ISC 1
Unit Outline

Module 1—National Institute of Standards and Technology (NIST) Frameworks

NIST Cybersecurity Framework (CSF)

- NIST was established to remove barriers to industrial competitiveness and improve access to resources to promote U.S. research capabilities.

  In 1995, NIST branched out into the cybersecurity field with the NIST Special Publication (SP) 800-12, *An Introduction to Information Security*.

- The NIST CSF is a voluntary framework that includes three primary components to manage cybersecurity risk:
  - CSF core
  - CSF tiers
  - CSF organization profiles
- The framework core consists of six functions that should be performed concurrently: govern, identify, protect, detect, respond, and recover.
- The NIST CSF measures information security infrastructure sophistication in the form of four tiers:
  - Tier 1 (partial)
  - Tier 2 (risk-informed)
  - Tier 3 (repeatable)
  - Tier 4 (adaptive)
- CSF organizational profiles are mechanisms by which NIST recommends companies measure cybersecurity risk and establish a road map to minimize risks. NIST recommends a five-step approach to using the organizational profiles:
  - Scope the organizational profile
  - Gather information needed to prepare the organizational profile
  - Create the organizational profile
  - Analyze the gap between the current and target profiles and create an action plan
  - Implement the actional plan and update the organizational profile

NIST Privacy Framework

- The NIST Privacy Framework was published in early 2020, to protect individuals' data as used in data processing applications.

  The Privacy Framework was developed to be industry-agnostic and to account for cultural and individual constructs around privacy.

- The Privacy Framework Core is divided into the following eight framework functions:
  - Identify
  - Govern
  - Control
  - Communicate
  - Protect

- Detect
- Respond
- Recover

NIST Security and Privacy Controls

- NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, has evolved into a set of security and privacy controls applicable to all information systems and has become the standard for federal information security systems.
  - These standards are designed to help organizations identify the security and privacy controls needed to manage risk and satisfy Office of Management and Budget (OMB) Circular A-130 and the Federal Information Security Modernization Act (FISMA).
  - Three control implementation approaches that are to be implemented on a per-control basis include common (inheritable), system-specific, and hybrid.

Module 2—Privacy and Data Security Standards

Data Privacy

- Privacy laws exist to protect an individual's private life and keep personal details out of the public domain.
  - These laws also create trust between consumers and enterprises so that when a consumer's personal information is shared, such as with a credit card company or a health care provider, sensitive information will be safeguarded according to rules outlined in applicable privacy regulations.
  - Privacy laws regulate how those entrusted with private information must collect, process, maintain, and disclose it.
- With society's use of the internet and the cloud, data exchange is more prevalent than ever. The rise in available data has led to a surge in data breaches. A data breach is the exposure of confidential information to unauthorized persons and comes in two categories: unintentional and intentional.
  - Examples of cost categories that may be incurred from data breaches include detection and escalation costs, notification costs, post-breach response costs, and loss of business and revenue.

Modern Privacy Regulations

- The Health Insurance Portability and Accountability Act (HIPAA) of 1996 required the Department of Health and Human Services to adopt national standards promoting health care privacy and security.
  - In response, the department adopted the Privacy Rule and the Security Rule.
  - HIPAA and the rules that resulted regulate how the health care industry maintains and discloses health information.
- General Data Protection Regulation (GDPR): Effective May 2018, GDPR became the European Union's general applicability law regulating the privacy of data.
  - GDPR provides circumstances when it is lawful to process personal data, such as with proper consent or when complying with a legal obligation.
  - This law is one of the strictest privacy laws in the world, as it imposes steep penalties for violators, with fines reaching millions of dollars.

Data Security Standards

- Payment Card Industry Data Security Standard (PCI DSS)—With the rise of cashless transactions, financial institutions in the payment card industry created the PCI (Payment Card Industry) Security Standards Council to enhance payment security. The council created the PCI Data Security Standard (DSS), an applicable framework for entities to promote data security when processing payments. Data subject to PCI DSS includes both cardholder data and sensitive authentication data, collectively referred to as account data. The six goals include:
  - Build and maintain a secure network and systems
  - Protect account data
  - Maintain a vulnerability management program
  - Implement strong access control measures
  - Regularly monitor and test networks
  - Maintain an information security policy

Module 3—Center for Internet Security Critical Security Controls: Part 1

- The Center for Internet Security (CIS) Controls are a recommended set of actions, processes, and best practices that can be adopted and implemented by organizations to strengthen their cybersecurity defenses.
- CIS Controls are currently supported by the SANS Institute, which provides training, administers certification, and performs research.

  Each iteration of control updates involves experts across industries, entity-type (government vs. public companies), and job roles (from operators to policymakers).
- The CIS Controls were designed with the following principles in mind:
  - Context: An enhancement to the scope and practical applicability of safeguards through the incorporation of examples and explanations.
  - Coexistence: Alignment with evolving industry standards and frameworks, including NIST's CSF 2.0 framework.
  - Consistency: Disruption to control users is minimized, not impacting implementation groups.
- The implementation of CIS Controls can be tailored to an organization's size by using one of three Implementation Groups (IGs)
  - IG1—This group is for small or medium-sized organizations that have limited cybersecurity defense mechanisms in place.
  - IG2 (Includes IG1)—This group is for companies that have IT staff who support multiple departments that have various risk profiles and typically handle sensitive client data.
  - IG3 (Includes IG1 and IG2)—This group is for companies that have security experts in all domains within cybersecurity such as penetration testing, risk management, and application security.

- Each CIS Control has recommendations prescribed to achieve the control objective. These recommendations are referred to as the Safeguards. These controls include:
  - Inventory and Control of Enterprise Assets (Control 01)—This control helps organizations actively track and manage all IT assets connected to a company's IT infrastructure physically or virtually within a cloud environment.
  - Inventory and Control of Software Assets (Control 02)—This control provides recommendations for organizations to track and actively manage all software applications so that only authorized software is installed on company devices.
  - Data Protection (Control 03)—This control helps organizations develop ways to securely manage the entire life cycle of their data, from the initial identification and classification data to its disposal.
  - Configuration of Enterprise Assets and Software (Control 04)—This control helps organizations establish and maintain secure baseline configurations for their enterprise assets.
  - Account Management (Control 05)—This control outlines best practices for companies to manage credentials and authorization for user accounts, privileged user accounts, and service accounts for company hardware and software applications.
  - Access Control Management (Control 06)—This control expands on Account Management (Control 05) by specifying the type of access that user accounts should have.
  - Continuous Vulnerability Management (Control 07)—This control assists organizations in continuously identifying and tracking vulnerabilities within its infrastructure so that it can remediate and eliminate weak points or windows of opportunity for bad actors.
  - Audit Log Management (Control 08)—This control establishes an enterprise log management process so that organizations can be alerted and recover from an attack in real time, or near real time, using log collection and analytic features.
  - Email and Web Browser Protections (Control 09)—This control provides recommendations on how to detect and protect against cybercrime attempted through email or the internet by directly engaging employees.

Module 4—Center for Internet Security Critical Security Controls: Part 2

- Each CIS Control has recommendations known as Safeguards which are prescribed to achieve the control objective. The CIS controls include:
  - Malware Defenses (Control 10)—This control assists companies in preventing the installation and propagation of malware onto company assets and its network.
  - Data Recovery (Control 11)—This control establishes data backup, testing, and restoration processes that allow organizations to effectively recover company assets to a pre-incident state.
  - Network Infrastructure Management (Control 12)—This control establishes procedures and tools for managing and securing a company's network infrastructure.
  - Network Monitoring and Defense (Control 13)—This control establishes processes for monitoring and defending a company's network infrastructure against internal and external security threats.
  - Security Awareness and Skill Training (Control 14)—This control guides organizations in establishing a security awareness and training program to reduce cybersecurity risk.
  - Service Provider Management (Control 15)—This control helps organizations develop processes to evaluate third-party service providers that have access to sensitive data or that are responsible for managing some or all of a company's IT functions.
  - Application Software Security (Control 16)—This control establishes safeguards that manage the entire life cycle of software that is acquired, hosted, or developed in-house to detect, deter, and resolve cybersecurity weaknesses before they are exploited.

- Incident Response Management (Control 17)—This control provides the recommendations necessary to establish an incident response management program to detect, respond, and prepare for potential cybersecurity attacks.
- Penetration Testing (Control 18)—This control helps organizations test the sophistication of their cybersecurity defense system in place by simulating actual attacks in an effort to find and exploit weaknesses.

Module 5—COBIT 2019 Framework

- In 1996, the Information Systems Audit and Control Association (ISACA) developed what would become one of the most widely used enterprise IT governance standards: the Control Objectives for Information and Related Technologies (COBIT).
  - To accomplish its mission, ISACA created the COBIT framework, which provides a road map that organizations can use to implement best practices for IT governance and management.
  - COBIT was originally developed as a set of standards for auditors that unified multiple different and disparate standards.
- As part of its foundation, COBIT® 2019 was developed using the following:
  - COBIT 5
  - Six principles for a governance system:
    - Provide stakeholder value
    - Holistic approach
    - Dynamic governance system
    - Governance distinct from management
    - Tailored to enterprise needs
    - End-to-end governance system
  - Three principles for a governance framework:
    - Based on a conceptual model
    - Open and flexible
    - Aligned to major standards
  - Other standards and regulations
  - Community contribution
- The COBIT 2019 core model includes governance objectives and management objectives.
  - Governance objectives are grouped into one domain: evaluate, direct, and monitor (EDM).
  - Management objectives have four domains: align, plan, and organize (APO); build, acquire, and implement (BAI); deliver, service, and support (DSS); and monitor, evaluate, and assess (MEA).

