

Domain 1: Security Principles

Chapter 1 Agenda:

Module 1: Understand the Security Concepts of Information Assurance (D1.1)

Module 2: Understand the Risk Management Process (D1.2)

Module 3: Understand Security Controls (D1.3)

Module 4: Understand Governance Elements (D1.5)

Module 5: Understand ISC2 Code of Ethics (D1.4)

Module 6: Summary

Module 1: Understand the Security Concepts of Information Assurance

The CIA Triad: To define security, it has become common to use Confidentiality, Integrity and Availability, also known as the CIA triad. The purpose of these terms is to describe security using relevant and meaningful words that make security more understandable to management and users and define its purpose.

Confidentiality:

Confidentiality relates to permitting authorized access to information, while at the same time protecting information from improper disclosure.

Integrity:

Integrity 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.

Availability:

Availability means that systems and data are accessible at the time users need them.



CIA Triad Deep Dive:

Confidentiality is a difficult balance to achieve when many system users are guests or customers, and it is not known if they are accessing the system from a compromised machine or vulnerable mobile application. So, the security professional's obligation is to regulate access—protect the data that needs protection, yet permit access to authorized individuals.

Personally Identifiable Information (PII) is a term related to the area of confidentiality. It pertains to any data about an individual that could be used to identify them. Other terms related to confidentiality are **protected health information (PHI)**, which is information regarding one's health status, and **classified or sensitive information**, which includes trade secrets, research, business plans and intellectual property.

Another useful definition is **sensitivity**, which is 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.

Integrity measures the degree to which something is whole and complete, internally consistent and correct. The concept of integrity applies to:

- information or data
- systems and processes for business operations
- organizations
- people and their actions

Data integrity is the assurance that data has not been altered in an unauthorized manner. This requires the protection of the data in systems and during processing to ensure that it is free from improper modification, errors or loss of information and is recorded, used and maintained in a way that ensures its completeness. Data integrity covers data in storage, during processing and while in transit.

Information must be accurate, internally consistent and useful for a stated purpose. The internal consistency of information ensures that information is correct on all related systems so that it is displayed and stored in the same way on all systems. Consistency, as part of data integrity, requires that all instances of the data be identical in form, content and meaning.

System integrity 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. For example, a **baseline** can refer to the current state of the information—whether it is protected. Then, 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.

Availability can be defined as (1) timely and reliable access to information and the ability to use it, and (2) 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](#), because it represents the importance an organization gives to data or an information system in performing its operations or achieving its mission.

Video: 1.1

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](#). 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](#), 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.



DRAG-AND-DROP Activity (D1, L1.1.1)

Instructions - Drag the term below into the box next to the correct definition listed below.
Click the submit button when complete.

| | |
|-----------------|---|
| Authorization | <i>The right or a permission that is granted to a system entity to access a system resource.</i> |
| Integrity | <i>The property that data has not been altered in an unauthorized manner.</i> |
| Confidentiality | <i>The characteristic of data or information when it is not made available or disclosed to unauthorized persons or processes.</i> |
| Privacy | <i>The right of an individual to control the distribution of information about themselves.</i> |
| Availability | <i>Ensuring timely and reliable access to and use of information by authorized users.</i> |
| Non-repudiation | <i>The inability to deny taking an action, such as sending an email message.</i> |
| Authentication | <i>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.</i> |

Video-1.2: Providing Identity.

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.

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.

Video-1.3 Privacy in the Working Environment.mp4

Video-1.4 Knowledge Check- Protecting Information.ts

Module 2: Understand the Risk Management Process

Video-1.5 Introduction to Risk Management.mp4

Video-1.6 Importance of Risk Management.mp4

Risk Management Terminology

Security professionals use their knowledge and skills to examine operational risk management, determine how to use risk data effectively, work cross-functionally and report actionable information and findings to the stakeholders concerned. Terms such as threats, vulnerabilities and assets are familiar to most cybersecurity professionals.

