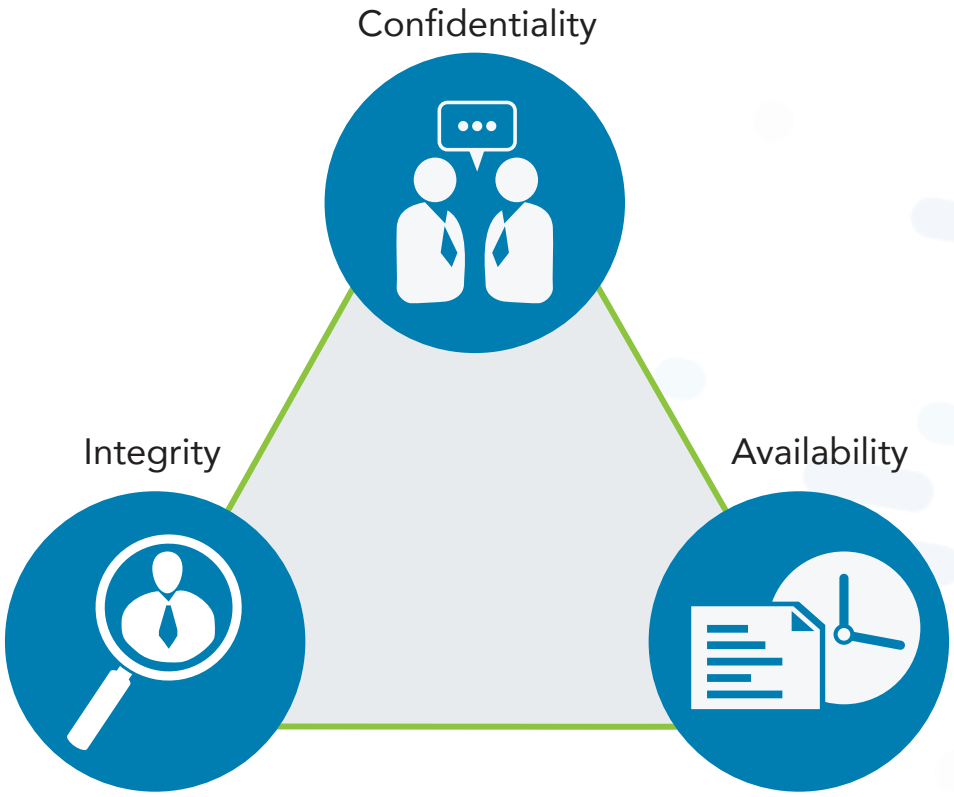
- The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

The (ISC)² member is expected to do the following:

- 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 principles.

Graphics

CIA Triad



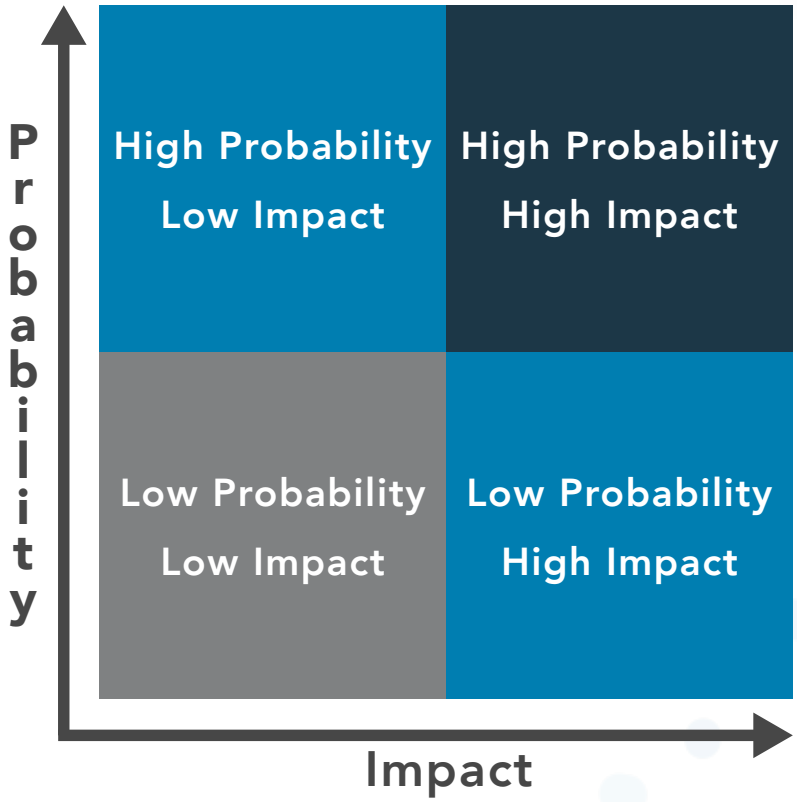
We must strive to provide information assurance, and these primary components help make information assurance possible: confidentiality, integrity and availability.

Confidentiality: protect the data that needs protection and permit access to authorized individuals while preventing access to unauthorized individuals.

Integrity: ensure the data has not been altered in an unauthorized manner.

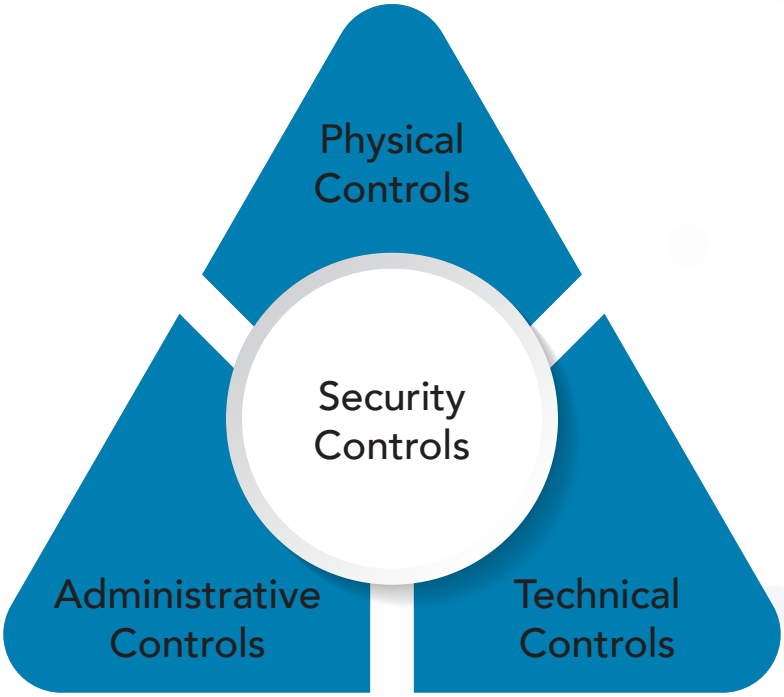
Availability: ensure the data is accessible to authorized users when and where it is needed, and in the form and format that is required.

Prioritizing Risk



You can use this simple probability and impact model to determine the level of risk and therefore prioritize risk. You can assign numbers to the level of probability and impact. For example, a risk with a high probability and high impact can be represented by a 1, low probability and high impact a 2, high probability and low impact a 3, and low probability and low impact a 4. This would put the risks in priority order, with 1s being your first priority and 4s being your last priority.

Security Controls



Physical controls: physical hardware devices, such as a badge reader, architectural features of buildings and facilities that address process-based security needs.

Technical controls (also called logical controls): security controls that computer systems and networks directly implement.

Administrative controls (also known as managerial controls): directives, guidelines or advisories aimed at the people within the organization.

Formulas and Calculations

Level of Risk = Probability + Impact

Chapter Terms and Definitions

Adequate Security

Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of information. Source: OMB Circular A-130

Administrative Controls

Controls implemented through policy and procedures. Examples include access control processes and requiring multiple personnel to conduct a specific operation. Administrative controls in modern environments are often enforced in conjunction with physical and/or technical controls, such as an access-granting policy for new users that requires login and approval by the hiring manager.

Artificial Intelligence

The ability of computers and robots to simulate human intelligence and behavior.

Asset

Anything of value that is owned by an organization. Assets include both tangible items such as information systems and physical property and intangible assets such as intellectual property.

Authentication

Access control process validating that the identity being claimed by a user or entity is known to the system, by comparing one (single-factor or SFA) or more (multi-factor authentication or MFA) factors of identification.

Authorization

The right or a permission that is granted to a system entity to access a system resource. NIST 800-82 Rev.2

Availability

Ensuring timely and reliable access to and use of information by authorized users.

Baseline

A documented, lowest level of security configuration allowed by a standard or organization.

Biometric

Biological characteristics of an individual, such as a fingerprint, hand geometry, voice, or iris patterns.

Bot

Malicious code that acts like a remotely controlled "robot" for an attacker, with other Trojan and worm capabilities.

Classified or Sensitive Information

Information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status and classification level when in documentary form.

Confidentiality

The characteristic of data or information when it is not made available or disclosed to unauthorized persons or processes. NIST 800-66

Criticality

A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. NIST SP 800-60 Vol. 1, Rev. 1

Data Integrity

The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing and while in transit. Source: NIST SP 800-27 Rev A

Encryption

The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.

