+WHILE READING YOU WOULD COME ACROSS A TERM “NB”, WHICH MEANS NOTE WELL OR TAKE NOTE, FOR THOSE WHO DON'T KNOW.
PLEASE TRY TO COMPLETE THIS CONTENT FOR YOUR ISC2 CC EXAM, THIS CONTENT ALONE WOULD GREATLY HELP IN YOUR SUCCESS IN THE EXAM AS IT DID FOR ME.

@ L1: Security Principles

“Module 1 Understand the Security Concepts of Information Assurance

Domain D1.1.1, D1.1.2, D1.1.3, D1.1.4, D1.1.5, D1.1.6
“Confidentiality

It relates to permitting authorized access to information, while at the same time protecting information from improper disclosure. Difficulties to achieve confidentiality are related to: **many users are guests or customers**, and it is not clear if the access comes from a compromised machine or vulnerable mobile application. To avoid those difficulties, security professionals must regulate access, permitting access to authorized individuals, for protecting the data that needs protection.

Data that needs protections is also known **as PII or PHI**.
PII stands for Personally Identifiable Information and it is related to the area of confidentiality and it means any data that could be used to identify an individual.
PHI stands for Protected Health Information and it comprehends information about one's health status, and classified or sensitive information, which includes trade secrets, research, business plans and intellectual property.

Related to confidentiality is **the concept sensitivity a measure of the importance assigned to information by its owner**, or the purpose of denoting its need for protection. **Sensitive information** is information that if improperly disclosed (confidentiality) or modified (integrity) would harm an organization or individual. In many cases, sensitivity is related to the harm to external stakeholders; that is, people or organizations that may not be a part of the organization that processes or uses the information.

Threat related to confidentiality are:

1. Snooping involves gathering information that is left out in the open. Clean desk policies protect against snooping.
2. Dumpster diving also looks for sensitive materials, but in the dumpster, a paper shredding protects against it.
3. Eavesdropping occurs when someone secretly listen to a conversation, and it can be prevent with rules about sensitive conversations

4. Wiretapping is the electronic version of eavesdropping, the best way against that is using encryption to protect the communication.
5. Social Engineering, the best defense is to educate users to protect them against social engineering.

Integrity

It is 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, which can be applied **to information or data**, **system and process for business operations**, **organizations**, **people and their actions**. Furthermore, restrict to data integrity, it is an assurance that data has not been altered in an unauthorized manner, covering data **in storage**, during **processing**, and while **in transit**.

Consistency is another concept related to integrity and requires that all instances of the data be identical in form, content and meaning. When related to system integrity, it refers to the maintenance of a known good configuration and expected operational function as the system processes the information. Ensuring integrity begins with an awareness of state, which is the current condition of the system. Specifically, this awareness concerns the ability to document and understand the state of data or a system at a certain point, **creating a baseline**. A baseline, which means a documented, lowest level of security configuration allowed by a standard or organization, can refer to the current state of the information—whether it is protected.

To preserve that state, the information must always continue to be protected through a transaction. Going forward from that baseline, the integrity of the data or the system can always be ascertained by comparing the baseline with the current state. If the two match, then the integrity of the data or the system is intact; if the two do not match, then the integrity of the data or the system has been compromised. Integrity is a primary factor in the reliability of information and systems. The need to safeguard information and system integrity may be dictated by laws and regulations. Often, it is dictated by the needs of the organization to access and use reliable, accurate information.

1. Unauthorized modification attacks make changes without permission. The best way to protect against that is the least privilege principle.
2. Impersonation attacks pretend to be someone else. User education protects against impersonation attacks.
3. Man-In-The-Middle (MITM) attacks place the attacker in the middle of a communication session, monitoring everything that's occurring.
4. Replay attacks eavesdrop on logins and reuse the captured credentials.

NB: To both MiTM and Replay attacks the best approach is encryption.

Availability

It means that systems and data are accessible at the time users need them. It can be defined as timely and reliable access to information and the ability to use it, and for authorized users, timely and reliable access to data and information services.
The core concept of availability is that data is accessible **to authorized users when and where it is needed and in the form and format required**. This does not mean that data or systems are available 100% of the time. Instead, the systems and data meet the requirements of the business for timely and reliable access.
Some systems and data are far more critical than others, so the security professional **must ensure that the appropriate levels of availability are provided**. This requires consultation with the involved business to ensure that critical systems are identified and available.
Availability is often associated with the term **criticality**, which means 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), because it represents the importance an organization gives to data or an information system in performing its operations or achieving its mission

1. Denial of Service can be mitigated using firewalls to block unauthorized connections
2. Power outages can be mitigated using redundant power and generators
3. Hardware failures can be mitigated using redundant components
4. Destruction can be mitigated using backups
5. Service outages

Three steps to gain access, known as triple A, which means Authentication, Authorization, Accounting

Identification

Consist of making a claim of identity

Authentication

When users have stated their identity, it is necessary **to validate that they are the rightful owners of that identity**. This process of verifying or proving the user's identification is known as authentication, which means in another terms 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 authentication. Simply put, authentication is a process to prove the identity of the requestor.

There are three common methods of authentication:

* Something you know: Passwords or paraphrases
* Something you have: Tokens (NISTIR 7711), memory cards, smart cards
* Something you are: Biometrics , measurable characteristics

Methods of Authentication

There are two types of authentication. Using only one of the methods of authentication stated previously is **known as single-factor authentication (SFA)**. Granting users access only after successfully demonstrating or displaying two or more of these methods is **known as multi-factor authentication (MFA)**.

Common best practice is to implement at least two of the three common techniques for authentication:

* Knowledge-based
* Token-based
* Characteristic-based

Knowledge-based authentication uses a passphrase or secret code to differentiate between an authorized and unauthorized user. If you have selected a personal identification number (PIN), created a password or some other secret value that only you know, then you have experienced knowledge-based authentication. The problem with using this type of authentication alone is that it is often vulnerable to a variety of attacks. For example, the help desk might receive a call to reset a user's password. The challenge is ensuring that the password is reset only for the correct user and not someone else pretending to be that user. For better security, a second or third form of authentication that is based on a token or characteristic would be required prior to resetting the password. The combined use of a user ID and a password consists of two things that are known, and because it does not meet the requirement of using two or more of the authentication methods stated, it is not considered MFA.

Password

* Password length requirements set a minimum number of chars
* Password complexity requirements describe the types of characters that must be included
* Password expiration requirements force password changes. Nowadays, that requirement isn't used, companies change to an approach where force password change is required when there is any evidence that the password has been compromised.
* Password history requirements prevent password reuse.
* Provide a way to change the password quickly and easily.
* Encourage users to not reuse the same password across multiple sites

* Password managers facilitate the use of strong, unique passwords

Authorization

Ensuring that an action is allowed.

Accounting

Its maintains logs of activity

Non-repudiation

Non-repudiation is a legal term and is defined as the protection against an individual falsely denying having performed a particular action. It provides the capability to determine whether a given individual took a particular action, such as created information, approved information or sent or received a message.

In today's world of e-commerce and electronic transactions, **there are opportunities for the impersonation of others or denial of an action, such as making a purchase online and later denying it**. It is important that all participants trust online transactions. **Non-repudiation methodologies ensure that people are held responsible for transactions they conducted**.

Base Concepts

1. Authorization: the right or a permission that is granted to a system entity to access a system resource
2. Integrity: the property that data has not been altered in an unauthorized manner
3. Confidentiality: the characteristic of data or information when it is not made available or disclosed to unauthorized persons or process
4. Privacy: the right of an individual to control the distribution of information about themselves
5. Availability: Ensuring timely and reliable access to and use of information by authorized users
6. Non-repudiation: The inability to deny taking an action, such as sending an email message
7. Authentication: Access control process that compares one or more factors of identification to validate that the identity claimed by a user or entity is known to the system

Privacy

Privacy is **the right of an individual to control the distribution of information about themselves**. While security and privacy both focus on the protection of personal and sensitive data, there is a difference between them. With the increasing rate at which data is collected and digitally stored across all industries, the push for privacy legislation and

compliance with existing policies steadily grows. In today's global economy, privacy legislation and regulations on privacy and data protection can impact corporations and industries regardless of physical location. **Global privacy is an especially crucial issue when considering requirements regarding the collection and security of personal information**. There are several laws that define privacy and data protection, which periodically change. Ensuring that protective security measures are in place is not enough to meet privacy regulations or to protect a company from incurring penalties or fines from mishandling, misuse, or improper protection of personal or private information. An example of a law with multinational implications is the European Union's General Data Protection Regulation (GDPR) which applies to all organizations, foreign or domestic, doing business in the EU or any persons in the EU. Companies operating or doing business within the United States may also fall under several state legislations that regulate the collection and use of consumer data and privacy. Likewise, member nations of the EU enact laws to put GDPR into practice and sometimes add more stringent requirements. These laws, including national- and state-level laws, dictate that any entity anywhere in the world handling the private data of people in a particular legal jurisdiction must abide by its privacy requirements. As a member of an organization's data protection team, you will not be required to interpret these laws, but you will need an understanding of how they apply to your organization.

Module 2 Understand the risk management process

Domain D1.2.1, D1.2.2

Risks and security-related issues represent **an ongoing concern** of businesses as well as the field of cybersecurity. Assessing and analyzing risk should be **a continuous and comprehensive** exercise in any organization. As a member of an organization's security team, you will work through **risk assessment, analysis, mitigation, remediation and communication**.

Risk ** is a measure of the extent to which an entity is threatened by a **potential circumstance or event. It is often expressed as a combination of:
- the **adverse impacts that would arise if the circumstance or event occurs**, and
- the **likelihood** occurrence.

Information security risk reflects the potential adverse impacts that result from the possibility of unauthorized access, use, disclosure, disruption, modification or destruction of information and/or information systems. This definition represents that **risk is associated with threats, impact and likelihood**, and it also indicates that IT risk is a subset of business risk.

Matrix: Probability X Impact generates four possible combinations:

1. low probability, low impact

2. low probability, high impact
3. high probability, low impact
4. high probability, high impact

Risk Management Terminology

* **An asset** is something in need of protection because it has value to the organization. It could be a tangible asset or intangible, such as information.
* **A vulnerability** is a gap or weakness in an organization's protection of its valuable assets, including information. (NIST SP 800-30). A vulnerability is an inherent weakness or flaw in a system or component, which, if triggered or acted upon, could cause a risk event to occur. An organization's security team strives to decrease its vulnerability. To do so, **they view their organization with the eyes of the threat actor**, asking themselves, **"Why would we be an attractive target?"** The answers might provide steps to take that will discourage threat actors, cause them to look elsewhere or simply make it more difficult to launch an attack successfully. **Managing vulnerabilities starts with one simple step: Learn what they are**.
* **A threat** is something or someone that aims to exploit a vulnerability to gain unauthorized access. A threat is a person or thing that takes action to exploit (or make use of) a target organization's system vulnerabilities, as part of achieving or furthering its goal or objectives.
* Likelihood, when determining an organization's vulnerabilities, the security team will consider **the probability**, or likelihood , of **a potential vulnerability being exploited within the construct of the organization's threat environment**. **Likelihood of occurrence is a weighted factor based on a subjective analysis of the probability that a given threat or set of threats is capable of exploiting a given vulnerability or set of vulnerabilities.**

Finally, the security team will consider the likely results if a threat is realized and an event occurs. Impact is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Think about the impact and the chain of reaction that can result when an event occurs by revisiting the pickpocket scenario: **Risk comes from the intersection of those three concepts**.

Risk Identification

In the world of cyber, **identifying risks is not a one-and-done activity**. It's a recurring process of identifying different possible risks, characterizing them and then estimating their potential for disrupting the organization.

Takeaways to remember about 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.

As a security professional, you are likely to assist in risk assessment at a system level, focusing **on process, control, monitoring or incident response and recovery activities**. If you're working with a smaller organization, or one that lacks any kind of risk management and mitigation plan and program, you might have the opportunity to help fill that planning void.

Risk Assessment

Risk assessment is defined as **the process of identifying**, **estimating and prioritizing risks to an organization's operations** (including its mission, functions, image and reputation), **assets**, **individuals**, **other organizations and even the nation**. Risk assessment should result in aligning (or associating) **each identified risk resulting from the operation of an information system with the goals, objectives, assets or processes that the organization uses, which in turn aligns with or directly supports achieving the organization's goals and objectives**. A risk assessment can prioritize items for management to determine the method of mitigation that best suits the assets being protected. The result of the risk assessment process is **often documented as a report or presentation given to management for their use in prioritizing the identified risk(s)**. This report is provided to management for review and approval. In some cases, management may indicate a need for a more in-depth or detailed risk assessment performed by internal or external resources.

Risk Treatment

Risk treatment relates **to making decisions about the best actions to take regarding the identified and prioritized risk**. The decisions made are dependent on the attitude of management toward risk and the availability — and cost — of risk mitigation. The options commonly used to respond to risk are:

* Avoidance: **It is the decision to attempt to eliminate the risk entirely**. This could include ceasing operation for some or all of the activities of the organization that are exposed to a particular risk. **Organization leadership may choose risk avoidance when the potential impact of a given risk is too high or if the likelihood of the risk being realized is simply too great**.

* Acceptance: Risk acceptance is taking **no action to reduce the likelihood of a risk occurring**. Management may opt for conducting the business function that is associated with the risk **without any further action on the part of the organization**, either because the impact or likelihood of occurrence is negligible, or because the benefit is more than enough to offset that risk.

* Mitigation: 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**. Mitigation can involve **remediation measures**, **or controls**, **such as security controls, establishing policies, procedures, and standards to minimize adverse risk**. Risk cannot always be mitigated, but mitigations such as safety measures should always be in place.

* Transfer: **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. Typically, this is an insurance policy.

Base Concepts

* Mitigation: Taking action to prevent or reduce the impact of an event
* Acceptance: Ignoring the risks and continuing risky activities
* Avoidance: Ceasing the risky activity to remove the likelihood that an event will occur
* Vulnerability: An inherent weakness or flaw
* Asset: Something of value that is owned by an organization, including physical hardware and intellectual property
* Threat: A person or an entity that deliberately takes actions to exploit a target
* Transference: Passing risk to a third party

Risk Priorities

When risks have been identified, it is time to prioritize and analyze core risks through qualitative risk analysis and/or quantitative risk analysis. This is necessary to determine **root cause and narrow down apparent risks and core risks**. Security professionals work with their teams to conduct both qualitative and quantitative analysis.

Understanding the organization's overall mission and the functions that support the mission helps **to place risks in context**, **determine the root causes and prioritize the assessment and analysis of these items**. In most cases, management will provide direction for using the findings of the risk assessment to determine a prioritized set of risk-response actions.

One effective method to prioritize risk is to use **a risk matrix**, which helps identify priority **as the intersection of likelihood of occurrence and impact**. It also gives the team a common language to use with management when determining the final priorities. For example, a low likelihood and a low impact might result in a low priority, while an incident with a high likelihood and high impact will result in a high priority. Assignment of priority may relate to business priorities, the cost of mitigating a risk or the potential for loss if an incident occurs.

Decision Making Based on Risk Priorities

When making decisions based on risk priorities, organizations must evaluate the likelihood and impact of the risk as well as their tolerance for different sorts of risk. **A company in Hawaii is more concerned about the risk of volcanic eruptions than a company in Chicago, but the Chicago company will have to plan for blizzards**. In those cases, determining risk tolerance is up to the executive management and board of directors. If a company chooses to ignore or accept risk, exposing workers to asbestos, for example, it puts the company in a position of tremendous liability.

Risk Tolerance

The perception management takes toward risk is often likened to the **entity's appetite for risk**. **How much risk are they willing to take?** Does management welcome risk or want to avoid it? The level of risk tolerance varies across organizations, and even internally: Different departments may have different attitudes toward what is acceptable or unacceptable risk.

Understanding the organization and senior management's attitude toward risk is usually the starting point for getting management to take action regarding risks. Executive management and/or the Board of Directors determines what is an acceptable level of risk for the organization. Security professionals aim to maintain the levels of risk within management's limit of risk tolerance.

Often, risk tolerance is dictated by geographic location. For example, companies in Iceland plan for the risks that nearby volcanoes impose on their business. Companies that are outside the projected path of a lava flow will be at a lower risk than those directly in the path's flow. Similarly, the likelihood of a power outage affecting the data center is a real threat in all areas of the world. In areas where thunderstorms are common, power outages may occur more than once a month, while other areas may only experience one or two power outages annually. Calculating the downtime that is likely to occur with varying lengths of downtime will help to define a company's risk tolerance. If a company has a low tolerance of the risk of downtime, they are more likely to invest in a generator to power critical systems. A company with an even lower tolerance for downtime will invest in multiple generators with multiple fuel sources to provide a higher level of assurance that the power will not fail.

Module 3 Understand Security Control

Domain D1.3.1, D1.3.2, D1.3.3

What are security controls? (FIPS PUB 199)

Security controls pertain to the **physical**, **technical** and **administrative mechanisms** that 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 controls should **reduce risk**, hopefully to an acceptable level.

* Physical control: it addresses process-based security needs using **physical hardware devices**, such as **badge readers**, **architectural features of buildings and facilities**, **and specific security actions to be taken by people**. They typically provide ways of controlling, directing or preventing the movement of people and equipment throughout a specific physical location, such as an office suite, factory or other facility. **Physical controls also provide protection and control over entry onto the land surrounding the buildings**, **parking lots or other areas that are within the organization's control**. In most situations, physical controls are supported by technical controls as a means of incorporating them into an overall security system.

* Technical control: it (also called logical controls) is security controls that **computer systems and networks directly implement**. These controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations and support security requirements for applications and data. 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. However, the implementation of technical controls always requires significant operational considerations and should be consistent with the management of security within the organization. Many of these will be examined in more depth as we look at them in later sections in this chapter and in subsequent chapters.

* Administrative control: it (also known as managerial controls) is **directives**, **guidelines** or **advisories aimed at the people within the organization**. They provide frameworks, constraints and standards for human behavior, and should cover the entire scope of the organization's activities and its interactions with external parties and stakeholders. It is vitally important to realize that administrative controls **can and should be powerful, effective tools for achieving information security**. Even the simplest security awareness policies can be an effective control, if you can help the organization fully implement them through systematic training and practice. Many organizations are improving their overall security posture by integrating their administrative controls into the task-level activities and operational decision processes that their workforce uses throughout the day. This can be done by providing them as in-context ready reference and advisory resources, or by linking them directly into training activities. These and other techniques bring the policies to a more neutral level and away from the decision-making of only the senior executives. It also makes them immediate, useful and operational on a daily and per-task basis.