- The COBIT 2019 core model uses seven components to satisfy management and governance objectives:
  - Process
  - Organizational structures
  - Principles, policies, and frameworks
  - Information
  - Culture, ethics, and behavior
  - People, skills, and competencies
  - Services, infrastructure, and applications
- COBIT Core Publications—The COBIT 2019 framework was designed so that companies could adopt its recommendations in a way that is customized to their own organizational needs. The following publications are the road map to help achieve that customization:
  - COBIT 2019 Framework: Introduction and Methodology
  - COBIT 2019 Framework: Governance and Management Objectives
  - COBIT 2019 Design Guide: Designing an Information and Technology Governance
  - COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution

ISC 2
Unit Outline

Module 1—IT Infrastructure

IT Infrastructure

- The supporting IT architecture within most modern companies has multiple interconnected technological components, with the core infrastructure involving a combination of on-premises and outsourced hardware, software, and specialized personnel.
- Computer Hardware—Organizations designing their IT infrastructure must decide what hardware will be utilized to conduct business.
  - Computers and End-User Devices—End-user devices (EUDs) are electronic machines, typically computers or minicomputers, that directly interact with employees or consumers at the "edge" of a network.
  - Internal Computer Hardware—Key hardware components within a computer include microprocessors, graphics and sound cards, hard drives (permanent storage), random access memory or RAM (temporary storage), the power supply, and the motherboard, which connects most of these critical pieces.
  - External Computer Hardware—Some hardware devices may be external peripheral devices and do not need to be integrated into the machine itself.
  - Infrastructure Housing—Although not hardware, the facilities and the safeguards at those facilities that contain hardware, such as data centers or offices, are part of the broader IT infrastructure.
- Network infrastructure refers to the hardware, software, layout, and topology of network resources that enable connectivity and communication between devices on a computer network.
- Traditional hardware found in most networks is as follows:
  - Modems—Modems receive analog signals from the internet service provider and translate those signals into digital signals.
  - Routers—Routers manage network traffic by connecting devices to/from a network. They read the source and destination fields in information packet headers to determine the most efficient path through the network for the packet to travel.
  - Switches—Switches are similar to routers in that they connect and divide devices within a computer network.
  - Gateways—A gateway transforms data from one protocol into another so that information can flow between networks.
  - Edge-enabled Devices—Edge-enabled devices allow computing, storage, and networking functions closer to the devices where the data or system request originates, rather than a distant central location.
  - Servers—Servers are physical or virtual machines that coordinate the computers, programs, and data that are part of the network.
  - Firewalls—Firewalls are software applications or hardware devices that protect a person's or a company's network traffic by filtering it through security protocols with predefined rules.
- Network topology refers to the physical layout of equipment, or "nodes," in a network. The four most common types of network topologies include bus topology, mesh topology, ring topology, and star topology.

- Devices in a network communicate with other devices using protocols. The Open Systems Interconnection (OSI) model segregates network functions into seven different layers: application (level 7), presentation (level 6), session (level 5), transport (level 4), network (level 3), data link (level 2), and physical (level 1).
- Network Infrastructure Architecture—A company's network infrastructure architecture refers to the way an organization structures its network from a holistic design standpoint, considering factors such as geographical layout, physical and logical layout, and network protocols used. Common types of network architecture designs include:
  - Local-Area Networks (LAN)—Provide network access to a limited geographic area such as a home or single-location office.
  - Wide-Area Networks (WAN)—Provide access to a larger geographic area such as cities, regions, or countries.
  - Software-defined WAN (SD-WAN)—Monitors the performance of WAN connections and manages traffic to optimize connectivity. In an SD-WAN setup, control and management are separated from the hardware and included in software.
  - VPNs—These are virtual connections through a secure channel or tunnel that provide remote and secure access to an existing network.
  - Demilitarized Zone (DMZ): A subnetwork that separates a LAN from other untrusted networks such as the internet. It is set up by creating a physical or logical subnetwork outside of the LAN's firewall.
- Software consists of the applications, procedures, or programs that provide instructions for a computer to execute. Software is controlled by a user interacting with the program, which in turn gives instructions to the physical computer's operating system.

Cloud Computing

- Cloud computing is a computing model that uses shared resources over the internet. Cloud customers rent storage space, processing power, proprietary software, or a combination of the three on remote servers from another company.
- There are three primary cloud computing models, in addition to a fully on-site or on-premises solution:
  - IaaS (Infrastructure-as-a-Service)—The CSP provides an entire virtual data center of resources in an IaaS model, and organizations can outsource servers, storage, hardware, networking services, and networking components to third-party providers, which are generally billed on a per-use basis.
  - PaaS (Platform-as-a-Service)—The CSP provides proprietary tools or solutions remotely that are used to fulfill a specific business purpose. In a PaaS model, the tools facilitate the creation of programs and delivery of services, such as building an online platform to sell merchandise, advertise products, or build other websites, all of which run on a CSP's hosted infrastructure.
  - SaaS (Software-as-a-Service)—The CSP provides a business application or software that organizations use to perform specific functions or processes. In a SaaS model, customers generally purchase the service through licensing. The CSP offers access to the application via the internet and is responsible for recurring upgrades, security enhancements, and other support functions.
- There are four common types of cloud computing deployment models: public, private, hybrid, and community.

Module 2—Enterprise and Accounting Information Systems

Enterprise Resource Planning (ERP) Systems

- Enterprise resource planning (ERP) systems are cross-functional systems that support different business functions and facilitate integration of information across departments, such as accounting, customer management, finance, human resources, inventory management, manufacturing, marketing, and vendor management.
- The system that accountants and financial managers interact with the most is the AIS.
  - An AIS collects, records, and stores accounting information, then compiles that information using accounting rules to report both financial and nonfinancial information to decision makers in an enterprise.
  - An AIS is typically made up of three main subsystems (or modules): Transaction Processing System (TPS), Financial Reporting System (FRS), and Management Reporting System (MRS).
  - An AIS processes transactions in the following order:
    - Transaction data from source documents is entered into the AIS by an end user.
    - Original source documents, if they exist, are filed.
    - Transactions are recorded in the appropriate journal.
    - Transactions are posted to the general and subsidiary ledgers.
    - Trial balances are prepared.
    - Adjustments, accruals, and corrections are entered.
    - Financial reports are generated.
- The transaction cycles are the core functions within an accounting department, such as the revenue cycle, purchasing and disbursement cycle, and other processes that involve the recognition and/or facilitation of transactions.

IT Systems and Process Improvement

- An organization can improve the performance of its information systems by improving business processes that provide inputs to those systems.
  - Improving consistency and reliability in processes results in better data. Better processes lead to fewer errors, more efficient accounting, and enhanced reporting.
  - Four broad areas of process improvements that can enhance accounting information system performance are automation, shared services, outsourcing, and offshore operations.
- There are three specific forms of technology that are gaining mass adoption in process improvement: robotic process automation (RPA), natural language processing software, and neural networks.

Detecting Design Deficiencies in Processing Integrity

- Processing integrity refers to a system's ability to initiate and complete transactions so that they are valid, accurate, completed timely, and authorized to meet a company's objective.
  - Integrity also refers to confidentiality and privacy of the details related to transactions involving data that identifies customers, patient health records, employees, or financial accounts.
  - Additionally, processing integrity is one of the five trust services criteria.

- Deficiencies in the operation of a control in a SOC 2® engagement are defined by the AICPA as a properly designed control that either:
  - does not operate as designed; or
  - is performed by a person who lacks authority or competence to perform the control effectively.

COSO Internal Control Framework and Blockchain

- The Committee of Sponsoring Organizations (COSO) has developed guidance and frameworks covering the areas of internal control, risk management, and fraud deterrence.
  - Within its five-point Internal Control—Integrated Framework (the framework) there are two categories with principles that pertain specifically to internal control over information technology.
- Within the Information and Communication category, Principle 13 states that organizations should acquire, create, and use quality information in order to support internal controls. This includes:
  - identifying the company's information needs;
  - capturing both external and internal sources of data;
  - processing relevant data into useful information; and
  - maintaining quality when processing that data.

Module 3—Availability, Resiliency, and Disaster Recovery

System Availability

- Availability, or being able to perform business functions or meet business objectives, is critical to a business's success. The concept of availability has various components.
  - Availability—Being able to perform business functions or meet business objectives is critical to a business's success.
  - Business Resiliency—Business resiliency is the integration of system availability controls, disaster recovery plans, business continuity plans, and crisis management plans into a central set of procedures to consider whether a business can continue to operate or quickly return to operations without irreparable harm to its people, information, or assets.
  - Disaster Recovery—Disaster recovery consists of an entity's plans for restoring and continuing its information technology function in the event of the destruction of not only program and data files but also computer processing capability.
    - In the event of a disaster, an organization has three main options for how to maintain IT operations through the use of alternative processing facilities: cold site (least expensive), warm site (moderately expensive), and hot site (most expensive).
  - Business Continuity Plans—Business continuity plans are more comprehensive than disaster recovery plans and contain contingency and mitigation procedures around all business processes, including relocating facilities, human resource tasks, and managing relationships with customers and suppliers.
  - Business Impact Analysis—Performing a BIA helps identify and assess risks by identifying business units, departments, and processes that are essential to the survival of an entity and the organizational impact in the event of failure/disruption.
  - Crisis Management Plans—These policies address the potential crises an organization could face and how to properly respond, the procedures for implementation, the crisis response command center, roles and responsibilities, the internal and external communications, and the proper training of employees.

System Availability Risks

- Failure of IT Infrastructure—Availability of systems may directly be affected by failures in hardware, software, and network applications. These failures can result from:
- Insufficient Capacity and Resources—System availability may be slowed down or disrupted if an organization's IT infrastructure is unable to meet the processing or storage needs of current operational demands.
- Lack of Business Resiliency—If a business resiliency program is insufficient or nonexistent, organizations may lose critical, confidential, or private data, recover slowly from a disruption, or potentially never recover.
- Metrics for system availability include maximum tolerable downtime (MTD), recovery point objective (RPO), recovery time objective (RTO), mean time to repair (MTTR), recovery time actual (RTA), and recovery point actual (RPA).

System Availability Controls

- System availability controls include activities to prevent system disruptions and loss of information. Controls include physical controls, IT infrastructure controls, uninterrupted power supply (UPS), redundancy, and system backup.
- When planning a business resiliency program or evaluating system availability risks, organizations must decide what types of backups to perform in order to recover lost data.
  - Full—An exact copy of the entire database. Full backups are time-consuming, so most organizations only do full backups weekly and supplement them with daily partial backups.
  - Incremental—Involves copying only the data items that have changed since the last backup. This produces a set of incremental backup files, each containing the results of one day's transactions. Restoration involves first loading the last full backup and then installing each subsequent incremental backup in the proper sequence.
  - Differential—Copies all changes made since the last full backup. Thus, each new differential backup file contains the cumulative effects of all activity since the last full backup. Consequently, except for the first day following a full backup, daily differential backups take longer than incremental backups.

Module 4—Change Management

Change Management Overview

- Change Management—Change management is a term used to describe the policies, procedures, and resources employed to govern change in an organization.
- Change Management Process—The following steps can help a company chart its path from change inception to implementation:
  1. Identify and define the need for system changes.
  2. Design a high-level plan including goals to be achieved because of the system change.
  3. Obtain approval from management for the change.
  4. Develop an appropriate budget and timeline.
  5. Assign personnel responsible for managing the system change.
  6. Identify and address potential risks that could occur during the change or post-implementation.
  7. Provide an implementation road map.
  8. Procure necessary resources and train the appropriate personnel.
  9. Test the system change.

