Module 22: Governance and Compliance

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Governance and Compliance

Module Objective: Create documents and policies related to cybersecurity governance and compliance.

Topic Title	Topic Objective
Governance	Create cybersecurity policy documents.
The Ethics of Cybersecurity	Create a personal code of ethical conduct.
IT Security Management Framework	Evaluate security controls.

22.1 Governance

Governance

- IT security governance determines who is authorized to make decisions about cybersecurity risks within an organization.
- It demonstrates accountability and provides oversight to ensure that any risks are adequately mitigated and that security strategies are aligned with the organization’s business objectives and are compliant with regulations.
- There are several key roles in good data governance programs:

Data owner	A person who ensures compliance with policies and procedures, assigns the proper classification to information assets, and determines the criteria for accessing information assets.
Data controller	A person who determines the purposes for which, and the way in which, personal data is processed.
Data processor	A person or organization who processes personal data on behalf of the data controller.
Data custodian	A person who implements the classification and security controls for the data in accordance with the rules set out by the data owner. In other words, data custodians are responsible for the technical control of the data.
Data steward	A person who ensures that data supports an organization’s business needs and meets regulatory requirements.
Data protection officer	A person who oversees an organization’s data protection strategy.

Cybersecurity Policies

- A cybersecurity policy is a high-level document that outlines an organization’s vision for cybersecurity, including its goals, needs, scope, and responsibilities.

- Specifically, it:
  - Demonstrates an organization’s commitment to security.
  - Sets the standards of behavior and security requirements for carrying out activities, processes and operations, and protecting technology and information assets within an organization.
  - Ensures that the acquisition, use, and maintenance of system operations, software, and hardware are consistent across the organization.
  - Defines the legal consequences of policy violations.
  - Gives the security team the support they need from senior management.

Cybersecurity Policies (Cont.)

- There are various types of cybersecurity policies.
- Some of the most common ones are:
  - **Master cybersecurity policy**
    - The blueprint for an organization’s cybersecurity program, this policy serves as the strategic plan for implementing cybersecurity controls.
  - **System-specific policy**
    - This policy is developed for specific devices or computer systems and aims to establish standardization for approved applications, software, operating system configurations, hardware, and hardening countermeasures within an organization.
  - **Issue-specific policy**
    - This policy is developed for certain operational issues, circumstances, or conditions that may require more detailed requirements and directions.

Governance

Types of Security Policies

- An organization needs to establish clear and detailed security policies that all employees are aware of.
- Some of the security-related policies that an organization may have in place are:

Identification and authentication policy	Specifies who should be permitted access to network resources and what verification procedures are in place to facilitate this.
Password policy	Defines minimum password requirements.
Acceptable use policy	Highlights a set of rules that determine access to and use of network resources.
Remote access policy	Sets out how to remotely connect to an organization's internal network and explains what information is remotely accessible.
Network maintenance policy	Outlines procedures for updating an organization's specified operating systems and end-user applications.
Incident handling policy	Provides guidance on how to report and respond to security-related incidents within an organization.
Data policy	Sets out measurable rules for processing data within an organization, such as specifying where data is stored, how data is classified, and how data is handled and disposed of.
Credential policy	Enforces the rules for composing credentials.
Organizational policy	Provides guidance for how work should be carried out in an organization.

Lab - Developing Cybersecurity Policies and Procedures

- In this Lab, you will meet the following objectives:
  - Part 1: Review the scenario.
  - Part 2: Review and prioritize audit findings.
  - Part 3: Develop policy documents.
  - Part 4: Develop a plan to disseminate and evaluate policies.

22.2 The Ethics of Cybersecurity

Ethics of a Cybersecurity Specialist

- Ethics is the little voice in your head that tells you what is right and what is wrong, guiding you to make the right decisions.
- A cybersecurity specialist needs to understand both the law and an organization’s interests to be able to make such decisions.
- Ethics can be viewed from many different perspectives:

Utilitarian ethics	It is based on the guiding principle that the consequence of an action is the most important factor in determining if the action is moral or not. For example, an action that maximizes the greatest good for the greatest amount of people is an ethical choice.
The rights approach	It is guided by the principle which states that an individual has the right to make their own choices, which cannot be violated by another person’s decision. This decision must respect and consider the fundamental rights of the individual. These fundamental rights include the right to truth, privacy, safety, and for society to apply laws fairly to all members of society.
The common good approach	It proposes that ethical actions are those that benefit the entire community. It challenges individuals to recognize and pursue the values and goals shared with other members of a community.

