

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. **What is risk appetite? Explain why risk appetite varies from organization to organization.**

**Ans:**

**Define**

Risk appetite is the amount and type of risk that an organization is willing to accept or tolerate in pursuit of its objectives. It serves as a boundary that guides decision-making about which risks to take, mitigate, transfer, or avoid. Think of it as a strategic compass, helping organizations balance opportunity and risk while achieving goals.

**How it works**

Risk appetite is set by executive leadership and typically documented in a risk management policy. It affects:

**Decision-making:** Determines which risks are acceptable and which must be managed more closely.

**Investment choices:** Guides how much risk to assume when investing in new projects or technologies.

**Security measures:** Influence how strict or flexible controls need to be.

**Compliance strategies:** Help define which risks must be managed to meet regulatory requirements.

**Benefits**

**Improved decision-making:** Ensures alignment between risk exposure and business strategy.

**Resource optimization:** Helps allocate resources where they are most needed based on acceptable risk levels.

**Enhances communication:** Creates clarity and consistency across departments about risk-related decisions.

**Supports compliance:** Shows auditors and regulators that the organization understands and manages its risks.

**Enables innovation:** Encourages calculated risk-taking in areas aligned with the organization’s values and capacity.

1. **In risk management strategies, why must periodic reviews be a part of the process?**

**Ans:**

**Define**

Periodic reviews in risk management refer to scheduled reassessments of an organization’s risk landscape, controls, and mitigation strategies. These reviews ensure that risk management remains aligned with evolving threats, business objectives, and regulatory requirements**.**

**How It Works**

* Evaluates Current Risks: Identifies new threats (e.g., emerging cyberattacks) or changes in existing risks.
* Assesses Control Effectiveness: Checks if implemented safeguards (firewalls, policies) still work.
* Updates Risk Appetite: Adjusts tolerance levels based on business growth or industry shifts.
* Ensures Compliance: Verifies alignment with updated laws (GDPR, NIST, ISO 27001).
* Informs Decision-Making: Provides data for budget allocations and strategic pivots.

**Benefits / Advantages**

* Proactive Risk Mitigation: Catches vulnerabilities before exploitation
* Cost Savings: Prevents wasteful spending on outdated controls.
* Regulatory Adherence: Avoids fines by maintaining compliance.
* Business Continuity: Reduces downtime from unaddressed risks.
* Stakeholder Trust: Demonstrates commitment to robust risk practices.

**Difficulties**

* Resource Intensive: Requires time, expertise, and tools for thorough reviews.
* Dynamic Threat Landscape: Cyber risks evolve faster than review cycles.
* Stakeholder Resistance: Leadership may deprioritize reviews for short-term gains.
* Data Overload: Large datasets can obscure critical risks.
* Inconsistent Methods: Ad-hoc reviews lead to gaps in risk visibility.

1. **According to Sun Tzu, what two things must be achieved to secure information assets successfully?**

**Ans:**

**Define**

According to Sun Tzu's "The Art of War" (applied to cybersecurity), two fundamental things must be achieved:

**Know Yourself**: Complete understanding of your own information assets, systems, and vulnerabilities

**Know Your Enemy:** Comprehensive awareness of potential attackers, their methods, and motivations

**How It Works**

These principles work by:

**Know Yourself:** Conducting thorough asset inventories, risk assessments, and vulnerability scans

**Know Your Enemy:** Performing threat modeling, adversary analysis, and intelligence gathering

Together they create a defensive strategy that's both internally aware and externally vigilant

**Benefits/Advantages**

* Creates a 360-degree security posture
* Enables proactive rather than reactive defense
* Helps prioritize security investments effectively
* Improves incident response capabilities
* Reduces attack surfaces by understanding both sides
* Aligns security with business objectives

**Challenges**

**Know Yourself:**

* Difficulty maintaining accurate asset inventories
* Organizational silos hiding complete picture
* Constantly changing IT environments

**Know Your Enemy:**

* Attackers constantly evolve tactics
* Limited threat intelligence resources
* Difficulty predicting novel attack vectors

1. **What is risk management?**

**Ans:**

Risk management is the systematic process of identifying, assessing, prioritizing, and mitigating risks to an organization’s information assets, operations, and reputation. It involves balancing potential threats with business objectives to minimize harm while enabling growth.

Key Components:

Risk Identification (What could go wrong?)

Risk Assessment (How bad would it be?)

Risk Mitigation (How do we reduce the risk?)

Risk Monitoring (Is our strategy working?)

**How It Works**

Risk management follows a structured lifecycle:

**Identify Risks:** Catalog assets (data, systems), threats (hackers, outages), and vulnerabilities (weak passwords, unpatched software).

**Assess Risks:** Evaluate likelihood and impact.

**Prioritize Risks:** Rank risks using a matrix

**Treat Risks:** Apply controls

**Monitor & Review:** Continuously track risks and adjust strategies.

**Frameworks Used:** NIST RMF, ISO 27005, COBIT, FAIR.

**Benefits**

**Proactive Defense:** Prevents incidents before they occur.

**Cost Efficiency:** Allocates resources to high-impact risks.

**Regulatory Compliance:** Meets GDPR, HIPAA, and PCI DSS requirements.

**Business Continuity:** Minimizes downtime and financial losses.

**Stakeholder Confidence:** Builds trust with customers and investors.

**Challenges / Difficulties**

**Dynamic Threat Landscape:** Cyber risks evolve faster than defenses.

**Resource Constraints:** Limited budget/expertise for small organizations.

**Subjectivity:** Risk assessments can be biased or inconsistent.

**Over-Mitigation:** Excessive controls may hinder productivity.

**Siloed Data:** Poor communication between departments obscures risks.

1. **Describe residual risk.**

**Ans:**

Residual risk is the remaining level of risk that persists after an organization has implemented security controls and mitigation measures. It represents the "leftover" risk that the organization consciously accepts because:

* The cost of further mitigation outweighs the potential impact.
* The risk falls within the organization’s risk appetite.

**How It Works**

**Post-Mitigation Measurement:** Residual risk is calculated by assessing:

Inherent Risk (original risk before controls).

Effectiveness of Controls (e.g., encryption reduces data breach risk by 70%).

**Formula:**

Residual Risk = Inherent Risk − Risk Reduced by Controls

**Decision Point:** Organizations compare residual risk to their risk tolerance to decide if additional action is needed.

3. Benefits / Advantages

Informed Decision-Making: Clearly shows what risks remain after mitigation.

Cost Efficiency: Avoids over-spending on excessive controls.

Compliance Alignment: Meets regulatory requirements (e.g., ISO 27001 mandates residual risk assessment).

Transparency: Helps stakeholders understand accepted risks.

4. Challenges / Difficulties

Subjectivity: Hard to quantify precisely (e.g., "How much risk is 'acceptable'?").

Control Failures: Residual risk rises if controls are ineffective or misconfigured.

Dynamic Threats: New vulnerabilities can increase residual risk unexpectedly.

Over-Reliance on Controls: Assuming "set and forget" safeguards creates false confidence.

5. How to Resolve Challenges

Quantify Risks: Use models like FAIR to assign monetary values to residual risk.

Continuous Monitoring: Deploy SIEM tools to detect control gaps in real-time.

Risk Acceptance Policies: Document which residual risks are explicitly accepted (with leadership approval).

Red Team Exercises: Test controls to validate residual risk assumptions.

Insurance: Transfer residual risk via cyber insurance policies.