

Insider Threat in a Healthcare Organization

➤ **Group : 2**

Group member :

- | | |
|--------------------------|------------------|
| 1. Tushar Solanki | (2536692) |
| 2. Diya Patel | (2532979) |
| 3. Priti Bhoi | (2540464) |
| 4. Dhaval Rami | (2528086) |
| 5. Dhokiya Harsh | (2545109) |

Security Governance Principles, Policy Development, and Strategic Planning

1: Understanding Governance Components

1.1 Security Governance vs. Security Management

Organizations depend on information systems to support daily operations, making information security a business priority. To achieve effective protection, organizations require both **security governance** and **security management**. Although these concepts are related, they have different purposes and responsibilities.

Security Governance

Security governance is the process by which an organization's leadership directs and controls information security. It ensures that security objectives support the organization's strategic goals while protecting information assets and meeting legal, regulatory, and contractual obligations. Governance establishes accountability, defines risk tolerance, approves policies, and measures the effectiveness of the security programme.

The Board of Directors and executive management are responsible for governance because they determine the organization's security strategy and provide the resources needed to achieve it.

The key objectives of security governance include:

- Supporting business objectives through secure operations.
- Protecting organizational information and digital assets.
- Ensuring compliance with laws, regulations, and industry standards.
- Managing information security risks.
- Defining accountability and responsibilities.
- Monitoring the effectiveness of security controls.
- Encouraging continuous improvement.

Security Management

Security management is concerned with the practical implementation of security governance decisions. It focuses on planning, implementing, operating, monitoring, and maintaining security controls across the organization. Security managers and IT professionals ensure that policies are followed and that technical safeguards are functioning correctly.

Examples of security management activities include:

- Managing firewalls and intrusion detection systems.
- Conducting vulnerability assessments.
- Updating operating systems and software.
- Managing user access permissions.
- Investigating and responding to security incidents.
- Performing system backups and disaster recovery activities.
- Monitoring network traffic and system logs.

Differences Between Security Governance and Security Management

Security Governance	Security Management
Provides strategic direction for information security.	Executes the security strategy through operational activities.
Led by the Board of Directors and executive management.	Led by the Information Security Manager and IT staff.
Establishes policies, objectives, and risk appetite.	Implements technical controls and security procedures.
Focuses on long-term business value.	Focuses on daily security operations.
Measures organisational performance.	Maintains and improves security controls.

1.2 Key Governance Processes Based on ISO/IEC 27014:2013

ISO/IEC 27014 identifies six governance processes that enable organizations to effectively oversee information security.

Evaluate

The organization assesses its current security environment by identifying business objectives, analysing cyber risks, reviewing legal obligations, and understanding stakeholder expectations. This process helps management determine whether existing security arrangements are adequate.

Example: Before adopting cloud computing services, management evaluates potential risks related to data privacy and service availability.

Direct

Senior leadership establishes the organization's information security strategy by defining objectives, approving policies, assigning responsibilities, and providing sufficient financial and human resources.

Example: Management approves a policy requiring encryption of all confidential business information stored on laptops.

Monitor

The organization continuously monitors information security performance to ensure that policies are followed and security objectives are achieved. Monitoring involves reviewing audit reports, incident statistics, compliance results, and key performance indicators.

Communicate

Effective governance depends on clear communication between management, employees, contractors, and external stakeholders. Security policies, responsibilities, and updates must be communicated regularly through meetings, training sessions, emails, and awareness campaigns.

Assure

The organization obtains assurance that information security controls are effective through internal audits, independent assessments, penetration

testing, and compliance reviews. Assurance activities help identify weaknesses before they lead to security incidents.

Improve

Security governance is an ongoing process. Organizations should continuously improve their security framework by reviewing incidents, adopting new technologies, updating policies, and responding to changes in business operations or emerging cyber threats.

1.3 Role of Policies, Standards, and Guidelines

Security Policy

A security policy is a formal statement issued by senior management that defines the organization's commitment to protecting information assets. It establishes mandatory security requirements and provides a framework for managing information security risks.

Example: All employees must protect confidential business information from unauthorized disclosure.

Security Standards

Standards specify the technical and operational requirements that support the policy. They ensure that security controls are implemented consistently throughout the organization.

Examples:

- Passwords must contain a minimum of 14 characters.
- Multi-factor authentication must be enabled for remote access.
- Sensitive data must be encrypted using approved encryption methods.

Security Guidelines

Guidelines provide recommended practices that help employees comply with policies and standards. Unlike standards, guidelines are flexible and may be adapted to different situations.

Example: Employees should avoid opening email attachments received from unknown senders and should verify suspicious messages before responding.

Relationship Between Governance Documents

Information security governance follows a structured hierarchy:

1. **Policies** define what the organization expects.
 2. **Standards** specify mandatory technical requirements.
 3. **Procedures** explain how tasks should be performed.
 4. **Guidelines** provide recommended best practices.
-

2: High-Level Information Security Policy

Policy Title

Organization-Wide Information Security Policy

Purpose

The purpose of this policy is to establish a comprehensive framework for protecting the confidentiality, integrity, and availability of organizational information assets. The policy aims to reduce cyber risks, support business continuity, ensure compliance with legal and regulatory requirements, and maintain stakeholder confidence. It aligns with the governance principles of ISO/IEC 27014:2013 by promoting leadership, accountability, and continual improvement.