Some examples:
Administrative: acceptable use policy, emergency operations procedures, employee awareness training

Physical: Badge reader, stop sign in parking lot, door lock
Technical: access control list

Module 4 Understand Governance and Elements and Process

Domain D1.5.1, D1.5.2, D1.5.3, D1.5.4

Governance Elements

When leaders and management implement the systems and structures that the organization will use to achieve its goals, they are **guided by laws and regulations created by governments to enact public policy**. **Laws and regulations guide the development of standards, which cultivate policies, which result in procedures**.

* **Procedures** are the detailed steps to complete a task that support departmental or organizational policies.
* **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.
* **Standards** are often used by governance teams to provide a framework to introduce policies and procedures in support of regulations.
* **Regulations** are commonly issued in the form of laws, usually from the government (not to be confused with governance) and typically carry financial penalties for noncompliance.

Regulations -> Standards -> Policies -> Procedures

NB: A difference between a policy and standard is that a policy is a high level statement WHILE a standard is a more detailed and precise statement.

Module 5 Understand (ISC)² Code of Ethics

@L3 Access Control Concepts

Introduction

Types of access control, physical and logical controls and how they are combined to strengthen the overall security of an organization.

Module 1 Understand Access Control Concepts

Domain D3.1, D3.1.3, D3.1.5, D3.2, D3.2.1, D3.2.2, D3.2.5

What is Security Control?

Access control involves **limiting what objects can be available to what subjects according to what rules**.

Controls Overview

Earlier in this course we looked at security principles through foundations of risk management, governance, incident response, business continuity and disaster recovery. But in the end, security all comes down to, **“Who can get access to organizational assets (buildings, data, systems, etc.) and what can they do when they get access?”**

Access controls **are not just about restricting access** to information systems and data, **but also about allowing access**. It is about granting the appropriate level of access to authorized personnel and processes and denying access to unauthorized functions or individuals.

Access is based on three elements:

* subjects: **any entity that requests access to our assets**. The entity requesting access may be a **user**, a **client**, a **process** or a **program**, for example. A subject is the initiator of a request for service; therefore, a subject is referred to as “active.” A subject:
  * Is a user, a process, a procedure, a client (or a server), a program, a device such as an endpoint, workstation, smartphone or removable storage device with onboard firmware.
  * Is active: It initiates a request for access to resources or services.
  * Requests a service from an object.
  * Should have a level of clearance (permissions) that relates to its ability to successfully access services or resources.

* **Objects:** Objects represent the assets or resources that subjects seek to access within an organization. These assets can take various forms, including data stored in databases or files, systems such as servers or network devices, applications used for specific purposes, physical spaces like offices or storage rooms, or any other resource that holds value to the organization. Objects serve as the targets of access requests initiated by subjects, and their protection is essential for maintaining the security and integrity of the organization's assets.

* **Rules:** Rules form the foundation of the access control framework by defining the conditions under which access is granted or denied to objects. These rules establish the criteria and parameters that govern the access permissions and restrictions within the organization's environment. They can encompass a wide range of factors, including user roles and responsibilities, permission levels, time-based access policies, location-based restrictions,

and other attributes relevant to the organization's security policies. Rules ensure that access is managed in a consistent, predictable, and enforceable manner, helping to safeguard sensitive information, prevent unauthorized access, and mitigate security risks effectively.

Controls Assessments

Risk reduction depends on the effectiveness of the control. It must apply to the current situation and adapt to a changing environment.

Defense in Depth

We are looking at all access permissions including building access, access to server rooms, access to networks and applications and utilities. These are all implementations of access control and are part of **a layered defense strategy**, **also known as defense in depth**, developed by an organization.

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

A technical example of defense in depth, in which multiple layers of technical controls are implemented, **is when a username and password are required for logging in to your account, followed by a code sent to your phone to verify your identity**. **This is a form of multi-factor authentication using methods on two layers, something you have and something you know.** The combination of the two layers is much more difficult for an adversary to obtain than either of the authentication codes individually.

Another example of multiple technical layers is when additional firewalls are used to separate untrusted networks with differing security requirements, such as the internet from trusted networks that house servers with sensitive data in the organization. When a company has information at multiple sensitivity levels, it might require the network traffic to be validated by rules on more than one firewall, with the most sensitive information being stored behind multiple firewalls.

For a non-technical example, consider the multiple layers of access required to get to the actual data in a data center. First, a lock on the door provides a physical barrier to access the data storage devices. Second, a technical access rule prevents access to the data via the network. Finally, a policy, or administrative control defines the rules that assign access to authorized individuals.

Principle of Least Privilege

The Principle of Least Privilege (NIST SP 800-179) is a standard of permitting only minimum access necessary for users or programs to fulfill their function. Users are provided access only to the systems and programs they need to perform their specific job or tasks.

To preserve the confidentiality of information and ensure that it is only available to personnel who are authorized to see it, **we use privileged access management**, **which is based on the principle of least privilege**. **That means each user is granted access only to the items they need and nothing further**.

For example, only individuals working in billing will be allowed to view consumer financial data, and even fewer individuals will have the authority to change or delete that data. This maintains confidentiality and integrity while also allowing availability by providing administrative access with an appropriate password or sign-on that proves the user has the appropriate permissions to access that data.

Sometimes it is necessary to allow users to access the information via a temporary or limited access, for instance, for a specific time period or just within normal business hours. Or access rules can limit the fields that the individuals can have access to. One example is a healthcare environment. Some workers might have access to patient data but not their medical data. Individual doctors might have access only to data related to their own patients. In some cases, this is regulated by law, such as HIPAA in the United States, and by specific privacy laws in other countries.

Systems often monitor access to private information, and if logs indicate that someone has attempted to access a database without the proper permissions, that will automatically trigger an alarm. The security administrator will then record the incident and alert the appropriate people to take action.

The more critical information a person has access to, the greater the security should be around that access. They should definitely have multi-factor authentication, for instance.

Privileged Access Management

Privileged access management provides the first and perhaps most familiar use case. Consider a human user identity that is granted various create, read, update, and delete privileges on a database. Without privileged access management, the system's access control would have those privileges assigned to the administrative user in a static way, effectively "on" 24 hours a day, every day. Security would be dependent upon the login process to prevent misuse of that identity. Just-in-time privileged access management, by contrast, includes role-based specific

subsets of privileges that only become active in real time when the identity is requesting the use of a resource or service.

Privileged Accounts

Privileged accounts are those with permissions beyond those of normal users, such as managers and administrators. Broadly speaking, these accounts have **elevated privileges** and are used by many different classes of users, including:

* Systems administrators, who have the principal responsibilities for operating systems, applications deployment and performance management.
* Help desk or IT support staff, who often need to view or manipulate endpoints, servers and applications platforms by using privileged or restricted operations.
* Security analysts, who may require rapid access to the entire IT infrastructure, systems, endpoints and data environment of the organization.

Other classes of privileged user accounts may be created on a per-client or per-project basis, to allow a member of that project or client service team to have greater control over data and applications. These few examples indicate that organizations often need to delegate the capability to manage and protect information assets to various managerial, supervisory, support or leadership people, with differing levels of authority and responsibility. This delegation, of course, should be contingent upon trustworthiness, since misuse or abuse of these privileges could lead to harm for the organization and its stakeholders.

Typical measures used for moderating the potential for elevated risks from misuse or abuse of privileged accounts include the following:

* More extensive and detailed logging than regular user accounts. The record of privileged actions is vitally important, as both a deterrent (for privileged account holders that might be tempted to engage in untoward activity) and an administrative control (the logs can be audited and reviewed to detect and respond to malicious activity).
* More stringent access control than regular user accounts. As we will see emphasized in this course, even non privileged users should be required to use MFA methods to gain access to organizational systems and networks. Privileged users—or more accurately, highly trusted users with access to privileged accounts—should be required to go through additional or more rigorous authentication prior to those privileges. Just-in-time identity should also be considered as a way to restrict the use of these privileges to specific tasks and the times in which the user is executing them.
* Deeper trust verification than regular user accounts. Privileged account holders should be subject to more detailed background checks, stricter nondisclosure agreements and acceptable use policies, and be willing to be subject to financial investigation. Periodic or

event-triggered updates to these background checks may also be in order, depending on the nature of the organization's activities and the risks it faces.
  * More auditing than regular user accounts. Privileged account activity should be monitored and audited at a greater rate and extent than regular usage.

Segregation of Duties

A core element of authorization is the **principle of segregation of duties** (also known as separation of duties). **Segregation of duties is based on the security practice that no one person should control an entire high-risk transaction from start to finish**. **Segregation of duties breaks the transaction into separate parts and requires a different person to execute each part of the transaction**. For example, an employee may submit an invoice for payment to a vendor (or for reimbursement to themselves), but it must be approved by a manager prior to payment; in another instance, almost anyone may submit a proposal for a change to a system configuration, but the request must go through technical and management review and gain approval, before it can be implemented.

These steps can prevent fraud or detect an error in the process before implementation. It could be that the same employee might be authorized to originally submit invoices regarding one set of activities, but not approve them, and yet also have approval authority but not the right to submit invoices on another. It is possible, of course, that two individuals can willfully work together to bypass the segregation of duties, so that they could jointly commit fraud. This is called collusion.

Another implementation of segregation of duties is dual control. This would apply at a bank where there are two separate combination locks on the door of the vault. Some personnel know one of the combinations and some know the other, but no one person knows both combinations. Two people must work together to open the vault; thus, the vault is under dual control.

The two-person rule is a security strategy that requires a minimum of two people to be in an area together, making it impossible for a person to be in the area alone. Many access control systems prevent an individual cardholder from entering a selected high-security area unless accompanied by at least one other person. Use of the two-person rule can help reduce insider threats to critical areas by requiring at least two individuals to be present at any time. It is also used for life safety within a security area; if one person has a medical emergency, there will be assistance present.

How Users Are Provisioned

Other situations that call for provisioning new user accounts or changing privileges include:

* **A new employee**: When a new employee is hired, the hiring manager sends a request to the security administrator to create a new user ID. This request authorizes creation of the new ID and provides instructions on appropriate access levels. Additional authorization may be required by company policy for elevated permissions.

* **Change of position**: When an employee has been promoted, their permissions and access rights might change as defined by the new role, which will dictate any added privileges and updates to access. At the same time, any access that is no longer needed in the new job will be removed.

* **Separation of employment**: When employees leave the company, depending on company policy and procedures, their accounts must be disabled after the termination date and time. It is recommended that accounts be disabled for a period before they are deleted to preserve the integrity of any audit trails or files that may be owned by the user. Since the account will no longer be used, it should be removed from any security roles or additional access profiles. This protects the company, so the separated employee is unable to access company data after separation, and it also protects them because their account cannot be used by others to access data.

Module 2: Understand Physical Access Controls

Domain D3.1, D3.1.1, D3.1.2

What Are Physical Security Controls?

Physical access controls are items you can physically touch, which include physical mechanisms deployed to prevent, monitor, or detect direct contact with systems or areas within a facility. Examples of 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.

Physical access controls are necessary to protect the assets of a company, including its most important asset, people. When considering physical access controls, the security of the personnel always comes first, followed by securing other physical assets.

Why Have Physical Security Controls?

Physical access controls include **fences, barriers, turnstiles, locks and other features that prevent unauthorized individuals from entering a physical site**, such as a workplace. This is to protect not only physical assets such as computers from being stolen, but also to protect the health and safety of the personnel inside.

Types of Physical Access Controls

Many types of physical access control mechanisms can be deployed in an environment to control, monitor and manage access to a facility. These range from deterrents to detection mechanisms. Each area requires unique and focused physical access controls, monitoring and prevention mechanisms.

Badge Systems and Gate Entry

Physical security controls for human traffic are often done with technologies such as turnstiles, mantraps and remotely or system-controlled door locks. For the system to identify an authorized employee, an access control system needs to have some form of enrollment station used to assign and activate an access control device. Most often, a badge is produced and issued with the employee's identifiers, with the enrollment station giving the employee specific areas that will be accessible. In high-security environments, enrollment may also include biometric characteristics. In general, an access control system compares an individual's badge against a verified database. If authenticated, the access control system sends output signals allowing authorized personnel to pass through a gate or a door to a controlled area. The systems are typically integrated with the organization's logging systems to document access activity (authorized and unauthorized)

A range of card types allow the system to be used in a variety of environments. These cards include: Bar code, Magnetic stripe, Proximity, Smart, Hybrid

Environmental Design

Crime Prevention through Environmental Design (CPTED) approaches the challenge of creating safer workspaces through passive design elements. This has great applicability for the information security community as security professionals design, operate and assess the organizational security environment. Other practices, such as standards for building construction and data centers, also affect how we implement controls over our physical environment. Security professionals should be familiar with these concepts so they can successfully advocate for functional and effective physical spaces where information is going to be created, processed and stored.

CPTED provides direction to solve the challenges of crime with organizational (people), mechanical (technology and hardware) and natural design (architectural and circulation flow) methods. By directing the flow of people, using passive techniques to signal who should and should not be in a space and providing visibility to otherwise hidden spaces, the likelihood that someone will commit a crime in that area decreases.

Biometrics

To authenticate a user's identity, biometrics uses characteristics unique to the individual seeking access. A biometric authentication solution entails two processes.

Enrollment—during the enrollment process, the user's registered biometric code is either stored in a system or on a smart card that is kept by the user.
Verification—during the verification process, the user presents their biometric data to the system so that the biometric data can be compared with the stored biometric code.

Even though the biometric data may not be secret, it is personally identifiable information, and the protocol should not reveal it without the user's consent. Biometrics takes two primary forms, physiological and behavioral.

Physiological systems measure the characteristics of a person such as a fingerprint, iris scan (the colored portion around the outside of the pupil in the eye), retinal scan (the pattern of blood vessels in the back of the eye), palm scan and venous scans that look for the flow of blood through the veins in the palm. Some biometrics devices combine processes together—such as checking for pulse and temperature on a fingerprint scanner—to detect counterfeiting.

Behavioral systems measure how a person acts by measuring voiceprints, signature dynamics and keystroke dynamics. As a person types, a keystroke dynamics system measures behavior such as the delay rate (how long a person holds down a key) and transfer rate (how rapidly a person moves between keys).

Biometric systems are considered highly accurate, but they can be expensive to implement and maintain because of the cost of purchasing equipment and registering all users. Users may also be uncomfortable with the use of biometrics, considering them to be an invasion of privacy or presenting a risk of disclosure of medical information (since retina scans can disclose medical conditions). A further drawback is the challenge of sanitization of the devices.

Monitoring

The use of physical access controls and monitoring personnel and equipment entering and leaving as well as auditing/logging all physical events are primary elements in maintaining overall organizational security.

Cameras

Cameras are normally integrated into the overall security program and centrally monitored. Cameras provide a flexible method of surveillance and monitoring. They can be a deterrent to

criminal activity, can detect activities if combined with other sensors and, if recorded, can provide evidence after the activity They are often used in locations where access is difficult or there is a need for a forensic record.While cameras provide one tool for monitoring the external perimeter of facilities, other technologies augment their detection capabilities. A variety of motion sensor technologies can be effective in exterior locations. These include infrared, microwave and lasers trained on tuned receivers. Other sensors can be integrated into doors, gates and turnstiles, and strain-sensitive cables and other vibration sensors can detect if someone attempts to scale a fence. Proper integration of exterior or perimeter sensors will alert an organization to any intruders attempting to gain access across open space or attempting to breach the fence line.

Logs

In this section, we are concentrating on the use of physical logs, such as a sign-in sheet maintained by a security guard, or even a log created by an electronic system that manages physical access. Electronic systems that capture system and security logs within software will be covered in another section.

A log is a record of events that have occurred. Physical security logs are essential to support business requirements. They should capture and retain information as long as necessary for legal or business reasons. Because logs may be needed to prove compliance with regulations and assist in a forensic investigation, the logs must be protected from manipulation. Logs may also contain sensitive data about customers or users and should be protected from unauthorized disclosure.

The organization should have a policy to review logs regularly as part of their organization's security program. As part of the organization's log processes, guidelines for log retention must be established and followed. If the organizational policy states to retain standard log files for only six months, that is all the organization should have.

A log anomaly is anything out of the ordinary. Identifying log anomalies is often the first step in identifying security-related issues, both during an audit and during routine monitoring. Some anomalies will be glaringly obvious: for example, gaps in date/time stamps or account lockouts. Others will be harder to detect, such as someone trying to write data to a protected directory. Although it may seem that logging everything so you would not miss any important data is the best approach, most organizations would soon drown under the amount of data collected.

Business and legal requirements for log retention will vary among economies, countries and industries. Some businesses will have no requirements for data retention. Others are mandated by the nature of their business or by business partners to comply with certain retention data. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires that

businesses retain one year of log data in support of PCI. Some federal regulations include requirements for data retention as well.

If a business has no business or legal requirements to retain log data, how long should the organization keep it? The first people to ask should be the legal department. Most legal departments have very specific guidelines for data retention, and those guidelines may drive the log retention policy.

Security Guards

Security guards are an effective physical security control. No matter what form of physical access control is used, a security guard or other monitoring system will discourage a person from masquerading as someone else or following closely on the heels of another to gain access. This helps prevent theft and abuse of equipment or information.

Alarm Systems

Alarm systems are commonly found on doors and windows in homes and office buildings. In their simplest form, they are designed to alert the appropriate personnel when a door or window is opened unexpectedly.

For example, an employee may enter a code and/or swipe a badge to open a door, and that action would not trigger an alarm. Alternatively, if that same door was opened by brute force without someone entering the correct code or using an authorized badge, an alarm would be activated.

Another alarm system is a fire alarm, which may be activated by heat or smoke at a sensor and will likely sound an audible warning to protect human lives in the vicinity. It will likely also contact local response personnel as well as the closest fire department.

Finally, another common type of alarm system is in the form of a panic button. Once activated, a panic button will alert the appropriate police or security personnel.

Module 3: Understand Logical Access Controls

Domain D3.2, D3.2.3, D3.2.4, D3.2.5

What are Logical Access Controls?

Whereas physical access controls are tangible methods or mechanisms that limit someone from getting access to an area or asset, logical access controls are electronic methods that

limit someone from getting access to systems, and sometimes even to tangible assets or areas. Types of logical access controls include:

* Passwords
* Biometrics (implemented on a system, such as a smartphone or laptop)
* Badge/token readers connected to a system

These types of electronic tools limit who can get logical access to an asset, even if the person already has physical access.

Discretionary Access Control (DAC)

Discretionary access control (DAC) is a specific type of access control policy that is **enforced over all subjects and objects in an information system**. In DAC, the policy specifies that **a subject who has been granted access to information can do one or more of the following**:

* Pass the information to other subjects or objects
* Grant its privileges to other subjects
* Change security attributes on subjects, objects, information systems or system components
* Choose the security attributes to be associated with newly created or revised objects; and/or
* Change the rules governing access control; mandatory access controls restrict this capability

Most information systems in the world are DAC systems. In a DAC system, a user who has access to a file is usually able to share that file with or pass it to someone else. This grants the user almost the same level of access as the original owner of the file. **Rule-based access control systems are usually a form of DAC**.