The Ten Commandments of Computer Ethics

- Based in Washington, DC, the Computer Ethics Institute is a resource for identifying, assessing, and responding to ethical issues throughout the information technology industry.

- It was one of the first organizations to recognize the ethical and public policy issues arising from the rapid growth of the information technology field.

- They created the **ten commandments of computer ethics** presented here.

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Cybercrime

Cybercrime falls into three categories:

1. **Computer-targeted crime** is where a computer is the target of criminal activity. Examples include malware, hacking, or denial of service attacks.

2. **Computer-assisted crime** occurs when a computer is used to commit a crime, such as theft or fraud.

3. **Computer-incidental crime** is where a computer provides information that is incidental to an actual crime. For example, a computer is used to store illegally downloaded videos, not the actual tool used to commit the crime.

Cybercrime (Cont.)

- There are lots of tools connected to the internet — many of which do not require a great deal of expertise to use — that are contributing to the exponential growth of cybercrime.

- In fact, cybercrime is growing much faster than the ability of the legal system to create the laws and regulations that prohibit it.

- There are several agencies working to combat cybercrime, including the Federal Bureau of Investigation Internet Crime Complaint Center (IC3), InfraGard, and Software and Information Industry Association (SIIA) in the U.S.

Cyber Laws

Laws are in place to prohibit undesired behaviors. In the U.S, there are three primary sources of laws and regulations, all of which involve aspects of computer security:

Statutory law	The U.S. Congress has established federal administrative agencies and a regulatory framework that includes both civil and criminal penalties for failing to follow the rules. Criminal laws enforce a commonly accepted moral code backed by the authority of the government. For example, the Computer Fraud and Abuse Act is a statutory law that prohibits accessing a computer without authorization, or in excess of authorization. Violating these rules could result in a fine or prison sentence.
Administrative law	A legal framework that governs the activities of administrative agencies of government, administrative law ensures that public bodies act in accordance with the law. For example, the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) have been concerned with issues such as intellectual property theft and fraud.
Common law	Common law cases work their way through the judicial system providing precedents and constitutional bases for lawmaking.

The Federal Information Security Management Act (FISMA)

- Federal IT systems contain and use a large amount of valuable information and are therefore considered high-value targets for cybercriminals.

- In 2002, the U.S. Congress created FISMA to cover federal agencies’ IT systems.

- Specifically, FISMA stipulates that federal agencies must create an information security program that includes:
  - Risk assessments
  - An annual inventory of IT systems
  - Policies and procedures to reduce risk
  - Security awareness training
  - Testing and evaluation of all IT system controls
  - Incident response procedures
  - A continuity of operations plan

Industry Specific Laws

The laws and standards which organizations working in these industries in the U.S. must be compliant with are:

Finance	The **Gramm-Leach-Bliley Act (GLBA)** is a piece of legislation that mainly affects the financial industry. However, a portion of that legislation also provides opt-out provisions for individuals, putting them in control of how the information they share with an organization during a business transaction is used. The GLBA restricts information sharing with third party organizations.
Corporate accounting	Following several high-profile corporate accounting scandals in the U.S., Congress passed the **Sarbanes-Oxley Act (SOX)** in 2002 to overhaul financial and corporate accounting standards. Specifically, it targeted the financial standards and practices of publicly traded firms in the country.
Credit card	The **Payment Card Industry Data Security Standard (PCI DSS)** is a set of contractual rules that seek to protect cardholder payment data during a transaction and reduce fraud. In theory, the PCI DSS is a voluntary standard. However, in practice, any organization that stores, processes, or transmits cardholder data that fails to comply with the PCI DSS standard may face significantly higher transaction fees, fines up to $500,000, and, in extreme circumstances, lose the ability to process payment cards.
Cryptography	Organizations that **import or export commercial encryption products** are subject to regulations that are overseen by the Bureau of Industry and Security in the Department of Commerce. Export restrictions to rogue states and terrorist organizations may be in place due to national security concerns. Also, some countries may decide to restrict the import of cryptography technologies due to concerns that: • The technology contains a backdoor or security vulnerability. • Citizens can use this technology to communicate anonymously and elude monitoring by the authorities. • Privacy levels could increase above an acceptable level.

