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 that 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 looking 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 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 attack.
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.

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** of 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? (FIBS 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 government (not to be confused with governance) and typically carry financial penalties for noncompliance.

Regulations -> Standards -> Policies -> Procedures

Module 5 Understand (ISC)² Code of Ethics