This methodology relies on the discretion of the owner of the access control object to determine the access control subject's specific rights. Hence, security of the object is literally up to the discretion of the object owner. DACs are not very scalable; they rely on the access control decisions made by each individual object owner, and it can be difficult to find the source of access control issues when problems occur.

Mandatory Access Control (MAC)

A mandatory access control (MAC) policy is one that is **uniformly enforced across all subjects and objects within the boundary of an information system**. In simplest terms, **this means that only properly designated security administrators, as trusted subjects, can modify any of the security rules that are established for subjects and objects within the system**. This also means that for all subjects defined by the organization (that is, known to its integrated identity management and access control system), the organization assigns a subset of total

privileges for a subset of objects, such that the subject is constrained from doing any of the following:

* Passing the information to unauthorized subjects or objects
* Granting its privileges to other subjects
* Changing one or more security attributes on subjects, objects, the information system or system components
* Choosing the security attributes to be associated with newly created or modified objects
* Changing the rules governing access control

Although MAC sounds very similar to DAC, **the primary difference is who can control access**. With Mandatory Access Control, **it is mandatory for security administrators to assign access rights or permissions**; **with Discretionary Access Control, it is up to the object owner's discretion**.

Role-Based Access Control (RBAC)

Role-based access control (RBAC), as the name suggests, sets up user permissions based on roles. Each role represents users with similar or identical permissions.

Role-based access control provides each worker privileges based on what role they have in the organization. Only Human Resources staff have access to personnel files, for example; only Finance has access to bank accounts; each manager has access to their own direct reports and their own department. Very high-level system administrators may have access to everything; new employees would have very limited access, the minimum required to do their jobs.

Monitoring these role-based permissions is important, because if you expand one person's permissions for a specific reason—say, a junior worker's permissions might be expanded so they can temporarily act as the department manager—but you forget to change their permissions back when the new manager is hired, then the next person to come in at that junior level might inherit those permissions when it is not appropriate for them to have them. This is called privilege creep or permissions creep. We discussed this before, when we were talking about provisioning new users.

Having multiple roles with different combinations of permissions can require close monitoring to make sure everyone has the access they need to do their jobs and nothing more. In this world where jobs are ever-changing, this can sometimes be a challenge to keep track of, especially with extremely granular roles and permissions. Upon hiring or changing roles, a best practice is to not copy user profiles to new users. It is recommended that standard roles are established, and new users are created based on those standards rather than an actual user. That way, new employees start with the appropriate roles and permissions.

@L2 Incident Response, Business Continuity and Disaster Recovery Concepts

Introduction

When we're talking about IR, BC and DR, we focus on availability, which is accomplished through those concepts.

* **Incident Response** (IR) plan responds to unexpected changes in operating conditions to keep the business operating;
* **Business Continuity** (BC) plan enables the business to continue operating throughout the crisis;
* **Disaster Recovery** (DR) plan is activated to help the business to return to normal operations as quickly as possible, if Incident Response and Business Continuity plans fail.

Module 1: Understand Incident Response

Domain D2.3.1, D2.3.2, D2.3.3

Incident Terminology

* **Breach** (NIST SP 800-53 Rev. 5): 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.

* **Event** (NIST SP 800-61 Rev 2): **Any observable occurrence** in a network or system.

* **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.

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

* **Threat** (NIST SP 800-30 Rev 1): **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.

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

* **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.

The Goal of Incident Response

The priority of any incident response is to protect life, health and safety. When any decision related to priorities is to be made, **always choose safety first**. **The primary goal of incident management is to be prepared**. Preparation requires having a policy and a response plan that will **lead the organization through the crisis**. Some organizations use the term “crisis management” to describe this process, so you might hear this term as well. An event is any measurable occurrence, and most events are harmless. However, if the event has the potential to disrupt the business’s mission, then it is called an incident. **Every organization must have an incident response plan that will help preserve business viability and survival.** The incident response process is aimed at reducing the impact of an incident so the organization can resume the interrupted operations as soon as possible. Note that incident response planning is a subset of the greater discipline of business continuity management (BCM).

Components of the Incident Response Plan

The incident response policy should reference **an incident response plan** that all employees will follow, depending on their role in the process. **The plan may contain several procedures and standards related to incident response**. It is a living representation of an organization’s incident response policy. The organization’s vision, strategy and mission should shape the incident response process. Procedures to implement the plan should define the technical processes, techniques, checklists and other tools that teams will use when responding to an incident.

* Preparation: Develop a policy approved by management; **Identify critical data and systems**, **single points of failure**; **Train staff on incident response**; Implement an incident response team. (covered in subsequent topic); Practice Incident Identification. (First Response); Identify Roles and Responsibilities; Plan the coordination of communication

between stakeholders; **Consider the possibility that a primary method of communication may not be available.**

* Detection and Analysis: Monitor all possible attack vectors; Analyze incident using known data and threat intelligence; Prioritize incident response; Standardize incident documentation;

* Containment, eradication and recovery: Gather evidence; Choose an appropriate containment strategy;
Identify the attacker; Isolate the attack.

* Post-incident activity: Identify evidence that may need to be retained. Document lessons learned. Retrospective, Preparation, Detection and Analysis, Containment, Eradication and Recovery Post-incident Activity.

Incident Response Team

Along with the organizational need to establish a **Security Operations Center (SOC)** is the need to create a suitable **incident response team**. A typical incident response team is a cross-functional group of individuals who represent the management, technical and functional areas of responsibility most directly impacted by a security incident. Potential team members include the following:

* Representative(s) of senior management
* Information security professionals
* Legal representatives
* Public affairs/communications representatives
* Engineering representatives (system and network)

Team members should have training on incident response and the organization's incident response plan. Typically, team members assist with **investigating the incident**, **assessing the damage**, **collecting evidence**, **reporting the incident and initiating recovery procedures**. They would also participate in the remediation and lessons learned stages and help with root cause analysis.

Many organizations now have a dedicated team responsible for investigating any computer security incidents that take place. These teams are commonly known as computer incident response teams (CIRTs) or computer security incident response teams (CSIRTs). When an incident occurs, the response team has four primary responsibilities:

* Determine the amount and scope of damage caused by the incident.
* Determine whether any confidential information was compromised during the incident.

* Implement any necessary recovery procedures to restore security and recover from incident-related damage.
* Supervise the implementation of any additional security measures necessary to improve security and prevent recurrence of the incident.

Module 2 Understand Business Continuity (BC)

Domain D2.1.1, D2.1.2, D2.1.3

The Importance of Business Continuity

The intent of a **business continuity plan** is **to sustain business operations while recovering from a significant disruption**. A key part of the plan is **communication**, including multiple contact methodologies and backup numbers in case of a disruption of power or communications. Many organizations will establish a phone tree, so that if one person is not available, they know who else to call.

Management must be included, because sometimes priorities may change depending on the situation. Individuals with proper authority must be there to execute operations, for instance, **if there are critical areas that need to be shut down**. **We need to have at hand the critical contact numbers for the supply chain**, as well as law enforcement and other sites outside of the facility. For example, a hospital may suffer a severe cyberattack that affects communications from the pharmacy, the internet or phone lines. In the United States, in case of this type of cyberattack that knocks out communications, specific numbers in specific networks can bypass the normal cell phone services and use military-grade networks. Those will be assigned to authorized individuals for hospitals or other critical infrastructures in case of a major disruption or cyberattack, so they can still maintain essential activity.

Components of a Business Continuity Plan

Business continuity planning (BCP) is the **proactive development of procedures to restore business operations after a disaster or other significant disruption to the organization**. Members from across the organization should participate in creating the BCP to ensure all systems, processes and operations are accounted for in the plan. **In order to safeguard the confidentiality, integrity and availability of information, the technology must align with the business needs**.

* 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. It's important to include when and how the plan will be used.
* Contact numbers for critical members of the supply chain (vendors, customers, possible external emergency providers, third-party partners)

How often should an organization test its business continuity plan (BCP)?

Routinely. Each individual organization must determine how often to test its BCP, but it should be tested at predefined intervals as well as when significant changes happen within the business environment.

Module 3: Understand Disaster Recovery (DR)

Domain D2.2, D2.2.1, D2.2.2, D2.2.3

The Goal of Disaster Recovery

Disaster recovery planning **steps in where BC leaves off**. When a disaster strikes or an interruption of business activities occurs, the Disaster recovery plan (DRP) guides the actions of emergency response personnel **until the end goal is reached—which is to see the business restored to full last-known reliable operations.** Disaster recovery refers specifically to **restoring the information technology and communications services and systems needed by an organization**, **both during the period of disruption caused by any event and during restoration of normal services**. The recovery of a business function may be done independently of the recovery of IT and communications services; however, the recovery of IT is often crucial to the recovery and sustainment of business operations. Whereas business continuity planning is about maintaining critical business functions, disaster recovery planning is about restoring IT and communications back to full operations after a disruption.

Components of a Disaster Recovery Plan

* 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
* Checklists for certain individuals:
  * Critical disaster recovery team members will have checklists to help guide their actions amid the chaotic atmosphere of a disaster.
  * IT personnel will have technical guides helping them get the alternate sites up and running.
  * Managers and public relations personnel will have simple-to-follow, high-level documents to help them communicate the issue accurately without requiring input from team members who are busy working on the recovery.

* Executive management should approve the plan and should be provided with a high-level summary of the plan.
* Public Relations should be a member of the disaster recovery plan to handle communications to all stakeholders.
* IT Personnel are primarily responsible for the disaster recovery team.

@L4 Network Security

Module 1: Understand Computer Networking

Domain D4.1.1, D4.1.2

What is Networking

A network is simply two or more computers linked together to share data, information or resources.

To properly establish secure data communications, it is important to explore all of the technologies involved in computer communications. From hardware and software to protocols and encryption and beyond, there are many details, standards and procedures to be familiar with.

Types of Networks

There are two basic types of networks:

* Local area network (LAN) - A local area network (LAN) is a network typically spanning a single floor or building. This is commonly a limited geographical area.
* Wide area network (WAN) - Wide area network (WAN) is the term usually assigned to the long-distance connections between geographically remote networks.

Network Devices

* **Hubs** are used to connect multiple devices in a network. They’re less likely to be seen in business or corporate networks than in home networks. Hubs are wired devices and are not as smart as switches or routers.

* You might consider using **a switch**, or what is also known as an intelligent hub. Switches are wired devices that know the addresses of the devices connected to them and route traffic to that port/device rather than retransmitting to all devices. Offering greater efficiency for traffic delivery and improving the overall throughput of data, switches are smarter than hubs,

but not as smart as routers. Switches can also create separate broadcast domains when used to create VLANs, which will be discussed later.

* **Routers** are used to control traffic flow on networks and are often used to connect similar networks and control traffic flow between them. Routers can be wired or wireless and can connect multiple switches. Smarter than hubs and switches, routers determine the most efficient “route” for the traffic to flow across the network.

* **Firewalls** are essential tools in managing and controlling network traffic and protecting the network. A firewall is a network device used to filter traffic. It is typically deployed between a private network and the internet, but it can also be deployed between departments (segmented networks) within an organization (overall network). Firewalls filter traffic based on a defined set of rules, also called filters or access control lists.

* A **server** is a computer that provides information to other computers on a network. Some common servers are web servers, email servers, print servers, database servers and file servers. All of these are, by design, networked and accessed in some way by a client computer. Servers are usually secured differently than workstations to protect the information they contain.

* **Endpoints** are the ends of a network communication link. One end is often at a server where a resource resides, and the other end is often a client making a request to use a network resource. An endpoint can be another server, desktop workstation, laptop, tablet, mobile phone or any other end user device.

Other Networking Terms

* Ethernet (IEEE 802.3) is a standard that defines wired connections of networked devices. This standard defines the way data is formatted over the wire to ensure disparate devices can communicate over the same cables.

* Media Access Control (MAC) Address - Every network device is assigned a Media Access Control (MAC) address. An example is 00-13-02-1F-58-F5. The first 3 bytes (24 bits) of the address denote the vendor or manufacturer of the physical network interface. No two devices can have the same MAC address in the same local network; otherwise an address conflict occurs.

* Internet Protocol (IP) Address - While MAC addresses are generally assigned in the firmware of the interface, IP hosts associate that address with a unique logical address. This logical IP address represents the network interface within the network and can be useful to maintain communications when a physical device is swapped with new hardware. Examples are 192.168.1.1 and 2001:db8::ffff:0:1.

Networking Models

Many different models, architectures and standards exist that provide ways to interconnect different hardware and software systems with each other for the purposes of sharing information, coordinating their activities and accomplishing joint or shared tasks.

Computers and networks emerge from the integration of communication devices, storage devices, processing devices, security devices, input devices, output devices, operating systems, software, services, data and people.

Translating the organization's security needs into safe, reliable and effective network systems needs to start with a simple premise. The purpose of all communications is to exchange information and ideas between people and organizations so that they can get work done.

Those simple goals can be re-expressed in network (and security) terms such as:

* Provide reliable, managed communications between hosts (and users)
* Isolate functions in layers
* Use packets (representation of data at L3 of OSI model) as the basis of communication
* Standardize routing, addressing and control
* Allow layers beyond internetworking to add functionality
* Be vendor-agnostic, scalable and resilient

In the most basic form, a network model has at least two layers:

* UPPER LAYER APPLICATION: also known as the host or application layer, is responsible for managing the integrity of a connection and controlling the session as well as establishing, maintaining and terminating communication sessions between two computers. It is also responsible for transforming data received from the Application Layer into a format that any system can understand. And finally, it allows applications to communicate and determines whether a remote communication partner is available and accessible.
  * APPLICATION
    * APPLICATION 7
    * PRESENTATION 6
    * SESSION 5
* LOWER LAYER: it is often referred to as the media or transport layer and is responsible for receiving bits from the physical connection medium and converting them into a frame. Frames are grouped into standardized sizes. Think of frames as a bucket and the bits as water. If the buckets are sized similarly and the water is contained within the buckets, the data can be transported in a controlled manner. Route data is added to the frames of data to create

packets. In other words, a destination address is added to the bucket. Once we have the buckets sorted and ready to go, the host layer takes over.

* DATA TRANSPORT
  * TRANSPORT 4
  * NETWORK 3
  * DATA LINK 2
  * PHYSICAL 1

Open Systems Interconnection (OSI) Model

The OSI Model was developed to establish a common way to describe the communication structure for interconnected computer systems. The OSI model serves as an abstract framework, or theoretical model, for how protocols should function in an ideal world, on ideal hardware. Thus, the OSI model has become a common conceptual reference that is used to understand the communication of various hierarchical components from software interfaces to physical hardware.

The OSI model divides networking tasks into seven distinct layers. Each layer is responsible for performing specific tasks or operations with the goal of supporting data exchange (in other words, network communication) between two computers. The layers are interchangeably referenced by name or layer number. For example, Layer 3 is also known as the Network Layer. The layers are ordered specifically to indicate how information flows through the various levels of communication. Each layer communicates directly with the layer above and the layer below it. For example, Layer 3 communicates with both the Data Link (2) and Transport (4) layers.

The Application, Presentation, and Session Layers (5-7) are commonly referred to simply as data. However, each layer has the potential to perform 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.). Encapsulation is the addition of header and possibly footer (trailer) data by a protocol used at that layer of the OSI model. Encapsulation is particularly important when discussing Transport, Network and Data Link layers (2-4), which all generally include some form of header. At the Physical Layer (1), the data unit is converted into binary, i.e., 01010111, and sent across physical wires such as an ethernet cable.

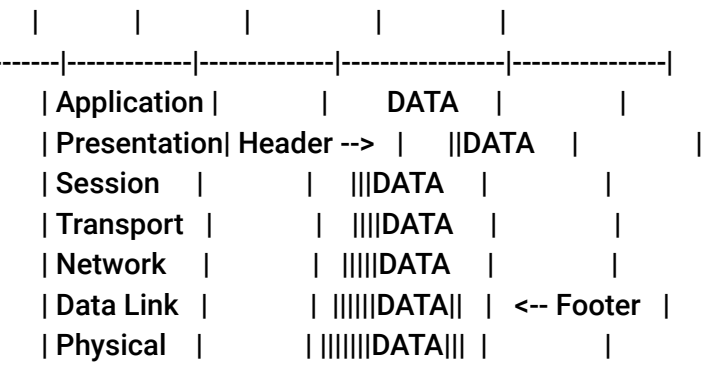
It's worth mapping some common networking terminology to the OSI Model so you can see the value in the conceptual model.

Consider the following examples:

* When someone references an image file like a JPEG or PNG, we are talking about the Presentation Layer (6).
* When discussing logical ports such as NetBIOS, we are discussing the Session Layer (5).
* When discussing TCP/UDP, we are discussing the Transport Layer (4).
* When discussing routers sending packets, we are discussing the Network Layer (3).
* When discussing switches, bridges or WAPs sending frames, we are discussing the Data Link Layer (2).

Encapsulation occurs as the data moves down the OSI model from Application to Physical. As data is encapsulated at each descending layer, the previous layer's header, payload and footer are all treated as the next layer's payload. The data unit size increases as we move down the conceptual model and the contents continue to encapsulate.

The inverse action occurs as data moves up the OSI model layers from Physical to Application. This process is known as de-encapsulation (or decapsulation). The header and footer are used to properly interpret the data payload and are then discarded. As we move up the OSI model, the data unit becomes smaller. The encapsulation/de-encapsulation process is best depicted visually below:



NB: Each of the OSI layers have their type of data as stated below:

OSI LAYER	TYPE OF DATA
-Application layer	Message
-Presentation layer	Message
-Session layer	Message
-Transport layer	Segment
-Network layer	Packets
-Data link layer	Frames
-Physical layer	Binary

NB: A simple way to memorize the 7 osi layers is using the mnemonics "ALL PEOPLE SEEM TO NEED DATA PROTECTION". ALL - Application, PEOPLE - Presentation, TO - Transport, NEED - Network, DATA - Data link, PROTECTION - Physical.

Transmission Control Protocol/Internet Protocol (TCP/IP)

The OSI model wasn't the first or only attempt to streamline networking protocols or establish a common communications standard. In fact, the most widely used protocol today, TCP/IP, was developed in the early 1970s. The OSI model was not developed until the late 1970s. The TCP/IP protocol stack focuses on the core functions of networking.

||TCP/IP Protocol Architecture Layers||
{**********}
Application Layer	Defines the protocols for the transport layer
Transport Layer	Permits data to move among devices
Internet Layer	Creates/inserts packets
Network Interface Layer	How data moves through the network

NB: Use mnemonics to memorize.

