(ISC)²

Chapter 1 Resource

Security Principles

Chapter Summary

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

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

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

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

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

Module Names

Module 1: Understand the Security Concepts of Information Assurance

Module 2: Understand the Risk Management Process

Module 3: Understand Security Controls

Module 4: Understand Governance Elements

Module 5: Understand (ISC)² Code of Ethics

Chapter to Domain Mapping

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

Learning Objectives

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

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

Chapter Takeaways

Module 1: Understand the Security Concepts of Information Assurance

CIA Triad:

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

Module 2: Understand the Risk Management Process

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

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

Risk Identification:

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

Risk Assessment:

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

Risk Treatment:

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

Chapter Takeaways

Module 3: Understand Security Controls

Security Controls:

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

Module 4: Understand Governance Elements

Governance Elements:

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

Module 5: Understand (ISC)² Code of Ethics

(ISC)² Code of Ethics Preamble:

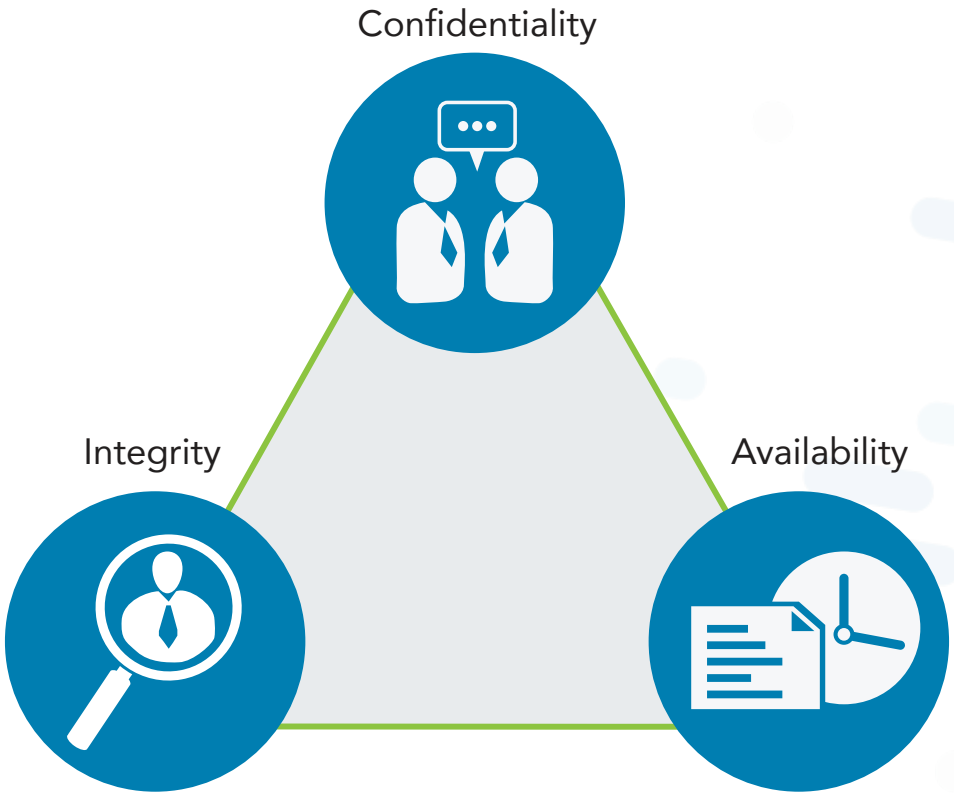
- The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

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

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorably, honestly, justly, responsibly and legally.
- Provide diligent and competent service to principles.

