CENTRAL UNIVERSITY

FAITH • INTEGRITY • EXCELLENCE

School Of Engineering & Technology
Department of Computer Science &
Information technology

**Name:** Nsiah Joshua

**Index number:** CSC/21/01/1022

**Course:** COMP 404 – COMPUTER SYSTEM SECURITY

**Assignment II**

**Date:** 15th May, 2025

## COMP 404 – COMPUTER SECURITY

### Questions

1. **Briefly describe management, operational, and technical controls, and explain when each would be applied as part of a security framework.**
**Ans:**

**Define**
Management, operational, and technical controls are the three primary categories of security safeguards used to protect information systems:

**Management controls** (administrative controls) are the policies and procedures that govern security
**Operational controls** (procedural controls) are the day-to-day security mechanisms implemented by people
**Technical controls** (logical controls) are the technology-based protections implemented in systems

**How It Works**
These controls work together in a security framework:

**Management controls** establish the security governance structure through risk assessments, policies, and training programs
**Operational controls** put these policies into practice through activities like backup procedures, incident response, and physical security
**Technical controls** enforce security through systems like firewalls, encryption, and access control mechanisms

**Benefits**
Provides comprehensive, layered security (defense in depth). Aligns security with organizational objectives through management controls

**Operational controls** ensure consistent security practices
**Technical controls** provide automated, scalable protection
Meets compliance requirements for most security frameworks

**Challenges**
Management: Policies may become outdated or ignored

**Operational:** Requires ongoing staff training and compliance monitoring
**Technical:** Can be complex to implement and maintain properly
**Integration challenges** between different control types
**Resource-intensive** to implement all three effectively

**How to Resolve Challenges**
Regular policy reviews and updates for management controls
Comprehensive training and documented procedures for operational controls
Continuous monitoring and testing of technical controls
Clear assignment of responsibilities for each control type
Periodic audits to ensure all controls are working together effectively

**Application in Security Frameworks:**
Each type is applied at different levels:
Management controls are applied first to establish the security program foundation
Operational controls are implemented to ensure security on a daily basis
Technical controls are deployed to protect specific systems and data
All three are typically required simultaneously in frameworks like NIST CSF, ISO 27001, or CIS Controls.

2. **What is the purpose of the SETA program?**
**Ans:**

**Define**

The SETA (Security Education, Training, and Awareness) program is a comprehensive approach to developing an organization's human firewall. It's a structured initiative designed to educate employees about security risks, train them on proper procedures, and maintain ongoing awareness of cybersecurity threats.

**How It Works**

The SETA program operates through three key components:
**Security Education**: Provides foundational knowledge about security concepts and policies
**Security Training**: Offers specific skill development for security-related tasks
**Security Awareness**: Maintains constant vigilance through regular reminders and updates
It typically includes formal training sessions, simulated phishing exercises, security newsletters, and mandatory compliance training.

**Benefits**

- Reduces human error (the cause of most security breaches)
- Creates a security-conscious organizational culture
- Helps meet regulatory compliance requirements (like HIPAA, GDPR)
- Empowers employees to recognize and report security threats
- Lowers overall organizational risk profile
- Improves incident response through better-prepared staff

**Challenges**

- Employee resistance or disengagement with training
- Keeping content relevant as threats evolve
- Measuring program effectiveness quantitatively
- Resource-intensive to develop and maintain
- Language/cultural barriers in global organizations
- Information overload leading to disengagement

The fundamental purpose of the SETA program is to transform employees from potential security vulnerabilities into active participants in organizational defense by equipping them with the knowledge, skills, and mindset needed to protect company assets and data.

3. **What are the differences between a policy, a standard, and a practice?**
**Ans:**

**Define**
**Policy:** A policy is a high-level statement that outlines an organization's principles and expectations regarding security. It defines what must be done but not how it will be done.
Example: "All employees must use strong passwords to access corporate systems."

**Standard:** A standard provides specific mandatory rules to support the policy. It offers detailed, measurable requirements.
Example: "Passwords must be at least 12 characters and include a mix of upper/lowercase, numbers, and symbols."

**Practice (or Procedure):** A practice or procedure provides step-by-step instructions on how to implement the standard or policy.
Example: "To reset your password, go to the Settings page, click 'Change Password', and follow the prompts..."

**What it does**
Policies set the foundation and expectations across the organization.
Standards ensure consistent implementation of the policies across systems and departments.
Practices provide a practical, repeatable method for users or admins to follow the standards.
Together, these three ensure that security controls are clear, enforceable, and actionable at all levels of the organization.

**Benefits or Advantages**

- Clear alignment between business objectives and security actions.
- Consistency across departments and systems.
- Accountability and enforceability of security rules.
- Helps meet compliance requirements (e.g., ISO 27001, NIST, GDPR).
- Reduces risk by minimizing ambiguity in security responsibilities.

**Challenges or Difficulties Associated**

- Employees may not understand or follow them properly.
- Policies may become outdated with evolving technology or threats.
- Difficulties in balancing strict standards with usability.
- Resistance to change from staff or departments.

**How to Resolve the Challenges**

- Regularly review and update policies, standards, and practices.
- Ensure clear communication and training across all staff levels.
- Involve stakeholders in policy development to increase buy-in.
- Use monitoring tools to verify compliance and spot deviations.
- Provide accessible documentation and support to clarify procedures.

4. **How can a security framework assist in the design and implementation of a security infrastructure?**

**Ans:**

**Define**

A security framework is a structured set of guidelines, best practices, standards, and policies that help organizations protect their information systems from threats. It provides a roadmap for building, assessing, and managing cybersecurity practices effectively.

**How it works**

- A security framework assists in the design and implementation of a security infrastructure by:
- Guiding Risk Assessments: Identifies what needs protection and how to prioritize threats.
- Defining Roles & Responsibilities: Specifies who is responsible for which controls and processes.
- Standardizing Controls: Ensures the use of proven technical, operational, and management practices.
- Benchmarking Progress: Helps measure the maturity of an organization's security.
- Enabling Compliance: Aligns infrastructure with legal and regulatory requirements.

**Benefits**

- Consistent and structured approach to building and maintaining secure systems.
- Improves risk management by prioritizing critical assets and vulnerabilities.
- Facilitates compliance with regulatory standards like GDPR, HIPAA, or PCI-DSS.
- Enhances communication between technical and non-technical stakeholders.
- Helps in planning budgets and resource allocation based on risk.
- Reduces duplication of efforts and improves operational efficiency.

**Difficulties Associated**

- Complexity: Frameworks can be large and difficult to fully understand or implement.
- Resource Intensive: Implementation may require skilled staff, time, and budget.
- Resistance to Change: Some staff may be unwilling to adjust to new procedures.
- Overgeneralization: Frameworks may not always address organization-specific needs.
- Keeping up-to-date: Evolving threats require frequent updates and reviews.