The most widely used protocol suite is TCP/IP, but it is not just a single protocol; rather, it is a protocol stack comprising dozens of individual protocols. TCP/IP is a platform-independent protocol based on open standards. However, this is both a benefit and a drawback. TCP/IP can be found in just about every available operating system, but it consumes a significant amount of resources and is relatively easy to hack into because it was designed for ease of use rather than for security.

At the Application Layer, TCP/IP protocols include **Telnet**, File Transfer Protocol (**FTP**), Simple Mail Transport Protocol (**SMTP**), and Domain Name Service (**DNS**). The two primary Transport Layer protocols of TCP/IP are **TCP and UDP**. **TCP is a full-duplex connection-oriented protocol, whereas UDP is a simplex connectionless protocol**. In the Internet Layer, **Internet Control Message Protocol (ICMP)** is used to determine the health of a network or a specific link. **ICMP is utilized by ping, traceroute and other network management tools**. The ping utility employs ICMP echo packets and bounces them off remote systems. Thus, you can use ping to determine whether the remote system is online, whether the remote system is responding promptly, whether the intermediary systems are supporting communications, and the level of performance efficiency at which the intermediary systems are communicating.

* Application, Presentation and Session layers at OSI model is equivalent to Application Layer at TCP/IP, and the protocol suite is: FTP, Telnet, SNMP, LPD, TFPT, SMTP, NFS, X Window.
* Transport layer are the same between OSI model and TCP/IP model, protocol suite: TCP, UDP
* Network layer at OSI model is equivalent to Internet layer at TCP/IP model, and protocol suite is: IGMP, IP, ICMP

* Data link and Physical layer at OSI model is equivalent at Network Interface layer at TCP/IP, and protocol suite is: Ethernet, Fast Ethernet, Token Ring, FDDI

Base concepts

* Switch: A device that routes traffic to the port of a known device
* Server: A computer that provides information to other computers
* Firewall: A device that filters network traffic based on a defined set of rules
* Ethernet: A standard that defines wired communications of networked devices
* IP Address: Logical address representing the network interface
* MAC Address: Address that denotes the vendor or manufactures of the physical network interface

Internet Protocol (IPv4 and IPv6)

IPv4 provides a 32-bit address space. IPv6 provides a 128-bit address space. The first one is exhausted nowadays, but it is still used because of NAT technology. 32 bits means 4 octets of 8 bits, which is represented in a dotted decimal notation such as 192.168.0.1, which means in binary notation 11000000 10101000 00000000 00000001

IP hosts/devices associate an address with a unique logical address. An IPv4 address is expressed as four octets separated by a dot (.), for example, 216.12.146.140. Each octet may have a value between 0 and 255. However, **0 is the network itself (not a device on that network), and 255 is generally reserved for broadcast purposes**. Each address is subdivided into two parts: **the network number and the host**. The network number assigned by an external organization, such as the Internet Corporation for Assigned Names and Numbers (ICANN), represents the organization's network. The host represents the network interface within the network.

To ease network administration, networks are typically divided into subnets. Because subnets cannot be distinguished with the addressing scheme discussed so far, a separate mechanism, **the subnet mask**, is used to define the part of the address used for the subnet. The mask is usually converted to decimal notation like 255.255.255.0. **With the ever-increasing number of computers and networked devices, it is clear that IPv4 does not provide enough addresses for our needs.** To overcome this shortcoming, **IPv4 was sub-divided into public and private address ranges.** Public addresses are limited with IPv4, but this issue was addressed in part with private addressing. Private addresses can be shared by anyone, and it is highly likely that everyone on your street is using the same address scheme.

The nature of the addressing scheme established by IPv4 meant that network designers had to start thinking in terms of IP address reuse. IPv4 facilitated this in several ways, such as its

creation of the private address groups; this allows every LAN in every SOHO (small office, home office) situation to use addresses such as 192.168.2.xxx for its internal network addresses, without fear that some other system can intercept traffic on their LAN. This table shows the private addresses available for anyone to use:

RANGE
10.0.0.0 to 10.255.255.254
172.16.0.0 to 172.31.255.254
192.168.0.0 to 192.168.255.254

The first octet of **127 is reserved for a computer's loopback address**. Usually, the address 127.0.0.1 is used. **The loopback address is used to provide a mechanism for self-diagnosis and troubleshooting at the machine level**. This mechanism allows a network administrator to treat a local machine as if it were a remote machine and ping the network interface to establish whether it is operational.

IPv6 is a modernization of IPv4, which addressed a number of weaknesses in the IPv4 environment:

* A much larger address field: IPv6 addresses are **128 bits**, which supports 2128 or 340,282,366,920,938,463,463,374,607,431,768,211,456 hosts. **This ensures that we will not run out of addresses**.
* Improved security:** IPsec is an optional part of IPv4 networks, but a mandatory component of IPv6 networks**. This will help ensure the integrity and confidentiality of IP packets and allow communicating partners **to authenticate with each other**.
* Improved quality of service (QoS): This will help services obtain an appropriate share of a network's bandwidth.

An IPv6 address is shown as **8 groups of four digits**. Instead of numeric (0-9) digits like IPv4, **IPv6 addresses use the hexadecimal range (0000-ffff) and are separated by colons (:)** rather than periods (.). An example IPv6 address is **2001:0db8:0000:0000:0000:ffff:0000:0001**. To make it easier for humans to read and type, it can be shortened by removing the leading zeros at the beginning of each field and substituting two colons (::) for the longest consecutive zero fields. All fields must retain at least one digit. After shortening, the example address above is rendered as 2001:db8::ffff:0:1, which is much easier to type. As in IPv4, there are some addresses and ranges that are reserved for special uses:

* ::1 is the local loopback address, used the same as 127.0.0.1 in IPv4.
* The range 2001:db8:: to 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff is reserved for documentation use, just like in the examples above.

* **fc00**:: to **fdff**:ffff:ffff:ffff:ffff:ffff:ffff:ffff are addresses reserved for internal network use and are not routable on the internet.

What is WiFi?

Wireless networking is a popular method of connecting corporate and home systems because of the ease of deployment and relatively low cost. It has made networking more versatile than ever before. Workstations and portable systems are no longer tied to a cable but can roam freely within the signal range of the deployed wireless access points. However, with this freedom comes additional vulnerabilities.

Wi-Fi range is generally wide enough for most homes or small offices, and range extenders may be placed strategically to extend the signal for larger campuses or homes. Over time the Wi-Fi standard has evolved, with each updated version faster than the last.

In a LAN, threat actors need to enter the physical space or immediate vicinity of the physical media itself. For wired networks, this can be done by placing sniffer taps onto cables, plugging in USB devices, or using other tools that require physical access to the network. By contrast, wireless media intrusions can happen at a distance.

Security of the Network

TCP/IP's vulnerabilities are numerous. Improperly implemented TCP/IP stacks in various operating systems are vulnerable to various **DoS/DDoS attacks**, **fragment attacks**, **oversized packet attacks**, **spoofing attacks**, **and man-in-the-middle attacks**. TCP/IP (as well as most protocols) is also subject to passive attacks via monitoring or sniffing. Network monitoring, or sniffing, is the act of monitoring traffic patterns to obtain information about a network.

Ports and Protocols (Applications/Services)

* Physical Ports: Physical ports are the ports on the routers, switches, servers, computers, etc. that you connect the wires, e.g., fiber optic cables, Cat5 cables, etc., to create a network.

* Logical Ports: When a communication connection is established between two systems, it is done using ports. A logical port (also called a socket) is little more than an address number that both ends of the communication link agree to use when transferring data. Ports allow a single IP address to be able to support multiple simultaneous communications, each using a different port number. In the Application Layer of the TCP/IP model (which includes the Session, Presentation, and Application Layers of the OSI model) reside numerous application- or service-specific protocols. Data types are mapped using port numbers associated with services. For example, web traffic (or HTTP) is port 80. Secure web traffic (or HTTPS) is port

443. Table 5.4 highlights some of these protocols and their customary or assigned ports. You'll note that in several cases a service (or protocol) may have two ports assigned, one secure and one insecure. When in doubt, systems should be implemented using the most secure version as possible of a protocol and its services.

* Well-known ports (0–1023): These ports are related to the common protocols that are at the core of the Transport Control Protocol/Internet Protocol (TCP/IP) model, Domain Name Service (DNS), Simple Mail Transfer Protocol (SMTP), etc.
* Registered ports (1024–49151): These ports are often associated with proprietary applications from vendors and developers. While they are officially approved by the Internet Assigned Numbers Authority (IANA), in practice many vendors simply implement a port of their choosing. Examples include Remote Authentication Dial-In User Service (RADIUS) authentication (1812), Microsoft SQL Server (1433/1434) and the Docker REST API (2375/2376).
* Dynamic or private ports (49152–65535): Whenever a service is requested that is associated with well-known or registered ports, those services will respond with a dynamic port that is used for that session and then released.

Secure Ports

Some network protocols transmit information in clear text, meaning it is not encrypted and should not be used. Clear text information is subject to network sniffing. This tactic uses software to inspect packets of data as they travel across the network and extract text such as usernames and passwords. Network sniffing could also reveal the content of documents and other files if they are sent via insecure protocols. The table below shows some of the insecure protocols along with recommended secure alternatives.

Insecure Port	Description	Protocol	Secure Alternative Port	Protocol
21	Port 21, File Transfer Protocol (FTP) sends the username and password **using plaintext from the client to the server**. This could be intercepted by an attacker and later used to retrieve confidential information from the server. **The secure alternative, SFTP, on port 22 uses encryption to protect the user credentials and packets of data being transferred**	File Transfer Protocol	22* - SFTP	Secure File Transfer Protocol
23	Port 23, telnet, is used by many Linux systems and any other systems **as a basic text-based terminal**. All information to and from the host on a telnet connection is sent in plaintext and **can be intercepted by an attacker**. This includes username and password as well as all information that is being presented on the screen, since this interface is all text. **Secure Shell (SSH) on port 22 uses encryption to ensure that traffic between the host and terminal is not sent in a plaintext format**	Telnet	22* - SSH	Secure Shell
25	Port 25, Simple Mail Transfer Protocol (SMTP) is the default unencrypted port for sending email messages. Since it is unencrypted, data contained within the emails could be discovered

by network sniffing. The secure alternative is to use port 587 for SMTP using Transport Layer Security (TLS) which will encrypt the data between the mail client and the mail server| Simple Mail Transfer Protocol | 587 - SMTP | SMTP with TLS |
37	Port 37, Time Protocol, may be in use by legacy equipment and has mostly been replaced by using port 123 for Network Time Protocol (NTP). NTP on port 123 offers better error-handling capabilities, which reduces the likelihood of unexpected errors	Time Protocol	123 - NTP	Network Time Protocol
53	Port 53, Domain Name Service (DNS), is still used widely. However, using DNS over TLS (DoT) on port 853 protects DNS information from being modified in transit	Domain Name Service	853 - DoT	DNS over TLS (DoT)
80	Port 80, HyperText Transfer Protocol (HTTP) is the basis of nearly all web browser traffic on the internet. Information sent via HTTP is not encrypted and is susceptible to sniffing attacks. HTTPS using TLS encryption is preferred, as it protects the data in transit between the server and the browser. Note that this is often notated as SSL/TLS. Secure Sockets Layer (SSL) has been compromised and is no longer considered secure. It is now recommended for web servers and clients to use Transport Layer Security (TLS) 1.3 or higher for the best protection	HyperText Transfer Protocol	443 - HTTPS	HyperText Transfer Protocol (SSL/TLS)
143	Port 143, Internet Message Access Protocol (IMAP) is a protocol used for retrieving emails. IMAP traffic on port 143 is not encrypted and susceptible to network sniffing. The secure alternative is to use port 993 for IMAP, which adds SSL/TLS security to encrypt the data between the mail client and the mail server	Internet Message Access Protocol	993 - IMAP	IMAP for SSL/TLS
161/162	Ports 161 and 162, Simple Network Management Protocol, are commonly used to send and receive data used for managing infrastructure devices. Because sensitive information is often included in these messages, it is recommended to use SNMP version 2 or 3 (abbreviated SNMPv2 or SNMPv3) to include encryption and additional security features. Unlike many others discussed here, all versions of SNMP use the same ports, so there is not a definitive secure and insecure pairing. Additional context will be needed to determine if information on ports 161 and 162 is secured or not	Simple Network Management Protocol	161/162 - SNMP	SNMPv3
445	Port 445, Server Message Block (SMB), is used by many versions of Windows for accessing files over the network. Files are transmitted unencrypted, and many vulnerabilities are well-known. Therefore, it is recommended that traffic on port 445 should not be allowed to pass through a firewall at the network perimeter. A more secure alternative is port 2049, Network File System (NFS). Although NFS can use encryption, it is recommended that NFS not be allowed through firewalls either	Server Message Block	2049 - NFS	Network File System
389	Port 389, Lightweight Directory Access Protocol (LDAP), is used to communicate directory information from servers to clients. This can be an address book for email or usernames for logins. The LDAP protocol also allows records in the directory to be updated, introducing additional risk. Since LDAP is not encrypted, it is susceptible to sniffing and manipulation attacks. Lightweight Directory Access Protocol Secure (LDAPS) adds SSL/TLS

security to protect the information while it is in transit | Lightweight Directory Access Protocol | 636 - LDAPS | Lightweight Directory Access Protocol Secure |

NB: There is a high chance of seeing a question on protocols and their port numbers.
–FTP(file transfer protocol) port number is 21.
–SSH (secure shell) port number is 22.
–SFTP(ssh file transfer protocol) port number is 22
–TELNET(Teletype network) port number is 23
–SMTP(simple mail transfer protocol) port number is 25
–DNS(domain name system) port number is 53
–HTTP(hypertext transfer protocol) port number is 80
–HTTPS(hypertext transfer protocol secure) port number is 443
–FTPS(file transfer protocol secure) port number is 990

SYN, SYN-ACK, ACK

Module 2 Understand Network (Cyber) Threats and Attacks

Domain D4.1.2, D4.2.2, D4.2.3

Types of Threats

* Spoofing: an attack with the goal of **gaining access to a target system through the use of a falsified identity**. Spoofing can be used against IP addresses, MAC address, usernames, system names, wireless network SSIDs, email addresses, and many other types of logical identification.

* Phishing: an attack that **attempts to misdirect legitimate users to malicious websites through** the abuse of **URLs or hyperlinks in emails could be considered phishing**.

* DoS/DDoS: a denial-of-service (DoS) attack is a network resource consumption attack that has the **primary goal of preventing legitimate activity on a victimized system**. Attacks involving numerous unsuspecting secondary victim systems are known as distributed denial-of-service (DDoS) attacks.

* Virus: The computer virus is perhaps the earliest form of malicious code to plague security administrators. As with biological viruses, **computer viruses have two main functions—propagation and destruction**. A virus is a **self-replicating** piece of code that

spreads without the consent of a user, but frequently with their assistance (a user has to click on a link or open a file).

* Worm: Worms pose a significant **risk to network security**. They contain the same destructive potential as other malicious code objects with an added twist—they propagate themselves without requiring any human intervention.

* Trojan: the Trojan is a software program **that appears benevolent but carries a malicious**, behind-the-scenes payload that has the potential to wreak havoc on a system or network. For example, ransomware often uses a Trojan to infect a target machine and then uses encryption technology to encrypt documents, spreadsheets and other files stored on the system with a key known only to the malware creator.

* On-path attack: In an on-path attack, attackers place themselves between two devices, often between a web browser and a web server, to intercept or modify information that is intended for one or both of the endpoints. **On-path attacks** are also known as **man-in-the-middle (MITM) attacks**.

* Side-channel: A side-channel attack is a **passive**, **noninvasive attack** to **observe the operation of a device**. Methods include power monitoring, timing and fault analysis attacks.

* Advanced Persistent Threat: Advanced persistent threat (APT) refers to **threats that demonstrate an unusually high level of technical and operational sophistication spanning months or even years**. APT attacks are often conducted by highly organized groups of attackers.

* Insider Threat: Insider threats are threats that **arise from individuals who are trusted by the organization**. These could be disgruntled employees or employees involved in espionage. Insider threats are not always willing participants. A trusted user who falls victim to a scam could be an unwilling insider threat.

* Malware: A program that is inserted into a system, usually covertly, **with the intent of compromising the confidentiality, integrity or availability of the victim's data**, applications or operating system or otherwise annoying or disrupting the victim.

* Ransomware: Malware used for the purpose of facilitating a ransom attack. Ransomware attacks often use cryptography to “lock” the files on an affected computer and require the payment of a ransom fee in return for the “unlock” code.

Identify Threats and Tools Used to Prevent Them

Here are some examples of steps that can be taken to protect networks.

* If a system doesn't need a service or protocol, it should not be running. Attackers cannot exploit a vulnerability in a service or protocol that isn't running on a system.
* Firewalls can prevent many different types of attacks. Network-based firewalls protect entire networks, and host-based firewalls protect individual systems.

Identify Threats and Tools Used to Prevent Them Continued

* Intrusion Detection System (IDS) is a form of monitoring to detect abnormal activity; it detects intrusion attempts and system failures. Identifies Threats, Do not prevent threats
* Host-based IDS (HIDS) monitors activity on a single computer. Identify threats, Do not prevent Threats.
* Network-based IDS (NIDS) monitors and evaluates network activity to detect attacks or event anomalies. Identify threats, Do not prevent Threats.
* SIEM gathers log data from sources across an enterprise to understand security concerns and apportion resources. Identify threats, Do not prevent Threats.
* Anti-malware/Antivirus seeks to identify malicious software or processes. Identifies and Prevent threats.
* Scans evaluate the effectiveness of security controls. Identify threats, Do not prevent Threats.
* Firewall filters network traffic - managers and controls network traffic and protects the network. Identifies and Prevent threats.
* Intrusion Protection System (IPS-NIPS/HIPS) is an active IDS that automatically attempts to detect and block attacks before they reach target systems. Identifies and Prevent threats.

Intrusion Detection System (IDS)

An intrusion occurs when an attacker is able to bypass or thwart security mechanisms and gain access to an organization's resources. Intrusion detection is a specific form of monitoring **that monitors recorded information and real-time events to detect abnormal activity indicating a potential incident or intrusion**. An intrusion detection system (IDS) **automates the inspection of logs and real-time system events to detect intrusion attempts and system failures**. An IDS is intended as part of a **defense-in-depth security plan**. **IDSs can** recognize attacks that come from external connections and attacks that spread internally. Once they detect a suspicious event, they respond by sending alerts or raising alarms. A primary goal of an IDS is to provide a means for a timely and accurate response to intrusions.

IDS types are commonly classified as host-based and network-based. A host-based IDS (HIDS) monitors a single computer or host. A network-based IDS (NIDS) monitors a network by observing network traffic patterns.

