01- Comparing Security Roles and Security Controls

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

1.1- Compare and Contrast Information Security Roles

1.2- Compare and Contrast Security Control And Framework Types

1.1- Compare and Contrast Information Security Roles

1.2- Compare and Contrast Security Control And Framework Types

INFORMATION SECURITY

- **Information Security** (or infosec) refers to the protection of data resources from unauthorized access, attack, theft, or damage.
- Data may be vulnerable because of the way it is stored, the way it is transferred, or the way it is processed.
- Secure information has three properties, often referred to as the **CIA Triad**:
  - ✓ **Confidentiality:** means that certain information should only be known to certain people.
  - ✓ **Integrity:** means that the data is stored and transferred as intended and that any modification is authorized.
  - ✓ **Availability:** means that information is accessible to those authorized to view or modify it.

INFORMATION SECURITY (cont.)

- Some security models and researchers identify other properties that secure systems should exhibit.
- The most important of these is **non-repudiation**.
- **Non-repudiation** means that a subject cannot deny doing something, such as creating, modifying, or sending a resource.
- **For Example:** a legal document, such as a will, must usually be witnessed when it is signed.
- If there is a dispute about whether the document was correctly executed, the witness can provide evidence that it was.

INFORMATION SECURITY COMPETENCIES

- IT professionals working in a role with security responsibilities must be competent in a wide range of disciplines, from network and application design to procurement and human resources (HR).
- The following activities might be typical of such a role:
  - ✓ Participate in risk assessments and testing of security systems and make recommendations.
  - ✓ Specify, source, install, and configure secure devices and software.
  - ✓ Set up and maintain document access control and user privilege profiles.
  - ✓ Monitor audit logs, review user privileges, and document access controls.
  - ✓ Manage security-related incident response and reporting.
  - ✓ Create and test business continuity and disaster recovery plans and procedures.
  - ✓ Participate in security training and education programs.

INFORMATION SECURITY ROLES AND RESPONSIBILITIES

- A **Security Policy** is a formalized statement that defines how security will be implemented within an organization.
- It describes the means the organization will take to protect the confidentiality, availability, and integrity of sensitive data and resources.
- The implementation of a security policy to support the goals of the CIA triad might be very different for a school, a multinational accountancy firm, or a machine tool manufacturer.
- However, each of these organizations, or any other organization should have the same interest in ensuring that its employees, equipment, and data are secure against attack or damage.

INFORMATION SECURITY ROLES AND RESPONSIBILITIES (cont.)

- As part of the process of adopting an effective organizational security posture, employees must be aware of their responsibilities.
- The structure of security responsibilities will depend on the size and hierarchy of an organization, but these roles are typical.
  - ✓ Overall internal responsibility for security might be allocated to a dedicated department, run by a **Director of Security, Chief Security Officer (CSO)**, or **Chief Information Security Officer (CISO)**.
  - ✓ Managers may have responsibility for a domain, such as building control, ICT, or accounting.
  - ✓ Technical and specialist staff have responsibility for implementing, maintaining, and monitoring the policy.
  - ✓ Non-technical staff have the responsibility of complying with policy and with any relevant legislation.

INFORMATION SECURITY BUSINESS UNITS

1. Security Operations Center (SOC)

- A **security operations center (SOC)** is a location where security professionals monitor and protect critical information assets across other business functions, such as finance, operations, sales/marketing, and so on.

INFORMATION SECURITY BUSINESS UNITS (cont.)

2. Incident Response

- A dedicated **cyber incident response team (CIRT)/computer security incident response team (CSIRT)/computer emergency response team (CERT)** as a single point-of-contact for the notification of security incidents.
- This function might be handled by the **SOC**, or it might be established as an independent business unit.