- An [asset](#) is something in need of protection.
- A [vulnerability](#) is a gap or weakness in those protection efforts.
- A [threat](#) is something or someone that aims to exploit a vulnerability to thwart protection efforts.

Risk is the intersection of these terms. Let's look at them more closely.

Threats

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. To better understand threats, consider the following scenario:

Video-1.7 Threats.mp4

In the context of cybersecurity, typical [threat actors](#) include the following:

- Insiders (either deliberately, by simple human error, or by gross incompetence).
- Outside individuals or informal groups (either planned or opportunistic, discovering vulnerability).

- Formal entities that are nonpolitical (such as business competitors and cybercriminals).
- Formal entities that are political (such as terrorists, nation-states, and hacktivists).
- Intelligence or information gatherers (could be any of the above).
- Technology (such as free-running [bots](#) and [artificial intelligence](#) , which could be part of any of the above).

**Threat Vector: The means by which a threat actor carries out their objectives.*

Vulnerabilities

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. Consider the pickpocket scenario from below.

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. For example, to protect yourself from the pickpocket, you could carry your wallet in an inside pocket instead of the back pant pocket or behave alertly instead of ignoring your surroundings. Managing vulnerabilities starts with one simple step: Learn what they are.

Video-1.8 Vulnerabilities.mp4

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:

Video-1.9 Likelihood.mp4

Risk Identification

How do you identify risks? Do you walk down the street watching out for traffic and looking for puddles on the ground? Maybe you've noticed loose wires at your desk or water on the office floor? If you're already on the lookout for risks, you'll fit with other security professionals who know it's necessary to dig deeper to find possible problems.

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.

It involves looking at your unique company and analyzing its unique situation. Security professionals know their organization's strategic, tactical and operational plans.

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 common risk assessment activity identifies the risk of fire to a building. While there are many ways to mitigate that risk, the primary goal of a risk assessment is to estimate and prioritize. For example, fire alarms are the lowest cost and can alert personnel to evacuate and reduce the risk of personal injury, but they won't keep a fire from spreading or causing more damage. Sprinkler systems won't prevent a fire but can minimize the amount of damage done. However, while sprinklers in a data center limit the fire's spread, it is likely they will destroy all the systems and data on them. A gas-based system may be the best solution to protect the systems, but it might be cost-prohibitive. A risk assessment can prioritize these 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:

Select each plus sign hotspot to learn more about each topic.

Avoidance: Risk avoidance 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.

Video-1.10 Risk Management Process.mp4

 **DRAG-AND-DROP Activity (D1, L1.2.1)**

*Instructions - Drag the term below into the box next to the correct definition listed below.
Click the submit button when complete.*

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

Video-1.11 Risk Management- Susan's Good News.mp4

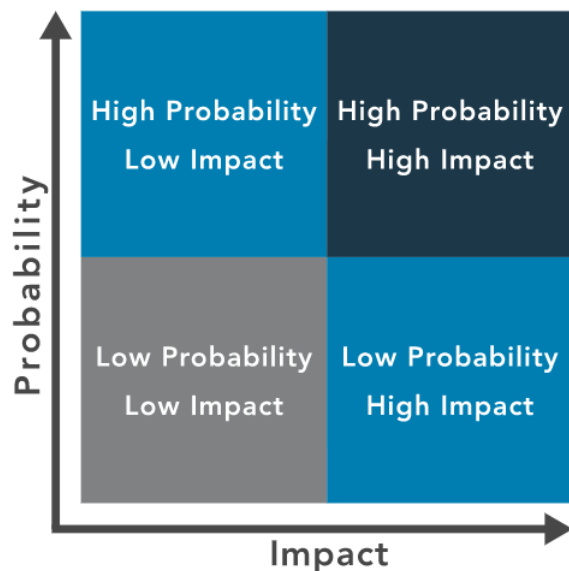
Video-1.12 Risk in Our Lives.mp4

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.