General Data Protection Regulation (GDPR)

In 2016, the European Union passed comprehensive legislation that addresses personal privacy, deeming it an individual human right.

Governance

The process of how an organization is managed; usually includes all aspects of how decisions are made for that organization, such as policies, roles and procedures the organization uses to make those decisions.

Health Insurance Portability and Accountability Act (HIPAA)

This U.S. federal law is the most important healthcare information regulation in the United States. It directs the adoption of national standards for electronic healthcare transactions while protecting the privacy of individual's health information. Other provisions address fraud reduction, protections for individuals with health insurance and a wide range of other healthcare-related activities. Est. 1996.

Impact

The magnitude of harm that could be caused by a threat's exercise of a vulnerability.

Information Security Risk

The potential adverse impacts to an organization's operations (including its mission, functions and image and reputation), assets, individuals, other organizations, and even the nation, which results from the **possibility** of unauthorized access, use, disclosure, disruption, modification or destruction of information and/or information systems.

Institute of Electrical and Electronics Engineers

IEEE is a professional organization that sets standards for telecommunications, computer engineering and similar disciplines.

Integrity

The property of information whereby it is recorded, used and maintained in a way that ensures its completeness, accuracy, internal consistency and usefulness for a stated purpose.

International Organization of Standards (ISO)

The ISO develops voluntary international standards in collaboration with its partners in international standardization, the International Electro-technical Commission (IEC) and the International Telecommunication Union (ITU), particularly in the field of information and communication technologies.

Internet Engineering Task Force (IETF)

The internet standards organization, made up of network designers, operators, vendors and researchers, that defines protocol standards (e.g., IP, TCP, DNS) through a process of collaboration and consensus. Source: NIST SP 1800-16B

Likelihood

The probability that a potential vulnerability may be exercised within the construct of the associated threat environment.

Likelihood of Occurrence

A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or set of vulnerabilities.

Multi-Factor Authentication

Using two or more distinct instances of the three factors of authentication (something you know, something you have, something you are) for identity verification.

National Institutes of Standards and Technology (NIST)

The NIST is part of the U.S. Department of Commerce and addresses the measurement infrastructure within science and technology efforts within the U.S. federal government. NIST sets standards in a number of areas, including information security within the Computer Security Resource Center of the Computer Security Divisions.

Non-repudiation

The inability to deny taking an action such as creating information, approving information and sending or receiving a message.

Personally Identifiable Information (PII)

The National Institute of Standards and Technology, known as NIST, in its Special Publication 800-122 defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information."

Physical Controls

Controls implemented through a tangible mechanism. Examples include walls, fences, guards, locks, etc. In modern organizations, many physical control systems are linked to technical/logical systems, such as badge readers connected to door locks.

Privacy

The right of an individual to control the distribution of information about themselves.

Probability

The chances, or likelihood, that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. Source: NIST SP 800-30 Rev. 1

Protected Health Information (PHI)

Information regarding health status, the provision of healthcare or payment for healthcare as defined in HIPAA (Health Insurance Portability and Accountability Act).

Qualitative Risk Analysis

A method for risk analysis that is based on the assignment of a descriptor such as low, medium or high. Source: NISTIR 8286

Quantitative Risk Analysis

A method for risk analysis where numerical values are assigned to both impact and likelihood based on statistical probabilities and monetarized valuation of loss or gain. Source: NISTIR 8286

Risk

A possible event which can have a negative impact upon the organization.

Risk Acceptance

Determining that the potential benefits of a business function outweigh the possible risk impact/likelihood and performing that business function with no other action.

Risk Assessment

The process of identifying and analyzing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals and other organizations. The analysis performed as part of risk management which incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place.

Risk Avoidance

Determining that the impact and/or likelihood of a specific risk is too great to be offset by the potential benefits and not performing a certain business function because of that determination.

Risk Management

The process of identifying, evaluating and controlling threats, including all the phases of risk context (or frame), risk assessment, risk treatment and risk monitoring.

Risk Management Framework

A structured approach used to oversee and manage risk for an enterprise. Source: CNSSI 4009

Risk Mitigation

Putting security controls in place to reduce the possible impact and/or likelihood of a specific risk.

Risk Tolerance

The level of risk an entity is willing to assume in order to achieve a potential desired result. Source: NIST SP 800-32. Risk threshold, risk appetite and acceptable risk are also terms used synonymously with risk tolerance.

Risk Transference

Paying an external party to accept the financial impact of a given risk.

Risk Treatment

The determination of the best way to address an identified risk.

Security Controls

The management, operational and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information. Source: FIPS PUB 199

Sensitivity

A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. Source: NIST SP 800-60 Vol 1 Rev 1

Single-Factor Authentication

Use of just one of the three available factors (something you know, something you have, something you are) to carry out the authentication process being requested.

State

The condition an entity is in at a point in time.

System Integrity

The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. Source: NIST SP 800-27 Rev. A

Technical Controls

Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations or the nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service. Source: NIST SP 800-30 Rev 1

Threat Actor

An individual or a group that attempts to exploit vulnerabilities to cause or force a threat to occur.

Threat Vector

The means by which a threat actor carries out their objectives.

Token

A physical object a user possesses and controls that is used to authenticate the user's identity. NISTIR 7711

Vulnerability

Weakness in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source. Source: NIST SP 800-30 Rev 1

Chapter 2 Resource

Incident Response (IR), Business Continuity (BC) and Disaster Recovery (DR)

Chapter Summary

This chapter focused mainly on the availability part of the CIA triad and the importance of maintaining availability for business operations. Maintaining business operations during or after an incident, event, breach, intrusion, exploit or zero day is accomplished through the implementation of Incident Response (IR), Business Continuity (BC), and/or Disaster Recovery (DR) plans. While these three plans may seem to overlap in scope, they are three distinct plans that are vital to the survival of any organization facing out of the ordinary operating conditions. Here are the primary things to remember from this chapter:

First, the Incident Response plan responds to abnormal operating conditions to keep the business operating. The four main components of Incident Response are: Preparation; Detection and Analysis; Containment, Eradication and Recovery; and Post-Incident Activity. Incident Response teams are typically a cross-functional group of individuals who represent the management, technical and functional areas of responsibility most directly impacted by a security incident. The team is trained on incident response and the organization's incident response plan. When an incident occurs, the team is responsible for determining the amount and scope of damage and whether any confidential information was compromised, implementing recovery procedures to restore security and recover from incident-related damage, and supervising implementation of future measures to improve security and prevent recurrence of the incident.

Second, the Business Continuity plan is designed to keep the organization operating through the crisis. Components of the Business Continuity plan include details about how and when to enact the plan and notification systems and call trees for alerting the team members and organizational associates that the plan has been enacted. In addition, it includes contact numbers for contacting critical third-party partners, external emergency providers, vendors and customers. The plan provides the team with immediate response procedures and checklists and guidance for management.

Finally, if both the Incident Response and Business Continuity plans fail, the Disaster Recovery plan is activated to return operations to normal as quickly as possible. The Disaster Recovery plan may include the following components: executive summary providing a high-level overview of the plan, department-specific plans, technical guides for IT personnel responsible for implementing and maintaining critical backup systems, full copies of the plan for critical disaster recovery team members, and checklists for certain individuals.

Module Names

Module 1: Understand Incident Response (IR)

Module 2: Understand Business Continuity (BC)

Module 3: Understand Disaster Recovery (DR)

Chapter to Domain Mapping

Module Number	Module Title	Domains
1	Understand Incident Response (IR)	2.3, 2.3.1, 2.3.2, 2.3.3
2	Understand Business Continuity (BC)	2.1, 2.1.1, 2.1.2, 2.1.3
3	Understand Disaster Recovery (DR)	2.2, 2.2.1, 2.2.2, 2.2.3

Learning Objectives

After completing this chapter, the participant will be able to:

- Explain how organizations respond to, recover from and continue to operate during unplanned disruptions
- Recall the terms and components of incident response
- Summarize the components of a business continuity plan
- Identify the components of disaster recovery
- Practice the terminology of and review business continuity, disaster recovery and incident response concepts

Chapter Takeaways

Module 1: Understand Incident Response (IR)

Incident Response Terminology:

- Breach
- Event
- Exploit
- Incident
- Intrusion
- Threat
- Vulnerability
- Zero Day

Four main components of Incident Response are:

- Preparation
- Detection and Analysis
- Containment, Eradication and Recovery
- Post-Incident Activity

Three possible models for an Incident Response Team (IRT):

- Leveraged
- Dedicated
- Hybrid

Module 2: Understand Business Continuity (BC)

Components of a Business Continuity (BC) plan include:

- List of the BCP team members, including multiple contact methods and backup members
- Immediate response procedures and checklists (security and safety procedures, fire suppression procedures, notification of appropriate emergency-response agencies, etc.)
- Notification systems and call trees for alerting personnel that the BCP is being enacted
- Guidance for management, including designation of authority for specific managers
- How/when to enact the plan
- Contact numbers for critical members of the supply chain (vendors, customers, possible external emergency providers, third-party partners)
- How/when to enact the plan
- Contact numbers for critical members of the supply chain (vendors, customers, possible external emergency providers, third-party partners)