Host-based Intrusion Detection System (HIDS): A HIDS monitors activity **on a single computer**, including **process calls and information recorded in system, application, security and host-based firewall logs**. It can often examine events in more detail than a NIDS can, and it can pinpoint specific files compromised in an attack. **It can also track processes employed by the attacker.** A benefit of HIDSs over NIDSs is that HIDSs can detect anomalies on the host system that NIDSs cannot detect. For example, **a HIDS can detect infections where an intruder has infiltrated a system and is controlling it remotely.** HIDSs are more costly to manage than NIDSs because they require administrative attention on each system, whereas NIDSs usually support centralized administration. A HIDS cannot detect network attacks on other systems.

Network Intrusion Detection System (NIDS): A NIDS monitors and **evaluates network activity to detect attacks or event anomalies**. **It cannot monitor the content of encrypted traffic but can monitor other packet details**. A single NIDS can monitor **a large network by using remote sensors to collect data at key network locations that send data to a central management console**. These sensors can monitor traffic at **routers, firewalls, network switches that support port mirroring, and other types of network taps**. **A NIDS has very little negative effect on the overall network performance**, and when it is deployed on a single-purpose system, it doesn't adversely affect performance on any other computer. A NIDS is usually able to detect the initiation of an attack or ongoing attacks, but they can't always provide information about the success of an attack. They won't know if an attack affected specific systems, user accounts, files or applications.

Security Information and Event Management (SIEM): Security management involves the **use of tools that collect information about the IT environment from many disparate sources to better examine the overall security of the organization and streamline security efforts**. These tools are generally known as **security information and event management** (or S-I-E-M, pronounced "SIM") solutions. The general **idea of a SIEM solution is to gather log data from various sources across the enterprise to better understand potential security concerns and apportion resources accordingly**. SIEM systems can be used along with other components (defense-in-depth) as part of an overall information security program.

Preventing Threats

* Keep systems and applications up to date. Vendors regularly release patches to correct bugs and security flaws, but these only help when they are applied. Patch management ensures that systems and applications are kept up to date with relevant patches.
* **Remove or disable unneeded services and protocols**. If a system doesn't need a service or protocol, it should not be running. Attackers cannot exploit a vulnerability in a service or protocol that isn't running on a system. As an extreme contrast, imagine a web server is running every available service and protocol. It is vulnerable to potential attacks on any of these services and protocols.

* **Use intrusion detection and prevention systems**. As discussed, intrusion detection and prevention systems observe activity, attempt to detect threats and provide alerts. They can often block or stop attacks.
* **Use up-to-date anti-malware software**. We have already covered the various types of malicious code such as viruses and worms. A primary countermeasure is anti-malware software.
* **Use firewalls**. Firewalls can prevent many different types of threats. Network-based firewalls protect entire networks, and host-based firewalls protect individual systems. This chapter included a section describing how firewalls can prevent attacks.

Antivirus: it is a requirement for **compliance with the Payment Card Industry Data Security Standard (PCI DSS)**. Antivirus systems try to identify malware based **on the signature of known malware or by detecting abnormal activity on a system**. This identification is done with various **types of scanners, pattern recognition and advanced machine learning algorithms**. Anti-malware now goes beyond just virus protection as modern solutions try to provide a more holistic approach detecting rootkits, ransomware and spyware. Many endpoint solutions also include software firewalls and IDS or IPS systems.

Scans: Regular vulnerability and port scans are a good way to evaluate the effectiveness of security controls used within an organization. They may reveal areas where patches or security settings are insufficient, where new vulnerabilities have developed or become exposed, and where security policies are either ineffective or not being followed. Attackers can exploit any of these vulnerabilities.

Firewalls: Early computer security engineers borrowed that name for the devices and services that isolate network segments from each other, as a security measure. As a result, firewalling refers to the process of designing, using or operating different processes in ways that **isolate high-risk activities from lower-risk ones**. **Firewalls enforce policies by filtering network traffic based on a set of rules.** While a firewall should always be placed at internet gateways, other internal network considerations and conditions determine where a firewall would be employed, such as network zoning or segregation of different levels of sensitivity. Firewalls have rapidly evolved over time to provide enhanced security capabilities. **It integrates a variety of threat management capabilities into a single framework, including proxy services, intrusion prevention services (IPS) and tight integration with the identity and access management (IAM) environment to ensure only authorized users are permitted to pass traffic across the infrastructure.** While firewalls can manage traffic **at Layers 2 (MAC addresses)**, **3 (IP ranges)** and **7 (application programming interface (API)** and **application firewalls**), **the traditional implementation has been to control traffic at Layer 4**. Traditional firewalls have PORTS IP Address, IDS/IPS, Antivirus Gateway, WebProxy, VPN; NG Firewalls have PORTS IP Address, IAM Attributes, IDS/IPS, WebProxy, Anti-Bot, Antivirus Gateway, VPN, FaaS.

Intrusion Prevention System (IPS): An intrusion prevention system (IPS) is a special type of active IDS **that automatically attempts to detect and block attacks before they reach target systems**. A distinguishing difference between an IDS and an IPS is that the **IPS is placed in line with the traffic**. In other words, **all traffic must pass through the IPS and the IPS can choose what traffic to forward and what traffic to block after analyzing it**. This allows the IPS to prevent an attack from reaching a target. Since IPS systems are most effective at preventing network-based attacks, it is common to see the IPS function integrated into firewalls. Just like IDS, there are Network-based IPS (NIPS) and Host-based IPS (HIPS).

Module 3 Understand Network Security Infrastructure

Domain D4.3.1, D4.3.2

On-Premises Data Centers

When it comes to data centers, there are two primary options: organizations can **outsource the data center or own the data center**. If the data center is owned, it will likely be built on premises. A place, like a building for the data center is needed, along with **power, HVAC, fire suppression and redundancy**.

* **Data Center/Closets**: The facility wiring infrastructure is **integral to overall information system security and reliability**. **Protecting access to the physical layer of the network is important** in minimizing intentional or unintentional damage. **Proper protection of the physical site** must address these sorts of security challenges. Data centers and wiring closets may include the following: Phone, network, special connections; ISP or telecommunications provider equipment; Servers; Wiring and/or switch components.

* **Heating, Ventilation and Air Conditioning (HVAC) / Environmental**: High-density equipment and equipment within enclosed spaces **requires adequate cooling and airflow**. Well-established standards for the operation of computer equipment exist, and equipment is tested against these standards. For example, the recommended range for optimized maximum uptime and hardware life is **from 18° to 27°C**, and it is recommended that a rack have three temperature sensors, positioned at the top, middle and bottom of the rack, to measure the actual operating temperature of the environment. Proper management of data center temperatures, including cooling, is essential. **Cooling is not the only issue with airflow**: Contaminants like dust and noxious fumes require appropriate controls to minimize their impact on equipment. Monitoring for water or gas leaks, sewer overflow or HVAC failure should be integrated into the building control environment, with appropriate alarms to signal to organizational staff. Contingency planning to respond to the warnings should prioritize the systems in the building, so the impact of a major system failure on people, operations or other infrastructure can be minimized.

* Power: Data centers and information systems in general consume a tremendous amount of electrical power, **which needs to be delivered both constantly and consistently**. Wide fluctuations in the quality of power affect system lifespan, while disruptions in supply completely stop system operations. Power at the site is always an integral part of data center operations. Regardless of fuel source, backup generators must be sized to provide for the critical load (the computing resources) and the supporting infrastructure. Similarly, battery backups must be properly sized to carry the critical load until generators start and stabilize. As with data backups, testing is necessary to ensure the failover to alternate power works properly.

* Fire Suppression: For server rooms, appropriate fire detection/suppression must be considered based on the size of the room, typical human occupation, egress routes and risk of damage to equipment. For example, water used for fire suppression would cause more harm to servers and other electronic components. Gas-based fire suppression systems are more friendly to the electronics, but can be toxic to humans.

Which of the following is typically associated with an on-premises data center? **Fire suppression is associated**, **HVAC is associated**, **Power is associated** are all associated with an on-premises data center.

Which of the following is not a source of redundant power? **HVAC is not a source of redundant power**, but it is something that needs to be protected by a redundant power supply, which is what the other three options will provide. What happens if the HVAC system breaks and equipment gets too hot? If the temperature in the data center gets too hot, then there is a risk that the server will shut down or fail sooner than expected, which presents a risk that data will be lost. So that is another system that requires redundancy in order to reduce the risk of data loss. But it is not itself a source of redundant power.

Redundancy

The concept of redundancy is to design systems with **duplicate components so that if a failure were to occur, there would be a backup**. This can apply to the data center as well. Risk assessments pertaining to the data center should identify when multiple separate utility service entrances are necessary for redundant communication channels and/or mechanisms.

If the organization requires full redundancy, devices should have two power supplies connected to diverse power sources. Those power sources would be backed up by batteries and generators. In a high-availability environment, even generators would be redundant and fed by different fuel types.

Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA)

Some organizations seeking to minimize downtime and **enhance BC (Business Continuity) and DR (Disaster Recovery) capabilities** will create agreements with other, similar organizations. They agree that if one of the parties experiences an emergency and cannot operate within their own facility, the other party will share its resources and let them operate within theirs in order to maintain critical functions. These agreements often even include competitors, because their facilities and resources meet the needs of their particular industry.

These agreements are called joint operating agreements (JOA) or memoranda of understanding (MOU) or memoranda of agreement (MOA). Sometimes these agreements are mandated by regulatory requirements, or they might just be part of the administrative safeguards instituted by an entity within the guidelines of its industry.

The difference between an MOA or MOU and an SLA is that a Memorandum of Understanding is more directly related to what can be done with a system or the information.

The service level agreement goes down to the granular level. For example, if I'm outsourcing the IT services, then I will need to have two full-time technicians readily available, at least from Monday through Friday from eight to five. With cloud computing, I need to have access to the information in my backup systems within 10 minutes. An SLA specifies the more intricate aspects of the services.

We must be very cautious when outsourcing with cloud-based services, because we have to make sure that we understand exactly what we are agreeing to. If the SLA promises 100 percent accessibility to information, is the access directly to you at the moment, or is it access to their website or through their portal when they open on Monday? That's where you'll rely on your legal team, who can supervise and review the conditions carefully before you sign the dotted line at the bottom.

Cloud

Cloud computing is usually associated with an internet-based set of computing resources, and typically sold as a service, provided by a **cloud service provider (CSP)**. **It is a very scalable, elastic and easy-to-use “utility” for the provisioning and deployment of Information Technology (IT) services**. There are various definitions of what cloud computing means according to the leading standards, **including NIST**. This NIST definition is commonly used around the globe, cited by professionals and others alike to clarify what the term “cloud” means: “**a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.**” NIST SP 800-145

Cloud Characteristics

Cloud-based assets include any resources that an organization accesses using cloud computing. **Cloud computing refers to on-demand access to computing resources available from almost anywhere**, **and cloud computing resources are highly available and easily scalable**. Organizations typically lease cloud-based resources from outside the organization. Cloud computing has many benefits for organizations, which include but are not limited to:

* Resource Pooling
  * Broad Network Access
  * Rapid Elasticity
  * Measured Service
  * On-Demand Self-Service

* Usage is metered and priced according to units (or instances) consumed. This can also be billed back to specific departments or functions.
* Reduced cost of ownership. There is no need to buy any assets for everyday use, no loss of asset value over time and a reduction of other related costs of maintenance and support.
* Reduced energy and cooling costs, along with “green IT” environment effect with optimum use of IT resources and systems.
* Allows an enterprise to scale up new software or data-based services/solutions through cloud systems quickly and without having to install massive hardware locally.

Service Models

Some cloud-based services only provide data storage and access. When storing data in the cloud, organizations must ensure that security controls are in place to prevent unauthorized access to the data. There are varying levels of responsibility for assets depending on the service model. This includes maintaining the assets, ensuring they remain functional, and keeping the systems and applications up to date with current patches. In some cases, the cloud service provider is responsible for these steps. In other cases, the consumer is responsible for these steps.

Types of cloud computing service models include Software as a Service (SaaS) , Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

* Services
  * Software As Service (SaaS): A cloud provides access to **software applications such as email or office productivity tools**. SaaS **is a distributed model** where software applications are hosted by a vendor or cloud service provider and made available to customers over network resources. SaaS has many benefits for organizations, which include but are not limited to: **Ease of use and limited/minimal administration**. **Automatic updates and patch

management**. **The user will always be running the latest version and most up-to-date deployment of the software release, as well as any relevant security updates, with no manual patching required**. Standardization and compatibility. All users will have the same version of the software release.

* Platform As Service (PaaS): **A cloud provides an environment for customers to use to build and operate their own software**. PaaS is **a way for customers to rent hardware, operating systems, storage and network capacity over the internet from a cloud service provider**. The service delivery model allows customers **to rent virtualized servers and associated services for running existing applications or developing and testing new ones**. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application-hosting environment configurations. **A PaaS cloud provides a toolkit for conveniently developing, deploying and administering application software that is structured to support large numbers of consumers, process very large quantities of data and potentially be accessed from any point on the internet**. PaaS clouds will typically provide a set of software building blocks and a set of development tools such as programming languages and supporting run-time environments that facilitate the construction of high-quality, scalable applications. Additionally, PaaS clouds will typically provide tools that assist with the deployment of new applications. In some cases, deploying a new software application in a PaaS cloud is not much more difficult than uploading a file to a web server. PaaS clouds will also generally provide and maintain the computing resources (e.g., processing, storage and networking) that consumer applications need to operate. PaaS clouds provide many benefits for developers, including that the operating system can be changed and upgraded frequently, along with associated features and system services.

* Infrastructure As Service (IaaS): A cloud provides network access **to traditional computing resources such as processing power and storage**. IaaS models **provide basic computing resources to consumers**. This includes **servers, storage, and in some cases, networking resources.** Consumers install operating systems and applications and perform all required maintenance on the operating systems and applications. Although the consumer has use of the related equipment, the cloud service provider retains ownership and is ultimately responsible for hosting, running and maintenance of the hardware. IaaS is also referred to as hardware as a service by some customers and providers. IaaS has a number of benefits for organizations, which include but are not limited to: Ability to scale up and down infrastructure services based on actual usage. This is particularly useful and beneficial where there are significant spikes and dips within the usage curve for infrastructure. Retain system control at the operating system level.

Deployment Models

Clouds

* Public: what we commonly **refer to as the cloud for the public user**. **There is no real mechanism, other than applying for and paying for the cloud service**. It is **open to the public and is**, therefore, **a shared resource that many people will be able to use as part of a resource pool**. A public cloud deployment model includes assets available for any consumers to rent or lease and is hosted by an external cloud service provider (CSP). Service level agreements can be effective at ensuring the CSP provides the cloud-based services at a level acceptable to the organization.

* Private: it begins with the same technical concept as public clouds, **except that instead of being shared with the public, they are generally developed and deployed for a private organization that builds its own cloud**. Organizations can create and host private clouds using their own resources. Therefore, this deployment model includes cloud-based assets for a single organization. As such, the organization is responsible for all maintenance. However, an organization can also rent resources from a third party and split maintenance requirements based on the service model (SaaS, PaaS or IaaS). Private clouds provide organizations and their departments private access to the computing, storage, networking and software assets that are available in the private cloud.

* Hybrid: it is created by **combining two forms of cloud computing deployment models, typically a public and private cloud**. Hybrid cloud computing **is gaining popularity with organizations by providing them with the ability to retain control of their IT environments**, conveniently allowing them to use public cloud service to fulfill non-mission-critical workloads, and taking advantage of flexibility, scalability and cost savings. Important drivers or benefits of hybrid cloud deployments include: Retaining ownership and oversight of critical tasks and processes related to technology, Reusing previous investments in technology within the organization, Control over most critical business components and systems, and Cost-effective means to fulfilling noncritical business functions (utilizing public cloud components).

* Community: it can be either public or private. **What makes them unique is that they are generally developed for a particular community**. An example could be a public community cloud focused primarily on organic food, or maybe a community cloud focused specifically on financial services. The idea behind the community cloud is that people of like minds or similar interests can get together, share IT capabilities and services, and use them in a way that is beneficial for the particular interests that they share.

Managed Service Provider (MSP)

A managed service provider (MSP) is **a company that manages information technology assets for another company**. Small- and medium-sized businesses commonly **outsource part or all of their information technology functions to an MSP to manage day-to-day operations or to provide expertise in areas the company does not have**. Organizations may also use an MSP to provide network and security monitoring and patching services. Today,

many MSPs offer cloud-based services augmenting SaaS solutions with active incident investigation and response activities. One such example is a managed detection and response (MDR) service, where a vendor monitors firewall and other security tools to provide expertise in triaging events.

Some other common MSP implementations are: Augment in-house staff for projects; Utilize expertise for implementation of a product or service; Provide payroll services; Provide Help Desk service management; Monitor and respond to security incidents; Manage all in-house IT infrastructure.

Service-Level Agreement (SLA)

The cloud computing **service-level agreement (cloud SLA)** is an agreement **between a cloud service provider and a cloud service customer based on a taxonomy of cloud computing–** specific terms to set the quality of the cloud services delivered. It characterizes quality of the cloud services delivered in terms of a set of measurable properties specific to cloud computing (business and technical) and a given set of cloud computing roles (cloud service customer, cloud service provider, and related sub-roles).

Think of a **rule book and legal contract—that combination is what you have in a service-level agreement (SLA)**. Let us not underestimate or downplay the importance of this document/ agreement. In it, **the minimum level of service, availability, security, controls, processes, communications, support and many other crucial business elements are stated and agreed to by both parties**.

The purpose of an **SLA is to document specific parameters, minimum service levels and remedies for any failure to meet the specified requirements**. It should also affirm data ownership and specify data return and destruction details. Other important SLA points to consider include the following: Cloud system infrastructure details and security standards; Customer right to audit legal and regulatory compliance by the CSP; Rights and costs associated with continuing and discontinuing service use; Service availability; Service performance; Data security and privacy; Disaster recovery processes; Data location; Data access; Data portability; Problem identification and resolution expectations; Change management processes; Dispute mediation processes; Exit strategy;

Network Design

* **Network segmentation** involves controlling traffic **among networked devices**. Complete or physical network segmentation occurs when a network is isolated from all outside communications, so transactions can only occur between devices within the segmented network.

* **A DMZ, which stands for Demilitarized Zone,** is a network area that is designed to be **accessed by outside visitors but is still isolated from the private network of the organization**. The DMZ is often the host of public web, email, file and other resource servers.

* **VLANs, which stands for Virtual Private Network**, are created by **switches to logically segment a network without altering its physical topology**.

* **A virtual private network (VPN)** is a **communication tunnel that provides point-to-point transmission of both authentication and data traffic over an untrusted network**.

* **Defense in depth** uses multiple **types of access controls in literal or theoretical layers** to help an organization avoid a monolithic security stance.