10. Execute the implementation plan.
11. Review and monitor change implementation and test as needed to verify effective implementation.

- The different forms of computing environments include development, testing, staging, production, and disaster recovery.

Change Management Risks

- Selection and Acquisition Risks—Selecting and acquiring new IT resources is a fundamental area in which risks exist in the change management process. Examples include:
  - Lack of expertise
  - Lack of a formal selection and acquisition process
  - Software/hardware vulnerability and incompatibility
- Integration Risks—Once the software has been selected and acquired, it must be integrated into existing systems and processes. Examples include:
  - User resistance
  - Lack of management support
  - Lack of stakeholder support
  - Resource concerns
  - Business disruption
  - Lack of system integration
- Outsourcing Risks—When planning a significant IT change or system upgrade, some organizations choose to outsource the change management process. Examples include:
  - Lack of organizational knowledge
  - Uncertainty of the third party's knowledge and management
  - Lack of security

Change Management Controls

- Once all risks in the change management process have been identified, controls are designed to minimize the possibility that the inherent risks will cause business disruptions or negatively impact IT systems. Change management controls include:
  - Policies and procedures
  - Emergency change policies
  - Standardized change requests
  - Impact assessment
  - Authorization
  - Separation of duties
  - Conversion controls
  - Reversion access
  - Pre-implementation and post-implementation testing
  - Ongoing monitoring

- There are different procedures for testing controls to enhance the likelihood that they are operating as intended. Acceptance criteria metrics may be qualitative or quantitative and include examples such as performance, functionality, scalability, and compliance.
- Analyzing logs is also a part of testing and implementing change control policies. Frequently used log types include application logs, change logs, event logs, firewall logs, network logs, and proxy logs.

Managing Change in Systems

- Two of the most common IT change management methodologies are the waterfall model and the agile model. Their principles are flexible enough to be applied more generally to modern change management practices across different organizational functions.
- Waterfall Model—The waterfall model is characterized by different teams of employees performing separate tasks in sequence, with each team beginning work from the pre-written authoritative agreement of the preceding team and then ending work when the business requirements for the team have been met.
- Agile Method—Agile offers a more flexible approach to change management and is characterized by cross-functional teams, each dedicated to particular functions or improvements of a system drawn from a prioritized list of the customer's remaining needs for the system.

Patch Management

- Patch management is the systematic process of identifying specific vulnerabilities or software bugs in operating systems or applications and addressing them with patches, or fixes, between releases.
- Patch management promotes system security and enhances the likelihood that systems are running smoothly. An effective patch management process includes evaluating new patch releases, using a vulnerability tool, testing patches in a test environment, approving and deploying patches, and verifying patches deployed.

System Conversion Methods

- Organizations have various options when converting their computer systems, such as software, hardware, and data, from one information system to another. The different conversion methods include direct, parallel, pilot, phased, and hybrid.
- The choice will vary for each company depending on its own unique need, with smaller companies more likely to select a more aggressive approach such as the direct changeover method, while larger companies may take a more cautious path, choosing a parallel or phased approach.

System Conversion Methods

- Every system within an organization should be subject to ongoing change management testing to determine whether newly installed systems and updates to existing systems do not lead to functional issues or security vulnerabilities.

Module 5—Introduction to Data Collection and the Data Life Cycle

Data Life Cycle

The data life cycle describes the sequential steps all business data must go through from creation, through its use, storage, and final disposal. This process can be summarized in eight steps:

1. Define
2. Capture
3. Preparation
4. Synthesis
5. Analytics and usage

6. Publication
7. Archiving
8. Purging

Types of Data Collection

Creating or capturing data is the first step in the data life cycle, and data can be collected through a variety of methods. Three such methods are:

- Extract, transform, and load (ETL)
- Active data collection
- Passive data collection

Types of Input Checks

- Field check
- Reasonableness check
- Completeness check
- Validity check
- Limit check
- Size check

Module 6—Data Storage and Database Design

Storage Processing and Repositories

- Data storage is a type of technology specifically designed for the retention of information and help with accessibility to authorized users to perform business activities effectively and efficiently. Common types of data storage include the following:
  - Operational Data Store (ODS)—An ODS is a repository of transactional data from multiple sources and is often an interim area between data sources and data warehouses.
  - Data Warehouse—Data warehouses are very large data repositories that are centralized and used for reporting and analysis rather than for transaction purposes.
  - Data Mart—A data mart is much like a data warehouse but is more focused on a specific purpose such as marketing or logistics and is often a subset of a data warehouse.
  - Data Lake—A data lake is a repository similar to a data warehouse, but it contains both structured and unstructured data, with data mostly being in its natural or raw format.

Relational Database Design

- Within an organization, data can be stored in a variety of ways; however, one of the most efficient and effective methods is to store data in a relational database.
- The benefits associated with relational databases include:
  - Completeness—Assists with the goal that all data required for a business process are included in the dataset.
  - No Redundancy—Storing redundant data is to be avoided for several reasons:
  - Business Rules Enforcement—Relational databases can be designed and used to aid in the placement and enforcement of internal controls and business rules.

  - Communication and Integration of Business Processes—Relational databases should be designed to support business processes across the organization, which results in improved communication across functional areas and more integrated business processes.

- Relational databases store data across a series of related tables. Each table contains columns (attributes) and rows (records) that are made of data. Each column in a table must be both unique and relevant to the purpose of the table. There are three types of columns:
  - primary keys;
  - foreign keys; and
  - descriptive attributes.
- Each column must be designated a specific data type. Data elements include tables, attributes, records, fields, data types, and database keys.

Data Dictionary

- Once processes come together to be supported in one database, the amount of data can be massive. Understanding the processes and the basics of how data are stored is critical, but even with a sound foundation, it would be nearly impossible for an individual to remember where each piece of data is stored, or what each piece of data represents.
  - Data dictionaries are a type of metadata—data about data.
  - Data dictionaries provide and summarize information about the data in a database to make it easier to work with the data and understand how it can be used to inform decisions and build meaningful reports.
- When working with data stored in a relational database, more attributes are available to keep track of in the data dictionary, such as whether the attribute is a database key (primary or foreign), whether the field is required, the data type, if there is a default value (and if so, what the default value is), the field size, and any notes necessary to further understand each field.
- Normalization is a database design technique that reduces data redundancy and eliminates undesirable characteristics like insertion, update, and deletion anomalies.
- Normalization rules divide larger tables into smaller tables and link them using relationships. The purpose is to eliminate redundant (repetitive) data and reasonably assure data is stored logically. Normalization occurs in three steps:
  - First normal form (1NF)
  - Second normal form (2NF)
  - Third normal form (3NF)
- The forms are progressive, meaning that to qualify for 3NF, a table must first satisfy the rules for 2NF, and the 2NF must adhere to those for 1NF.

Database Models and Schemas

- Relational databases must be designed with normalization in mind, and databases are supported by data models and database schemas. Data models are conceptual representations of the data structures in an information system and are not restricted to relational databases only.
- A database schema is a set of instructions to tell the database engine how to organize data to be compliant with the data models. It defines the actual structure of the database, including the tables, columns, and relationships between the data entities. Data models can be conceptual, logical, or physical.
- A database schema specifies how the data will be stored in the database, and ultimately how it will be accessed in the database. Two of the most common database schemas are star schemas and snowflake schemas.

Module 7—Data Storage and Database Design

Data Extraction with SQL Queries

- Structured query language (SQL) is a computer language to interact with data (tables, records, and attributes) in a relational database. Through SQL statements, records and entire tables can be created, updated, deleted, and viewed (and ultimately extracted).
- SQL queries are written to indicate which subset of data is intended for extraction—including the intention to filter results based on any criteria (such as filtering by a particular date, customer, or location) or aggregate existing data (such as sum total sales or sum quantity sold). SQL queries are made up of SQL commands and database elements, which make up SQL clauses.
  - SQL Commands—SQL commands are language-specific words, such as SELECT, FROM, JOIN, GROUP BY, HAVING, WHERE, ORDER BY. Case does not matter for SQL commands; however, upper case is commonly used for SQL commands to differentiate them from database elements. Information on common SQL commands is as follows:
    - SELECT—This is required as the first clause in most SQL queries and indicates which attributes are requested to view.
    - FROM—This is required as the second clause in most SQL queries and indicates which table the attribute(s) requested to SELECT are located in.
    - WHERE—This clause is used to filter results.
    - GROUP BY—When needing to aggregate data into subtotals based on categories, this clause is necessary to create subtotals.
    - HAVING—This clause is used to filter data, but instead of filtering attributes, it is used to filter aggregated data.
    - JOIN, ON—When needing to retrieve data from more than one table, these clauses are required to indicate the second table and how the tables are related.
  - Database Elements—Database elements are references to table names, attribute names, or criteria. Database elements must be spelled exactly the same as the table names or record names in the database, however, case does not matter. It is common to use proper case for database elements to improve readability and to differentiate the database elements from the SQL commands.

Data Integration

- Data stored in relational databases are stored across many different tables, but often reports and decisions need to be made based on data stored across several different tables, and sometimes reports and decisions require data not just across different tables in the same database but even from different data sources altogether.

Visualizing the Flow of Processes and Data

- Organizations are made up of many complex processes, and those complex processes are supported by an abundance of data.

  Visualizing the steps of processes across roles in an organization and the flow of data that supports processes can explain how a business works and help users understand when data is created and how it is used.

- Flowcharts are common tools for depicting process or data flows that help analysts understand processes and analyze those processes for improvement—whether that improvement is based on effectiveness, efficiency, or improved internal controls.
  - There is a variety of templates for flowcharts, including the Business Process Modeling Notation (BPMN), which is used to create flowcharts referred to as activity models and data flow diagrams (DFD), which are used to describe the flow of the data through a process.
  - Within a BPMN model, common flow activity symbols include pools and swim lanes. Common event symbols include start events, end events, and intermediate events. Common task symbols are shown as a rectangle with rounded edges. Common connecting objects include sequence flows and message flows. Also, a gateway is a point at which the path of the process diverges, such as a decision point.

ISC 3
Unit Outline

Module 1—Threats and Attacks

Cybersecurity Risk Management Overview

- Breaches of data, theft, service interruptions, and regulatory non-compliance are the highest of security concerns for senior executives and others who are charged with IT governance.
  - Data Breaches—Occur when information is compromised and utilized without the authorization of the owner.
  - Service Disruptions—An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time.
  - Compliance Risk—Regulators can require organizations to comply with cybersecurity regulations. Failure to comply with these regulations can result in fines and financial penalties.