Security Breach Notification Laws

- Organizations big and small recognize the value of collecting and analyzing data and, as a result, are collecting an ever-increasing amount of personal information about their customers.

- Cybercriminals are always on the lookout for ways to gain access to and exploit this valuable data for their own personal gain.

- Therefore, all organizations who collect sensitive data must be good data custodians.

Security Breach Notification Laws (Cont.)

- There are several laws in the U.S. that require organizations to notify individuals if a breach of their personal data occurs:
  - **Electronic Communications Privacy Act (ECPA) 1986**
    - The ECPA aims to ensure workplace privacy and protects a range of electronic communications such as email and telephone conversations from unauthorized interception, access, use, and disclosure.
  - **Computer Fraud and Abuse Act (CFAA)**
    - Enacted in 1986 as an amendment to the Comprehensive Crime Control Act of 1984, CFAA prohibits unauthorized access to computer systems.
    - Knowingly accessing a government computer without permission or accessing any computer used in or affecting interstate or foreign commerce is a criminal offense.
    - The Act also criminalizes the trafficking of passwords or similar access information, as well as knowingly transmitting a program, code, or a command that results in damage.

Protecting Privacy

There is no one central federal level privacy law in the U.S., but rather a range of laws and regulations that serve to protect the personal data of U.S. citizens:

Private Act of 1974	It establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.
Freedom of Information Act (FOIA)	It enables public access to U.S. government records. It carries a presumption of disclosure, which means that the burden is on the government to provide a good reason as to why any information cannot be released. There are nine disclosure exemptions pertaining to FOIA.
Family Education Records and Privacy Act (FERPA)	This federal law governs access to education records. It operates on an opt-in basis. This means that parents must approve the disclosure of a student’s educational information to public entities prior to the actual disclosure. When a student turns 18 years old, or enters a postsecondary institution at any age, their rights under FERPA transfer from the parents to the student.
U.S. Children´s Online Privacy Protection Action (COPPA)	This federal law was created to protect the privacy of children under 13 years of age by imposing certain requirements on website operators and online services under U.S. jurisdiction. For example, parental consent needs to be obtained before an organization can collect and use information from children under the age of 13.

Protecting Privacy (Cont.)

U.S. Children´s Internet Protection Act (CIPA)	The U.S. Congress passed CIPA in 2000 to protect children under the age of 17 from exposure to offensive Internet content and obscene material.
Video Privacy Protection Act (VPPA)	It was originally enacted to prevent the sharing of videotape, DVD, and video game rental information to another party. This was amended in 2013 to allow organizations such as Netflix to collect customer consent that allows them to store their rental histories and/or make them public for up to two years. This amendment means that these organizations can provide recommendations to or on behalf of their users.
Health Insurance Portability and Accountability Act (HIPAA)	It required the creation of national standards to impose safeguards for the physical storage, maintenance, transmission, and access to individuals' health information. Any organization that uses electronic signatures must meet these standards ensuring information integrity, signer authentication, and nonrepudiation (meaning the validity of the signature cannot be denied).
California Senate Bill 1386 (SB1386)	It requires that all affected individuals should be given notice and be advised of their rights and responsibilities in the event of their personal information being lost or disclosed.
Privacy policies	A direct outcome of the range of legal statutes relating to privacy and data collection has been the generation of privacy policies that help to ensure organizational compliance with the law.
Privacy impact assessment (PIA)	A process that helps ensure that PII is properly handled throughout an organization.

International Laws

- With the growth of the internet, cybercrime has emerged as a security concern, with both national and international consequences.
- National cyber laws exist in many countries, but these vary significantly, making it difficult to investigate and prosecute cybercrime that operates across country borders.
- International efforts to target cybercrime are growing.
- Ratified by 65 states, the Convention on Cybercrime is the first international treaty that seeks to address internet and digital crimes, dealing particularly with copyright infringement, computer-related fraud, child pornography and violations of network security.
- **Electronic Privacy Information Center (EPIC)** is a nonprofit research center in Washington, which aims to promote privacy and open government laws and policies.
- With strong ties to organizations around the world, EPIC has a global focus on digital privacy.

Lab - Create Your Personal Code of Ethical Conduct

- In this Lab, you will meet the following objectives:
  - Part 1: Research approaches to ethical decision making.
  - Part 2: Research code of ethics.
  - Part 3: Develop your own personal code of ethical conduct.