* **Network access control (NAC)** is a concept of controlling access to an environment through strict adherence to and implementation of security policy.

Defense in Depth

Defense in depth uses **a layered approach when designing the security posture of an organization**. Think about a castle that holds the crown jewels. The jewels will be placed in a vaulted chamber in a central location guarded by security guards. The castle is built around the vault with additional layers of security—soldiers, walls, a moat. The same approach is true when designing the logical security of a facility or system. Using layers of security will deter many attackers and encourage them to focus on other, easier targets.

Defense in depth **provides more of a starting point for considering all types of controls—administrative, technological, and physical—that empower insiders and operators to work together to protect their organization and its systems**.

Some examples that further explain the concept of defense in depth:

* **Data**: Controls that protect the actual data with technologies such as **encryption, data leak prevention, identity and access management and data controls**.
* **Application**: Controls that protect the application itself with technologies such as **data leak prevention, application firewalls and database monitors**.
* **Host**: Every control that is placed at the endpoint level, such as **antivirus, endpoint firewall, configuration and patch management**.
* **Internal network**: Controls that are in place to protect **uncontrolled data flow and user access across the organizational network**. Relevant technologies include **intrusion detection systems, intrusion prevention systems, internal firewalls and network access controls**.

* **Perimeter**: Controls that protect against **unauthorized access to the network**. This level includes the use of technologies such as **gateway firewalls, honeypots, malware analysis and secure demilitarized zones (DMZs)**.
* **Physical**: Controls that provide a physical barrier, such as **locks, walls or access control**.
* **Policies, procedures and awareness**: Administrative controls that reduce **insider threats (intentional and unintentional) and identify risks as soon as they appear**.

Zero Trust

Zero trust networks are often **micro segmented networks, with firewalls at nearly every connecting point**. Zero trust encapsulates information assets, the services that apply to them and their security properties. **This concept recognizes that once inside a trust-but-verify environment, a user has perhaps unlimited capabilities to roam around, identify assets and systems and potentially find exploitable vulnerabilities**. Placing a greater number of firewalls or other security boundary control devices throughout the network increases the number of opportunities to detect a troublemaker before harm is done. **Many enterprise architectures are pushing this to the extreme of microsegmenting their internal networks, which enforces frequent re-authentication of a user ID**.

Zero trust is an evolving design approach **which recognizes that even the most robust access control systems have their weaknesses**. It adds defenses at the user, asset and data level, rather than relying on perimeter defense. In the extreme, **it insists that every process or action a user attempts to take must be authenticated and authorized**; **the window of trust becomes vanishingly small**.

While microsegmentation adds internal perimeters, zero trust places the focus on the assets, or data, rather than the perimeter. Zero trust builds more effective gates to protect the assets directly rather than building additional or higher walls.

Network Access Control (NAC)

We need to be able to see **who and what is attempting to make a network connection**. At one time, network access was limited to internal devices. Gradually, that was extended to remote connections, **although initially those were the exceptions rather than the norm**. This started to change with the concepts of bring your own device (BYOD) and Internet of Things (IoT).

Considering just IoT for a moment, it is important to understand the range of devices that might be found within an organization.

The organization's **access control policies and associated security policies should be enforced via the NAC device(s). Remember, of course, that an access control device only enforces a policy and doesn't create one**.

The NAC device will provide **the network visibility needed for access security and may later be used for incident response**. Aside from identifying connections, it should also be able to provide isolation for non compliant devices within a quarantined network and provide a mechanism to "fix" the noncompliant elements, such as turning on endpoint protection. In short, the goal is to ensure that all devices wishing to join the network do so only when they comply with the requirements laid out in the organization policies. This visibility will encompass internal users as well as any temporary users such as guests or contractors, etc., and any devices they may bring with them into the organization.

Let's consider some possible use cases for NAC deployment: Medical devices; IoT devices; BYOD/mobile devices (laptops, tablets, smartphones); Guest users and contractors;

It is critically important that all mobile devices, regardless of their owner, go through an onboarding process, ideally each time a network connection is made, and that the device is identified and interrogated to ensure the organization's policies are being met.

Network Segmentation (Demilitarized Zone (DMZ))

Network segmentation is also **an effective way to achieve defense in depth for distributed or multi-tiered applications**. The use of a demilitarized zone (DMZ), for example, is a common practice in security architecture. **With a DMZ**, host systems that are accessible through the firewall **are physically separated from the internal network** by means of secured switches or by using an additional firewall to control traffic between the web server and the internal network. Application DMZs (or semi-trusted networks) are frequently used today to limit access to application servers to those networks or systems that have a legitimate need to connect.

Segmentation for Embedded Systems and IoT

Network-enabled devices are any type of portable or non portable device that has native network capabilities. This generally assumes the **network in question is a wireless type of network**, typically provided by a mobile telecommunications company. Network-enabled devices include **smartphones, mobile phones, tablets, smart TVs or streaming media players**, network-attached printers, game systems, and much more.

The Internet of Things (IoT) **is the collection of devices that can communicate over the internet with one another or with a control console in order to affect and monitor the real world.** IoT devices might be labeled as smart devices or smart-home equipment. Many of the

ideas of industrial environmental control found in office buildings are finding their way into more consumer-available solutions for small offices or personal homes.

Embedded systems and network-enabled devices that communicate with the internet are considered IoT devices and need special attention to ensure that communication is not used in a malicious manner. Because an embedded system is often in control of a mechanism in the physical world, a security breach could cause harm to people and property. Since many of these devices have multiple access routes, such as ethernet, wireless, Bluetooth, etc., special care should be taken to isolate them from other devices on the network. You can impose logical network segmentation with switches using VLANs, or through other traffic-control means, including MAC addresses, IP addresses, physical ports, protocols, or application filtering, routing, and access control management. Network segmentation can be used to isolate IoT environments.

Microsegmentation

The toolsets of current adversaries are polymorphic in nature and allow threats to bypass static security controls. **Modern cyberattacks take advantage of traditional security models to move easily between systems within a data center**. Microsegmentation aids in protecting against these threats. A fundamental design requirement of **microsegmentation is to understand the protection requirements for traffic within a data center and traffic to and from the internet traffic flows**.

When organizations avoid infrastructure-centric design paradigms, they are more likely to become more efficient at service delivery in the data center and become apt at detecting and preventing advanced persistent threats.

Virtual Local Area Network (VLAN)

Virtual local area networks (VLANs) allow network administrators **to use switches to create software-based LAN segments**, which can **segregate or consolidate traffic across multiple switch ports**. **Devices that share a VLAN communicate through switches as if they were on the same Layer 2 network**. Since VLANs act as discrete networks, communications between VLANs must be enabled. Broadcast traffic is limited to the VLAN, reducing congestion and reducing the effectiveness of some attacks. Administration of the environment is simplified, as the VLANs can be reconfigured when individuals change their physical location or need access to different services. VLANs can be configured based on switch port, IP subnet, MAC address and protocols. VLANs do not guarantee a network's security. At first glance, it may seem that traffic cannot be intercepted because communication within a VLAN is restricted to member devices. However, there are attacks that allow a malicious user to see traffic from other VLANs (so-called VLAN hopping). The VLAN technology is only one tool that can improve the overall security of the network environment.

Virtual Private Network (VPN)
A virtual private network (VPN) **is not necessarily an encrypted tunnel**. It is simply **a point-to-point connection between two hosts that allows them to communicate**. Secure communications can, of course, be provided by the VPN, but only if the security protocols have been selected and correctly configured to provide a trusted path over an untrusted network, such as the internet. Remote users employ VPNs to access their organization's network, and depending on the VPN's implementation, they may have most of the same resources available to them as if they were physically at the office. As an alternative to expensive dedicated point-to-point connections, organizations use gateway-to-gateway VPNs to securely transmit information over the internet between sites or even with business partners.

Risk Management

Understanding Risks

Risks within an organization can broadly be categorized into two types: Internal Risks, which originate from within the organization, and External Risks, which stem from factors outside the organization's control. Additionally, there are Multiparty Risks that affect more than one organization, as well as risks specific to knowledge-based organizations such as Intellectual Property Theft and Software License Compliance issues.

Risk Assessment

Risk assessment is the process of identifying and evaluating potential risks. It involves analyzing Threats, which are external forces that pose security risks, and Vulnerabilities, which are weaknesses in the organization's security controls. Risks, therefore, arise from the combination of a Threat and a Vulnerability. Risks are typically assessed based on their Likelihood, the probability of occurrence, and their Impact, the potential damage they may cause.

There are two primary techniques for assessing risks:

1. **Qualitative Risk Assessment**: This method utilizes subjective ratings to evaluate the likelihood and impact of risks. It often involves qualitative descriptions or ranking scales to assess risks.

2. **Quantitative Risk Assessment**: In contrast, quantitative risk assessment employs objective numeric ratings to evaluate the likelihood and impact of risks. It involves mathematical models and statistical analysis to quantify risks more precisely.

Risk Treatment

Risk treatment involves analyzing and implementing responses to manage and control identified risks. There are four main options for treating risks:

1. **Risk Avoidance**: This strategy involves altering business practices to make certain risks irrelevant, effectively eliminating them from consideration.

2. **Risk Transference**: Risk transference involves shifting the financial burden of a risk to another party, such as through insurance or contractual agreements.

3. **Risk Mitigation**: Risk mitigation aims to reduce the likelihood or impact of a risk through various measures, such as implementing security controls or enhancing protective measures.

4. **Risk Acceptance**: Sometimes, organizations choose to accept certain risks, acknowledging them as part of doing business while implementing measures to monitor and manage them effectively.

Selecting Security Controls

Security controls play a crucial role in reducing the likelihood or impact of risks. They can be categorized based on their purpose and mechanism:

1. **Control Purpose**: Controls can be preventive, detective, or corrective, depending on whether they aim to prevent security issues, identify them, or address them after they occur.

2. **Control Mechanism**: Controls can be technical, administrative, or physical, utilizing technology, processes, or physical measures, respectively, to achieve control objectives.

Configuration Management

Configuration management involves tracking and maintaining specific device settings to ensure a stable operating environment. It includes activities such as establishing baselines, versioning configurations, and standardizing device settings through naming conventions and IP addressing schemes. Change management processes help implement and track changes to configurations, ensuring consistency and stability.

Security Concepts
CIA Triad are three main goals

Confidentiality
- Confidentiality protects information from unauthorized disclosure.

Confidentiality_Concerns
1. Snooping
    - snooping gathering information that is left out in the open.
    - "Clean desk policies" protect against snooping.
2. Dumpster Diving
    - Dumpster diving is to dump data anywhere or in a dustbin.
    - "Shedding" protects against dumpster diving.
3. Eavesdropping
    - listing sensitive information
    - "Rules about sensitive conversations" prevent eavesdropping
4. Wiretapping
    - Electronic eavesdropping - listing through wire(internet)
    - "Encryption" protects against Wiretapping
5. Social Engineering
    - The attacker uses psychological tricks to persuade an employee to give them sensitive information or access to internal systems.
    - Best defense is to "Educating users"

Integrity
- Integrity protects information from unauthorized changes.
Integrity_Concerns
1. Unauthorized modification
    - Attacks make changes without permission.
    - "Least privilege" protects against integrity attacks
2. Impersonation
    - Attacks pretend to be someone else
    - "User education" protects against attacks
3. Man-in-the-middle (MITM)
    - Attacks place the attacker in the middle of a communications session.
    - "Encryption" protects against MITM attacks
4. Replay
    - Attacks eavesdrop on logins and reuse the captured credentials.
    - "Encryption" protects against Replay attacks

Availability
- Availability protects authorized access to systems and data.
Availability_Concerns

1. Denial of service (DoS)
    - Unlimited request to a server
    - "Block unauthorized connections" to protect against denial of service attacks.
2. Power outages
    - Naturally or Man-made
    - "Redundant power and generators" protect against power outages.
3. Hardware failures
    - any component failures
    - "Redundant components" protect against hardware failure
4. Destruction
    - Naturally or Man-made
    - "Backup data centers" protect against destruction.
5. Service outages
    - Programing error and the failure of underlying equipment.
    - building systems that are resilient in the face of errors and hardware failures.

Authentication and authorization

The access control process consists of three steps that you must understand. These steps are identification, authentication and authorization.

1. Identification involves making a claim of identity.
    - Electronic identification commonly uses usernames
2. Authentication requires proving a claim of identity.
    - Electronic authentication commonly used passwords.
3. Authorization ensures that an action is allowed.
    - Electronic authorization commonly uses access control lists.

Authentication and authorization process, access control systems also provide "Accounting" functionality that allows administrators to track user activity and reconstruct that activity from logs. This may include tracking user activity on systems and even logging user web browsing history.

Password security

Password mechanisms

- Password length requirements set a minimum number of characters.
- Password complexity requirements describe the types of characters that must be included.
- Password expiration requirements force password changes.
- Password requirements prevent password reuse.

Multi Factor authentication
Multi Factor authentication combines two different authentication factors.

Three different authentication factors. Something you know, something you are and something you have.

something you know
- Passwords, PIN's, Security questions.
something you are
- Biometric security mechanisms.
something you have
- Software and hardware tokens.

single sign-On (SSO)
Shares authenticated sessions across systems

- In a single sign on approach, users log on to the first SSO enabled system that they encounter. And then that login session persists across other systems until it expires. If the organization sets the expiration period to be the length of a business day, that means that users will only need to log in once a day and their single sign on is then going to last the entire day.

Non-repudiation
Non-repudiation prevents someone from denying the truth.

Solved the issue with

1. Signed contracts
2. Digital signatures
3. Video surveillance

Privacy
Privacy Concerns
1. Protecting our own data.
2. Educating our users.
3. Protecting data collected by our organizations.

Private information may come in many forms. Two of the most common elements of private information are "Personally identifiable information" and "Protected health information".
1. Personally identifiable information, or PII, includes all information that can be tied back to a specific individual.

2. Protected health information, or PHI, includes healthcare records that are regulated under the Health Insurance Portability and Accountability Act. Otherwise known as HIPAA.

@L5 Security Operations

Module 1: Understand Data Security

Domain D5.0, D5.1.1, D5.1.2, D5.1.3

Hardening is the process of applying secure configurations (to reduce the attack surface) and locking down various hardware, communications systems and software, including the operating system, web server, application server and applications, etc. This module introduces configuration management practices that will ensure systems are installed and maintained according to industry and organizational security standards.

Data Handling

Data itself goes through **its own life cycle as users create**, **use**, **share and modify it**. The data security life cycle model is useful because **it can align easily with the different roles that people and organizations perform during the evolution of data from creation to destruction (or disposal)**. It also helps put the different **data states of in use, at rest and in motion, into context**.

All ideas, data, information or knowledge can be thought of as going through six major sets of activities throughout its lifetime. Conceptually, these involve:

1. Creating the knowledge, which is usually tacit knowledge at this point.
2. Storing or recording it in some fashion (which makes it explicit).
3. Using the knowledge, which may cause the information to be modified, supplemented or partially deleted.
4. Sharing the data with other users, whether as a copy or by moving the data from one location to another.
5. Archiving the data when it is temporarily not needed.
6. Destroying the data when it is no longer needed.

NB: The 6 steps of handling data orderly are CREATE – STORE – USE – SHARE – ARCHIVE – DESTROY. There may be a question about this so know the order.

Data Handling Practices

* **Classification**: classifications dictate **rules and restrictions about how that information can be used**, **stored** or **shared with others**. All of this is done to keep the temporary value and importance of that information from leaking away. Classification of data, which asks the question “Is it secret?” determines the labeling, handling and use of all data. **Classification is the process of recognizing the organizational impacts if the information suffers any security compromises related to its characteristics of confidentiality**, **integrity** and **availability**. **Information is then labeled and handled accordingly**. Classifications are derived from laws, regulations, contract-specified standards or other business expectations. One classification might indicate “minor, may disrupt some processes” while a more extreme one might be “grave, could lead to loss of life or threaten ongoing existence of the organization.” These descriptions should reflect the ways in which the organization has chosen (or been mandated) to characterize and manage risks. The immediate benefit of classification is that it can lead to more efficient design and implementation of security processes, if we can treat the protection needs for all similarly classified information with the same controls strategy.

* **Labeling**: **security labels are part of implementing controls to protect classified information**. It is reasonable to want a simple way of assigning a level of sensitivity to a data asset, such that the higher the level, the greater the presumed harm to the organization, and thus the greater security protection the data asset requires. This spectrum of needs is useful, but it should not be taken to mean that clear and precise boundaries exist between the use of “low sensitivity” and “moderate sensitivity” labeling, for example.
  * **Data Sensitivity Levels and Labels**: unless otherwise mandated, organizations are free to create classification systems that best meet their own needs. In professional practice, it is typically best if the organization has enough classifications to distinguish between sets of assets with differing sensitivity/value, but not so many classifications that the distinction between them is confusing to individuals. Typically, two or three classifications are manageable, and more than four tend to be difficult.

  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.

* **Retention**: **Information and data should be kept only for as long as it is beneficial, no more and no less**. Certain industry standards, laws and regulations define retention periods,

when such external requirements are not set, it is an organization's responsibility to define and implement its own data retention policy. **Data retention policies are applicable both for hard copies and for electronic data**, and no data should be kept beyond its required or useful life. **Security professionals should ensure that data destruction is being performed when an asset has reached its retention limit**. For the security professional to succeed in this assignment, an accurate inventory must be maintained, including the asset location, retention period requirement, and destruction requirements. Organizations should conduct a periodic review of retained records in order to reduce the volume of information stored and to ensure that only necessary information is preserved.

Records retention policies indicate how long an organization is required to maintain information and assets. Policies should guarantee that:

* Personnel understand the various retention requirements for data of different types throughout the organization.
* The organization appropriately documents the retention requirements for each type of information.
* The systems, processes and individuals of the organization retain information in accordance with the required schedule but no longer.
* A common mistake in records retention is applying the longest retention period to all types of information in an organization. This not only wastes storage but also increases risk of data exposure and adds unnecessary "noise" when searching or processing information in search of relevant records. It may also be in violation of externally mandated requirements such as legislation, regulations or contracts (which may result in fines or other judgments). Records and information no longer mandated to be retained should be destroyed in accordance with the policies of the enterprise and any appropriate legal requirements that may need to be considered.

* Destruction: Data that might be left on media after deleting is known as remanence and may be a significant security concern. Steps must be taken to reduce the risk that data remanence could compromise sensitive information to an acceptable level. This can be done by one of several means:

* Clearing the device or system, which usually involves **writing multiple patterns of random values throughout all storage media**. This is sometimes **called "overwriting" or "zeroizing" the system**, although writing zeros has the risk that a missed block or storage extent may still contain recoverable, sensitive information after the process is completed.
* Purging the device or system, which eliminates (or greatly reduces) the chance that residual physical effects from the writing of the original data values may still be recovered, even after the system is cleared. Some magnetic disk storage technologies, for example, can still have residual "ghosts" of data on their surfaces even after being overwritten multiple times. Magnetic media, for example, can often be altered sufficiently to meet security requirements; in more stringent cases, degaussing may not be sufficient.