1.1- Compare and Contrast Information Security Roles

1.2- Compare and Contrast Security Control And Framework Types

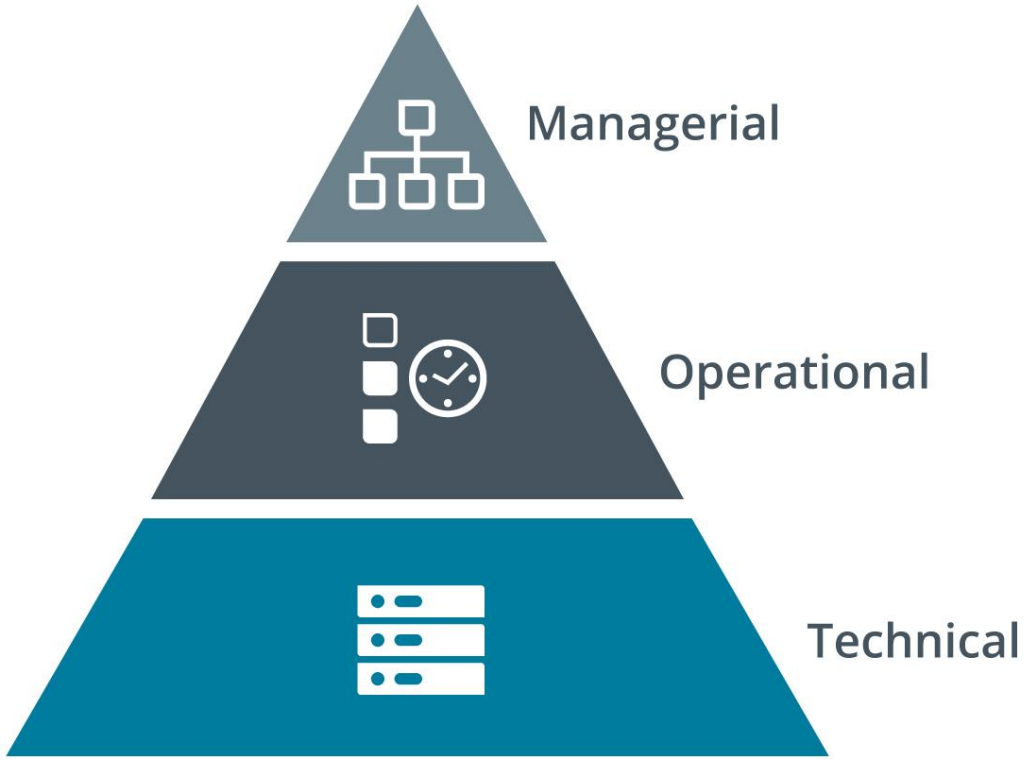
SECURITY CONTROL CATEGORIES

- Information and cybersecurity assurance is usually considered to take place within an overall process of **business risk management**.
- Implementation of cybersecurity functions is often the **responsibility of the IT department**.
- Some organizations have developed IT service frameworks to provide best practice guides to implementing IT and cybersecurity.
- These frameworks can shape company policies and provide checklists of procedures, activities, and technologies that should ideally be in place.

SECURITY CONTROL CATEGORIES (cont.)

- A **Security Control** is something designed to give a system or data asset the properties of **confidentiality**, **integrity**, **availability**, and **non-repudiation**.
- Controls can be divided into three broad categories, representing the way the control is implemented:
  - ✓Technical—the control is implemented as a system (hardware, software, or firmware), For example, firewalls, antivirus software, and OS access control models are technical controls. Technical controls may also be described as logical controls.
  - ✓Operational—the control is implemented primarily by people rather than systems, For example, security guards and training programs are operational controls rather than technical controls.
  - ✓Managerial—the control gives oversight of the information system, Examples could include risk identification or a tool allowing the evaluation and selection of other security controls.

SECURITY CONTROL CATEGORIES (cont.)



SECURITY CONTROL FUNCTIONAL TYPES

- Security controls can also be classified in types according to the **goal** or **function** they perform:

  ✓Preventive—the control acts to eliminate or reduce the likelihood that an attack can succeed, A preventative control **operates before an attack can take place**, Access control lists (ACL) configured on firewalls and file system objects are preventative-type controls, Anti-malware software also acts as a preventative control, by blocking processes identified as malicious from executing.