Lab - Recommend Security Measures to Meet Compliance Requirements

- In this Lab, you will meet the following objectives:
    - Part 1: Investigate compliance requirements.
    - Part 2: Recommend compliance solutions.

22.3 IT Security Management Framework

IT Security Management Framework

The Twelve Domains of Cybersecurity

- ISO/IEC 27000 is a series of information security standards or best practices to help organizations improve their information security.
- Published by the ISO and the ICO, the ISO 27000 standards set out comprehensive information security management system (ISMS) requirements.
- An ISMS consists of all administrative, technical, and operational controls that address information security within an organization.
- The ISO 27000 standard is represented by twelve independent domains.
- These twelve domains provide the basis for developing security standards and effective security management practices within organizations, as well as helping to facilitate communication between organizations.

The Twelve Domains of Cybersecurity (Cont.)

A summary of these twelve domains:

Risk assessment	This is the first step in the risk management process, which determines the quantitative and qualitative value of risk related to a specific situation or threat.
Security policy	This document addresses the constraints and behaviors of individuals within an organization and often specifies how data can be accessed, and what data is accessible by whom.
Organization of information security	This is the governance model set out by an organization for information security.
Asset management	This is an inventory of and classification scheme for information assets within an organization.
Human resources security	This refers to the security procedures in place that relate to employees joining, moving within, and leaving an organization.
Physical and environmental security	This refers to the physical protection of an organization’s facilities and information.
Communications and operations management	This refers to the management of technical security controls of an organization’s systems and networks.

The Twelve Domains of Cybersecurity (Cont.)

Information systems acquisition, development, and maintenance	This refers to security as an integral part of an organization's information systems.
Access controls	This describes how an organization restricts access rights to networks, systems, applications functions, and data to prevent unauthorized user access.
Information security incident management	This describes an organization's approach to the anticipation of and response to information security breaches.
Business continuity management	This describes the ability of an organization to protect, maintain, and recover business-critical activities following a disruption to information systems.
Compliance	This describes the process of ensuring conformance with information security policies, standards, and regulations.

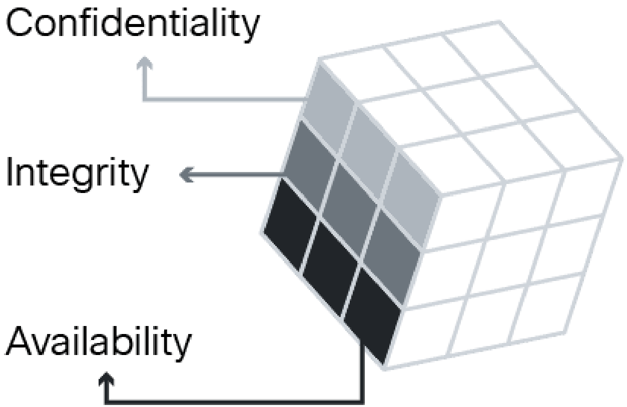
- The structure of this ISO cybersecurity model differs from the OSI model in that it is a peer model that uses domains rather than layers to describe the security categories.
- Each domain has a direct relationship with the other domains.

Control Objectives and Controls

- These twelve domains are made up of **control objectives** (ISO 27001) and **controls** (ISO 27002):
  - **Control objectives**
    - They define the high-level requirements for implementing a comprehensive information security management system within an organization, and usually provide a checklist to use during an ISMS audit.
    - Passing this audit indicates that an organization is ISO 27001 compliant and provides partners with confidence in the security of the organization's data and operations.
  - **Controls**
    - They set out how to accomplish an organization's control objectives.
    - They establish guidelines for implementing, maintaining, and improving the management of information security in an organization.
- An organization's **control objective** is to control access to networks by using the appropriate authentication mechanisms for users and equipment.
- A relevant **control** is to use strong passwords consisting of at least eight characters and a combination of upper and lowercase letters, numbers, and symbols.

ISO 27000 and the CIA Triad

- ISO 27000 is a universal framework that is applicable to every type of organization.
- An organization must identify which domains, control objectives, and controls apply to its environment and operations to use them effectively.
- Most organizations do this by producing a statement of applicability (SOA) which allows them to tailor the available control objectives and controls to best meet their priorities around **confidentiality**, **integrity,** and **availability**.