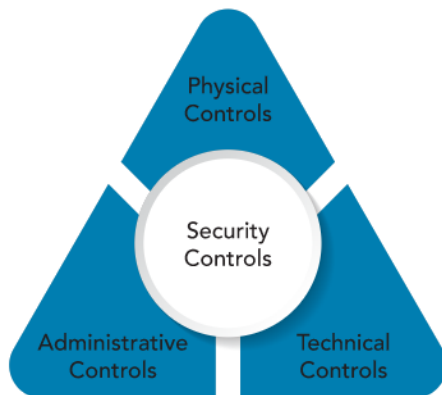
Video-1.13 Risk Tolerance Drives Decision Making.mp4

Module 3: Understand Security Controls

Classify types of security controls.

What are Security Controls?

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 Controls

Physical controls address 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.

Visitors and guests accessing a workplace, for example, must often enter the facility through a designated entrance and exit, where they can be identified, their visit's purpose assessed, and then allowed or denied entry. Employees would enter, perhaps through other entrances, using company-issued badges or other tokens to assert their identity and gain access. These require technical controls to integrate the badge or

token readers, the door release mechanisms and the identity management and access control systems into a more seamless security system.

Technical Controls

Technical controls (also called logical controls) are 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 Controls

Administrative controls (also known as managerial controls) are 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.

| Administrative Control | Physical Control | Technical Control |
|---------------------------------|--------------------------|---------------------|
| Acceptable Use Policy | Badge Reader | Access Control List |
| Emergency Operations Procedures | Stop Sign in Parking Lot | |
| Employee Awareness Training | Door Lock | |
| | | |

Video-1.15 Making Connections

Module 4: Understand Governance Elements and Processes

Module Objectives

- L1.4.1 Distinguish between policies, procedures, standards, regulations and laws.
- L1.4.2 Demonstrate the relationship among governance elements.

Video-1.16 Module 4- Understand Governance Elements and Processes.mp4

Governance Elements

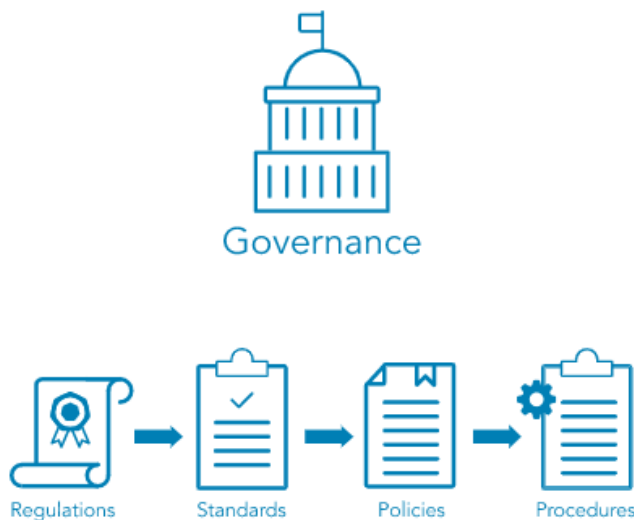
Any business or organization exists to fulfill a purpose, whether it is to provide raw materials to an industry, manufacture equipment to build computer hardware, develop software applications, construct buildings or provide goods and services. To complete the objective requires that decisions are made, rules and practices are defined, and policies and procedures are in place to guide the organization in its pursuit of achieving its goals and mission.

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.

How are regulations, standards, policies and procedures related? It might help to look at the list in reverse.

- 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.

Now that we see how they are connected, we'll look at some details and examples of each.



Regulations and Laws

Regulations and associated fines and penalties can be imposed by governments at the national, regional or local level. Because regulations and laws can be imposed and enforced differently in different parts of the world, here are a few examples to connect the concepts to actual regulations.

The [Health Insurance Portability and Accountability Act \(HIPAA\) of 1996](#) is an example of a law that governs the use of protected health information (PHI) in the United States. Violation of the HIPAA rule carries the possibility of fines and/or imprisonment for both individuals and companies.