Chapter Takeaways (Continued)

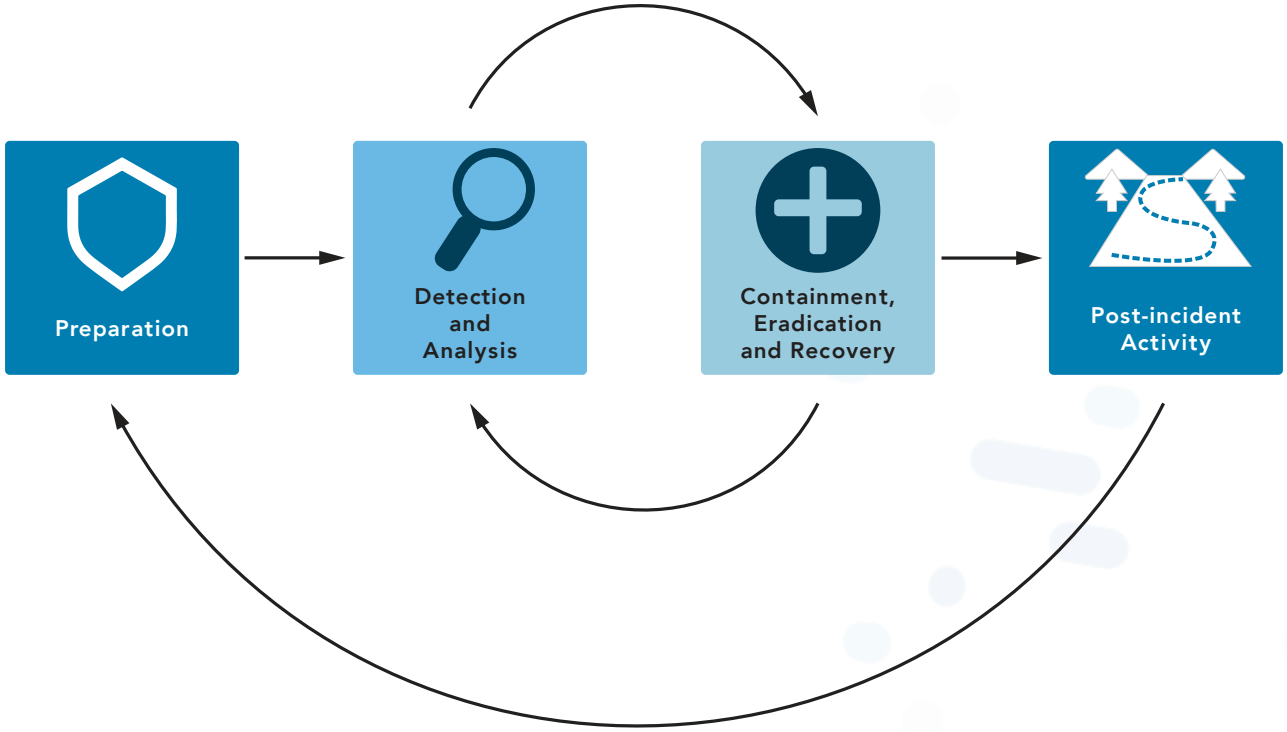
Module 3: Understand Disaster Recovery (DR)

Five possible components to include in a Disaster Recovery (DR) plan:

1. Executive summary providing a high-level overview of the plan
2. Department-specific plans
3. Technical guides for IT personnel responsible for implementing and maintaining critical backup systems
4. Full copies of the plan for critical disaster recovery team members
5. Checklists for certain individuals

Graphics

Components of an Incident Response Plan



Knowing the components of and their relationship to each other will help you build and follow an Incident Response Plan.

Chapter Terms and Definitions

Adverse Events

Events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, defacement of a web page or execution of malicious code that destroys data.

Breach

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for other than an authorized purpose. Source: NIST SP 800-53 Rev. 5

Business Continuity (BC)

Actions, processes and tools for ensuring an organization can continue critical operations during a contingency.

Business Continuity Plan (BCP)

The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

Business Impact Analysis (BIA)

An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. NIST SP 800-34 Rev. 1

Disaster Recovery (DR)

In information systems terms, the activities necessary to restore IT and communications services to an organization during and after an outage, disruption or disturbance of any kind or scale.

Disaster Recovery Plan (DRP)

The processes, policies and procedures related to preparing for recovery or continuation of an organization's critical business functions, technology infrastructure, systems and applications after the organization experiences a disaster. A disaster is when an organization's critical business function(s) cannot be performed at an acceptable level within a predetermined period following a disruption.

Event

Any observable occurrence in a network or system. Source: NIST SP 800-61 Rev 2

Exploit

A particular attack. It is named this way because these attacks exploit system vulnerabilities.

Incident

An event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits.

Incident Handling

The mitigation of violations of security policies and recommended practices. Source: NIST SP 800-61 Rev 2

Incident Response (IR)

The mitigation of violations of security policies and recommended practices. Source: NIST SP 800-61 Rev 2

Incident Response Plan (IRP)

The documentation of a predetermined set of instructions or procedures to detect, respond to and limit consequences of a malicious cyberattack against an organization's information systems(s). Source: NIST SP 800-34 Rev 1

Intrusion

A security event, or combination of security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization. Source: IETF RFC 4949 Ver 2

Security Operations Center

A centralized organizational function fulfilled by an information security team that monitors, detects and analyzes events on the network or system to prevent and resolve issues before they result in business disruptions.

Vulnerability

Weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source. Source: NIST SP 800-128.

Zero Day

A previously unknown system vulnerability with the potential of exploitation without risk of detection or prevention because it does not, in general, fit recognized patterns, signatures or methods.

Chapter 3 Resource

Access Control Concepts

Chapter Summary

In this chapter, we described who gets access to what, why access is necessary, and how that access is managed. Access is based on three elements: subjects (who), objects (what), and rules (how and when). Trustworthiness and the need for access also determine access.

We also discussed defense in depth (an information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization) and how it applies to the types of access control (physical, logical/technical, and administrative) that every information security professional should be familiar with. At the same time, we stressed the importance of the Principle of Least Privilege (users should only have the minimum access necessary to accomplish their job).

We then discussed Privileged Access Management and how it relates to risk and the CIA Triad: it reduces risk by allowing admin privileges to be used only when needed, provides confidentiality by limiting the need for administrative access that is used during routine business, ensures integrity by only allowing authorized administrative access during approved activities, and confirms availability by providing administrative access when needed. We also differentiated between a Regular User Account and a Privileged User Account.

We further discussed segregation of duties, two-person integrity, and how users are provisioned, from being hired to being terminated. We then explored physical and logical access controls and how they are combined to strengthen the overall security of an organization. Physical access controls include security guards, fences, motion detectors, locked doors/gates, sealed windows, lights, cable protection, laptop locks, badges, swipe cards, guard dogs, cameras, mantraps/turnstiles and alarms. Logical access controls (also called technical controls) can be configuration settings or parameters stored as data, managed through a software graphical user interface (GUI), or they can be hardware settings done with switches, jumper plugs or other means.

We concluded the chapter discussing three logical access controls: DAC, MAC, and RBAC. Discretionary access control (DAC) is a specific type of access control policy that is controlled by the owner of the resource and enforced at the subject level over objects in an information system. A mandatory access control (MAC) policy is one that is uniformly enforced across all subjects and objects within the boundary of an information system. Role-based access control (RBAC), as the name suggests, sets up user permissions based on roles.

Module Names

Module 1: Understand Access Control Concepts

Module 2: Understand Physical Access Controls

Module 3: Understand Logical Access Controls

Chapter to Domain Mapping

Module Number	Module Title	Domains
1	Understand Access Control Concepts	3.1, 3.1.3, 3.1.5, 3.2, 3.2.1, 3.2.2, 3.2.5
2	Understand Physical Access Controls	3.1, 3.1.1, 3.1.2
3	Understand Logical Access Controls	3.2, 3.2.3, 3.2.4, 3.2.5

Learning Objectives

After completing this chapter, the participant will be able to:

- Select access controls that are appropriate in a given scenario.
- Relate access control concepts and processes to given scenarios.
- Compare various physical access controls.
- Describe logical access controls.
- Practice the terminology of access controls and review concepts of access controls.

Chapter Takeaways

Module 1: Understand Access Control Concepts

Access is based on three elements:

- Subjects (Who)
- Objects (What)
- Rules (How and When)

Defense in Depth

- An information security strategy that integrates people, technology and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
- Applies multiple countermeasures in a layered fashion to fulfill security objectives.
- Should be implemented to prevent or deter a cyberattack, but it cannot guarantee that an attack will not occur.

Privileged Access Management

- Reduces risk by allowing admin privileges to be used only when needed.
- Provides confidentiality by limiting the need for administrative access that is used during routine business.
- Ensures integrity by only allowing authorized administrative access during approved activities.
- Confirms availability by providing administrative access when needed.