Graphics

CIA Triad



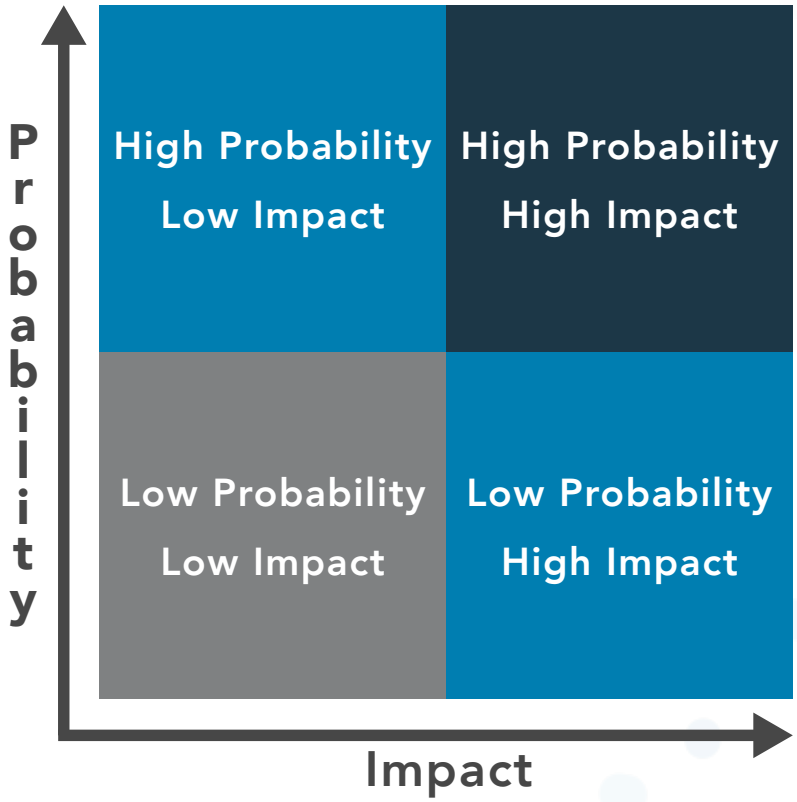
We must strive to provide information assurance, and these primary components help make information assurance possible: confidentiality, integrity and availability.

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

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

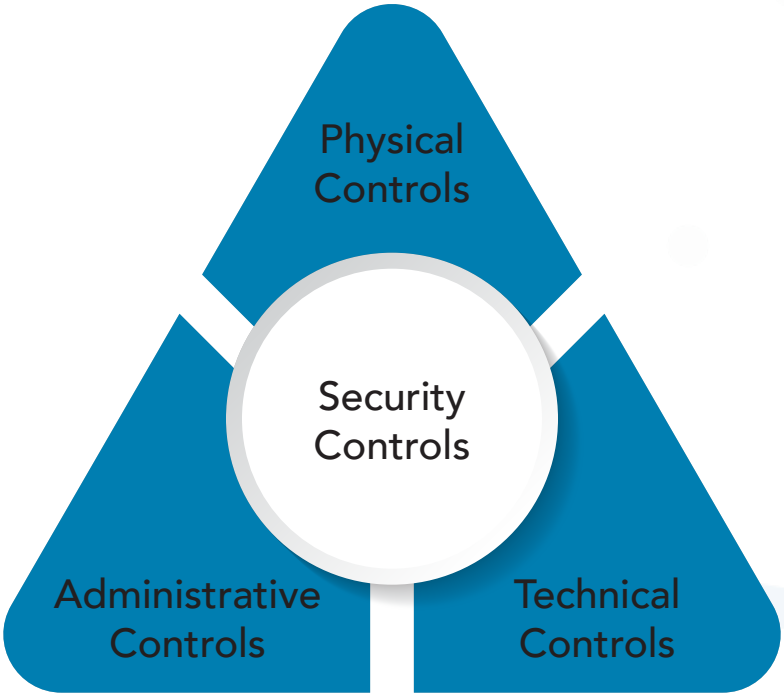
Availability: ensure the data is accessible to authorized users when and where it is needed, and in the form and format that is required.

Prioritizing Risk



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

Security Controls



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

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

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

Formulas and Calculations

Level of Risk = Probability + Impact

Chapter Terms and Definitions

Adequate Security

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

Administrative Controls

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

Artificial Intelligence

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

Asset

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

Authentication

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

Authorization

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

Availability

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

Baseline

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

Biometric

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

Bot

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

Classified or Sensitive Information

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

Confidentiality

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

Criticality

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

Data Integrity

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

Encryption

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

General Data Protection Regulation (GDPR)

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

Governance

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

Health Insurance Portability and Accountability Act (HIPAA)

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

Impact

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

Information Security Risk

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

Institute of Electrical and Electronics Engineers

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

Integrity

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

International Organization of Standards (ISO)

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

Internet Engineering Task Force (IETF)

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

Likelihood

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

Likelihood of Occurrence

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

Multi-Factor Authentication

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

National Institutes of Standards and Technology (NIST)

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

Non-repudiation

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

Personally Identifiable Information (PII)

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

Physical Controls

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

Privacy

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

Probability

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

Protected Health Information (PHI)

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

Qualitative Risk Analysis

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

Quantitative Risk Analysis

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

Risk

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

Risk Acceptance

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

Risk Assessment

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

Risk Avoidance

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

Risk Management

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

Risk Management Framework

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

Risk Mitigation

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

Risk Tolerance

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

Risk Transference

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

Risk Treatment

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

Security Controls

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

Sensitivity

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

Single-Factor Authentication

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

State

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

System Integrity

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

Technical Controls

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

Threat

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

Threat Actor

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

Threat Vector

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

Token

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

Vulnerability

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