Production and Operation Management

Farid Mehdiyev

IT Process and Design

ITIL – Information

Security Management

Table of Contents

Introduction

This paper provides detailed overview of the Information Security Management (ISM) that is in relation to healthcare company. By choosing ISM aims that how important is information security in the healthcare sector that provided (CIA) integrity, confidentiality, availability data of the patient and suggesting that improving data security throught the industry. This International Standard is applicable and meant to by all kinds of organizations regardless it is sizes, type or nature.

Information Security Management Purposes, objectives, scopes

Purposes: Management of the information security is one of the primary evolutions of the information technology sector. In the era of the modern world technology – digital transformation comes with some obstacles – which is not securing data efficiently. Information Security Management (ISM) creates policies, processes, and control into that creates a system that is continuously monitors, instructs, and improves information security. ISM detailed all the mitigation necessary to achieve infosec goals.

Goals: One of the significant purpose or the goal of the Information Security management is ensuring that all the sensitive information such as Personal Health Information (PHI), Personally Identifiable Information (PII) and others are protected and minimized all of the risks to the lowest level and likewise ensuring operational (business) continuity without any interruption.

Objectives:

- Increasing importance of the information security within the organization that is strongly essential for the patient's confidentiality of data, availability and integrity.
- Robusting security of the Information Security Monitoring System (ISMS) for tracking and analyzing all the threats without any interruption
- By tracking and analyzing all the vulnerabilities maximized improvements as a continuous regularly with the updating all the details or reviewing information.
- Evaluating and detecting risks for the critical information that is established robust risk management.

Scope: In today's world cyber attacks and data breaches present a threat and vulnerability to the organizations. Business need to put in place a strong Information Security Management System (ISMS) to reduce these risks and improve integrity of the data.

- **Encryption and Data Protection –** sending information securely and ensuring data security comes with the practice of data encryption
- **Risk Management and Assessment –** identifying vulnerability and threats and mitigating security risks that is included in regular risk assessments.
- **Development of Policy and management** – Guiding with the best practices and requirements for compliance through the creation, maintenance, and administration of the security policies inside the company.

Benefits

In the constantly evolving landscape of the cybersecurity world – Information Security Management Systems (ISMS) has been brought as significant amount of the advantages. By implementing productive and effective Information Security Management processes will lead to achieve several quantitative and qualitative benefits for the Customers and likewise IT Service Providers.

Benefits to IT Service Providers

- **Strong client relationships** – improving trust and credibility of the clients building importance place of the data security which is dealing with the Protected Health Information (PHI)
- **Compliance with regulations** – by the following well-driven ISMS can lead to reducing risk of the legal complications and penalties
- **Security of Breaches** – Healthcare services has a strong relationship where breaches for integrity of data and patient safety – reducing incidents of the security and risk of the data breaches.
- **Operational Efficiency** – by implementation of the ISMS is resulted eliminating repetitive and minimizing not necessary tasks to make it more effective and efficient.

Benefits to Customers

- **Legal documentation** - Having part of the legal, regulatory and governance requirements.
- **Service Quality** – ISMS lead to healthcare providers to having high level of the security standards that is experienced by customers for better healthcare services because of the efficient way of operations and focusing on security

Roles, Responsibilities and authorities

Information Security Management Process Owner

Role	This person is for handling and supervising all of the information security processes within the company
Responsibilities	• Continuously monitoring and analyzing vulnerabilities and security threats • Updating and Reviewing all the security for evolving from threats and improving without any interruption as a continuously • Ensuring that Information Security Management process is fit to the purpose
Authority	• Implementing risk assessments to identify threats and vulnerabilities • Implementing strategies of the risk mitigation for saving organization's assets of information

Chief Information Security Officer (CISO)

Roles	This person is for policies and compliance, guides and overall security of the strategies
Responsibilities	• Guiding policies and compliances over the organization • Leading strategical and tactical responsibilities of the security • Ensuring integrity, confidentiality and security • Serving and Planning long-term security risks
Authority	• Implementing risks of mitigation strategies and allocate them • Implementing everyday security operations and ensuring that all of the operations are in monitoring and responding to the security attacks or incidents.

IT Security Manager

Roles	This person is controlling and managing accessing to the controls, encryption and decryption and firewalls
Responsibilities	• Managing infrastructure of the security such as configuration, maintenance and deployment • Controlling firewalls, intrusion detection systems (IDS) and Virtual

	Private Networks (VPN) • Ensuring that controlling and implementation of the Data Loss Prevention (DLP) systems • Strongly created backups of data and systems.
Authority	• Setting accessing of the roles, privileges and users to ensure that having access to the sensitive data • Ensuring that responding to the incidents and leading the investigations

Incident Response Team

Role	This person is coordinating the responses to the security incidents and breaches
Responsibility	• Monitoring and analyzing systems of the security to detecting signs of security incidents • Immediately actioning to prevent incident and also preventing further attacks
Authority	• Investigating incidents and gathering information

CSF (Critical Success Factor)

Critical Success Factor (CSF) is important components for creating successful implemented and managed Information Security Management Systems (ISMS)

- **Regular Risk and Risk Management Assessment** – Healthcare information systems must have an effective risk and risk management procedures to detect any of vulnerabilities and threats. Regular assessments serve to address the risk in a proactive way, minimizing the chance of an incident.

- **Respond Incidents and Business Continuity** – Organization's business continuity and responding incident's on time to security incidents are one of the essential components of applying efficient and effective Information Security Management operations for having minimized impact to the data security.

- **Training employee** – Staff with the proper training knowledge is one of the critical success points for ISMS. For creating safe work environment, employees are
made more aware of new security concerns and encouraged to adopt best pract ices by regular training sessions on security regulations

- **Commitment and Support of Executive -** The effectiveness of ISMS depends critically on the strong commitment of senior management. Information security must be given high importance by upper management, which also has to allocate the necessary funds for security program coverage and present a clear roadmap for security activities. They have to make sure that security is a top priority at all times.

KPS (Key Performance Indicators)

- **Response time of Incident** – Responding an incidents amount of the short time will reduce the critical impact of the breaches of the security on healthcare operations and patient data
- **Recovery Plans –** effectiveness of the business continuity and disaster recovery plans are included metrics such as Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) that in how quickly an organization able to recover after a disruption
- **Regulation compliance –** Measuring number of the compliance violations or regulatory breaches

Key Terms and Definitions

ISMS (Information Security Management System) – framework that brings processes, controls and policies for providing strong security within an organization.
PHI (Personal Health Information) – Health details about individual's medical history and services received by and individual.
PII (Personally Identifiable Information) – Information related to a named or identifiable natural person.
Encryption – used for the critical information or data that is in the secure format for preventing unauthorized access
Incident Response – Minimizing impact of the attacks to the security breaches and restoring normal operations.
CIA Triad – Model for the information security that is included Confidentiality, Integrity and Availability (CIA) for implementing policies and tools.
Risk Assessment – Evaluating risks, analyzing threats and identifying them to information assets for prioritization of security efforts and implementing controls, processes or preventing vulnerabilities.
Compliance – Regulatory and law standards for the information security that meets with the requirements for protection of the important data.