Cyberattacks

- A cyberattack is any kind of malicious activity that targets computer information systems, infrastructures, computer networks, or personal computer devices and attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
- A threat agent is an internal or external attacker that could negatively impact data security through theft, manipulation, or control of sensitive information or systems.
- Examples of the different types of threat agents include:
  - Attacker, Threat Actor, or Hacker—These are individuals or groups of individuals known as hacking rings or Advanced Persistent Threats (APTs) that target people or organizations to gain access to systems, networks, and data.
  - Adversary—These are actors with interests in conflict with the organization.
  - Government-Sponsored/State-Sponsored Actors—These threat actors are funded, directed, or sponsored by nations.
  - Hacktivists—These are usually groups of hackers that operate to promote certain social causes or political agendas.
  - Insiders—Insiders are employees who either organically develop into someone with malicious intentions or intentionally infiltrate an organization to achieve nefarious objectives.
  - External Threats—Threats that occur from outside of the organization, entity, or individual that is the source of the cyberattack.
- Examples of the different types of cyberattacks include:
  - Network-based Attacks—These attacks target the infrastructure of a network, including switches, routers, servers, and cabling, with the intent to gain unauthorized access or disrupt operations for users.
    - Examples of these types of attacks include backdoors and trapdoors, covert channels, buffer overflows, denial-of-service (DoS), distributed denial-of-service (DDoS), man-in-the-middle (MITM), port scanning, ransomware, reverse shell, replay (eavesdropping), return-oriented, and spoofing.

- Application-based Attacks—These forms of attacks target specific software or applications (desktop or web), such as databases or websites, to gain unauthorized access or disrupt functionality.
  - Examples of application-based attacks include structured query language (SQL) injection, cross-site scripting (XSS), race condition, and malicious mobile code.
- Host-based Attacks—These attacks target a single host, such as a laptop, mobile device, or server, to disrupt functionality or obtain unauthorized access.
  - Examples of host-based attacks include brute force attacks, keystroke logging, malware, and rogue mobile apps.
- Social Engineering Attacks—These attacks involve the use of psychological manipulation or deception to get employees to divulge sensitive information, provide unauthorized access, or assist an attacker in committing fraud.
  - Examples of social engineering attacks include phishing, spear phishing, business email compromise (BEC), pretexting, catfishing, pharming, and vishing.
- Physical (On-premises) Attacks—This is a security breach carried out on an organization's premises or performed in some way that physically involves a bad actor gaining control of sensitive data, hardware, and/or software.
  - Examples of physical attacks include intercepting discarded equipment, piggybacking, infrastructure targeted by attackers, tampering, and theft.
- Supply Chain Attacks—These attacks use cyber tactics to target the production and distribution of goods within a supply chain so that there are larger disruptions in the normal operations of a company, government, or other entity.
  - Examples of supply chain attacks include embedded software code, foreign-sourced attacks, pre-installed malware on hardware, vendor attacks, and watering hole attacks.

- Stages in a Cyberattack—While there are a variety of cyberattacks, they all share some of the following steps or phases:
  - Reconnaissance—In this first stage, attackers discover and collect as much information about the target IT system as possible.
  - Gaining Access—This is the step in a cyberattack when the information collected in the previous steps is used to gain access to the target of an attack using a variety of techniques.
  - Escalation of Privileges—Once unauthorized access into a system is obtained, attackers attempt to gain higher levels of access in this stage.
  - Maintaining Access—In this stage, the attacker remains in the system for a sustained period of time until the attack is completed and looks for alternative ways to prolong access or return later.
  - Network Exploitation and Exfiltration—In this stage, attackers proceed with the objective of disrupting system operations by stealing sensitive data, modifying data, disabling access to systems or data, or performing other malicious activities.
  - Covering Tracks—This step occurs while the attack is in progress or after the attack is completed and involves the attacker concealing the entry or exit points in which access was breached.

Risks Related to Cloud Computing

- Cloud computing is a way for organizations to store, use, process, and share data, software, and applications without the need to own or manage the resources required to perform those functions on company premises.
- Risks specific to cloud computing for which a firm should be aware include additional industry exposure, cloud malware injection attacks, compliance violations, loss of control, loss of data, loss of visibility, multi-cloud and hybrid management issues, and theft or loss of intellectual property.

Risks Related to Mobile Devices

- Mobile devices such as smartphones, tablets, and wearables that can access the internet all have risks for both users and their employers. They face similar security threats as an organization.
- Threats specific to mobile devices include application malware, lack of updates, lack of encryption, physical threats, unsecured Wi-Fi networks, and location tracking.

Risks Related to the Internet of Things (IoT)

- The Internet of Things (IoT) is a class of smart devices connected to the internet that provide automation and remote control for other devices in a home or office setting, such as cameras, tablets, wearable devices, phones, and alarm systems.
- Relevant cyber threats specific to IoT technology include device mismanagement, device spoofing, escalated cyberattacks, expanded footprint, information theft, network attacks, and outdated firmware.

Threat Modeling and Overall Threat Landscape

- Threat modeling is the process of identifying, analyzing, and mitigating threats to a network, system, or application. The goal is to understand all risks a system could face and develop controls and countermeasures to minimize the impact of a risk or to try and prevent it from happening.
- The first step of threat modeling is to use the Confidentiality Integrity and Availability (CIA or CIA Triad) method to define what needs to be protected in the organization.
- Threat modeling typically involves the following phases:
  - Identify assets
  - Identify threats
  - Perform reduction analysis
  - Analyze the impact of an attack
  - Develop countermeasures and controls
  - Review and evaluate
- Threat Methodologies—There are three commonly used methodologies for threat models:
  - Process for Attack Simulation and Threat Analysis (PASTA)
  - Visual, Agile, and Simple Threat
  - Spoofing, Tampering, Repudiation, Information disclosure, Denial-of-service attack, and Elevation of privilege (STRIDE)

Module 2—Mitigation of Threats and Attacks

COSO Framework and its Relationship With Cyber Risks and Controls

- COSO is the Committee of Sponsoring Organizations, an advisory group that provides guidance on internal controls, fraud deterrence, and risk management. The most recent version of the framework, titled COSO 2013, often refers to the COSO cube, a three-dimensional diagram showing how the various elements of an internal control system work together.
- The framework classifies internal control objectives into three groups: operations, reporting, and compliance.

- There are five components of the COSO internal control framework. These can be applied to cybersecurity efforts to prevent, detect, and respond to cyber threats:
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring Activities

Security Policies, Standards, and Procedures

- To enhance cybersecurity defenses and enhance IT infrastructure resiliency, security rules must be carefully coupled with technology at multiple levels of an organization.
  - At the uppermost level is a collection of security policies, which serve as an overview of an organization's security needs and strategic plan for what should be implemented.
  - At the next level is a set of standards that organizations use as a benchmark to accomplish the goals defined by the security policies.
  - At the bottom level, there are standard operating procedures that are typically detailed documents that specifically outline how to perform business processes.
- An acceptable use policy (AUP) is a control document created by an organization to regulate and protect technology resources by assigning varying levels of responsibilities to job roles, listing acceptable behaviors by employees and vendors, and specifying consequences for those who violate the AUP.
- A bring-your-own-device (BYOD) policy allows employees to use their personally owned devices for work-related activities. It may include some of the same elements as an AUP but will address monitoring and enforcement of actions on personnel devices, ownership of the data on the device, personal liability and indemnification, and restricted activities and application downloads on personal devices.

Network Protection Methods

- A network is a system of physical and virtual devices that are connected using wired cables or wireless technology that communicate using a mixture of different protocols so that users can send, receive, and store data.
- Protocols are sets of rules that govern how a device communicates with other devices in a network. Some of the hardware used in a network includes access points (AP), bridges, computers, gateways, hubs, mobile phones and tablets, modems, proxies, routers, servers, signal modifiers, and switches.
- There are a variety of security methods available to companies that focus specifically on network security to defend against cyberattacks, including the following:
  - Network Segmentation or Isolation
  - Firewall
  - Service Set Identifier (SSID)
  - Virtual Private Network (VPN)
  - Wi-Fi Protected Access (WPA)
  - Endpoint Security
  - System Hardening

- Database Hardening
- Media Access Control (MAC) filtering

Authorization and Authentication

- In addition to employing advanced cybersecurity applications and devices, organizations must also implement practices that complement those defense tools to thwart evolving threats.
- Some of the more prevalent practices include:
  - Zero-trust
  - Least-privilege
  - The need-to-know principle
  - Allowlisting

Identification and Authentication Techniques

- Identification and authentication are two separate concepts that occur in one multi-step process when users validate their right to access systems, applications, or physical locations.
- Identification is the process of claiming or asserting one's identity through means such as a username or identification card.
- Authentication is the process of validating that identity claim, which could be done by using a password or scanning identification cards with proprietary technology.
- There are various authentication technologies available to secure access to confidential data, applications, and networks, including context-aware authentication, digital signatures, single sign-on (SSO), multifactor authentication, personal identification numbers (PINs), smart cards, tokens, and biometrics.
- Strong password protections are critical and can be enhanced with password complexity standards.

Definition and Purpose of Vulnerability Management

- Vulnerability management is a proactive security practice designed to prevent the exploitation of IT vulnerabilities that could potentially harm a system or organization. The practice involves identifying, classifying, mitigating, and fixing known vulnerabilities within a system.
- Vulnerability management can be administered using tools such as vulnerability assessments and vulnerability scanners, as well as through the application of frameworks (i.e., NIST Cybersecurity Framework).
- The Common Vulnerabilities and Exposure (CVE) dictionary is a database of security vulnerabilities that provides unique identifiers for different vulnerabilities and risk exposures.
- Patch management works in conjunction with vulnerability management solutions. Patches are updates released by vendors as bugs are discovered in applications so customers can correct those vulnerabilities.

Layered Security in Cyber Defense

- The purpose of layered security is to protect an organization by using a diversified set of security tactics so that a single cyberattack or security vulnerability does not compromise an entire system.
- Layered approaches typically combine physical access controls, logical and technical controls, and administrative controls to provide control redundancy.
- Defense in depth is one of the most common layered security solutions, as it focuses on a multilayered security approach that relies on a combination of people, policies, technology, physical access controls, and logical access controls.

- Redundancy and diversification help organizations counter attacks that target different weaknesses an organization might have. Duplication is a form of redundancy that can be administered through layering processes, isolating processes, concealing data, and segmenting hardware.