* Physical destruction of the device or system is the ultimate remedy to data remanence. Magnetic or optical disks and some flash drive technologies may require being mechanically shredded, chopped or broken up, etched in acid or burned; their remains may be buried in protected landfills, in some cases.
* In many routine operational environments, security considerations may accept that clearing a system is sufficient. But when system elements are to be removed and replaced, either as part of maintenance upgrades or for disposal, purging or destruction may be required to protect sensitive information from being compromised by an attacker.

Logging and Monitoring Security Events

Logging is the primary form of instrumentation that attempts to capture signals generated by events. Events are any actions that take place within the system's environment and cause measurable or observable change in one or more elements or resources within the system. **Logging imposes a computational cost but is invaluable when determining accountability**. Proper design of logging environments and regular log reviews remain best practices regardless of the type of computer system.

Major controls frameworks emphasize the importance of organizational logging practices. Information that may be relevant to being recorded and reviewed include (but is not limited to): user IDs, system activities, dates/times of key events (e.g., logon and logoff), device and location identity, successful and rejected system and resource access attempts, system configuration changes and system protection activation and deactivation events.

Logging and monitoring the health of the information environment is essential to identifying inefficient or improperly performing systems, detecting compromises and providing a record of how systems are used. **Robust logging practices provide tools to effectively correlate information from diverse systems to fully understand the relationship between one activity and another**.

Log reviews are an essential function not only for security assessment and testing but also **for identifying security incidents, policy violations, fraudulent activities and operational problems near the time of occurrence**. Log reviews support audits – forensic analysis related to internal and external investigations – and provide support for organizational security baselines. Review of historic audit logs can determine if a vulnerability identified in a system has been previously exploited.

It is helpful for an organization to create components of a log management infrastructure and determine how these components interact. This aids in preserving the integrity of log data from accidental or intentional modification or deletion and in maintaining the confidentiality of log data.

Controls are implemented to protect against unauthorized changes to log information. Operational problems with the logging facility are often related to alterations to the messages that are recorded, log files being edited or deleted, and storage capacity of log file media being exceeded. Organizations must maintain adherence to retention policy for logs as prescribed by law, regulations and corporate governance. Since attackers want to hide the evidence of their attack, the organization's policies and procedures should also address the preservation of original logs. Additionally, the logs contain valuable and sensitive information about the organization. Appropriate measures must be taken to protect the log data from malicious use.

Event Logging Best Practices

Different tools are used depending on whether the risk from the attack is from traffic coming into or leaving the infrastructure.

Ingress monitoring refers to surveillance and assessment of all inbound communications traffic and access attempts. Devices and tools that offer logging and alerting opportunities for ingress monitoring include: Firewalls, Gateways, Remote authentication servers, IDS/IPS tools, SIEM solutions,
Anti-malware solutions.

Egress monitoring is used to regulate data leaving the organization's IT environment. The term currently used in conjunction with this effort is **data loss prevention (DLP)** or **data leak protection**. The DLP solution should be deployed so that it can inspect all forms of data leaving the organization, including: Email (content and attachments), Copy to portable media, File Transfer Protocol (FTP), Posting to web pages/websites, Applications/application programming interfaces (APIs).

Encryption Overview

Almost every action we take in our modern digital world involves cryptography. Encryption protects our personal and business transactions; digitally signed software updates verify their creator's or supplier's claim to authenticity. Digitally signed contracts, binding on all parties, are routinely exchanged via email without fear of being repudiated later by the sender.

Cryptography is used to protect information by keeping its meaning or content secret and making it unintelligible to someone who does not have a way to decrypt (unlock) that protected information. The objective of every encryption system is to transform an original set of data, called the plaintext, into an otherwise unintelligible encrypted form, called the ciphertext.

Properly used, singly or in combination, **cryptographic solutions provide a range of services that can help achieve required systems security postures in many ways**:

confidentiality: Cryptography provides confidentiality by hiding or obscuring a message so that it cannot be understood by anyone except the intended recipient. Confidentiality keeps information secret from those who are not authorized to have it.

integrity: hash functions and digital signatures can provide integrity services that allow a recipient to verify that a message has not been altered by malice or error. These include simple message integrity controls. Any changes, deliberate or accidental, will result in the two results (by sender and by recipient) being different.

Module 2: Understand System Hardening

Domain D5.2.1

Configuration Management Overview

Configuration management is a process and discipline used **to ensure that the only changes made to a system are those that have been authorized and validated**. It is both a decision-making process and a set of control processes. If we look closer at this definition, the basic configuration management process includes components such as **identification**, **baselines**, **updates** and **patches**.

* Configuration Management

1. **Identification**: baseline identification of a system and all its components, interfaces and documentation.
2. **Baseline**: a security baseline is a minimum level of protection that can be used as a reference point. Baselines provide a way to ensure that updates to technology and architectures are subjected to the minimum understood and acceptable level of security requirements.
3. **Change Control**: An update process for requesting changes to a baseline, by means of making changes to one or more components in that baseline. A review and approval process for all changes. This includes updates and patches.
4. **Verification & Audit**: A regression and validation process, which may involve testing and analysis, to verify that nothing in the system was broken by a newly applied set of changes. An audit process can validate that the currently in-use baseline matches the sum total of its initial baseline plus all approved changes applied in sequence.

Effective use of configuration management gives systems owners, operators, support teams and security professionals another important set of tools they can use to monitor and oversee the configuration of the devices, networks, applications and projects of the organization.An organization may mandate the configuration of equipment **through standards and baselines**. The use of **standards and baselines can ensure that network devices, software, hardware and endpoint devices are configured in a consistent way and that all such devices are compliant with the security baseline established for the organization**. If a

device is found that is not compliant with the security baseline, it may be **disabled or isolated into a quarantine area** until it can be **checked and updated**.

* **Inventory**: Making an inventory, catalog or registry of all the information assets **is the first step in any asset management process**. **You can't protect what you don't know you have**.

* **Baselines**: The baseline **is a total inventory of all the system's components, hardware, software, data, administrative controls, documentation and user instructions**. **All further comparisons and development are measured against the baselines.** **When protecting assets, baselines can be particularly helpful in achieving a minimal protection level of those assets based on value.** If classifications such as high, medium and low are being used, baselines could be developed for each of our classifications and provide that minimum level of security required for each.

* Updates: Such modifications **must be acceptance tested to verify that newly installed (or repaired) functionality works as required**. They must also be **regression tested to verify that the modifications did not introduce other erroneous or unexpected behaviors** in the system. **Ongoing security assessment and evaluation testing evaluates whether the same system that passed acceptance testing is still secure**.

* Patches: **The challenge for the security professional is maintaining all patches**. **Some patches are critical and should be deployed quickly, while others may not be as critical but should still be deployed because subsequent patches may be dependent on them**. Standards such as the **PCI DSS require organizations to deploy security patches within a certain time frame**. **An organization should test the patch before rolling it out across the organization**. If the patch does not work or has unacceptable effects, it might be necessary to **roll back to a previous (pre-patch) state**. Typically, **the criteria for rollback are previously documented and would automatically be performed when the rollback criteria were met**. The risk of using unattended patching should be weighed against the risk of having unpatched systems in the organization's network. Unattended (or automated) patching might result in unscheduled outages as production systems are taken offline or rebooted as part of the patch process.

Module 3: Understand Best Practice Security Policies

Domain D5.3, D5.3.1, D5.3.2, D5.3.3, D5.3.4, D5.3.5, D5.3.6

An organization's security policies define what "security" means to that organization, which in almost all cases reflects the tradeoff between security, operability, affordability and potential risk impacts. Security policies express or impose behavioral or other constraints on the system and its use. Well-designed systems operating within these constraints should reduce the potential of security breaches to an acceptable level.

Security governance that does not align properly with organizational goals can lead to implementation of security policies and decisions that unnecessarily inhibit productivity, impose undue costs and hinder strategic intent.

Common Security Policies

All policies must support any regulatory and contractual obligations of the organization. Sometimes it can be challenging to ensure the policy encompasses all requirements while remaining simple enough for users to understand.

Here are six common security-related policies that exist in most organizations.

* Data Handling Policy: Appropriate use of data: This aspect of the policy defines whether data is for use within the company, is restricted for use by only certain roles or can be made public to anyone outside the organization. In addition, some data has associated legal usage definitions. The organization's policy should spell out any such restrictions or refer to the legal definitions as required. Proper data classification also helps the organization comply with pertinent laws and regulations. For example, classifying credit card data as confidential can help ensure compliance with the PCI DSS. One of the requirements of this standard is to encrypt credit card information. Data owners who correctly defined the encryption aspect of their organization's data classification policy will require that the data be encrypted according to the specifications defined in this standard.

* Password Policy: Every organization should have a password policy in place that defines expectations of systems and users. The password policy should describe senior leadership's commitment to ensuring secure access to data, outline any standards that the organization has selected for password formulation, and identify who is designated to enforce and validate the policy.

* Acceptable Use Policy (AUP): The acceptable use policy (AUP) defines acceptable use of the organization's network and computer systems and can help protect the organization from legal action. It should detail the appropriate and approved usage of the organization's assets, including the IT environment, devices and data. Each employee (or anyone having access to the organization's assets) should be required to sign a copy of the AUP, preferably in the presence of another employee of the organization, and both parties should keep a copy of the signed AUP.

Policy aspects commonly included in AUPs: Data access, System access, Data disclosure, Passwords, Data retention, Internet usage, Company device usage

* Bring Your Own Device (BYOD): An organization may allow workers to acquire equipment of their choosing and use personally owned equipment for business (and personal) use. This is sometimes called bring your own device (BYOD). Another option is to present the teleworker or employee with a list of approved equipment and require the employee to select one of the products on the trusted list.

Letting employees choose the device that is most comfortable for them may be good for employee morale, but it presents additional challenges for the security professional because it means the organization loses some control over standardization and privacy. If employees are allowed to use their phones and laptops for both personal and business use, this can pose a challenge if, for example, the device has to be examined for a forensic audit. It can be hard to ensure that the device is configured securely and does not have any backdoors or other vulnerabilities that could be used to access organizational data or systems.

All employees must read and agree to adhere to this policy before any access to the systems, network and/or data is allowed. If and when the workforce grows, so too will the problems with BYOD. Certainly, the appropriate tools are going to be necessary to manage the use of and security around BYOD devices and usage. The organization needs to establish clear user expectations and set the appropriate business rules.

* Privacy Policy: Often, personnel have access to personally identifiable information (PII) (also referred to as electronic protected health information [ePHI] in the health industry). It is imperative that the organization documents that the personnel understand and acknowledge the organization's policies and procedures for handling that type of information and are made aware of the legal repercussions of handling such sensitive data. This type of documentation is similar to the AUP but is specific to privacy-related data.

The organization's privacy policy should stipulate which information is considered PII/ePHI, the appropriate handling procedures and mechanisms used by the organization, how the user is expected to perform in accordance with the stated policy and procedures, any enforcement mechanisms and punitive measures for failure to comply as well as references to applicable regulations and legislation to which the organization is subject. This can include national and international laws, such as the GDPR in the EU and Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada; laws for specific industries in certain countries such as HIPAA and Gramm–Leach–Bliley Act (GLBA); or local laws in which the organization operates.

The organization should also create a public document that explains how private information is used, both internally and externally. For example, it may be required that a medical provider present patients with a description of how the provider will protect their information (or a reference to where they can find this description, such as the provider's website).

* Change Management Policy: Change management is the discipline of transitioning from the current state to a future state. It consists of three major activities: deciding to change, making the change, and confirming that the change has been correctly accomplished. Change management focuses on making the decision to change and results in the approvals to systems support teams, developers and end users to start making the directed alterations.

Throughout the system life cycle, changes made to the system, its individual components and its operating environment all have the capability to introduce new vulnerabilities and thus undermine the security of the enterprise. Change management requires a process to implement the necessary changes so they do not adversely affect business operations.

Common Security Policies Deeper Dive

Policies will be set according to the needs of the organization and its vision and mission. Each of these policies should have a penalty or a consequence attached in case of noncompliance. The first time may be a warning; the next might be a forced leave of absence or suspension without pay, and a critical violation could even result in an employee's termination. All of this should be outlined clearly during onboarding, particularly for information security personnel. It should be made clear who is responsible for enforcing these policies, and the employee must sign off on them and have documentation saying they have done so. This process could even include a few questions in a survey or quiz to confirm that the employees truly understand the policy. These policies are part of the baseline security posture of any organization. Any security or data handling procedures should be backed up by the appropriate policies.

Change Management Components

The change management process includes the following components.

Documentation: All of the major change management practices address a common set of core activities that start with a request for change (RFC) and move through various development and test stages until the change is released to the end users. From first to last, each step is subject to some form of formalized management and decision-making; each step produces accounting or log entries to document its results.

Approval: These processes typically include: Evaluating the RFCs for completeness, Assignment to the proper change authorization process based on risk and organizational practices, Stakeholder reviews, resource identification and allocation, Appropriate approvals or rejections, and Documentation of approval or rejection.

Rollback: Depending upon the nature of the change, a variety of activities may need to be completed. These generally include: Scheduling the change, Testing the change, Verifying the rollback procedures, Implementing the change, Evaluating the change for proper and effective operation, and Documenting the change in the production environment. Rollback authority would generally be defined in the rollback plan, which might be immediate or scheduled as a subsequent change if monitoring of the change suggests inadequate performance.

Module 4: Understand Security Awareness Training

Domain D5.4, D5.4.1, D5.4.2, D5.3.2

To reduce the effectiveness of certain types of attacks (such as social engineering), it is crucial that the organization informs its **employees and staff** **how to recognize security problems and how to operate in a secure manner**. While the specifics of secure operation differ in each organization, there are some general concepts that are applicable to all such programs.

Purpose

The purpose of awareness training is to make sure everyone knows what is expected of them, based on responsibilities and accountabilities, and to find out if there is any carelessness or complacency that may pose a risk to the organization. We will be able to align the information security goals with the organization's missions and vision and have a better sense of what the environment is.

What is Security Awareness Training?

Let's start with a clear understanding of the **three different types of learning activities that organizations use**, whether for information security or for any other purpose:

* **Education**: The overall goal of education is to help learners **improve their understanding of these ideas and their ability to relate them to their own experiences and apply that learning in useful ways**.

* **Training**: Focuses on **building proficiency in a specific set of skills or actions**, including sharpening the perception and judgment needed to make decisions as to which skill to use, when to use it and how to apply it. **Training can focus on low-level skills, an entire task or complex workflows consisting of many tasks**.

* **Awareness**: These are activities that attract and engage the learner's attention by acquainting them with aspects of an issue, concern, problem or need.

You'll notice that none of these have an expressed or implied degree of formality, location or target audience. (Think of a newly hired senior executive with little or no exposure to the specific compliance needs your organization faces; first, someone has to get their attention and make them aware of the need to understand. The rest can follow.)

Security Awareness Training Examples

Let's look at an example of security awareness training by using an organization's strategy to improve fire safety in the workplace:

Education may help workers in a secure server room understand the interaction of the various fire and smoke detectors, suppression systems, alarms and their interactions with electrical power, lighting and ventilation systems.
Training would provide those workers with task-specific, detailed learning about the proper actions each should take in the event of an alarm, a suppression system going off without an alarm, a ventilation system failure or other contingency. This training would build on the learning acquired via the educational activities.
Awareness activities would include not only posting the appropriate signage, floor or doorway markings, but also other indicators to help workers detect an anomaly, respond to an alarm and take appropriate action. In this case, awareness is a constantly available reminder of what to do when the alarms go off.

Translating that into an anti-phishing campaign might be done by:

Education may be used to help select groups of users better understand the ways in which social engineering attacks are conducted and engage those users in creating and testing their own strategies for improving their defensive techniques.
Training will help users increase their proficiency in recognizing a potential phishing or similar attempt, while also helping them practice the correct responses to such events. Training may include simulated phishing emails sent to users on a network to test their ability to identify a phishing email.
Raising users' overall awareness of the threat posed by phishing, vishing, SMS phishing (also called "smishing) and other social engineering tactics. Awareness techniques can also alert selected users to new or novel approaches that such attacks might be taking.
Let's look at some common risks and why it's important to include them in your security awareness training programs.

Phishing

The use of phishing attacks to target individuals, entire departments and even companies is a significant threat that the security professional needs to be aware of and be prepared to defend

against. Countless variations on the basic phishing attack have been developed in recent years, leading to a variety of attacks that are deployed relentlessly against individuals and networks in a never-ending stream of emails, phone calls, spam, instant messages, videos, file attachments and many other delivery mechanisms.

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 are known as whaling attacks .

Social Engineering

Social engineering is an important part of any security awareness training program for one very simple reason: bad actors know that it works. For the cyberattackers, social engineering is an inexpensive investment with a potentially very high payoff. Social engineering, applied over time, can extract significant insider knowledge about almost any organization or individual.

One of the most important messages to deliver in a security awareness program is an understanding of the threat of social engineering. People need to be reminded of the threat and types of social engineering so that they can recognize and resist a social engineering attack.

Most social engineering techniques are not new. Many have even been taught as basic fieldcraft for espionage agencies and are part of the repertoire of investigative techniques used by real and fictional police detectives. A short list of the tactics that we see across cyberspace currently includes:

Phone phishing or vishing: Using a rogue interactive voice response (IVR) system to re-create a legitimate-sounding copy of a bank or other institution's IVR system. The victim is prompted through a phishing email to call in to the "bank" via a provided phone number to verify information such as account numbers, account access codes or a PIN and to confirm answers to security questions, contact information and addresses. A typical vishing system will reject logins continually, ensuring the victim enters PINs or passwords multiple times, often disclosing several different passwords. More advanced systems may be used to transfer the victim to a human posing as a customer service agent for further questioning.

Pretexting: The human equivalent of phishing, where someone impersonates an authority figure or a trusted individual in an attempt to gain access to your login information. The pretexter may claim to be an IT support worker who is supposed to do maintenance or an investigator performing a company audit. Or they might impersonate a coworker, the police, a tax authority or some other seemingly legitimate person. The goal is to gain access to your computer and information.

Quid pro quo: A request for your password or login credentials in exchange for some compensation, such as a “free gift,” a monetary payment or access to an online game or service. If it sounds too good to be true, it probably is.
Tailgating: The practice of following an authorized user into a restricted area or system. The low-tech version of tailgating would occur when a stranger asks you to hold the door open behind you because they forgot their company RFID card. In a more sophisticated version, someone may ask to borrow your phone or laptop to perform a simple action when he or she is actually installing malicious software onto your device.
Social engineering works because it plays on human tendencies. Education, training and awareness work best to counter or defend against social engineering because they help people realize that every person in the organization plays a role in information security.

