

Data Security Governance and Compliance

Week 4

Tutorial

Member of group:

- | | |
|----------------------------|------------------|
| 1. Janki Patel | (2520611) |
| 2. Nirav Thummar | (2537379) |
| 3. Sameer Sukhadiya | (2536690) |

Governance and Strategic Planning for Security

Scenario: Healthcare Management System (MediCare Solutions)

Objective

Apply security governance principles to develop security policies, align with international security frameworks, and integrate strategic planning to protect patient information stored in the Electronic Health Records (EHR) system.

1. Understanding Governance Components

1.1 Security Governance vs. Security Management

Security Governance

Security Governance is the process by which senior management directs and controls information security within an organisation. It ensures that security supports the organisation's goals, complies with legal and regulatory requirements, and manages risks effectively.

Main Responsibilities

- Define the organisation's security vision and strategy.
- Approve security policies.
- Allocate budgets and resources.
- Ensure compliance with regulations.
- Review security performance.
- Manage information security risks.

Example (MediCare Solutions)

The hospital board decides that all patient records must be encrypted, employees must complete annual cybersecurity training, and the organisation must comply with UK GDPR and healthcare regulations.

Security Management

Security Management focuses on implementing and maintaining the security controls defined by governance. It is responsible for the day-to-day operation of security systems and protecting organisational assets.

Main Responsibilities

- Configure firewalls.
- Monitor networks.
- Install security updates.
- Manage user accounts.
- Respond to security incidents.
- Perform system backups.
- Conduct vulnerability assessments.

Example (MediCare Solutions)

The IT department enables Multi-Factor Authentication (MFA), updates antivirus software, monitors suspicious login attempts, and performs daily backups of the Electronic Health Records system.

Difference Between Security Governance and Security Management

Security Governance	Security Management
Strategic approach	Operational approach
Managed by senior executives	Managed by IT and security teams
Defines security objectives	Implements security controls
Focuses on business goals	Focuses on daily security operations
Long-term planning	Short-term operational tasks

1.2 Key Governance Processes (ISO/IEC 27014:2013)

ISO/IEC 27014 provides guidance for governing information security within an organisation. The main governance processes include:

1. Evaluate

Purpose:

Assess security risks, organisational objectives, legal requirements, and the current security posture.

Activities:

- Identify sensitive patient information.
- Assess cybersecurity risks.
- Review existing security controls.
- Analyse business requirements.

Example:

MediCare Solutions identifies that ransomware attacks pose a high risk to Electronic Health Records.

2. Direct

Purpose:

Provide leadership by defining security objectives, policies, and responsibilities.

Activities:

- Develop security policies.
- Assign security roles.
- Approve budgets.
- Establish security standards.

Example:

Management approves the use of Role-Based Access Control (RBAC), Multi-Factor Authentication, and data encryption.

3. Monitor

Purpose:

Ensure security controls remain effective through continuous monitoring and improvement.

Activities:

- Conduct internal audits.
- Review security reports.
- Monitor compliance.
- Evaluate employee awareness.
- Improve security controls.

Example:

Quarterly security audits verify that only authorised doctors can access patient records.

1.3 Role of Policies, Standards, and Guidelines

Security Policy

A security policy defines **what must be done** to protect organisational information.

Characteristics:

- Mandatory
- Approved by senior management
- High-level document

Example:

All patient information must remain confidential and only authorised personnel may access Electronic Health Records.

Security Standard

Security standards define **how security policies are implemented** through mandatory technical requirements.

Characteristics:

- Mandatory
- Technical requirements
- Consistent implementation

Examples:

- Passwords must contain at least 12 characters.
 - Multi-Factor Authentication is mandatory.
 - AES-256 encryption must be used for patient data.
-

Security Guideline

Guidelines provide **recommended best practices** to help employees follow policies and standards.

Characteristics:

- Optional but recommended
- Flexible
- Improve security awareness

Examples:

- Lock your computer before leaving your workstation.
 - Avoid opening suspicious email attachments.
 - Use secure hospital Wi-Fi when accessing patient records.
-

2. Policy Development Exercise

High-Level Security Policy

Purpose

The purpose of this policy is to protect patient information, maintain the confidentiality, integrity, and availability of Electronic Health Records (EHR), reduce cybersecurity risks, and ensure compliance with healthcare regulations.

Scope

This policy applies to:

- Doctors
 - Nurses
 - Pharmacists
 - Administrative staff
 - IT staff
 - Contractors
 - Third-party service providers
 - Students and trainees accessing hospital systems
-

Roles and Responsibilities

Senior Management

- Approve security policies.
- Provide funding.
- Ensure compliance.
- Review security performance.

IT Security Team

- Maintain firewalls and antivirus.
- Monitor security logs.
- Perform backups.

- Manage access controls.
- Respond to security incidents.

Employees

- Protect passwords.
- Follow security procedures.
- Report suspicious activities.
- Complete cybersecurity training.

Patients

- Keep patient portal passwords secure.
 - Report suspicious account activity.
-

Standards and Procedures

The organisation will implement:

- Multi-Factor Authentication (MFA)
 - Role-Based Access Control (RBAC)
 - Data encryption
 - Daily automated backups
 - Antivirus and endpoint protection
 - Firewalls
 - Security monitoring
 - Regular vulnerability assessments
 - Patch management
 - Incident response procedures
-

Compliance and Enforcement

Employees must comply with:

- UK GDPR
- Hospital security policies

- Healthcare information governance requirements

Violations may result in:

- Verbal warning
 - Written warning
 - Mandatory retraining
 - Suspension of system access
 - Disciplinary action
 - Legal action where appropriate
-

Alignment with ISO/IEC 27014:2013

The policy aligns with ISO/IEC 27014 by:

- Supporting executive leadership and accountability.
 - Aligning information security with organisational goals.
 - Managing information security risks.
 - Ensuring compliance with legal requirements.
 - Promoting continual improvement through monitoring and audits.
-

3. Strategic Planning & Security Awareness

Security Education, Training, and Awareness (SETA) Program

Objective

The SETA program aims to educate employees about cybersecurity risks, promote secure behaviour, and reduce human error that could compromise patient information.

Topics Covered

- Information security awareness
- Patient data privacy and confidentiality
- Password management
- Multi-Factor Authentication (MFA)

- Phishing and email security
 - Social engineering attacks
 - Ransomware prevention
 - Safe internet usage
 - Mobile device security
 - Incident reporting procedures
 - Data classification and handling
 - Secure use of Electronic Health Records (EHR)
-

Training Methods

- Classroom workshops
 - Online e-learning modules
 - Phishing simulation exercises
 - Cybersecurity awareness videos
 - Posters and awareness campaigns
 - Monthly security newsletters
 - Annual refresher training
 - Incident response drills
-

Measuring Effectiveness

The effectiveness of the SETA program will be measured using:

- Employee training completion rates
- Quiz and assessment scores
- Phishing simulation success rates
- Reduction in security incidents
- Internal audit results
- Compliance audit findings
- Employee feedback surveys

- Number of reported security incidents
 - Improvement in policy compliance
-

Conclusion

By implementing strong security governance, a comprehensive security policy, and an effective Security Education, Training, and Awareness (SETA) program, MediCare Solutions can protect sensitive patient information, comply with healthcare regulations, reduce cybersecurity risks, and ensure the confidentiality, integrity, and availability of its Electronic Health Records (EHR) system. This approach follows the governance principles of **ISO/IEC 27014:2013**, ensuring that information security supports organisational objectives and promotes continuous improvement