Common Preventive, Detective or Corrective Controls

- Well-designed cybersecurity controls include policies, procedures, and technology that mitigate threats at all points of discovery and all stages of a counterattack.
- Preventive controls are designed to thwart malicious activity from ever occurring. Tactics employed include safeguarding practices, education and training, regular security updates, encryption, firewalls, patches, physical barriers, device and software hardening, and intrusion prevention systems (IPS).
- Access controls are security measures organizations put in place to allow access only to authorized employees.
  - Discretionary access controls (DAC) are decentralized controls that allow data owners, custodians, or creators to manage their own access to the data or object they own or create.
  - Mandatory access controls are nondiscretionary controls that allow administrators to centrally manage and enforce rules consistently across an environment.
  - Role-based access controls administer access based on a user's job role.
  - A rule-based access control manages access to areas, devices, or databases according to a predetermined set of rules or access permissions independent of the user's role or position.
  - A policy-based access control (PBAC) uses a combination of user roles and policies consisting of rules to maintain and evaluate user access dynamically.
  - Risk-based access controls apply controls based on the risk level of the asset being accessed, the identity of the user, the intentions of accessing the asset, and the security risk that exists between the user and the system or asset being accessed.
- Detective controls are designed to detect a threat event while it is occurring and provide assistance during investigations and audits after the event has occurred. Examples include network intrusion detection systems (NIDS), antivirus software monitoring, network monitoring tools, log analysis, and intrusion detection systems (IDS).
- Corrective controls are intended to fix known vulnerabilities as a result of recent security incidents, security self-assessments, or changes in industry practices. Examples include reconfigurations, upgrades and patches, revised policies and procedures, updated employee training, recovery and continuity plans, antivirus software removal of malicious viruses, and virus quarantining.

Module 3—Security Testing

Security Assessments

- Risk Management Framework—Managing risk in an organization requires intricate planning and participation at all levels, from senior management to frontline employees. The National Institute of Standards and Technology (NIST) provides a framework for managing this risk in NIST Special Publication 800-39.

  The framework outlines a comprehensive process to manage risk by applying four components: risk framework, assess risk, respond to risk, and monitor risk.
- Security Assessment Engagement Procedures—The first step in a security assessment engagement is defining assessment procedures, which is a set of objectives that have assessment objects and methods.

  An assessment object identifies the items being assessed as part of a specific control, such as security specifications or job roles, whereas the methods (examination, interviewing, and testing) define the nature of the actions to take.

- Security Assessment Reports—Security Assessment Reports (SARs) are issued as evidence of controls complying or not complying with stated security goals and objectives.
  - The NIST defines a security assessment report as a report that provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified issues or vulnerabilities in the security controls.
  - SARs generally include a summary of findings, systems overview, assessment methodology, security assessment findings, recommendations, and action plans.

Communication of Security Knowledge and Awareness

- All employees play an important role in protecting a company's digital and physical assets, not just the IT department. As such, the need for education and training programs is critical as the sophistication, scope, and number of cyberattacks increases each year.
- Organizations must prioritize and invest in these security awareness programs to minimize the cyber risk and the damages that cyberattacks can inflict upon an organization.
- There are generally three relevant categories of personnel with differing levels of responsibility: management, specialized IT personnel, and all other employees.
- Components of a successful security awareness program may include phishing simulations, security program champions, and employee engagement.

Module 4—Confidentiality and Privacy

Confidentiality vs. Privacy

- *Privacy* protects the rights of an individual and gives the individual control over what information they are willing to share with others.
- *Confidentiality* protects unauthorized access to information gathered by the company.

Methods of Protection of Confidential Data

- Data Collection
  - Creating Policies and Procedures—Organizations should develop policies and procedures for protecting the confidentiality of personal identifiable information (PII).
  - Conducting Training—Organizations should reduce the possibility that PII will be accessed, used, or disclosed inappropriately by requiring that all individuals receive appropriate training.
- Data Processing
  - De-Identifying Personal Information—Organizations should remove enough personal information such that the remaining info does not identify an individual.
- Data Storage
  - Using Access Enforcement—Organizations should control access to personal information through access control policies and access enforcement mechanisms (e.g., access control lists).
  - Implementing Access Control for Mobile Devices—Organizations should prohibit or strictly limit access to personal information from portable and mobile devices, such as laptops, cell phones, and personal digital assistants.
  - Auditing Events—Organizations can monitor events that affect the confidentiality of personal information, such as inappropriate access to PII.
- Data Transmission
  - Organizations should protect the confidentiality of information transmitted. This is commonly accomplished through encrypting the communications (i.e., VPN) or by encrypting the information before it is transmitted.

- Data Deletion/Purging
  - Organizations should set up policies to determine the data sets subject to be archived or purged.
- Obfuscation is the process of replacing production data or sensitive information with data that is less valuable to unauthorized users. The most common data obfuscation applications are encryption, tokenization, and masking.

Data Encryption

- Symmetric Encryption—Involves a single shared, or private, key for encryption and decryption of data within a group.
- Asymmetric Encryption—This data encryption method uses two keys, a public and a private key. The public key is used to encrypt the message, and the private key to decrypt it, or vice versa.
- Cipher techniques apply encryption algorithms that encode unencrypted messages into an encrypted form. Two common cipher techniques include substitution ciphers and transposing ciphers.

Data Loss Prevention (DLP)

- Data loss prevention (DLP) systems enable organizations to detect and prevent attempts by employees or unauthorized users to transfer sensitive information out of the organization electronically across multiple protocols, ports, and communication methods.
- Two common types of DLP systems include network-based DLP systems and endpoint-based DLP systems.
- Protecting Data at Rest—Storing sensitive data requires a robust storage infrastructure that provides sufficient physical security, adequate digital security, authorization, proper access controls, change management controls, backup, and recovery mechanisms.

Walk-through of an Organization's Security, Confidentiality, and Privacy Procedures

- Effective security, confidentiality, and privacy policies and practices require a comprehensive strategy involving all departments within an organization.
- To enhance the likelihood that this strategy can be executed in the event of the examples below, performing periodic read-throughs and walk-throughs led by the IT departments or a joint task force of both IT and non-IT departments is necessary:
  - Data breaches (Confidentiality and privacy)
  - Security incidents or disasters (Security)
- The steps of performing a walk-through include the following: Plan and prep, obtain an understanding, perform the walk-through, create documentation, test, and evaluate and report.
- Walk-throughs of documented IT security, confidentiality, and privacy policies should occur for all functions and departments within an organization, including the following:
  - Finance and Accounting
  - Corporate Training and Education
  - Human Resources
  - IT Risk Management

Detect Deficiencies in a SOC 2® Engagement

- Service auditors in a SOC 2® engagement will also perform a walk-through of the service organization's IT security, confidentiality, and privacy policies. General walk-through procedures to be performed by SOC 2® engagement service auditors include:
  - Following a transaction, event, or activity from origination until final disposition through the service organization's system using the same documents used by service organization personnel.

    When considering confidentiality and privacy, the objective is to understand how PIIs and proprietary information are handled throughout the life cycle.
  - Inquiry, observation, inspection of relevant documentation, flowcharts, questionnaires, or decision tables to facilitate understanding the design of the controls.
  - Inquiry about instances during the period in which controls did not operate as described or designed.
  - Questioning variations in the process for different types of events or transactions.

Module 5—Incident Response

Incident Response Plan Contents

- An incident response plan (IRP) is the documentation of a set of procedures, people, and information to detect, respond to, and limit the consequences of a cyberattack against an organization.
- Contents included in an IRP are subject to the needs and risks associated with an organization. NIST names the key elements that most policies contain, including:
  - Mission
  - Strategies and goals
  - Senior management approval and statement of commitment
  - Organizational approach to incident response
  - Purpose and objectives of the policy
  - Scope of the policy
  - Metrics for measuring the incident response capability and its effectiveness
  - Roadmap for maturing the incident response capability
  - Definition of computer security incidents and related terms
  - Organizational structure and definition of roles, responsibilities, and levels of authority
  - Prioritization or severity ratings of incidents
  - Internal and external communication methods
- Robust IRPs require the recovery timeline to be charted when an incident occurs, delineating the point at which the incident starts; when it is detected, contained, and eradicated; and when normal business operations are restored.
- A critical component of an IRP is the human capital designated to respond to an incident. Depending on the entity's size and business model, the NIST recommends one of three models: A centralized incident response team, distributed incident response teams, and a coordinating team.
- NIST's Computer Security Incident Handling Guide recommends that organizations consider the following factors when selecting the appropriate structure and staffing models for incident response teams: 24/7 availability, full-time vs. part-time team members, employee morale, cost, and staff expertise.

- Incident response teams should perform additional duties to raise awareness of cybersecurity across the organization, including education and awareness, advisory distribution, and information sharing.

Responding to Cybersecurity Incidents in Accordance With the Incident Response Plan

- An organization's IRP must distinguish between recognizing and responding to an event versus a cybersecurity incident. Events may be benign, whereas incidents usually pose a threat to an organization's computer or network security.
- There are seven widely recognized steps in responding to incidents:
  - Preparation (Step 1)
  - Detection (Step 2)
  - Containment (Step 3)
  - Eradication (Step 4)
  - Reporting (Step 5)
  - Recovery (Step 6)
  - Learning (Step 7)
- Once a formal IRP is put in place, organizations periodically test whether those plans respond as expected to both hypothetical and actual cybersecurity incidents.

  Some of the most common methods of testing include the following: Simulations, IRP metrics, post-incident review, periodic audits, and continuous monitoring.

Insurance as a Mitigation Strategy for a Security Incident

- Cyber insurance policies help organizations hedge against cyberattacks by providing financial relief in the event of a successful attack.

  Some common losses related to a cyberattack that are typically covered include: Business interruption losses, cyber extortion losses, incident response costs, replacement costs for information systems, litigation and attorney fees, reputational damage, and information or identity theft.

ISC 4
Unit Outline

Module 1—SOC Engagement Categories and Types

Overview of SOC Engagements

- The organization utilizing the outsourced services is considered the user entity, and the outside organization providing services is known as the service organization.
- A service organization provides the user entity with the benefits of its personnel, expertise, equipment, and technology to operate tasks and functions that the user entity wishes to outsource.
- Examples of the types of services provided by service organizations:
  - Outsourced payroll processors
  - Cloud service providers
  - Credit card processing organizations
  - Enterprise IT outsourcing services
  - Financial technology (Fintech) services
  - Customer support
- SOC engagements assess the effectiveness of a service organization's controls. These engagements, which result in the issuance of a SOC report, promote reliance by third parties on service organizations.
- There are three main types of SOC engagements, including SOC 1®, SOC 2®, and SOC 3®:
  - **SOC 1® for Service Organizations**—Internal Control over Financial Reporting (SOC 1® engagement). The examination and reporting on controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting.