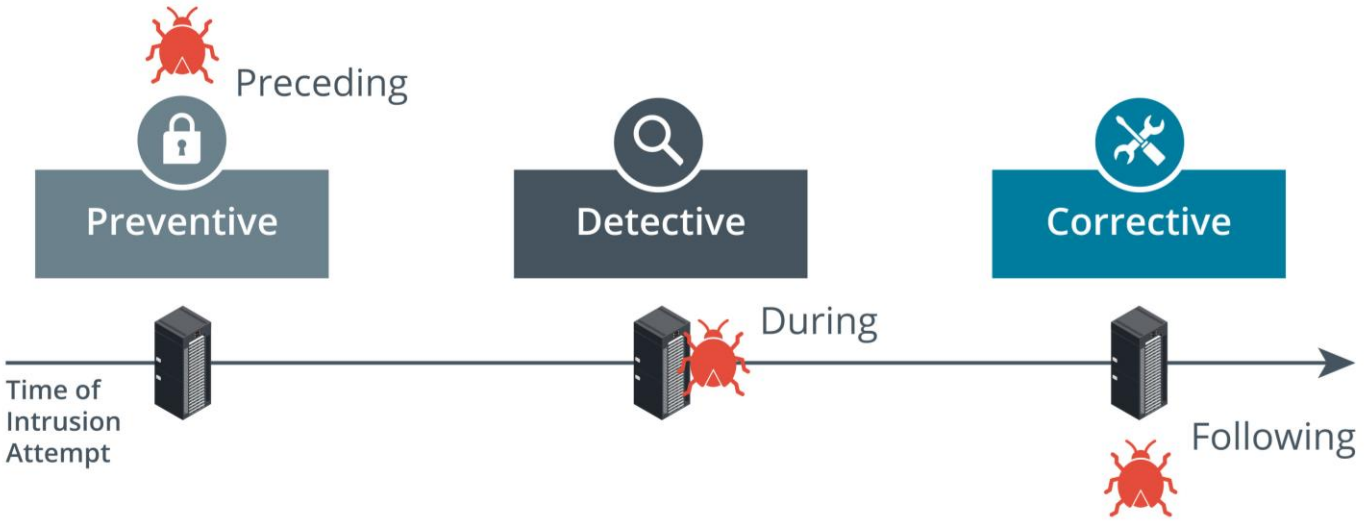
  ✓Detective—the control may not prevent or deter access, but it will identify and record any attempted or successful intrusion, A detective control **operates during the progress of an attack**, Logs provide one of the best examples of detective-type controls.

SECURITY CONTROL FUNCTIONAL TYPES (cont.)

- Security controls can also be classified in types according to the **goal** or **function** they perform (cont.)

  ✓Corrective—the control acts to eliminate or reduce the impact of an intrusion event, A corrective control is **used after an attack**, A good example is a backup system that can restore data that was damaged during an intrusion, Another example is a patch management system that acts to eliminate the vulnerability exploited during the attack.

SECURITY CONTROL FUNCTIONAL TYPES (cont.)



Other Control Functional Types:

Physical	Compensating	Deterrent

SECURITY CONTROL FUNCTIONAL TYPES (cont.)

- While most controls can be classed functionally as preventative, detective, or corrective, a few other types can be used to define other cases:

  - ✓Physical—controls such as alarms, gateways, locks, lighting, security cameras, and guards that deter and detect access to premises and hardware are often classed separately.
  - ✓Deterrent—the control may not physically or logically prevent access, but psychologically discourages an attacker from attempting an intrusion, This could include signs and warnings of legal penalties against trespass or intrusion.
  - ✓Compensating—the control serves as a substitute for a principal control, as recommended by a security standard, and affords the same (or better) level of protection but uses a different methodology or technology.

ISO AND CLOUD FRAMEWORKS

- The **International Organization for Standardization (ISO)** has produced a cybersecurity framework in conjunction with the **International Electrotechnical Commission (IEC)**.
- The framework was established in 2005 and revised in 2013.
- **ISO 27001** is part of an overall 27000 series of information security standards, also known as **27K**.
- Of these, **27002 classifies security controls**, **27017 and 27018 reference cloud security**, and **27701 focuses on personal data and privacy**.

ISO AND CLOUD FRAMEWORKS (cont.)

- ISO 31K (iso.org/iso-31000-risk-management.html) is an overall framework for **enterprise risk management (ERM).**
- **ERM** considers risks and opportunities beyond cybersecurity by including financial, customer service, competition, and legal liability factors.
- **ISO 31K** establishes best practices for performing risk assessments.
- The not-for-profit organization **Cloud Security Alliance (CSA)** produces various resources to assist **cloud service providers (CSP)** in setting up and delivering secure cloud platforms.
- These resources can also be useful for cloud consumers in evaluating and selecting cloud services.