The [General Data Protection Regulation \(GDPR\)](#) was enacted by the European Union (EU) to control use of Personally Identifiable Information (PII) of its citizens and those in the EU. It includes provisions that apply financial penalties to companies who handle data of EU citizens and those living in the EU even if the company does not have a physical presence in the EU, giving this regulation an international reach.

Finally, it is common to be subject to regulation on several levels. Multinational organizations are subject to regulations in more than one nation in addition to multiple regions and municipalities. Organizations need to consider the regulations that apply to their business at all levels—national, regional and local—and ensure they are compliant with the most restrictive regulation.

Standards

Organizations use multiple standards as part of their information systems security programs, both as compliance documents and as advisories or guidelines. Standards cover a broad range of issues and ideas and may provide assurance that an organization is operating with policies and procedures that support regulations and are widely accepted best practices.

The [International Organization for Standardization \(ISO\)](#) develops and publishes international standards on a variety of technical subjects, including information systems and information security, as well as encryption standards. ISO solicits input from the international community of experts to provide input on its

standards prior to publishing. Documents outlining ISO standards may be purchased online.

The [National Institute of Standards and Technology \(NIST\)](#) is a United States government agency under the Department of Commerce and publishes a variety of technical standards in addition to information technology and information security standards. Many of the standards issued by NIST are requirements for U.S. government agencies and are considered recommended standards by industries worldwide. NIST standards solicit and integrate input from industry and are free to download from the NIST website.

Finally, think about how computers talk to other computers across the globe. People speak different languages and do not always understand each other. How are computers able to communicate? Through standards, of course!

Thanks to the [Internet Engineering Task Force \(IETF\)](#), there are standards in communication protocols that ensure all computers can connect with each other across borders, even when the operators do not speak the same language.

The [Institute of Electrical and Electronics Engineers \(IEEE\)](#) also sets standards for telecommunications, computer engineering and similar disciplines.

Policies

Policy is informed by applicable law(s) and specifies which standards and guidelines the organization will follow. Policy is broad, but not detailed; it establishes context and sets out strategic direction and priorities. Governance policies are used to moderate and control decision-making, to ensure compliance when necessary and to guide the creation and implementation of other policies.

Policies are often written at many levels across the organization. High-level governance policies are used by senior executives to shape and control decision-making processes. Other high-level policies direct the behavior and activity of the entire organization as it moves toward specific or general goals and objectives. Functional areas such as human resources management, finance and accounting, and security and asset protection usually have their own sets of policies. Whether imposed by laws and regulations or by contracts, the need for compliance might also require the development of specific high-level policies that are documented and assessed for their effective use by the organization.

Policies are implemented, or carried out, by people; for that, someone must expand the policies from statements of intent and direction into step-by-step instructions, or procedures.

Procedures

Procedures define the explicit, repeatable activities necessary to accomplish a specific task or set of tasks. They provide supporting data, decision criteria or other explicit knowledge needed to perform each task. Procedures can address one-time or infrequent actions or common, regular occurrences. In addition, procedures establish the measurement criteria and methods to use to determine whether a task has been successfully completed. Properly documenting procedures and training personnel on how to locate and follow them is necessary for deriving the maximum organizational benefits from procedures.

Importance of Governance Elements

Video-1.17 Importance of Governance Elements

Module 5: Understand ISC2 Code of Ethics

Module Objective

- L1.5.1 Analyze appropriate outcomes according to the canons of the ISC2 Code of Ethics when given examples.

Video 1.18 Module 5- Understand ISC2 Code of Ethics.mp4

Importance of a Professional Code of Ethics

Video-1.18 Podcast- Importance of a Professional Code of Ethics.mp3

Professional Code of Conduct

All information security professionals who are certified by ISC2 recognize that certification is a privilege that must be both earned and maintained. Every ISC2 member is required to commit to fully support the ISC2 Code of Ethics.