Scope

This policy applies to all employees, contractors, consultants, temporary workers, third-party service providers, and any individual who accesses organizational information systems. It covers all business applications, networks, cloud services, databases, mobile devices, and physical information assets owned or managed by the organization.

Roles and Responsibilities

Board of Directors

The Board is responsible for approving the information security strategy, reviewing governance performance, allocating appropriate resources, and ensuring that information security supports business objectives.

Senior Management

Senior management must ensure that security policies are implemented, communicate security expectations, support compliance, and encourage a culture of information security throughout the organization.

Information Security Manager

The Information Security Manager is responsible for conducting risk assessments, developing security policies and standards, coordinating

security awareness activities, managing security incidents, and reporting security performance to executive management.

IT Department

The IT Department implements technical controls such as access management, network security, system monitoring, software updates, data backups, and vulnerability management.

Employees

Employees are responsible for protecting organizational information, following security policies, completing mandatory training, reporting security incidents, safeguarding passwords, and using organizational systems responsibly.

Third-Party Providers

Third-party suppliers must comply with contractual security requirements, protect organizational information, and promptly report any security incidents affecting shared systems or services.

Standards and Procedures

To support the policy, the organization will implement several operational standards and procedures:

- Multi-factor authentication will be required for privileged and remote access.
- Access to systems will be granted based on job responsibilities and reviewed regularly.
- Passwords must comply with organizational complexity requirements.
- Sensitive information will be encrypted both during transmission and while stored.
- Security patches will be applied according to risk-based timelines.
- Daily backups will be performed and tested regularly.

- Security incidents must be reported immediately through the established incident response process.
- Risk assessments will be conducted annually and whenever significant changes occur.

Compliance and Enforcement

Compliance with this policy will be monitored through internal audits, external assessments, security monitoring tools, vulnerability scanning, penetration testing, and management reviews.

Failure to comply with the policy may result in disciplinary action, including mandatory retraining, suspension of system access, formal warnings, termination of employment, or legal action depending on the severity of the violation.

Alignment with ISO/IEC 27014:2013

This policy supports ISO/IEC 27014 by ensuring that leadership evaluates security risks, directs organizational security strategy, monitors security performance, communicates responsibilities, verifies compliance through assurance activities, and continually improves the information security programme based on audit results and changing threats.

3: Security Education, Training and Awareness (SETA) Programme

Programme Purpose

The purpose of the Security Education, Training and Awareness (SETA) programme is to ensure that all employees understand their responsibilities for protecting organizational information. The programme aims to strengthen cybersecurity awareness, reduce human error, improve compliance with security policies, and create a security-conscious organizational culture.

Topics Covered

The training programme will cover a broad range of information security topics, including:

- Introduction to information security principles
- Confidentiality, Integrity, and Availability (CIA)
- Organizational security policies and employee responsibilities
- Password management and multi-factor authentication
- Email security and phishing awareness
- Social engineering attacks
- Malware, ransomware, and spyware
- Safe internet browsing practices
- Data classification and information handling
- Privacy and data protection regulations
- Mobile device and remote working security
- Cloud security awareness
- Physical security controls
- Incident identification and reporting procedures
- Business continuity and disaster recovery awareness

- Emerging cybersecurity threats and artificial intelligence risks

Training Methods

The organization will use a combination of educational methods to ensure effective learning and employee engagement. These methods include instructor-led workshops, online learning modules, cybersecurity webinars, phishing simulations, tabletop exercises, awareness campaigns, newsletters, security posters, video demonstrations, new employee induction training, annual refresher courses, and practical exercises based on real-world cyber incidents.

Measuring Effectiveness

The effectiveness of the SETA programme will be measured using both quantitative and qualitative indicators, including:

- Training completion rates.
- Scores achieved in knowledge assessments.
- Results of phishing simulation exercises.
- Number of reported security incidents.
- Reduction in successful phishing attacks.
- Compliance audit findings.
- Employee feedback surveys.
- Reduction in policy violations.
- Improvement in incident response times.
- Overall improvement in organizational cybersecurity maturity.

Programme performance will be reviewed annually, and training materials will be updated regularly to address new technologies, emerging cyber threats, and changes in organizational security requirements.

➤ Conclusion

Effective information security depends on strong governance, clear policies, and a well-informed workforce. Security governance provides strategic direction, while security management ensures that policies are implemented through operational controls. By developing a comprehensive information security policy aligned with **ISO/IEC 27014:2013** and implementing a robust Security Education, Training and Awareness (SETA) programme, organizations can reduce cyber risks, improve regulatory compliance, and build a culture in which every employee contributes to safeguarding information assets and supporting long-term business success.