    SOC 1® reports are restricted to the management of the service organization, user entities of the service organization's system, and the independent auditors of such user entities. It does not include potential users of the service organization.
  - **SOC 2® for Service Organizations**—Trust Services Criteria (SOC 2® engagement). The examination and reporting on the security, availability, or processing integrity of a system, or the confidentiality or privacy of the information processed by the system (the AICPA's five trust services categories).

    SOC 2® reports are intended for use by those who have sufficient knowledge and understanding of the service organization, the services it provides, and the system used to provide those services, among other matters. Management and the service auditor should agree on the intended users of the report (specified parties).
  - **SOC 3® for Service Organizations**—Trust Services Criteria for General Use Report (SOC 3® engagement). Like a SOC 2® engagement, the service auditor reports on whether controls within the system were effective to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Unlike a SOC 2® report, a SOC 3® report does not include a description of the system (detailed controls within the system are not disclosed) or a description of the service auditor's tests of controls and the results.

    A SOC 3® report is ordinarily for general users who need assurance about the controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy but lack the knowledge and understanding for a SOC 2® report.

Types of SOC Reports

- Type 1—A report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.
- Type 2—A report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design and operating effectiveness of controls to achieve the related control objectives included in the description throughout a specified period.
- Key Differences Between Type 1 and Type 2 SOC Reports:
  - A Type 1 report covers the design as of a given point in time, whereas a Type 2 report covers both the design and operating effectiveness over a period of time.
  - SOC 1® and SOC 2® reports can be issued as either Type 1 or Type 2 reports depending on the needs of the user, but a SOC 3® report is always issued as a Type 2 report.

Trust Services Criteria

- The trust services criteria set forth the outcomes that an entity's controls should meet to achieve the entity's unique objectives and enable practitioners to evaluate and report on controls over the security, availability, processing integrity, confidentiality, or privacy of information and systems for SOC 2® and SOC 3® engagements.
- The five trust services categories can be remembered using the mnemonic "CAPPS":
  - **Confidentiality**—Information designated as confidential is protected to meet the entity's objectives.
  - **Availability**—Information and systems are available for operation and use to meet the entity's objectives.
  - **Processing Integrity**—System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
  - **Privacy**—Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.
  - **Security**—Information and systems are protected against unauthorized access; unauthorized disclosure of information; and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- The types of subject matter a practitioner may be engaged to report on using the trust services criteria include:
  - SOC 2® engagement
  - SOC 3® engagement
  - SOC for cybersecurity engagement
  - The suitability of design and operating effectiveness of controls of an entity, other than a service organization, over one or more systems relevant to one or more of the trust services categories of security, availability, processing integrity, confidentiality, or privacy
  - The suitability of the design of an entity's controls over security, availability, processing integrity, confidentiality, or privacy to achieve the entity's objectives based on the related trust services criteria.

The COSO Framework Overview and Alignment to the Trust Services Criteria

- The AICPA has aligned the trust services criteria with the COSO (Committee of Sponsoring Organizations of the Treadway Commission) Internal Control—Integrated Framework (the COSO framework), a widely accepted control framework utilized by entities to establish and implement an effective system of internal control. The COSO framework includes five components that are supported by 17 principles.
- The trust services criteria have been aligned to the 17 COSO principles but include supplemental criteria for COSO principle 12, common criteria for all five of the trust services categories, and additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories.
  - COSO principles 1 through 5 relate to the **control environment** component.
  - COSO principles 6 through 9 relate to the **risk assessment** component.
  - COSO principles 10 through 12 relate to the **control activities** component. The trust services criteria expand on principle 12 by adding four supplemental criteria:
    - Logical and physical access controls
    - System operations
    - Change management
    - Risk mitigation
  - COSO principles 13 through 15 relate to the **information and communication** component.
  - COSO principles 16 and 17 relate to the **monitoring activities** component.

Module 2—Reporting on SOC Engagements: Part 1

Forming the Opinion in a SOC Engagement

- The service auditor should form an opinion about the subject matter of the engagement. When forming the opinion, the service auditor should evaluate:
  - the sufficiency and appropriateness of the evidence obtained; and
  - whether uncorrected misstatements, individually or in the aggregate, are material.

Types of Opinions in a SOC Engagement

- The opinions of the service auditor in a SOC engagement depend on the facts and circumstances of the evidence gathered throughout the engagement and may include an unmodified (unqualified) opinion, qualified opinion, adverse opinion, or disclaimer of an opinion.
- **Unmodified (Unqualified) Opinion**—The service auditor's opinion that, in all material respects, based on the criteria described in management's assertion that as of the specified date (Type 1) or throughout the specified period (Type 2):
  - Management's description of the system fairly presents the system that was designed and implemented.
  - The controls stated in management's description of the system were suitably designed.
  - The controls stated in management's description of the system operated effectively (Type 2 only).

Modifications to the Service Auditor's Opinion

- The service auditor's opinion should be modified, and the service auditor's report should include a description of the matter or matters giving rise to the modification when either of the following circumstances exist and, in the service auditor's professional judgment, the effect of the matter is or may be material:
  - The service auditor is unable to obtain sufficient appropriate evidence to conclude that the subject matter is in accordance with (or based on) the criteria in all material respects.
  - The service auditor concludes, based on evidence obtained, that the subject matter is not in accordance with (or based on) the criteria in all material respects.
- There are three types of modified opinions:
  - **Qualified Opinion**—A qualified opinion states that except for the effects of the matter(s) giving rise to the modification, the description is presented in accordance with the description criteria, and the controls were suitably designed and operating effectively (Type 2), in all material respects.
  - **Adverse Opinion**—An adverse opinion states that the description misstatements, either individually or in the aggregate, are material and pervasive, or deficiencies in the design or operation of controls are material and pervasive.
  - **Disclaimer of Opinion**—A disclaimer of opinion states that the auditor does not express an opinion.

Contents of the Auditor's Report for a SOC Engagement

- The SOC report includes the following key components:
  - Management's description of the system
  - Management's assertion
  - Independent service auditor's report
  - Auditor's tests of controls and results of tests

Management's Description of the System

- In a SOC 1® engagement, the service organization's management is responsible for documenting the description of the service organization's system. The description must provide sufficient information to allow a user auditor to understand how the service organization's processing affects the user entity's financial statements and to assess the risk of material misstatement of the user entity's financial statements.
- In a SOC 2® engagement, the service organization's management is responsible for presenting a description of the system to enable report users, such as user entities, business partners, or other relevant parties, to understand the system and the processing and flow of data throughout and from the system. The description is to be prepared in accordance with specific criteria and describes the procedures and controls in place to manage risk.
- Common sections of a system description in a SOC 1® engagement include:
  - Types of services provided
  - Procedures performed
  - System functionality
  - Subservice organizations
  - Controls

- Information on other aspects of the control environment, risk assessment process, information and communication, control activities, and monitoring activities that are relevant to the services provided.
- Prepare reports
- Deficiencies in information
- Complementary user entity controls (CUECs)
- Changes to the service organization's system during the period covered (Type 2 only).
- The description does not omit or distort information relevant to the system and is prepared to meet the common needs of a broad range of user entities and their auditors.

- Common sections of a system description in a SOC 2® engagement include:
  - Types of services provided
  - Principal service commitments and system requirements
  - Components of the system used to provide the services
  - Identified system incidents
  - Applicable trust services criteria
  - CUECs
  - Subservice organizations
  - Irrelevant specific criteria
  - Changes to the service organization's system or controls during the period that are relevant to the service organization's service commitments and system requirements (Type 2 only).
- Management's Description of the Entity's Cybersecurity Risk Management Program—Management is responsible for developing the entity's cybersecurity risk program and for making an assertion about whether the description is presented in accordance with the description criteria and about the effectiveness of the controls within the program based on a set of control criteria. The categories of description criteria include:
  - Nature of business and operations
  - Nature of information at risk
  - Cybersecurity risk management program objectives (cybersecurity objectives)
  - Factors that have a significant effect on inherent cybersecurity risks
  - Cybersecurity risk governance structure
  - Cybersecurity risk assessment process
  - Cybersecurity communications and the quality of cybersecurity information
  - Monitoring of the cybersecurity risk management program
  - Cybersecurity control processes

Management's Assertions

- In a SOC engagement, the service auditor is required to request a written assertion from management.
  - In a SOC 1® or SOC 2® engagement, management's assertion addresses whether:
    - — Management's description of the service organization's system fairly presents the service organization's system that was designed and implemented.

  - The controls stated in management's description of the system were suitably designed.
  - The controls stated in management's description of the system operated effectively (Type 2 only).
- In a SOC 3® engagement, management's assertion addresses whether:
  - The controls operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved, including the boundaries of the system and the principal service commitments and system requirements.

Contents of the Service Auditor's Report for a SOC Engagement

- The elements to be included in a service auditor's SOC report include:
  - Title
  - Addressee
  - Scope
  - Service organization's responsibilities
  - Service auditor's responsibilities
  - Inherent limitations
  - Description of tests of controls (Type 2 only)
  - Other matter (Type 1 only)
  - Opinion
  - Restricted use
  - Service auditor's signature
  - Service auditor's city and state
  - Date of the service auditor's report
- Key Differences Between Type 1 and Type 2 Reports—The addition of expanded language to include the operating effectiveness of control in a Type 2 report. The Type 1 report would not include a description of the service auditor's tests of controls and related results.
- Describing Test of Controls and Results in a SOC 2® Engagement—A service auditor's SOC 2® Type 2 report should contain a reference to the description of the service auditor's tests of controls and the results of such tests.
- Information required to be described includes:
  - Controls that were tested.
  - Whether the items tested represent all or a selection of the items in the population.
  - The nature of the tests performed in sufficient detail to enable report users to determine the effect of such tests on their risk assessments.
  - The number of items tested (if deviations were identified).
  - The number and nature of deviations (if deviations were identified).
  - Causative factors (optional if deviations were identified).

