Computer Security	Information Security
• Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.	• The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Confidentiality	• Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. • The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes. • The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.
Integrity	• Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. • The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. • The property whereby an entity has not been modified in an unauthorized manner
Availability	• Ensuring timely and reliable access to and use of information. • The property of being accessible and useable upon demand by an authorized entity.

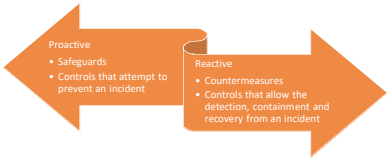
Vulnerability	Threat
• Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. • A weakness in a system, application, or network that is subject to exploitation or misuse. • Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. • Vulnerability Assessment- • Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. • Formal description and evaluation of the vulnerabilities in an information system.	• Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. The potential source of an adverse event. • Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

Security Threat

- Snooping
- Modification
- Masquerading
  - When an unauthorized agent claims the identity of another agent, it is said to be masquerading.
  - A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity.
- Repudiation of origin
- Denial of receipt
- Delay
- Denial of service

Security Controls

- An effective control is one that prevents, detects, and/or contains an incident and enables recovery from an event.
- Controls can be:



Control Methods

Managerial	Controls related to the oversight, reporting, procedures and operations of a process. These include policy, procedures, balancing, employee development and compliance reporting.
Technical	Controls also known as logical controls and are provided through the use of technology, piece of equipment or device. Examples include firewalls, network or host-based intrusion detection systems (IDSs), passwords and antivirus software. A technical control requires proper managerial (administrative) controls to operate correctly.
Physical	Controls that are locks, fences, closed-circuit TV (CCTV) and devices that are installed to physically restrict access to a facility or hardware. Physical controls require maintenance, monitoring and the ability to assess and react to an alert should a problem be indicated.

Source: ISACA, *CISA Review Manual 26th Edition*, figure 5.5

System Access Permission

- System access permission generally refers to a technical privilege, such as the ability to read, create, modify or delete a file or data; execute a program; or open or use an external connection.
- System access to computerized information resources is established, managed and controlled at the physical and/or logical level.

Physical access controls	Logical access controls
• Restrict the entry and exit of personnel to an area, such as an office building, suite, data center or room, containing information processing equipment.	• Restrict the logical resources of the system (transactions, data, programs, applications) and are applied when the subject resource is needed.

System Access Reviews

- Roles should be assigned by the information owner or manager.
- Access authorization should be regularly reviewed to ensure they are still valid.
- Evaluate the following criteria for defining permissions and granting access:
  - Need-to-know
  - Accountability
  - Traceability
  - Least privilege
  - SoD

Physical Access Issues

- Physical access exposures may originate from natural and man-made hazards, and can result in unauthorized access and interruptions in information availability.
- Exposures include:
  - Unauthorized entry
  - Damage, vandalism or theft to equipment or documents
  - Copying or viewing of sensitive or copyrighted information
  - Alteration of sensitive equipment and information
  - Public disclosure of sensitive information
  - Abuse of data processing resources
  - Blackmail
  - Embezzlement

Physical Access Controls

- Door locks (cipher, biometric, bolted, electronic)
- Security Guards
- Manual or electronic logging
- Controlled visitor access
- Computer workstation locks
- Controlled single entry point
- Alarm system
- Deadman doors

Key Terms

Key Term	Definition
Access control	The processes, rules and deployment mechanisms that control access to information systems, resources and physical access to premises.
Access control list (ACL)	An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals. Also referred to as access control tables.
Access path	The logical route an end user takes to access computerized information. Typically, it includes a route through the operating system, telecommunications software, selected application software and the access control system.

Key Terms (cont'd)

Logical access controls	The policies, procedures, organizational structure and electronic access controls designed to restrict access to computer software and data files.

Logical Access

- Logical access is the ability to interact with computer resources, granted using identification, authentication and authorization.
- Logical access controls are the primary means used to manage and protect information assets.
- Analyze and evaluate the effectiveness of a logical access control in accomplishing information security objectives and avoiding losses resulting from exposures.

Logical Access (cont'd)

- To effectively assess logical access controls, they first need to gain a technical and organizational understanding of the organization's IT environment, including the following security layers:
  - Network
  - OS platform
  - Database
  - Application

Paths of Logical Access

- Access or points of entry to an organization's IS infrastructure can be gained through the following paths:
  - Direct
  - Local network
  - Remote
- General points of entry to either front-end or back-end systems occur through network connectivity or remote access.

Paths of Logical Access (cont'd)

- Any point of entry not appropriately controlled can potentially compromise the security of an organization's sensitive and critical information resources.
- Determine whether all points of entry are identified and managed.

Logical Access Exposures

- Technical exposures are the unauthorized activities interfering with normal processing.
- They include:
  - Data leakage—Involves siphoning or leaking information out of the computer
  - Wiretapping—Involves eavesdropping on information being transmitted over telecommunications lines
  - Computer shutdown—Initiated through terminals or personal computers connected directly (online) or remotely (via the Internet) to the computer

Access Control Software

- Access control software is used to prevent the unauthorized access and modification to an organization's sensitive data and the use of system critical functions.
- Access controls must be applied across all layers of an organization's IS architecture, including networks, platforms or OSs, databases and application systems.
- Each access control usually includes:
  - Identification and authentication
  - Access authorization
  - Verification of specific information resources
  - Logging and reporting of user activities

Access Control Software Functions

General operating and/or application systems access control functions

- Create or change user profiles.
- Assign user identification and authentication.
- Apply user logon limitation rules.
- Notification concerning proper use and access prior to initial login.
- Create individual accountability and auditability by logging user activities.
- Establish rules for access to specific information resources (e.g., system-level application resources and data).
- Log events.
- Report capabilities.

Database and/or application-level access control functions

- Create or change data files and database profiles.
- Verify user authorization at the application and transaction level.
- Verify user authorization within the application.
- Verify user authorization at the field level for changes within a database.
- Verify subsystem authorization for the user at the file level.
- Log database/data communications access activities for monitoring access violations.

Access Control Types

Mandatory access controls (MACs)

- Logical access control filters used to validate access credentials
- Cannot be controlled or modified by normal users or data owners
- Act by default
- Prohibitive; anything that is not expressly permitted is forbidden

Discretionary access controls (DACs)

- Logical access controls that may be configured or modified by the users or data owners
- Cannot override MACs
- Act as an additional filter, prohibiting still more access with the same exclusionary principle