ISC2 Code of Ethics Preamble

The Preamble states the purpose and intent of the ISC2 Code of Ethics.

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

ISC2 Code of Ethics Canons

The Canons represent the important beliefs held in common by the members of ISC2. Cybersecurity professionals who are members of ISC2 have a duty to the following four entities in the Canons.

- 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.

Theoretical Example: Code of Ethics

Video-1.19 Theoretical Example- Code of Ethics.mp4

Module 6: Chapter 1 Summary

Chapter 1: Terms and Definitions

- **Adequate Security** - Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of information. Source: OMB Circular A-130
- **Administrative Controls** - Controls implemented through policy and procedures. Examples include access control processes and requiring multiple personnel to conduct a specific operation. Administrative controls in modern environments are often enforced in conjunction with physical and/or technical controls, such as an access-granting policy for new users that requires login and approval by the hiring manager.
- **Artificial Intelligence** - The ability of computers and robots to simulate human intelligence and behavior.
- **Asset** - Anything of value that is owned by an organization. Assets include both tangible items such as information systems and physical property and intangible assets such as intellectual property.
- **Authentication** - Access control process validating that the identity being claimed by a user or entity is known to the system, by comparing one (single factor or SFA) or more (multi-factor authentication or MFA) factors of identification.
- **Authorization** - The right or a permission that is granted to a system entity to access a system resource. NIST 800-82 Rev.2
- **Availability** - Ensuring timely and reliable access to and use of information by authorized users.
- **Baseline** - A documented, lowest level of security configuration allowed by a standard or organization.
- **Bot** - Malicious code that acts like a remotely controlled “robot” for an attacker, with other Trojan and worm capabilities.

- **Classified or Sensitive Information** - Information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status and classification level when in documentary form.
- **Confidentiality** - The characteristic of data or information when it is not made available or disclosed to unauthorized persons or processes. NIST 800-66
- **Criticality** - A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. NIST SP 800-60 Vol. 1, Rev. 1
- **Data Integrity** - The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing and while in transit. Source: NIST SP 800-27 Rev A
- **Encryption** - The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.
- **General Data Protection Regulation (GDPR)** - In 2016, the European Union passed comprehensive legislation that addresses personal privacy, deeming it an individual human right.
- **Governance** -The process of how an organization is managed; usually includes all aspects of how decisions are made for that organization, such as policies, roles, and procedures the organization uses to make those decisions.
- **Health Insurance Portability and Accountability Act (HIPAA)** - This U.S. federal law is the most important healthcare information regulation in the United States. It directs the adoption of national standards for electronic healthcare transactions while protecting the privacy of individual's health information. Other provisions address fraud reduction, protections for individuals with health insurance and a wide range of other healthcare-related activities. Est. 1996.
- **Impact** - The magnitude of harm that could be caused by a threat's exercise of a vulnerability.

- **Information Security Risk** - The potential adverse impacts to an organization's operations (including its mission, functions and image and reputation), assets, individuals, other organizations, and even the nation, which results from the possibility of unauthorized access, use, disclosure, disruption, modification or destruction of information and/or information systems.
- **Institute of Electrical and Electronics Engineers** - IEEE is a professional organization that sets standards for telecommunications, computer engineering and similar disciplines.
- **Integrity** - The property of information whereby it is recorded, used and maintained in a way that ensures its completeness, accuracy, internal consistency and usefulness for a stated purpose.
- **International Organization of Standards (ISO)** - The ISO develops voluntary international standards in collaboration with its partners in international standardization, the International Electro-technical Commission (IEC) and the International Telecommunication Union (ITU), particularly in the field of information and communication technologies.
- **Internet Engineering Task Force (IETF)** - The internet standards organization, made up of network designers, operators, vendors and researchers, that defines protocol standards (e.g., IP, TCP, DNS) through a process of collaboration and consensus. Source: NIST SP 1800-16B
- **Likelihood** - The probability that a potential vulnerability may be exercised within the construct of the associated threat environment.
- **Likelihood of Occurrence** - A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or set of vulnerabilities.
- **Multi-Factor Authentication** - Using two or more distinct instances of the three factors of authentication (something you know, something you have, something you are) for identity verification.
- **National Institutes of Standards and Technology (NIST)** - The NIST is part of the U.S. Department of Commerce and addresses the measurement infrastructure within science and technology efforts within the U.S. federal

government. NIST sets standards in a number of areas, including information security within the Computer Security Resource Center of the Computer Security Divisions.