Module 3—Reporting on SOC Engagements: Part 2

Overview of the Carve-out and Inclusive Methods

- When conducting a SOC engagement, the service auditor may need to consider outsourced functions that are performed for the service organization by other organizations.
- For SOC 1® engagements, a vendor used by a service organization is considered a subservice organization if:
  - The services provided by the vendor are likely relevant to user entities' internal control over financial reporting.
  - Controls implemented at the subservice organization are necessary to achieve the control objectives stated in management's description of the service organization's system. These controls are referred to as complementary subservice organization controls (CSOCs).
- For SOC 2® and SOC 3® engagements, a vendor used by a service organization is considered a subservice organization only if:
  - The services provided by the vendor are relevant to report users' understanding of the service organization's system as it relates to the applicable trust services criteria.
  - Controls at the subservice organization are necessary, in combination with the service organization's controls, to provide reasonable assurance that the service commitments and system requirements are achieved. These controls are referred to as CSOCs.
- Service organization management is responsible for determining whether it uses a subservice organization and for determining whether to carve out or include the subservice organization's controls within the scope of the engagement.
- The two methods are defined as follows:
  - **Carve-out Method**—The method of addressing the services provided by a subservice organization in which the complementary subservice organization controls (CSOCs) of the subservice organization are excluded from the description of the service organization's system and the scope of the engagement. This method identifies:
    - — The nature of the services performed by the subservice organization.
    - — The types of controls expected to be performed at the subservice organization that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the control objectives stated in management's description of the service organization's system (SOC 1®) or the service organization's service commitments and system requirements (SOC 2®) were achieved.
    - — The controls at the service organization are used to monitor the effectiveness of the subservice organization's controls.
  - **Inclusive Method**—The method of addressing the services provided by a subservice organization in which the description of the service organization's system includes a description of:
    - — The nature of the services provided by the subservice organization.
    - — The components of the subservice organization's system used to provide services to the service organization, including the subservice organization's controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the control objectives stated in management's description of the service organization's system (SOC 1®) or the service organization's service commitments and system requirements (SOC 2®) were achieved.

- When a service organization uses multiple subservice organizations, it may prepare its description using the carve-out method for one or more subservice organizations and the inclusive method for others.

Complementary User Entity Controls (CUECs)

- For SOC 1® and SOC 2® engagements, complementary user entity controls (CUECs) are controls that are necessary to be implemented by the user entity, in combination with the service organization's controls, to provide reasonable assurance that the control objectives stated in management's description of the service organization's system (SOC 1®), or the service organization's service commitments and system requirements (SOC 2®) were achieved.
- In some instances, a service organization's controls cannot provide reasonable assurance that its service commitments and system requirements were achieved without the user entity performing certain activities in a defined manner.
- In these cases, the service organization expects the user entity to implement necessary controls and perform them completely and accurately in a timely manner. Management of the service organization identifies such CUECs in their system description.
- Common examples of CUECs include:
  - Security monitoring
  - Managed service provider (MSP) environment changes
  - Encrypted financial data
  - Physical access controls
  - Authorization policies

Impact of Complementary User Entity Controls (CUECs) and Complementary Subservice Organization Controls (CSOCs) on the SOC Report

- A statement must be included in the opinion section of the auditor's report that the application of complementary user entity controls or complementary subservice organization controls (or both) are considered necessary to achieve the related control objectives stated in management's description of the service organization's system (SOC 1®) or the service organization's service commitments and system requirements (SOC 2®).
- A SOC 1® report should also include:
  - A description of relevant CUECs that ensure control objectives are met in the system description.
  - A statement (if applicable) that the service organization's controls could only be achieved if CUECs are designed and operating effectively.
- A SOC 2® report should also include:
  - Relevant CUECs and a statement that user entities are responsible for those controls.
  - A statement that the engagement did not include an evaluation of whether the CUECs were evaluated for design suitability or operating effectiveness.
  - Language about how CUECs interact with the service organization's controls.

Impact of Modified Opinions on the SOC Report

- For SOC 1® engagements, a qualified opinion is expressed when the misstatements in management's description of the service organization's system or deficiencies in the suitability of design or operating effectiveness (Type 2) of the controls are limited to one or more, but not all, aspects of the description of the system or control objectives and do not affect the service auditor's opinion on other aspects of the description.

- For SOC 2® engagements, a qualified opinion is expressed when:
  - The service auditor concludes that description misstatements, individually or in the aggregate, are material but not pervasive, or deficiencies in the design or operation (Type 2) of controls are material but not pervasive.
  - The service auditor is unable to obtain sufficient appropriate evidence on which to base the opinion, and the service auditor has concluded that the possible effects on the subject matter of undetected description misstatements or deficiencies could be material but not pervasive to the subject matter.

  When issuing a qualified opinion, the service auditor's report should be modified:
  - The service auditor's opinion paragraph should be amended.
  - A separate paragraph describing matters giving rise to modification should be included.
  - The service auditor's responsibilities (SOC 2®) should be amended.
- An adverse opinion is expressed when the practitioner concludes that the description misstatements, either individually or in the aggregate, are material and pervasive, or deficiencies in the design or operation of controls are material and pervasive.

  When issuing an adverse opinion, the service auditor's report should be modified:
  - The service auditor's opinion paragraph should be amended.
  - A separate paragraph describing matters giving rise to modification should be included.
  - The service auditor's responsibilities (SOC 2®) should be amended.
- A disclaimer of opinion is expressed when the service auditor is unable to obtain sufficient appropriate evidence on which to base the opinion, and the possible effects on the subject matter of undetected misstatements could be both material and pervasive.

  When disclaiming an opinion, the service auditor's report should be modified:
  - A separate paragraph describing matters giving rise to modification should include a description of the items in question in which the examination did not comply with the attestation standards.
  - The first sentence of the service auditor's report is revised.
  - The standards under which the service auditor conducts an examination are identified in the first paragraph of the report rather than the second.

  When disclaiming an opinion, the service auditor's report should be modified to omit statements:
  - Indicating what those standards require of the practitioner.
  - Indicating that the practitioner believes the evidence obtained is sufficient and appropriate to provide a reasonable basis for the service auditor's opinion.
  - Describing the nature of an examination engagement.
- Report paragraphs describing matters giving rise to modification:
  - A separate paragraph should be added to the service auditor's report to explain the matter giving rise to the modification when a service auditor concludes that a modified opinion is appropriate based on the evidence obtained during a SOC engagement.
  - A separate paragraph would be added when the description includes controls that have not been implemented.
  - A separate paragraph would be added to the auditor's report preceding the opinion paragraph when the auditor concludes the controls are not suitably designed.

Module 4—Planning and Risk Assessment in a SOC Engagement

Understanding Service Organization Management's Responsibilities

- The service auditor, when auditing the service organization:
  - Is required to establish, prior to acceptance of the SOC engagement, an understanding with service organization management about its responsibilities and the responsibilities of the service auditor.
  - Should establish communication with the management of the service organization.
  - Should determine the appropriate person(s) within the service organization's management or governance structure with whom to interact.
- The decisions a service organization's management makes prior to engaging the service auditor can affect the nature, extent, and timing of procedures the service auditor performs.

Objectives and Planning Considerations for a Service Auditor

- Planning a SOC engagement requires the service auditor to obtain an understanding of key areas and formulate assessments of risk relevant to the engagement. The planning requirements of a service auditor for SOC 1®, SOC 2®, and SOC 3® engagements are similar.
- During the planning of any SOC engagement, the service auditor is responsible for:
  - Determining whether to accept or continue the engagement.
  - Agreeing on engagement terms.
  - Reaching an understanding with management regarding a written assertion.
- During the planning of a SOC 1® engagement, the service auditor is also responsible for:
  - Assessing the risk of material misstatement.
  - Obtaining an understanding of the service organization's system and assessing the suitability of the criteria used by management in preparing its system description.
- During the planning of SOC 2® and SOC 3® engagements, the service auditor is also responsible for:
  - Establishing an Overall Strategy for the Engagement—Sets the scope, timing, and direction of the engagement and guides the development of the engagement plan, including the consideration of materiality and the identification of the risks of material misstatement (SOC 2®).
  - Performing Risk Assessment Procedures—Includes understanding of the service organization's system and how the system controls were designed, implemented, and operated to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria (SOC 2®).

Independence Considerations

- Independence is required in an engagement to report on controls at a service organization. However, the service auditor is not required to be independent of each user entity.
- **Service Organization and Service Auditor**—The service auditor needs to be independent with respect to the responsible party (or parties). The responsible party is most often the service organization.
- **Subservice Organization and Service Auditor**—If management elects to use the inclusive method, then subservice organization management is a responsible party and should be independent of the service auditor.

Materiality in a SOC 1® Engagement

- The service auditor's consideration of materiality should include the fair presentation of the description of the service organization's system.
  - The concept of materiality in the context of the fair presentation of the description relates to the information being reported on, not the financial statements of user entities.
- Materiality relates to qualitative factors, such as whether significant aspects of the processing have been included in the description or if relevant information has been omitted or distorted.
- Materiality with respect to the operating effectiveness of controls for a Type 2 report includes the consideration of quantitative and qualitative factors:
  - Quantitative—The tolerable and observed rate of deviations
  - Qualitative—The nature and cause of deviations

Materiality in a SOC 2® Engagement

- Materiality can be described as:
  - the likelihood and magnitude of the risks that threaten the achievement of the service organization's service commitments and system requirements; and
  - whether the controls the service organization has designed, implemented, and operated were effective in mitigating those risks to an acceptable level based on the applicable trust services criteria.
- The service auditor should consider the nature of threats and the likelihood and magnitude of the risks arising from those threats to the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria.
- The service auditor's consideration of materiality is a matter of professional judgment and is affected by the service auditor's perception of the common information needs of the broad range of report users as a group.
- When considering materiality, the service auditor typically considers whether misstatements in the description or deficiencies in the suitability of the design of controls and the operating effectiveness of controls (Type 2) could reasonably be expected to influence the relevant decisions made by the broad range of report users.
- If the engagement has been designed to meet the informational needs of a specific subset of such SOC 2® report users, and the report is restricted to those specific users, the service auditor considers the possible effect of such misstatements on the decisions that may be made by that specific subset of report users.

Risk Assessment in a SOC Engagement

- In a SOC 2® engagement, performing risk assessment procedures includes an understanding of the service organization's system and how the system controls were designed, implemented, and operated to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria.
  - A system is defined as the infrastructure, software, procedures, and data that are designed, implemented, and operated by people to achieve one or more of the organization's specific business objectives in accordance with management-specified requirements.
  - System components are comprised of infrastructure, software, people, data, and procedures.
  - The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures, and data necessary to provide its services. The boundaries of a system need to be clearly defined and communicated to report users in a SOC engagement.