How Users are Provisioned

- New employee – account created
- "Onboarding" – creating an account (or cloning a baseline account) for a new employee
- Changed position – account modified
- Temporary leave of absence – account disabled
- Separation of employment – account deleted
- "Offboarding" – deleting an account (or disabling then deleting an account) for a terminated employee

Chapter Takeaways (Continued)

Module 2: Understand Physical Access Controls

Examples of physical access controls:

- Security guards
- Fences
- Motion detectors
- Locked doors/gates
- Sealed windows
- Lights
- Cable protection
- Laptop locks
- Badges
- Swipe cards
- Guard dogs
- Cameras
- Mantraps/turnstiles
- Alarms

Log terminology:

- Log anomaly
- Log consolidation
- Log retention

Module 3: Understand Logical Access Controls

Logical access control types:

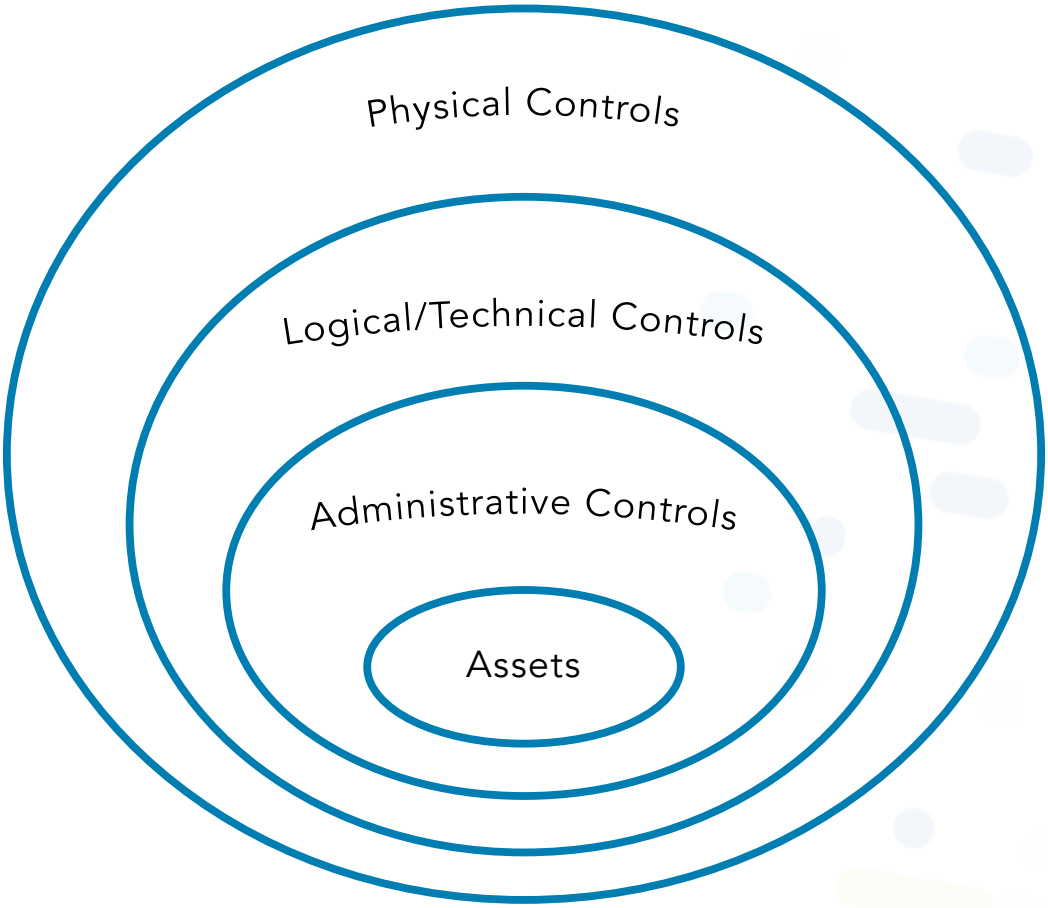
- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-based access control (RBAC)

Examples of logical access controls:

- Configuration settings or parameters stored as data, managed through a software graphical user interface (GUI)
- Hardware settings done with switches, jumper plugs or other means

Graphics

Defense in Depth



Chapter Terms and Definitions

Audit

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. NIST SP 1800-15B

Crime Prevention through Environmental Design (CPTED)

An architectural approach to the design of buildings and spaces which emphasizes passive features to reduce the likelihood of criminal activity.

Defense in Depth

Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. Source: NIST SP 800-53 Rev 4

Discretionary Access Control (DAC)

A certain amount of access control is left to the discretion of the object's owner, or anyone else who is authorized to control the object's access. The owner can determine who should have access rights to an object and what those rights should be. NIST SP 800-192

Encrypt

To protect private information by putting it into a form that can only be read by people who have permission to do so.

Firewalls

Devices that enforce administrative security policies by filtering incoming traffic based on a set of rules.

Insider Threat

An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. NIST SP 800-32

iOS

An operating system manufactured by Apple Inc. Used for mobile devices.

Layered Defense

The use of multiple controls arranged in series to provide several consecutive controls to protect an asset; also called defense in depth.

Linux

An operating system that is open source, making its source code legally available to end users.

Log Anomaly

A system irregularity that is identified when studying log entries which could represent events of interest for further surveillance.

Logging

Collecting and storing user activities in a log, which is a record of the events occurring within an organization's systems and networks. NIST SP 1800-25B.

Logical Access Control Systems

An automated system that controls an individual's ability to access one or more computer system resources, such as a workstation, network, application or database. A logical access control system requires the validation of an individual's identity through some mechanism, such as a PIN, card, biometric or other token. It has the capability to assign different access privileges to different individuals depending on their roles and responsibilities in an organization. NIST SP 800-53 Rev.5.

Mandatory Access Control

Access control that requires the system itself to manage access controls in accordance with the organization's security policies.

Mantrap

An entrance to a building or an area that requires people to pass through two doors with only one door opened at a time.

Object

Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object (by a subject) implies access to the information it contains. See subject. Source: NIST SP 800-53 Rev 4

Physical Access Controls

Controls implemented through a tangible mechanism. Examples include walls, fences, guards, locks, etc. In modern organizations, many physical control systems are linked to technical/logical systems, such as badge readers connected to door locks.

Principle of Least Privilege

The principle that users and programs should have only the minimum privileges necessary to complete their tasks. NIST SP 800-179

Privileged Account

An information system account with approved authorizations of a privileged user. NIST SP 800-53 Rev. 4

Ransomware

A type of malicious software that locks the computer screen or files, thus preventing or limiting a user from accessing their system and data until money is paid.

Role-based access control (RBAC)

An access control system that sets up user permissions based on roles.

Rule

An instruction developed to allow or deny access to a system by comparing the validated identity of the subject to an access control list.

Segregation of Duties

The practice of ensuring that an organizational process cannot be completed by a single person; forces collusion as a means to reduce insider threats. Also commonly known as Separation of Duties.

Subject

Generally an individual, process or device causing information to flow among objects or change to the system state. Source: NIST SP800-53 R4

Technical Controls

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.

Turnstile

A one-way spinning door or barrier that allows only one person at a time to enter a building or pass through an area.

Unix

An operating system used in software development.

User Provisioning

The process of creating, maintaining and deactivating user identities on a system.

(ISC)²

Chapter 4 Resource

Network Security

Chapter Summary

In this chapter, we covered computer networking and securing the network. A network is simply two or more computers linked together to share data, information or resources. There are many types of networks, such as LAN, WAN, WLAN and VPN, to name a few. Some of the devices found on a network can be hubs, switches, routers, firewalls, servers, endpoints (e.g., desktop computer, laptop, tablet, mobile phone, VOIP or any other end-user device). Other network terms you need to know and understand include ports, protocols, ethernet, Wi-Fi, IP address and MAC address.

The two models discussed in this chapter are OSI and TCP/IP. The OSI model has seven layers and the TCP/IP four. They both take the 1s and 0s from the physical or network interface layer, where the cables or Wi-Fi connect, to the Application Layer, where users interact with the data. The data traverses the network as packets, with headers or footers being added and removed accordingly as they get passed layer to layer. This helps route the data and ensures packets are not lost and remain together. IPv4 is slowly being phased out by IPv6 to improve security, improve quality of service and support more devices.

As mentioned, Wi-Fi has replaced many of our wired networks, and with its ease of use, it also brings security issues. Securing Wi-Fi, e.g., using WPA2, is very important.

We then learned about some of the attacks on a network, e.g., DoS/DDoS attacks, fragment attacks, oversized packet attacks, spoofing attacks, and man-in-the middle attacks. We also discussed the ports and protocols that connect the network and services that are used on networks, from physical ports, e.g., LAN port, that connect the wires, to logical ports, e.g., 80 or 443, that connect the protocols/services.