- **Non-repudiation** - The inability to deny taking an action such as creating information, approving information and sending or receiving a message.
- **Personally Identifiable Information (PII)** - The National Institute of Standards and Technology, known as NIST, in its Special Publication 800-122 defines PII as “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, Social Security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information.”
- **Physical Controls** - Controls implemented through a tangible mechanism. Examples include walls, fences, guards, locks, etc. In modern organizations, many physical control systems are linked to technical/logical systems, such as badge readers connected to door locks.
- **Privacy** - The right of an individual to control the distribution of information about themselves.
- **Probability** - The chances, or likelihood, that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. Source: NIST SP 800-30 Rev. 1
- **Protected Health Information (PHI)** - Information regarding health status, the provision of healthcare or payment for healthcare as defined in HIPAA (Health Insurance Portability and Accountability Act).
- **Qualitative Risk Analysis** - A method for risk analysis that is based on the assignment of a descriptor such as low, medium or high. Source: NISTIR 8286
- **Quantitative Risk Analysis** - A method for risk analysis where numerical values are assigned to both impact and likelihood based on statistical probabilities and monetarized valuation of loss or gain. Source: NISTIR 8286

- **Risk** - A possible event which can have a negative impact upon the organization.
- **Risk Acceptance** - Determining that the potential benefits of a business function outweigh the possible risk impact/likelihood and performing that business function with no other action.
- **Risk Assessment** - The process of identifying and analyzing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals and other organizations. The analysis performed as part of risk management which incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place.
- **Risk Avoidance** - Determining that the impact and/or likelihood of a specific risk is too great to be offset by the potential benefits and not performing a certain business function because of that determination.
- **Risk Management** - The process of identifying, evaluating and controlling threats, including all the phases of risk context (or frame), risk assessment, risk treatment and risk monitoring.
- **Risk Management Framework** - A structured approach used to oversee and manage risk for an enterprise. Source: CNSSI 4009
- **Risk Mitigation** - Putting security controls in place to reduce the possible impact and/or likelihood of a specific risk.
- **Risk Tolerance** - The level of risk an entity is willing to assume in order to achieve a potential desired result. Source: NIST SP 800-32. Risk threshold, risk appetite and acceptable risk are also terms used synonymously with risk tolerance.
- **Risk Transference** - Paying an external party to accept the financial impact of a given risk.
- **Risk Treatment** - The determination of the best way to address an identified risk.
- **Security Controls** - The management, operational and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to

protect the confidentiality, integrity and availability of the system and its information. Source: FIPS PUB 199

- **Sensitivity** - A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. Source: NIST SP 800-60 Vol 1 Rev 1
- **Single-Factor Authentication** - Use of just one of the three available factors (something you know, something you have, something you are) to carry out the authentication process being requested.
- **State** - The condition an entity is in at a point in time.
- **System Integrity** - The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. Source: NIST SP 800-27 Rev. A
- **Technical Controls** - Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.
- **Threat**- Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations or the nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.
- **Threat Actor** - An individual or a group that attempts to exploit vulnerabilities to cause or force a threat to occur.
- **Threat Vector** - The means by which a threat actor carries out their objectives.
- **Token**- A physical object a user possesses and controls that is used to authenticate the user's identity. Source: NISTIR 7711
- **Vulnerability** - Weakness in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source. Source: NIST SP 800-30 Rev 1