Service Commitments and System Requirements

- The service organization's principal service commitments and system requirements.
  - Service commitments are declarations made by service organization management to user entities and others (such as user entities' customers) about the system used to provide the service.
  - System requirements are specifications regarding how the system should function to meet the service organization's service commitments, to comply with relevant laws and regulations and guidelines of industry groups (such as business or trade associations), and to achieve other objectives of the service organization that are relevant to the trust services category or categories addressed by the description.
- A service organization's system of internal control is evaluated by using the trust services criteria to determine whether such controls provide reasonable assurance that its business objectives and sub-objectives were achieved. Objectives and sub-objectives relate primarily to:
  - The achievement of service commitments made to user entities related to the system used to provide the services and the system requirements necessary to achieve those commitments.
  - Service commitments may also be established for one or more of the trust services categories addressed by the description.
  - Compliance with laws and regulations regarding the provision of the services by the system.
  - The achievement of the other objectives the service organization has for the system.
- System requirements may also define how the system should function to meet the service commitments, comply with laws and regulations, and achieve other objectives. System requirements may result from the service organization's commitments related to one or more of the trust services categories.
- A service organization's management is responsible for:
  - Achieving its service commitments and system requirements.
  - Disclosing the principal system requirements and service commitments in the system description in a manner that allows SOC 2® report users to understand how the controls operate and how management and the service auditor evaluated the suitability of the controls' design and operating effectiveness (Type 2).
  - Disclosing service commitments that are relevant to the common needs of the broad range of SOC 2® report users.
- When deciding whether the disclosures stated in the description are appropriate, the service auditor should consider whether:
  - The service commitments are presented in sufficient detail for report users to understand the relationship between the controls implemented by the service organization, the service commitments, and system requirements.
  - The description summarizes the principal service commitments that are common to such report users when the SOC 2® report is designed for a broad range of users.

Risk Assessment Considerations of the Service Organization

- In a SOC engagement, risk assessment begins with the service organization identifying and assessing the types, likelihood, and impact of risks that affect the preparation of the description, the suitability of the design of controls, and the operating effectiveness of controls (Type 2) within the system.

- These risks may include:
  - Intentional and unintentional internal and external acts.
  - Identified threats and vulnerabilities to, and deficiencies of, the system.
  - The use of subservice organizations that store, process, or transmit sensitive information on the service organization's behalf.
  - The type of employee personnel with access to the system.
  - A lack of CUECs or CSOCs when those controls are considered necessary.
- Risk assessment primarily focuses on inherent risks that affect the preparation of the description of the system and the effectiveness of the service organization's controls.

Risk Assessment Considerations of a Service Auditor

- In a SOC engagement, the service auditor must perform risk assessment procedures that are sufficient to enable the auditor to identify and assess the risk of material misstatement and provide a basis for designing and performing procedures that are responsive to the risks.
- In a Type 1 or Type 2 engagement, the risk of material misstatement relates to the risk that, in all material respects, based on the criteria in management's assertion:
  - management's description of the service organization's system is not fairly presented;
  - the controls are not suitably designed; and
  - the controls did not operate effectively (Type 2 only).
- The service auditor should obtain an understanding of the service organization's system.
- The service auditor's risk assessment procedures to obtain an understanding of the service organization's system may include:
  - Inquiry.
  - Observing operations and inspecting documents, reports, and printed and electronic records of transaction processing.
  - Inspecting a selection of agreements between the service organization and its user entities and business partners.
  - Reperforming the application of a control.
  - Reading relevant reports received from regulators, internal auditors, or other specialists (SOC 2®).
- Service auditor risk assessment procedures may be performed:
  - Within a walk-through.
  - Concurrently with procedures performed to obtain information about whether the system description is presented in accordance with the description criteria and whether the controls were suitably designed and operated effectively to meet the control objectives.
- The service auditor should also perform risk assessment procedures to identify any fraud risk or risk of noncompliance with laws or regulations. Risks could include:
  - management override of controls;
  - misappropriation of assets; or
  - the creation of false or misleading documents or records.

Module 5—Performing SOC Engagements

Responding to the Assessed Level of Risk

- The service auditor is required:
  - To obtain sufficient audit evidence to reduce attestation risk to an acceptably low level.
  - To design and implement overall responses to address the assessed risks of material misstatement for the subject matter; and design and perform further procedures whose nature, extent, and timing are based on, and responsive to, the assessed risks of material misstatement.
- Assessment of the risks of material misstatement is impacted by several factors, including:
  - materiality considerations;
  - the service auditor's understanding of the effectiveness of the control environment; or
  - other components of internal control related to the service provided to user entities and business partners.

Evaluating Management's Description

SOC 1®—Evaluating Whether Management's Description of the Service Organization's System Is Fairly Presented

- The service auditor is required to obtain and read management's description of the service organization's system and evaluate whether those aspects of the description that are included in the scope of the engagement are presented fairly, in all material respects, based on the suitable criteria in management's assertion, including whether:
  - The control objectives stated in management's description of the service organization's system are reasonable in the circumstances.
  - Controls identified in management's description of the service organization's system were implemented.
  - Complementary user entity controls and complementary subservice organization controls, if any, are adequately described.
  - The services performed by a subservice organization, if any, are adequately described, including whether the carve-out method or the inclusive method has been used in relation to them.
- The attributes of suitable criteria for evaluating the fair presentation of management's description include:
  - Whether management's description of the service organization's system presents how the service organization's system was designed and implemented.
  - Whether management's description of the service organization's system includes relevant details of changes to the service organization's system during the period covered by the description (Type 2 only).
  - Whether management's description of the service organization's system does not omit or provide misleading information relevant to the service organization's system while acknowledging that management's description of the service organization's system is prepared to meet the common needs of a broad range of user entities and their auditors, and may not include every aspect of the service organization's system that each individual user entity may consider important in its own particular environment.

- A description is not fairly presented if:
  - the description states or implies that controls are being performed when they are not being performed; or
  - the description inadvertently or intentionally omits relevant controls performed by the service organization that are not suitably designed or operating effectively.

SOC 2®—Evaluating Whether the Description Presents the System That Was Designed and Implemented in Accordance With the Description Criteria

- The service auditor should obtain and read the description of the service organization's system and perform procedures to determine whether the description is presented in accordance with the description criteria by comparing the service auditor's understanding of the service provided to user entities to the system through which service is provided based on the trust services category or categories included in the scope of the engagement.
- A description of a service organization's system in a SOC 2® engagement is presented in accordance with the description criteria when the description:
  - Describes the system that the service organization has implemented.
  - Includes information about each description criterion to the extent it is relevant to the system being described.
  - Does not inadvertently or intentionally omit or distort information that is likely to be relevant to report users' decisions.
- A description is not presented in accordance with the description criteria if:
  - the description states or implies that certain IT components exist when they do not;
  - the description states or implies that certain processes and controls have been implemented when they are not being performed; or
  - the description contains statements that cannot be objectively evaluated.
- Determining whether the description is presented in accordance with the description criteria also involves evaluating whether each stated control has been implemented.
- The service auditor should:
  - Evaluate whether the description is misleading within the context of the engagement based on the evidence obtained.
  - Consider whether additional disclosures are necessary to supplement the description. Additional disclosures may include:
    - Significant interpretations made in applying the criteria in the engagement circumstances.
    - Subsequent events, depending on their nature and significance.
  - If the service auditor believes that the description is misstated or otherwise misleading, the service auditor should ask management to amend the description.

Performing Tests of Controls and Other Procedures in a SOC 2® Engagement

- In addition to obtaining evidence that the description presents the system that was designed and implemented in accordance with the description criteria, the service auditor must also obtain evidence that the controls were suitably designed and operated effectively during the specified period (Type 2).
- To supplement evidence, the auditor may perform an inquiry of service organization personnel, inspection of documents, additional walk-throughs, reading applicable supporting system documentation, and determining whether attacks, vulnerability exploitations, emerging risks, or threats have been adequately addressed.

- The evidence obtained from the tests of controls relates to how the controls were applied, the consistency with which they were applied, and by whom or in what manner they were applied.
- Service auditors should gain an understanding of the processes in place to report system failures, system incidents, and complaints by external or internal system users by inquiring of management about the controls in place.

Evaluating the Results of Procedures in a SOC 2® Engagement

- Sufficient evidence is necessary to support the service auditor's opinion and report. The service auditor must consider all information and evidence obtained during the engagement, including evidence from all sources (both internal and external) as well as evidence that corroborates or contradicts management's assertions.
- The service auditor must evaluate the results of all procedures performed and must conduct both quantitative and qualitative analysis.
- When evaluating the results of procedures, the service auditor investigates the nature and cause of any identified description misstatements and deficiencies or deviations in the effectiveness of controls.
- If the service auditor identifies material description misstatements, material deficiencies in the suitability of the design of controls, or deviations in the operating effectiveness of controls (Type 2), the service auditor should modify the opinion.

Subsequent Events and Subsequently Discovered Facts

- Transactions or events may occur after the engagement period but prior to the date of the service auditor's report that could have a significant effect on the description, the suitability of the design of controls, and the operating effectiveness of controls (Type 2), or management's assertion.
- The service auditor is required to inquire of management about whether it is aware of any subsequent events. If such events exist, the service auditor should apply the appropriate procedures to obtain evidence regarding the events.
- Upon becoming aware of a significant subsequent event, a service auditor should request that management disclose the event in either management's assertions or the description of the service organization's system. If management refuses to disclose an event that would mislead report users if undisclosed, the practitioner should consider taking the following actions:
  - Modifying the auditor's report and disclosing the event.
  - Withdrawing from the engagement.
- The service auditor is not required to perform procedures after the date of the service auditor's report but is responsible for responding appropriately to subsequently discovered facts that become known after the date of the report.
- The service auditor should determine whether the subsequently discovered facts, had they been known as of the report date, may have caused the service auditor to revise the report.

Obtaining Written Representations from Management

- The service auditor is required to obtain written representations from the management of the service organization.
  - Such representations are intended to confirm explicit or implicit representations given to the service auditor, indicate and document the continuing appropriateness of those representations, and reduce the possibility of a misunderstanding between the service auditor and management.

- The service auditor should determine the appropriate individuals within the service organization's management or governance structure based on their responsibilities and knowledge of the subject matter of the engagement.
- The written representations should be as of the date of the issued SOC report and should address the subject matter and periods covered by the service auditor's opinion.

- The written representations should:
  - Include management's assertion about the subject matter based on the criteria.
  - State that all relevant matters are reflected in the measurement or evaluation of the subject matter or assertion.
  - State that all known matters contradicting the subject matter or assertion and any communication from regulators or others affecting the subject matter have been disclosed to the service auditor.
  - Acknowledge responsibility for the subject matter, assertions, selection of the criteria, and determination that such criteria are appropriate for management's purposes.
  - State that any known subsequent events related to the subject matters of the report that would have a material effect on the subject matter or assertion have been disclosed.
  - State that management has provided the service auditor with all relevant access and information.
  - State that management believes the effect of uncorrected misstatements is immaterial to the subject matter.
  - State that management has made necessary, appropriate disclosures to the service auditor.
  - State that significant assumptions used in making any material estimates are reasonable (SOC 1®).