We then examined some possible threats to a network, including spoofing, DoS/DDoS, virus, worm, Trojan, on-path (man-in-the-middle) attack, and side-channel attack. The chapter went on to discuss how to identify threats, e.g., using IDS/NIDS/HIDS or SIEM, and prevent threats, e.g., using antivirus, scans, firewalls, or IPS/NIPS/HIPS. We discussed on-premises data centers and their requirements, e.g., power, HVAC, fire suppression, redundancy and MOU/MOA. We reviewed the cloud and its characteristics, to include service models: SaaS, IaaS and PaaS; and deployment models: public, private, community and hybrid. The importance of an MSP and SLA were also discussed.

Terminology for network design, to include network segmentation, e.g., microsegmentation and demilitarized zone (DMZ), virtual local area network (VLAN), virtual private network (VPN), defense in depth, zero trust and network access control, were described in great detail.

Module Names

Module 1: Understand Computer Networking

Module 2: Understand Network Threats and Attacks

Module 3: Understand Network Security Infrastructure

Chapter to Domain Mapping

Module Number	Module Title	Domains
1	Understand Computer Networking	4.1, 4.1.1, 4.1.2, 4.1.3
2	Understand Network Threats and Attacks	4.2, 4.2.1, 4.2.2, 4.2.3
3	Understand Network Security Infrastructure	4.3, 4.3.1, 4.3.2, 4.3.3

Learning Objectives

After completing this chapter, the participant will be able to:

- Explain the concepts of network security.
- Recognize common networking terms and models.
- Identify common protocols and ports and their secure counterparts.
- Identify types of network threats and attacks.
- Discuss common tools used to identify and prevent threats.
- Identify common data center terminology.
- Recognize common cloud service terminology.
- Identify secure network design terminology.
- Practice the terminology of and review network security concepts.

Chapter Takeaways

Module 1: Understand computer networking

Types of Computer Networks:

- LAN – Local Area Network
- WAN – Wide Area Network
- WLAN – Wireless Local Area Network
- VPN – Virtual Private Network
- EPN – Enterprise Private Network
- PAN – Personal Area Network
- CAN – Campus Area Network
- MAN – Metropolitan Area Network
- SAN – Storage Area Network
- SAN – System-Area Network
- POLAN – Passive Optical Local Area Network

Network Devices:

- Hubs
- Switches
- Routers
- Firewalls
- Servers
- Printers
- Fax Machines
- Gateways
- Repeaters
- Bridges
- Modems
- Access Points
- Endpoints (e.g., desktop computer, laptop, tablet, cellphone, VOIP, or any other end-user device)

Other Network Terms:

- Packet
- Port
- Protocol
- Ethernet
- Wi-Fi
- IP address
- MAC address

Network Models:

- OSI and TCP/IP

Chapter Takeaways

Module 1: Understand computer networking (continued)

IPv4 vs IPv6:

- IPv6 is a modernization of IPv4:
  - A much larger address field (support more devices)
  - Improved security
  - Improved quality of service (QoS)

Module 2: Understand network threats and attacks

Types of Network Attacks:

- DoS/DDoS
- Fragment
- Oversized Packet
- Spoofing
- Man-in-the-Middle
- Code/SQL Injection
- XSS (Cross Site Scripting)
- Privilege Escalation
- Insider Threat

Types of Network Threats:

- Spoofing
- DoS/DDoS
- Virus
- Worm
- Trojan
- On-Path (Man-in-the-Middle)
- Side-channel
- Phishing
- Rootkit
- Adware/Spyware
- Malware

Module 2: Understand network threats and attacks

Ports and Protocols:

Insecure Port	Protocol	Secure Alternative Port	Protocol
21 - FTP	File Transfer Protocol	22* - SFTP	Secure File Transfer Protocol
23 – Telnet	Telnet	22* - SSH	Secure Shell
25 – SMTP	Simple Mail Transfer Protocol	587 – SMTP	SMTP with TLS
37 – Time	Time Protocol	123 – NTP	Network Time Protocol
53 – DNS	Domain Name Service	853 - DoT	DNS over TLS (DoT)
80 – HTTP	HyperText Transfer Protocol	443 – HTTPS	HyperText Transfer Protocol (SSL/TLS)
143 - IMAP	Internet Message Access Protocol	993 – IMAP	IMAP for SSL/TLS
161/162 - SNMP	Simple Network Management Protocol	161/162 - SNMP	SNMPv3
445 – SMB	Server Message Block	2049 - NFS	Network File System
389 – LDAP	Lightweight Directory Access Protocol	636 - LDAPS	Lightweight Directory Access Protocol Secure

How we Identify Threats:

- IDS
- NIDS
- HIDS
- SIEM

How we Prevent Threats:

- Antivirus
- Scans
- Firewalls
- IPS
- NIPS
- HIPS

Module 3: Understand network security infrastructure

Requirements for a Data Center:

- Power
- HVAC
- Fire Suppression
- Redundancy
- MOU/MOA

Cloud Service Models:

- SaaS
- IaaS
- PaaS

Cloud Deployment Models:

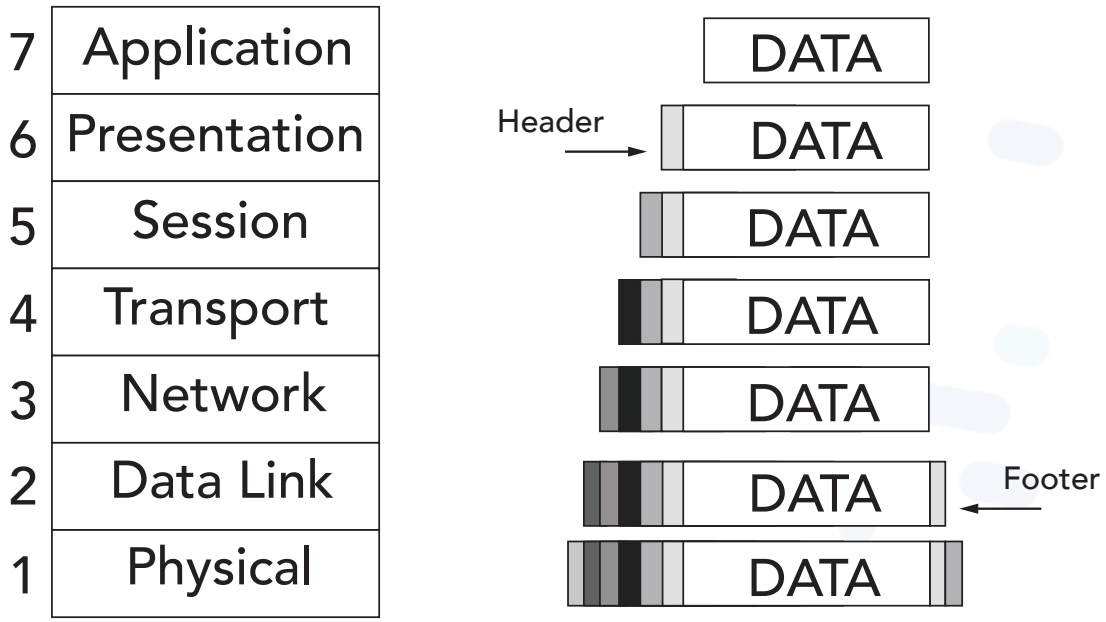
- Public
- Private
- Community
- Hybrid

Network Design Terminology:

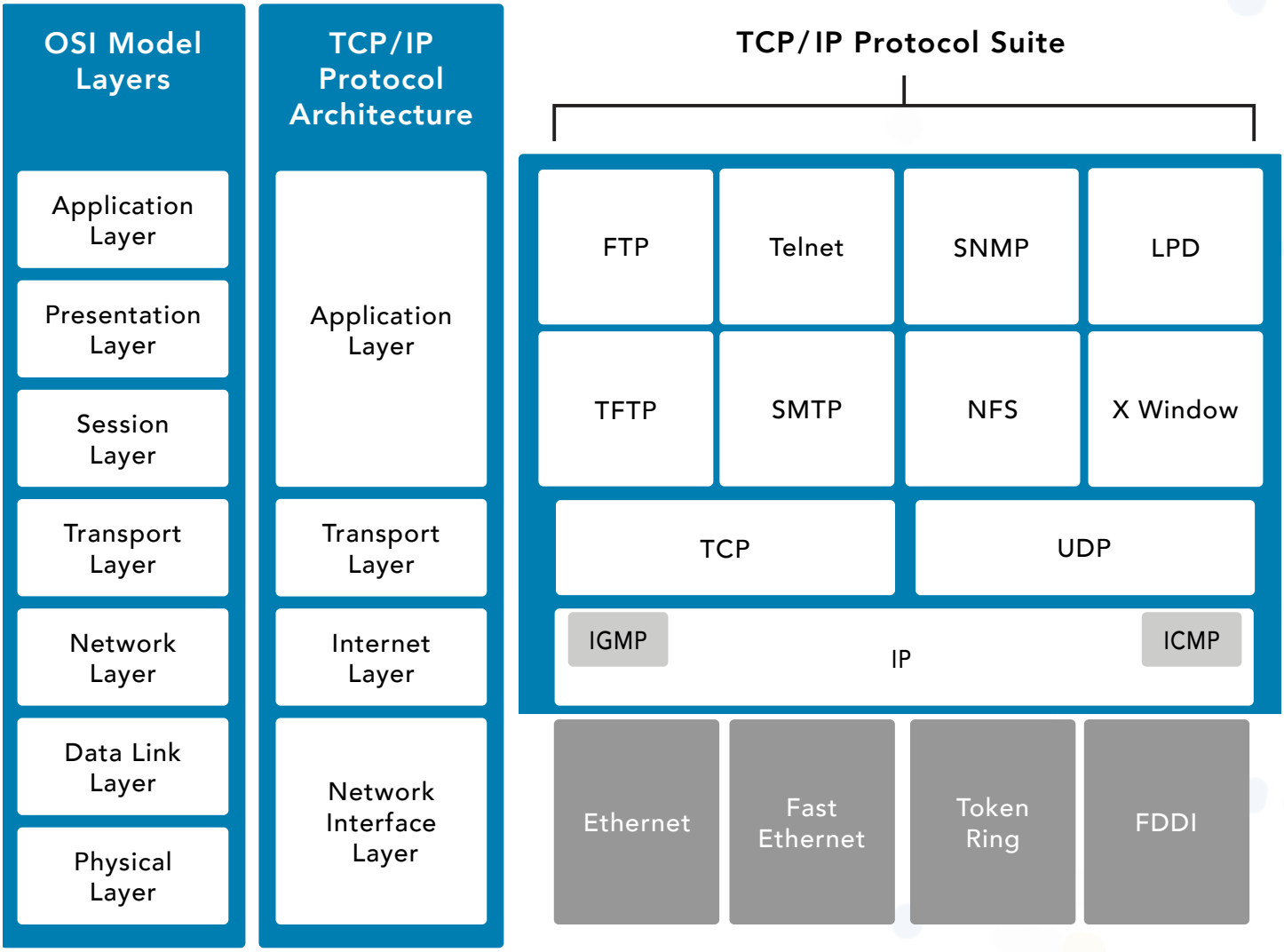
- Network Segmentation, e.g., microsegmentation and demilitarized zone (DMZ)
- Virtual Local Area Network (VLAN)
- Virtual Private Network (VPN)
- Defense in Depth
- Zero Trust
- Network Access Control

Graphics

Open Systems Interconnection (OSI) Model



Transmission Control Protocol/Internet Protocol (TCP/IP) Model



Chapter Terms and Definitions

Application programming interface (API)

A set of routines, standards, protocols, and tools for building software applications to access a web-based software application or web tool.

Bit

The most essential representation of data (zero or one) at Layer 1 of the Open Systems Interconnection (OSI) model.

Broadcast

Broadcast transmission is a one-to-many (one-to-everyone) form of sending internet traffic.

Byte

The byte is a unit of digital information that most commonly consists of eight bits.

Cloud computing

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST 800-145

Community cloud

A system in which the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. NIST 800-145

De-encapsulation

The opposite process of encapsulation, in which bundles of data are unpacked or revealed.

Denial-of-Service (DoS)

The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) Source: NIST SP 800-27 Rev A

Domain Name Service (DNS)

This acronym can be applied to three interrelated elements: a service, a physical server and a network protocol.

Encapsulation

Enforcement of data hiding and code hiding during all phases of software development and operational use. Bundling together data and methods is the process of encapsulation; its opposite process may be called unpacking, revealing, or using other terms. Also used to refer to taking any set of data and packaging it or hiding it in another data structure, as is common in network protocols and encryption.

Encryption

The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.

File Transfer Protocol (FTP)

The internet protocol (and program) used to transfer files between hosts.

Fragment attack

In a fragment attack, an attacker fragments traffic in such a way that a system is unable to put data packets back together.

Hardware

The physical parts of a computer and related devices.

Hybrid cloud

A combination of public cloud storage and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.

Infrastructure as a Service (IaaS)

The provider of the core computing, storage and network hardware and software that is the foundation upon which organizations can build and then deploy applications. IaaS is popular in the data center where software and servers are purchased as a fully outsourced service and usually billed on usage and how much of the resource is used.

Internet Control Message Protocol (ICMP)

An IP network protocol standardized by the Internet Engineering Task Force (IETF) through RFC 792 to determine if a particular service or host is available.

Internet Protocol (IPv4)

Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. CNSSI 4009-2015

Man-in-the-Middle

An attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them. Source: NISTIR 7711

Microsegmentation

Part of a zero-trust strategy that breaks LANs into very small, highly localized zones using firewalls or similar technologies. At the limit, this places firewall at every connection point.

Oversized Packet Attack

Purposely sending a network packet that is larger than expected or larger than can be handled by the receiving system, causing the receiving system to fail unexpectedly.

Packet

Representation of data at Layer 3 of the Open Systems Interconnection (OSI) model.

Payload

The primary action of a malicious code attack.

Payment Card Industry Data Security Standard (PCI DSS)

Security standards that apply to merchants and service providers who process credit or debit card transactions.

Platform as a Service (PaaS)

The web-authoring or application development middleware environment that allows applications to be built in the cloud before they're deployed as SaaS assets.

Private cloud

The phrase used to describe a cloud computing platform that is implemented within the corporate firewall, under the control of the IT department. A private cloud is designed to offer the same features and benefits of cloud systems, but removes a number of objections to the cloud computing model, including control over enterprise and customer data, worries about security, and issues connected to regulatory compliance.

Protocols

A set of rules (formats and procedures) to implement and control some type of association (that is, communication) between systems. NIST SP 800-82 Rev. 2

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. NIST SP 800-145

Simple Mail Transport Protocol (SMTP)

The standard communication protocol for sending and receiving emails between senders and receivers.

Software

Computer programs and associated data that may be dynamically written or modified during execution. NIST SP 80--37 Rev. 2

Software as a Service (SaaS)

The cloud customer uses the cloud provider's applications running within a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Derived from NIST 800-145

Spoofing

Faking the sending address of a transmission to gain illegal entry into a secure system. CNSSI 4009-2015

Transport Control Protocol/Internet Protocol (TCP/IP) Model

Internetworking protocol model created by the IETF, which specifies four layers of functionality: Link layer (physical communications), Internet Layer (network-to-network communication), Transport Layer (basic channels for connections and connectionless exchange of data between hosts), and Application Layer, where other protocols and user applications programs make use of network services.

VLAN

A virtual local area network (VLAN) is a logical group of workstations, servers, and network devices that appear to be on the same LAN despite their geographical distribution.

VPN

A virtual private network (VPN), built on top of existing networks, that can provide a secure communications mechanism for transmission between networks.

WLAN

A wireless area network (WLAN) is a group of computers and devices that are located in the same vicinity, forming a network based on radio transmissions rather than wired connections. A Wi-Fi network is a type of WLAN.

Zenmap

The graphical user interface (GUI) for the Nmap Security Scanner, an open-source application that scans networks to determine everything that is connected as well as other information.

Zero Trust

Removing the design belief that the network has any trusted space. Security is managed at each possible level, representing the most granular asset. Microsegmentation of workloads is a tool of the model.

Chapter 5 Resource

Security Operations

Chapter Summary

This chapter focused on the day-to-day, moment-by-moment, use of security controls and risk mitigation strategies in an organization. We discovered ways to secure data and the systems they reside on. Data (information) security as a process and discipline provides a structure for protecting the value of data as the organization creates, stores, shares, uses, modifies, archives and finally destroys that data (known as data handling). During data handling, an organization classifies (assigns data sensitivity levels), categorizes (determines type of data), labels (applies a name to the data), retains (determines how long to keep the data) and destroys (erases or destroys) the data.

A best practice for securing data is encrypting the data. We explored the process of encrypting data in plaintext with a key and algorithm to create ciphertext then using either the same key (symmetric) or a different key (asymmetric) and same algorithm to decrypt the ciphertext to convert it back to plaintext. Then hashing was methodically described; hashing takes an input set of data (of almost arbitrary size) and returns a fixed-length result called the hash value.

System hardening is the process of applying secure configurations (to reduce the attack surface) and locking down various hardware, communications systems and software, including operating system, web server, application server, application, etc. We also discussed configuration management, a process and discipline used to ensure that the only changes made to a system are those that have been authorized and validated. Configuration management consists of identification, baseline, change control, and verification and audit. During configuration management, one must conduct inventory, baselines, updates, and patches.

The following best practice security policies were examined: data handling (appropriate use of data), password (appropriate use of passwords), acceptable use (appropriate use of the assets, devices, and data), bring your own device (appropriate use of personal devices), privacy (appropriate protection of one's privacy), and change management (appropriate transition from current state to a future state). Change management practices address a common set of core activities: documentation, approval, and rollback. It starts with a request for change (RFC) and moves through various development and test stages until the change is released to the end users.

We ended the chapter by discussing the importance of security awareness training and how it reduces the internal threat to an organization. By breaking down the levels of security awareness training into education, training, and awareness, we identified that the training can be tailored to the security topic(s), organization, position and/or individual. We also emphasized the importance of password protection.