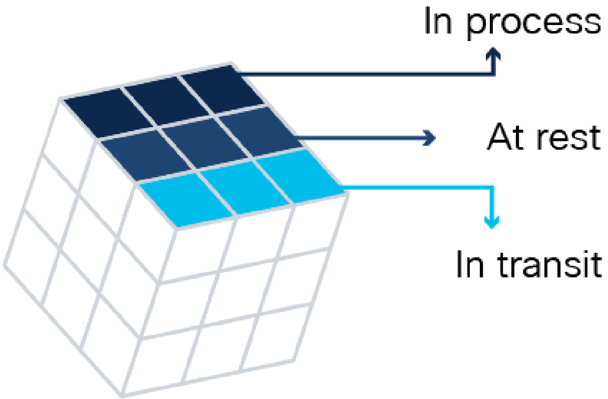


ISO 27000 and the States of Data

- The ISO controls specifically address security objectives for data in each of the three states: **in process**, **at rest** (in storage), and **in transit**.

- The responsibility for identifying and implementing the relevant controls may lie with different groups across an organization.

- For example, a network security team may be responsible for controls that ensure the confidentiality, integrity, and availability of all data being transmitted (data in transit), programmers and data entry analysts for data being processed (in process), and hardware support specialists for stored data (at rest/in storage).



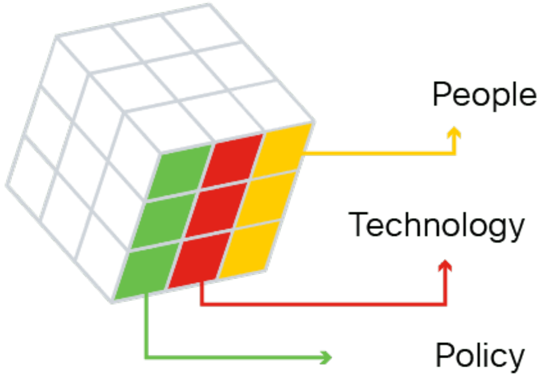
IT Security Management Framework

ISO 27000 and Safeguards

- The ISO controls also provide technical direction for control objectives that relate to the cybersecurity policies, procedures and guidelines set out by senior management within an organization.

- For example, let's imagine that a senior management team establishes a policy to protect all data coming into or going out of an organization.

- The responsibility for implementing and configuring the networks, systems, and equipment to be able to fulfill the policy directives will fall to the appropriate IT professionals within the organization, not the senior management team.



The National Cybersecurity Workforce Framework

The National Institute of Standards and Technologies (NIST) created the National Cybersecurity Workforce Framework to support organizations seeking cybersecurity professionals, organizing cybersecurity work into seven categories and outlining the main job roles, responsibilities, and skills needed for each one:

Operate and maintain	Provides the support, administration, and maintenance required to ensure effective and efficient IT system performance and security.
Protect and defend	Identifies, analyzes, and mitigates threats to internal systems and networks.
Investigate	Investigates cybersecurity events and/or cyber attacks involving IT resources.
Collect and operate	Provides specialized denial and deception operations and collection of cybersecurity information.
Analyze	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Oversee and govern	Provides leadership, management, direction or development, and advocacy so an organization may effectively conduct cybersecurity work.
Securely provision	Conceptualizes, designs, procures, or builds secure IT systems.

The CIS Critical Security Controls

- The CIS developed set of critical security controls to help organizations with different levels of resources and expertise at their disposal to improve their cyber defenses include:
    - **Basic controls -** Organizations with limited resources and cybersecurity expertise available should implement inventory and control of hardware and software assets, continuous vulnerability management, controlled use of administrative privileges, secure configurations for hardware and software, and maintenance, monitoring, and analysis of audit logs.
    - **Foundational controls -** Organizations with moderate resources and cybersecurity expertise available should implement the basic controls as well as email and web browser protections, malware defense, limitation and control of network ports, protocols and services, data recovery capabilities, secure configurations for network devices, boundary defense, data protections, controlled access based on the 'need to know' principle, wireless access control, and account monitoring and control.
    - **Organizational controls -** Organizations with significant resources and cybersecurity expertise available should implement the basic and foundational controls, as well as a security awareness and training program, application software security, Incident response and management, and penetration tests and red team exercises (simulated attack exercises to gauge an organization's security capabilities).