Password Protection

We use many different passwords and systems. Many password managers will store a user’s passwords for them so the user does not have to remember all their passwords for multiple systems. The greatest disadvantage of these solutions is the risk of compromise of the password manager.

These password managers may be protected by a weak password or passphrase chosen by the user and easily compromised. There have been many cases where a person’s private data was stored by a cloud provider but easily accessed by unauthorized persons through password compromise.

Organizations should encourage the use of different passwords for different systems and should provide a recommended password management solution for its users.

Examples of poor password protection that should be avoided are:

Reusing passwords for multiple systems, especially using the same password for business and personal use.
Writing down passwords and leaving them in unsecured areas.
Sharing a password with tech support or a co-worker.

NB: ISC2 Code Of Ethics Canon is to
-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.
Which can be memorized using the mnemonics PAPA.

*PII(personal identifiable information) ensures confidentiality
*Risk avoidance is not a part of the RMF(risk management framework).
*In IPS(intrusion prevention system), a false-negative is when a legitimate threat was unnoticed by the system.
*A three way handshake is establishing connection between 2 devices on a network.
*Policies are reviewed annually.
*Guidelines are optional.
* Awareness targets behavior, Education targets career, Training targets skill

Here are the ISC2 flashcards:

NB: The term being defined is in-between <summary> *** </summary>

Flashcards

Chapter 1: Security Principles

<details> <summary> Adequate Security </summary>
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

</details>

<details> <summary> Administrative Controls </summary>
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.

</details>

<details><summary> Artificial Intelligence </summary>
The ability of computers and robots to simulate human intelligence and behavior.

</details>

<details><summary> Asset </summary>
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.

</details>

<details><summary> Authentication </summary>

The act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information. Typically, a measure designed to protect against fraudulent transmissions by establishing the validity of a transmission, message, station or originator.

</details>

<details><summary> Authorization </summary>
The right or a permission that is granted to a system entity to access a system resource. NIST 800-82 Rev.2

</details>

<details><summary> Availability </summary>
Ensuring timely and reliable access to and use of information by authorized users

</details>

<details><summary> Baseline </summary>
A documented, lowest level of security configuration allowed by a standard or organization.

</details>

<details><summary> Biometric </summary>
Biological characteristics of an individual, such as a fingerprint, hand geometry, voice, or iris patterns.

</details>

<details><summary> Bot </summary>
Malicious code that acts like a remotely controlled "robot" for an attacker, with other Trojan and worm capabilities.

</details>

<details><summary> Classified or Sensitive Information </summary>
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.

</details>

<details><summary> Confidentiality </summary>
The characteristic of data or information when it is not made available or disclosed to unauthorized persons or processes. NIST 800-66

</details>

<details><summary> Criticality </summary>
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

</details>

<details><summary> Data Integrity </summary>
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

</details>

<details><summary> Encryption </summary>
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.

</details>

<details><summary>General Data Protection Regulation (GDPR) </summary>
In 2016, the European Union passed comprehensive legislation that addresses personal privacy, deeming it an individual human right.

</details>

<details><summary>Governance </summary>
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.

</details>

<details><summary>Health Insurance Portability and Accountability Act (HIPAA)
</summary>
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.

</details>

<details><summary>Impact </summary>
The magnitude of harm that could be caused by a threat's exercise of a vulnerability.

</details>

<details><summary>Information Security Risk </summary>
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.

</details>

<details><summary> Integrity</summary>
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.

</details>

<details><summary>International Organization of Standards (ISO) </summary>
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.

</details>

<details><summary>Internet Engineering Task Force (IETF) </summary>
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

</details>

<details><summary> Likelihood</summary>
The probability that a potential vulnerability may be exercised within the construct of the associated threat environment.

</details>

<details><summary>Likelihood of Occurrence </summary>
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.

</details>

<details><summary>Multi-Factor Authentication </summary>
Using two or more distinct instances of the three factors of authentication (something you know, something you have, something you are) for identity verification.

</details>

<details><summary>National Institutes of Standards and Technology (NIST) </summary>
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.

</details>

<details><summary>Non-repudiation </summary>
The inability to deny taking an action such as creating information, approving information and sending or receiving a message.

</details>

<details><summary>Personally Identifiable Information (PII) </summary>
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."

</details>

<details><summary>Physical Controls </summary>
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.

</details>

<details><summary>Privacy </summary>
The right of an individual to control the distribution of information about themselves.

</details>

<details><summary>Probability </summary>
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

</details>

<details><summary>Protected Health Information (PHI) </summary>
Information regarding health status, the provision of healthcare or payment for healthcare as defined in HIPAA (Health Insurance Portability and Accountability Act).

</details>

<details><summary>Qualitative Risk Analysis </summary>
A method for risk analysis that is based on the assignment of a descriptor such as low, medium or high. Source: NISTIR 8286

</details>

<details><summary>Quantitative Risk Analysis </summary>
A method for risk analysis where numerical values are assigned to both impact and likelihood based on statistical probabilities and monetary valuation of loss or gain. Source: NISTIR 8286

</details>

<details><summary>Risk </summary>
A measure of the extent to which an entity is threatened by a potential circumstance or event.

</details>

<details><summary>Risk Acceptance </summary>
Determining that the potential benefits of a business function outweigh the possible risk impact/likelihood and performing that business function with no other action.

</details>

<details><summary>Risk Assessment </summary>
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.

</details>

<details><summary>Risk Avoidance </summary>
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.

</details>

<details><summary>Risk Management </summary>
The process of identifying, evaluating and controlling threats, including all the phases of risk context (or frame), risk assessment, risk treatment and risk monitoring.

</details>

<details><summary>Risk Management Framework </summary>
A structured approach used to oversee and manage risk for an enterprise. Source: CNSSI 400

</details>

<details><summary>Risk Mitigation </summary>
Putting security controls in place to reduce the possible impact and/or likelihood of a specific risk.

</details>

<details><summary>Risk Tolerance </summary>
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.

</details>

<details><summary>Risk Transference </summary>
Paying an external party to accept the financial impact of a given risk.

</details>

<details><summary>Risk Treatment </summary>
The determination of the best way to address an identified risk.

</details>

<details><summary>Security Controls </summary>
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

</details>

<details><summary>Sensitivity </summary>
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

</details>

<details><summary>Single-Factor Authentication </summary>
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.

</details>

<details><summary>State </summary>
The condition an entity is in at a point in time.

</details>

<details><summary>System Integrity </summary>
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

</details>

<details><summary>Technical Controls </summary>
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.

</details>

<details><summary>Threat </summary>
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

</details>

<details><summary>Threat Actor </summary>
An individual or a group that attempts to exploit vulnerabilities to cause or force a threat to occur.

</details>

<details><summary>Threat Vector </summary>
The means by which a threat actor carries out their objectives.

</details>

<details><summary>Token </summary>
Token
A physical object a user possesses and controls that is used to authenticate the user's identity. Source: NISTIR 7711

</details>

<details><summary>Vulnerability </summary>
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

</details>

<details><summary>Institute of Electrical and Electronics Engineers </summary>
IEEE is a professional organization that sets standards for telecommunications, computer engineering and similar disciplines.

</details>

Chapter 2: Incident Response, Business Continuity and Disaster Recovery Concepts
<details><summary>Adverse Events</summary>
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.

</details>

<details><summary>Breach</summary>
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

</details>

<details><summary> Business Continuity (BC) </summary>
Actions, processes and tools for ensuring an organization can continue critical operations during a contingency.

</details>

<details><summary> Business Continuity Plan (BCP) </summary>
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.

</details>

<details><summary> Business Impact Analysis (BIA) </summary>
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. Reference: https://csrc.nist.gov/glossary/term/business-impact-analysis

</details>

<details><summary> Disaster Recovery (DR) </summary>
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.

</details>

<details><summary> Disaster Recovery Plan (DRP) </summary>
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.

</details>

<details><summary> Event </summary>
Any observable occurrence in a network or system. Source: NIST SP 800-61 Rev 2

</details>

<details><summary> Exploit </summary>
A particular attack. It is named this way because these attacks exploit system vulnerabilities

</details>

<details><summary> Incident </summary>
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.

</details>

<details><summary> Incident Handling or Incident Response (IR) </summary>
The process of detecting and analyzing incidents to limit the incident's effect.

</details>

<details><summary>Incident Response Plan (IRP) </summary>
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

</details>

<details><summary> Intrusion </summary>
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

</details>

<details><summary> Security Operations Center </summary>
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.

</details>

<details><summary> Vulnerability </summary>
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.

</details>

<details><summary> Zero Day </summary>
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.

</details>

Chapter 3: Access Controls Concepts

<details><summary> Audit </summary>
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

</details>

<details><summary> Crime Prevention through Environmental Design (CPTED) </summary>
An architectural approach to the design of buildings and spaces which emphasizes passive features to reduce the likelihood of criminal activity.

</details>

<details><summary> Defense in Depth </summary>
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

</details>

<details><summary>Discretionary Access Control (DAC) </summary>
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

</details>

<details><summary>Encrypt </summary>
To protect private information by putting it into a form that can only be read by people who have permission to do so.

</details>

<details><summary>Firewalls </summary>
Devices that enforce administrative security policies by filtering incoming traffic based on a set of rules.

</details>

<details><summary>Insider Threat </summary>
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

</details>

<details><summary>iOS </summary>
An operating system manufactured by Apple Inc. Used for mobile devices.

</details>

<details><summary>Layered Defense </summary>
The use of multiple controls arranged in series to provide several consecutive controls to protect an asset; also called defense in depth.

</details>

<details><summary>Linux </summary>
An operating system that is open source, making its source code legally available to end users.

</details>

<details><summary>Log Anomaly </summary>
A system irregularity that is identified when studying log entries which could represent events of interest for further surveillance.

</details>

<details><summary>Logging </summary>
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.

</details>

<details><summary>Logical Access Control Systems </summary>
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.

</details>

<details><summary>Mandatory Access Control </summary>
Access control that requires the system itself to manage access controls in accordance with the organization's security policies.

</details>

<details><summary>Mantrap </summary>
An entrance to a building or an area that requires people to pass through two doors with only one door opened at a time.

</details>

<details><summary>Object </summary>
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

</details>

<details><summary>Physical Access Controls </summary>
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.

</details>

<details><summary>Principle of Least Privilege </summary>
The principle that users and programs should have only the minimum privileges necessary to complete their tasks. NIST SP 800-179

</details>

<details><summary>Privileged Account </summary>
An information system account with approved authorizations of a privileged user. NIST SP 800-53 Rev. 4

</details>

<details><summary>Ransomware </summary>
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.

</details>

<details><summary>Role-based access control (RBAC) </summary>
An access control system that sets up user permissions based on roles.

</details>

<details><summary>Rule </summary>
An instruction developed to allow or deny access to a system by comparing the validated identity of the subject to an access control list.

</details>

<details><summary>Segregation of Duties </summary>
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.

</details>

<details><summary>Subject </summary>
Generally an individual, process or device causing information to flow among objects or change to the system state. Source: NIST SP 800-53 R4

</details>

<details><summary>Technical Controls </summary>
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

</details>

<details><summary>Turnstile </summary>
A one-way spinning door or barrier that allows only one person at a time to enter a building or pass through an area.

</details>

<details><summary>Unix </summary>
An operating system used in software development.

</details>

<details><summary>User Provisioning </summary>
The process of creating, maintaining and deactivating user identities on a system.

</details>

Chapter 4: Network Security

<details><summary>Application programming interface (API) </summary>
A set of routines, standards, protocols, and tools for building software applications to access a web-based software application or web tool.

</details>

<details><summary>Bit </summary>
The most essential representation of data (zero or one) at Layer 1 of the Open Systems Interconnection (OSI) mode

</details>

<details><summary> Broadcast </summary>
Broadcast transmission is a one-to-many (one-to-everyone) form of sending internet traffic.

</details>

<details><summary> Byte </summary>
The byte is a unit of digital information that most commonly consists of eight bits.

</details>

<details><summary> Cloud computing </summary>
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

</details>

<details><summary> Community cloud </summary>
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

</details>

<details><summary> De-encapsulation </summary>
The opposite process of encapsulation, in which bundles of data are unpacked or revealed.

</details>

<details><summary> Denial-of-Service (DoS) </summary>
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

</details>

<details><summary>Domain Name Service (DNS) </summary>
This acronym can be applied to three interrelated elements: a service, a physical server and a network protocol.

</details>

<details><summary> Encapsulation </summary>
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.

</details>

<details><summary> Encryption </summary>
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

</details>

<details><summary> File Transfer Protocol (FTP) </summary>
The internet protocol (and program) used to transfer files between hosts.

</details>

<details><summary> Fragment attack </summary>
In a fragment attack, an attacker fragments traffic in such a way that a system is unable to put data packets back together.

</details>

<details><summary> Hardware </summary>
The physical parts of a computer and related devices.

</details>

<details><summary> Hybrid cloud</summary>
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.

</details>

<details><summary> Infrastructure as a Service (IaaS) </summary>
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.

</details>

<details><summary> Internet Control Message Protocol (ICMP) </summary>
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.

</details>

<details><summary> Internet Protocol (IPv4) </summary>
Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. CNSSI 4009-2015

</details>

<details><summary> Man-in-the-Middle </summary>
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

</details>

<details><summary> Microsegmentation </summary>
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.

</details>

<details><summary>Oversized Packet Attack </summary>
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.

</details>

<details><summary> Packet </summary>
Representation of data at Layer 3 of the Open Systems Interconnection (OSI) model.

</details>

<details><summary> Payload </summary>
The primary action of a malicious code attack.

</details>

<details><summary> Payment Card Industry Data Security Standard (PCI DSS)
</summary>
An information security standard administered by the Payment Card Industry Security Standards Council that applies to merchants and service providers who process credit or debit card transactions.

</details>

<details><summary> Payment Card Industry Data Security Standard (PCI DSS)
</summary>
An information security standard administered by the Payment Card Industry Security Standards Council that applies to merchants and service providers who process credit or debit card transactions.

</details>

<details><summary> Platform as a Service (PaaS) </summary>
The web-authoring or application development middleware environment that allows applications to be built in the cloud before they're deployed as SaaS assets.

</details>

<details><summary> Private cloud </summary>
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.

</details>

<details><summary> Protocols </summary>
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

</details>

<details><summary> Public cloud </summary>
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

</details>

<details><summary> Simple Mail Transport Protocol (SMTP)</summary>
The standard communication protocol for sending and receiving emails between senders and receivers.

</details>

<details><summary> Software </summary>
Computer programs and associated data that may be dynamically written or modified during execution. NIST SP 80--37 Rev. 2

</details>

<details><summary>Software as a Service (SaaS) </summary>
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

</details>

<details><summary> Spoofing </summary>
Faking the sending address of a transmission to gain illegal entry into a secure system. CNSSI 4009-2015

</details>

<details><summary> Transport Control Protocol/Internet Protocol (TCP/IP) Model </summary>
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.

</details>

<details><summary> Transport Control Protocol/Internet Protocol (TCP/IP) Model </summary>
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.

</details>

<details><summary>VLAN </summary>
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.

</details>

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

</details>

<details><summary> WLAN </summary>
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.

</details>

<details><summary> Zenmap </summary>
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.

</details>

<details><summary> Zero Trust </summary>

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.

</details>

Chapter 5: Security Operations

<details><summary> Application Server </summary>
A computer responsible for hosting applications to user workstations. NIST SP 800-82 Rev.2

</details>

<details><summary> Asymmetric Encryption </summary>
An algorithm that uses one key to encrypt and a different key to decrypt the input plaintext.

</details>

<details><summary> Checksum </summary>
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.

</details>

<details><summary> Ciphertext </summary>
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.

</details>

<details><summary> Classification </summary>
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.

</details>

<details><summary>Configuration management </summary>
A process and discipline used to ensure that the only changes made to a system are those that have been authorized and validated.

</details>

<details><summary> Cryptanalyst </summary>
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.

</details>

<details><summary> Cryptography </summary>
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.

</details>

<details><summary> Data Loss Prevention (DLP) </summary>
System capabilities designed to detect and prevent the unauthorized use and transmission of information.

</details>

<details><summary> Decryption </summary>
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."

</details>

<details><summary> Degaussing</summary>
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.

</details>

<details><summary> Digital Signature </summary>
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

</details>

<details><summary> Egress Monitoring </summary>
Monitoring of outgoing network traffic.

</details>

<details><summary> Encryption </summary>
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.

</details>

<details><summary>Encryption System </summary>

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

</details>

<details><summary> Hardening </summary>
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).

</details>

<details><summary> Hash Function </summary>
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 800-15

</details>

<details><summary> Hashing </summary>
The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data. Source CNSSI 4009-2015

</details>

<details><summary> Information Sharing </summary>
The requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs. NIST SP 800-16

</details>

<details><summary> Ingress Monitoring </summary>
Monitoring of incoming network traffic.

</details>

<details><summary> Message Digest </summary>
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

</details>

<details><summary> Operating System</summary>

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

</details>

<details><summary> Patch</summary>
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

</details>

<details><summary> Patch Management </summary>
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

</details>

<details><summary> Plaintext </summary>
A message or data in its natural format and in readable form; extremely vulnerable from a confidentiality perspective.

</details>

<details><summary> Records </summary>
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

</details>

<details><summary> Records Retention </summary>
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.

</details>

<details><summary> Remanence </summary>
Residual information remaining on storage media after clearing. NIST SP 800-88 Rev. 1

</details>

<details><summary> Request for change (RFC) </summary>

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

</details>

<details><summary> Security Governance </summary>
The entirety of the policies, roles, and processes the organization uses to make security decisions in an organization.

</details>

<details><summary> Social engineering </summary>
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

</details>

<details><summary> Symmetric encryption</summary>
An algorithm that uses the same key in both the encryption and the decryption processes.

</details>

<details><summary> Web Server </summary>
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

</details>

<details><summary> Whaling Attack </summary>
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.

</details>

YOU CAN ALSO CHECK THIS YOUTUBE CHANNEL FOR MORE PRACTICE FOR YOUR EXAM:
Master ISC2 CC 2024 Practice Questions 2 : Unlock Your Success

KINDLY FOLLOW ON TWITTER: https://x.com/anyahuru18036

REMEMBER TO READ EXAM QUESTIONS TWICE AND BE CONFIDENT IN YOUR ANSWER BEFORE CHOOSING IT BECAUSE YOU CAN'T GO BACK TO THE PREVIOUS QUESTION AFTER ANSWERING IT. GOODLUCK IN YOUR EXAMS ><