Module Names

Module 1: Understand Data Security

Module 2: Understand System Hardening

Module 3: Understand Best Practice Security Policies

Module 4: Understand Security Awareness Training

Chapter to Domain Mapping

Module Number	Module Title	Domains
1	Understand Data Security	5.1, 5.1.1, 5.1.2, 5.1.3
2	Understand System Hardening	5.2, 5.2.1
3	Understand Best Practice Security Policies	5.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5, 5.3.6
4	Understand Security Awareness Training	5.4, 5.4.1, 5.4.2, 5.3.2

Learning Objectives

After completing this chapter, the participant will be able to:

- Explain concepts of security operations
- Discuss data handling best practices
- Identify key concepts of logging and monitoring
- Summarize the different types of encryption and their common uses
- Describe the concepts of configuration management
- Explain the application of common security policies
- Discuss the importance of security awareness training
- Practice the terminology of and review the concepts of network operations

Chapter Takeaways

Module 1: Understand data security

Data handling process:

- Create
- Store
- Share
- Use
- Modify
- Archive
- Destroy

Examples of data sensitivity levels:

- Highly restricted: Compromise of data with this sensitivity label could possibly put the organization's future existence at risk. Compromise could lead to substantial loss of life, injury or property damage, and the litigation and claims that would follow.
- Moderately restricted: Compromise of data with this sensitivity label could lead to loss of temporary competitive advantage, loss of revenue, or disruption of planned investments or activities.
- Low sensitivity (sometimes called "internal use only"): Compromise of data with this sensitivity label could cause minor disruptions, delays or impacts.
- Unrestricted public data: As this data is already published, no harm can come from further dissemination or disclosure.

Logging - Ingress monitoring tools:

- Firewalls
- Gateways
- Remote authentication servers
- IDS/IPS tools
- SIEM solutions
- Anti-malware solutions

Logging – Egress monitoring data types:

- Email (content and attachments)
- Copy to portable media
- File Transfer Protocol (FTP)
- Posting to web pages/websites
- Applications/application programming interfaces (APIs)

Two primary types of encryption:

- Symmetric – same key
- Asymmetric – different keys

Module 1: Understand data security (continued)

Five functions of a cryptographic hash:

1. Useful: It is easy to compute the hash value for any given message.
2. Nonreversible: It is computationally infeasible to reverse the hash process or otherwise derive the original plaintext of a message from its hash value (unlike an encryption process, for which there must be a corresponding decryption process).
3. Content integrity assurance: It is computationally infeasible to modify a message such that re-applying the hash function will produce the original hash value.
4. Unique: It is computationally infeasible to find two or more different, sensible messages that hash to the same value.
5. Deterministic: The same input will always generate the same hash, when using the same hashing algorithm.

Module 2: Understand system hardening

Configuration management procedures:

- Identification
- Baseline
- Change control
- Verification & Audit

Elements of configuration management:

- Inventory
- Baselines
- Updates
- Patches

Module 3: Understand best practice security policies

Best practice security policies:

- Data handling - appropriate use of data
- Password - appropriate use of passwords
- Acceptable use - appropriate use of the assets, devices, and data
- Bring your own device - appropriate use of personal devices
- Privacy - appropriate protection of one's privacy
- Change management - appropriate transition from current state to a future state

Data handling policy procedures:

- Classify
- Categorize
- Label
- Store
- Encrypt
- Backup
- Destroy

Module 3: Understand best practice security policies (continued)

Examples: Password policy procedures

- Password creation:
  - All user and admin passwords must be at least a certain length. Longer passphrases are encouraged.
  - Passwords cannot be the same or similar to other passwords used on any other websites, system, application or personal account.
  - Passwords should not be a single word or a commonly used phrase.
  - Avoid passwords that are easy to guess, such as the names and birthdays of your friends and family, your favorite bands or catchphrases you like to use.
  - Dictionary words and phrases should be avoided.
  - Default installation passwords must be changed immediately after installation is complete.
- Password aging:
  - User passwords must be changed on a schedule established by the organization. Previously used passwords may not be reused.
  - System-level passwords must be changed according to a schedule established by the organization.
- Password protection:
  - Passwords must not be shared with anyone, even IT staff or supervisors, and must not be revealed or sent electronically. Do not write down your passwords.

Acceptable use policy (AUP) procedures:

- Data access
- System access
- Data disclosure
- Passwords
- Data retention
- Internet usage
- Company device usage

Possible devices on the bring your own device (BYOD) policy:

- Cell phone
- Tablet
- Laptop
- Smartwatch
- Bluetooth devices

Privacy policy protects:

- PII
- ePHI
- Bank/credit card information

Examples of national and international privacy regulations/laws:

- GDPR in the EU
- Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada

Module 3: Understand best practice security policies (continued)

Change management policy consists of three major activities:

- Deciding to change
- Making the change
- Confirming that the change has been correctly accomplished

Module 4: Understand security awareness training

Security awareness training types:

- Education
- Training
- Awareness

Some social engineering techniques:

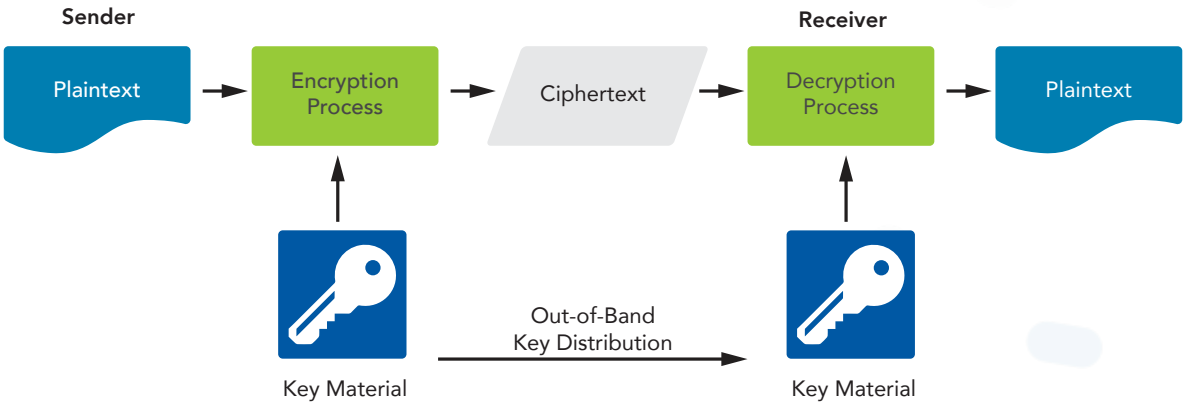
- Baiting
- Phone phishing or vishing
- Pretexting
- Quid pro quo
- Tailgating
- False flag or false front operations

