IT Security Management and Risk Assessment

1. IT Security Management

Definition: A formal process to protect IT assets by ensuring confidentiality, integrity, availability, accountability, authenticity, and reliability.

Core Questions:

- What assets need protection?
- How are these assets threatened?
- What measures can counter these threats?

Steps in IT Security Management:

1. Define security objectives, strategies, and policies.
2. Conduct risk assessments for IT assets.
3. Select cost-effective controls to mitigate risks.
4. Develop and implement security plans and procedures.
5. Monitor operations and maintain control effectiveness.
6. Detect and respond to incidents.

Iterative Nature: The process is cyclic due to the rapid changes in technology and risks.

2. Standards for IT Security

ISO/IEC 27000 Series:

- ISO 27001: Requirements for Information Security Management Systems (ISMS).
- ISO 27002: Best practices for information security management.

- ISO 27005: Guidelines for risk management in information security.

NIST Standards (U.S.):

- SP 800-18: Guide for developing security plans.

- SP 800-30: Guide for conducting risk assessments.

- SP 800-53: Security and privacy controls.

3. The Plan-Do-Check-Act Model

A cyclical process for managing IT security:

- Plan: Establish policies, perform risk assessments, and develop treatment plans.

- Do: Implement the treatment plan.

- Check: Monitor effectiveness.

- Act: Improve processes based on incidents or changes.

4. Organizational Context and Security Policy

Key Considerations:

- Assess the role of IT systems in achieving organizational goals.

- Identify critical data requiring protection.

- Evaluate consequences of security failures.

Components of a Security Policy:

- Scope, purpose, and alignment with legal/business objectives.

- IT security requirements (confidentiality, integrity, etc.).

- Assignment of responsibilities for IT security management.

- Risk management approach.

- Security awareness and training programs.
- Personnel issues (e.g., positions of trust).
- Legal sanctions for violations.
- Integration of security into system development/procurement.
- Information classification schemes.
- Contingency planning and incident handling processes.
- Policy review schedule and change control methods.

5. Security Risk Assessment Approaches

- Baseline Approach: Uses standard controls as a baseline for protection but lacks flexibility for unique risks.
- Informal Approach: Relies on expert judgment without formal documentation or analysis.
- Detailed Risk Analysis: Provides a thorough examination of threats, vulnerabilities, and consequences but is resource-intensive.
- Combined Approach: Balances simplicity with thoroughness by combining elements of the above methods.

6. Detailed Risk Analysis Process

1. Context Establishment: Define the system scope and environment.
2. Threat Identification: Identify potential threats, risks, and vulnerabilities.
3. Risk Analysis: Assess the likelihood and impact of risks.
4. Risk Evaluation: Compare risks against acceptable thresholds to prioritize actions.
5. Risk Treatment:
   - Accept the risk if it is within acceptable limits.
   - Mitigate through controls or transfer (e.g., insurance).

- Avoid by discontinuing risky activities.

7. Case Study: Silver Star Mines

A practical example demonstrating how an organization can apply IT security management principles to address specific challenges.