The Cloud Controls Matrix

- The Cloud Security Alliance (CSA) provides security guidance to any organization that uses cloud computing or wants to assess the overall security risk of a cloud provider.

- Their Cloud Controls Matrix (CCM) is a cybersecurity control framework that maps cloud-specific security controls to leading standards, best practices, and regulations.

- It is composed of 197 control objectives that are structured in 17 domains covering all aspects of cloud technology, including governance and risk management, human resources, and mobile security.

- The CCM is considered a de-facto standard for cloud security assurance and compliance.

Compliance

- Service providers may need to provide assurances to their client organizations that the security controls they implement are properly designed and operate effectively.
- The following show how a service provider can do this.

- **Statement on Standards for Attestation Engagements (SSAE) 18 Service Organization Control (SOC) 2 Audit**
  - This is an independent audit of an organization’s reporting controls as they relate to the security, availability, processing integrity, confidentiality, and privacy of a system.
  - An attestation report will confirm that controls are in place at a specific point in time (Type I) or managed over a period of at least six months (Type II).
  - These reports provide assurance to a client organization that there are controls in place and operating to protect sensitive data.

Compliance (Cont.)

- **Cybersecurity Maturity Model Certification (CMMC)**
  - This certification is aimed at any organizations providing a service to the U.S. Department of Defense (DoD) and verifies that these organizations have adequate cybersecurity practices and processes in place to ensure ‘basic’ cyber hygiene at a minimum.
  - It establishes five certification levels that range from ‘basic cyber hygiene practices’ to ‘enhanced practices that provide more sophisticated capabilities to detect and respond to APTs'.
  - It is likely that service providers will have to achieve the appropriate CMMC requirement to be considered for a DoD contract award.

22.4 Governance and Compliance Summary

Governance and Compliance Summary

What Did I Learn in this Module?

- IT security governance determines who is authorized to make decisions about cybersecurity risks within an organization.
- Good data governance programs have a data owner, controller, processor, custodian, steward, and protection officer.
- A cybersecurity policy is a high-level document that outlines an organization’s vision for cybersecurity, including its goals, needs, scope, and responsibilities.
- Specific security policies include ID and authentication, password, acceptable use, network maintenance, incident handling, data, credential, and organizational.
- The rights ethics approach is guided by the principle which states that an individual has the right to make their own choices, which cannot be violated by another person’s decision.
- There are ten commandments of computer ethics generally covering things you should not do with a computer.
- There are three categories of cybercrime: computer-targeted, computer-assisted, and computer-incidental.
- In the U.S, there are three primary sources of computer security laws and regulations: statutory law, administrative law, and common law.

What Did I Learn in this Module? (Cont.)

- Some industries also have specific laws about cybercrime: finance, corporate accounting, credit cards, and cryptography.
- The Convention on Cybercrime is the first international treaty that is addressing internet and digital crimes, dealing particularly with copyright infringement, computer-related fraud, child pornography, and violations of network security.
- There are twelve domains of cybersecurity.
- Control objectives define the high level requirements for implementing a comprehensive information security management system within an organization.
- Controls show how to accomplish an organization's control objectives and they establish guidelines for implementing, maintaining, and improving the management of information security in an organization.
- ISO 27000 is a universal framework that is applicable to every type of organization.
- An organization must identify which domains, control objectives, and controls apply to its environment and operations.
- Most organizations create an SOA to tailor the available control objectives and controls to best meet its priorities around confidentiality, integrity, and availability.
- The ISO controls specifically address security objectives for data in process, at rest (in storage) and in transit.

What Did I Learn in this Module? (Cont.)

- NIST created the National Cybersecurity Workforce Framework to support organizations seeking cybersecurity professionals.
- CIS developed a set of critical security controls (basic, foundational, and organizational) to help organizations with different levels of resources and expertise at their disposal to improve their cyber defenses.
- The CSA provides security guidance to any organization that uses cloud computing or wants to assess the overall security risk of a cloud provider.
- CCM maps cloud-specific security controls to leading standards, best practices, and regulations.
- The CSA CCM is considered a de-facto standard for cloud security assurance and compliance.
- An attestation report (SSAE or SOC) will confirm that controls are in place at a specific point in time (Type I) or managed over a period of at least six months (Type II).
- The CMMC establishes five certification levels that range from ‘basic cyber hygiene practices’ to ‘enhanced practices that provide more sophisticated capabilities to detect and respond to APTs'.