Graphics

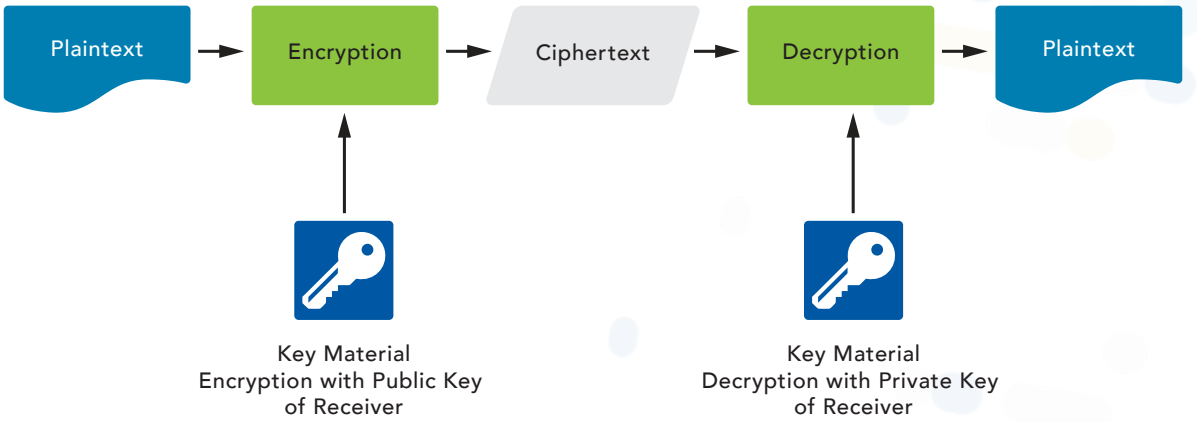
Data Security Lifecyle



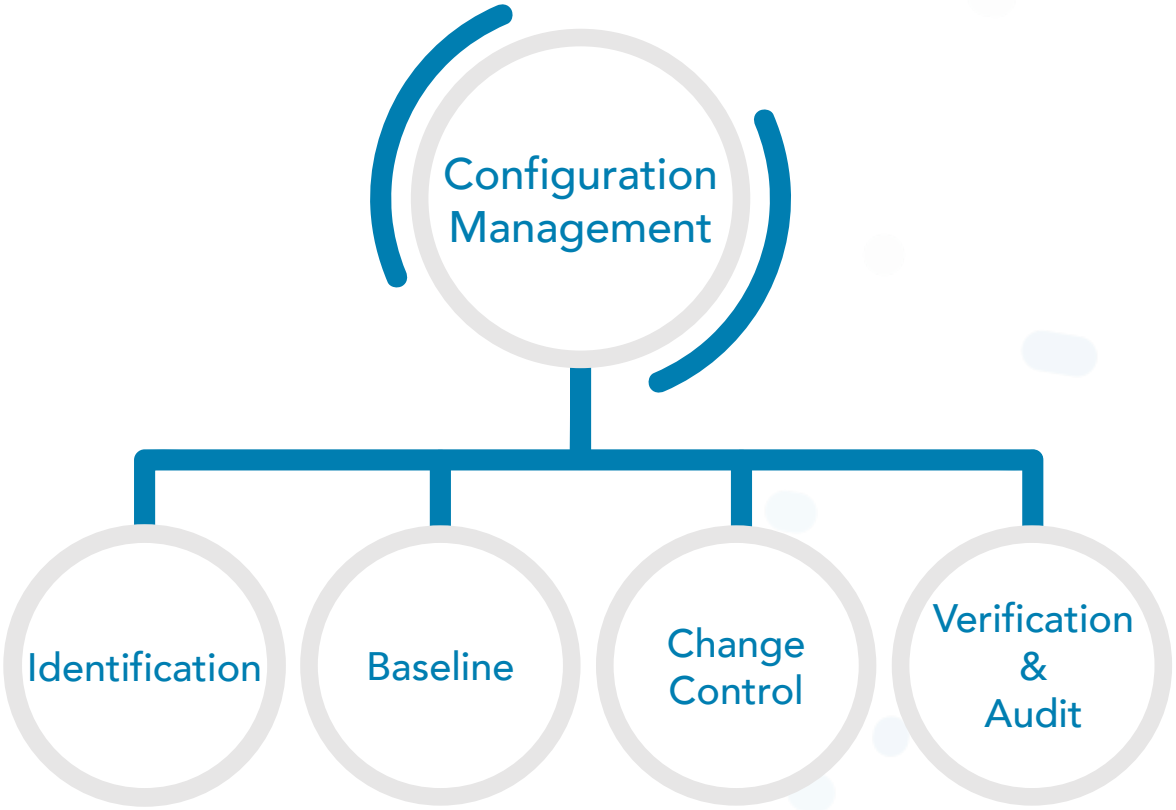
Use of Symmetric Algorithms



Use of Asymmetric Cryptography to Send a Confidential Message

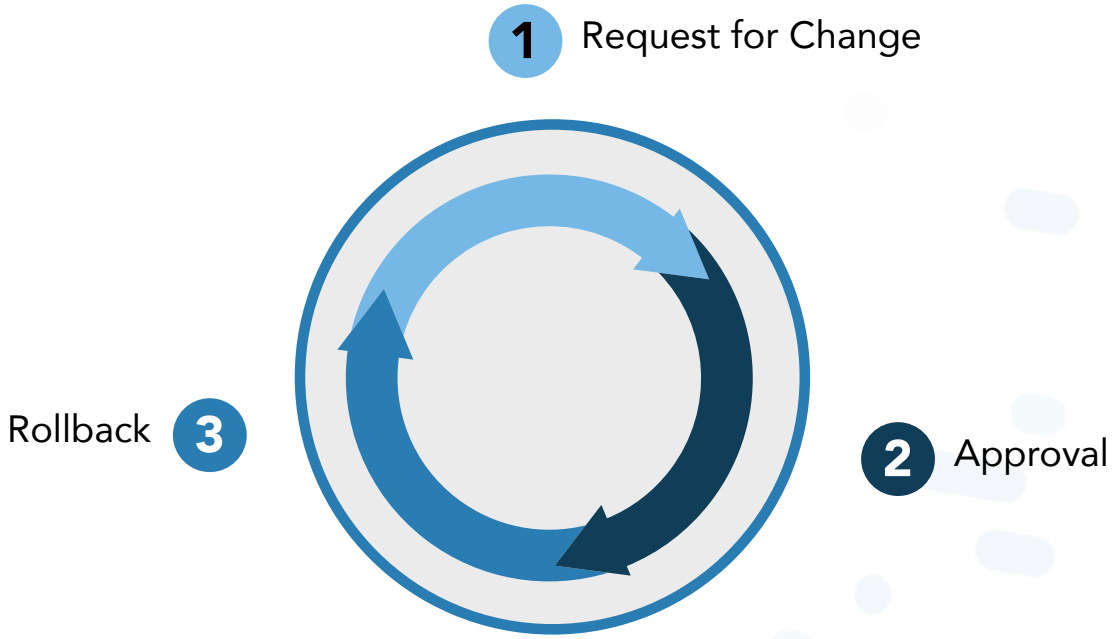


Configuration Management



Change Management Components

Change Management Components



Formulas and Calculations

Cryptographic Hash Function

variable data input

+

hashing algorithm

=

fixed bit size data output (the digest)

Chapter Terms and Definitions

Application Server

A computer responsible for hosting applications to user workstations. NIST SP 800-82 Rev.2

Asymmetric Encryption

An algorithm that uses one key to encrypt and a different key to decrypt the input plaintext.

Checksum

A digit representing the sum of the correct digits in a piece of stored or transmitted digital data, against which later comparisons can be made to detect errors in the data.

Ciphertext

The altered form of a plaintext message so it is unreadable for anyone except the intended recipients. In other words, it has been turned into a secret.

Classification

Classification identifies the degree of harm to the organization, its stakeholders or others that might result if an information asset is divulged to an unauthorized person, process or organization. In short, classification is focused first and foremost on maintaining the confidentiality of the data, based on the data sensitivity.

Configuration management

A process and discipline used to ensure that the only changes made to a system are those that have been authorized and validated

Cryptanalyst

One who performs cryptanalysis which is the study of mathematical techniques for attempting to defeat cryptographic techniques and/or information systems security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself.

Cryptography

The study or applications of methods to secure or protect the meaning and content of messages, files, or other information, usually by disguise, obscuration, or other transformations of that content and meaning.

Data Loss Prevention (DLP)

System capabilities designed to detect and prevent the unauthorized use and transmission of information.

Decryption

The reverse process from encryption. It is the process of converting a ciphertext message back into plaintext through the use of the cryptographic algorithm and the appropriate key for decryption (which is the same for symmetric encryption, but different for asymmetric encryption). This term is also used interchangeably with the "deciphering."

Degaussing

A technique of erasing data on disk or tape (including video tapes) that, when performed properly, ensures that there is insufficient magnetic remanence to reconstruct data.

Digital Signature

The result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation. NIST SP 800-12 Rev. 1

Egress Monitoring

Monitoring of outgoing network traffic.

Encryption

The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.

Encryption System

The total set of algorithms, processes, hardware, software, and procedures that taken together provide an encryption and decryption capability.

Hardening

A reference to the process of applying secure configurations (to reduce the attack surface) and locking down various hardware, communications systems, and software, including operating system, web server, application server, application, etc. Hardening is normally performed based on industry guidelines and benchmarks, such as those provided by the Center for Internet Security (CIS).

Hash Function

An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message. NIST SP 800-152

Hashing

The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data. Source CNSSI 4009-2015

Ingress Monitoring

Monitoring of incoming network traffic.

Message Digest

A digital signature that uniquely identifies data and has the property such that changing a single bit in the data will cause a completely different message digest to be generated. NISTIR-8011 Vol.3

Operating System

The software "master control application" that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the Web server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations. NIST SP 800-44 Version 2

Patch

A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component. Source: ISO/IEC 19770-2

Patch Management

The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. Source: CNSSI 4009

Plaintext

A message or data in its natural format and in readable form; extremely vulnerable from a confidentiality perspective.

Records

The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items). NIST SP 800-53 Rev. 4

Records Retention

A practice based on the records life cycle, according to which records are retained as long as necessary, and then are destroyed after the appropriate time interval has elapsed.

Remanence

Residual information remaining on storage media after clearing. NIST SP 800-88 Rev. 1

Request for change (RFC)

The first stage of change management, wherein a change in procedure or product is sought by a stakeholder.

Security Governance

The entirety of the policies, roles, and processes the organization uses to make security decisions in an organization.

Social engineering

Tactics to infiltrate systems via email, phone, text, or social media, often impersonating a person or agency in authority or offering a gift. A low-tech method would be simply following someone into a secure building.

Symmetric encryption

An algorithm that uses the same key in both the encryption and the decryption processes.

Web Server

A computer that provides World Wide Web (WWW) services on the Internet. It includes the hardware, operating system, Web server software, and Web site content (Web pages). If the Web server is used internally and not by the public, it may be known as an "intranet server." NIST SP 800-44 Version 2

Whaling Attack

Phishing attacks that attempt to trick highly placed officials or private individuals with sizable assets into authorizing large fund wire transfers to previously unknown entities.