Unit 4: Cyber Security Framework

4

Unit Structure

4.1 LEARNING OBJECTIVES

After studying this unit student should be able to:

- learn different cybersecurity-related frameworks which are essential for an organization to follow to create robust security infrastructure and enforce the strong policy mechanism.
- Understand compliances and regulatory frameworkto protect assets and data.

4.2 INTRODUCTION

We have already learned the concept of the importance of cybersecurity and many other technical aspects related to it. But it is also important to establish for an organization to comply according to business functions with security standards and norms which exist.

As there is a rise in a number of cyber attacks increases day by day on the different organization it has now become essential to protect their assets and data. So there are multiple compliances and regulatory framework which organization has to follow.

4.3CYBERSECURITY POLICY

The role of policy is to construct the guidelines and principles for the management. It will help them to take future decisions and serve them as an implementation roadmap. The policy has a clear and defined measure that how the organization will protect their assets and information systems and will make ensure it complies with legal and regulatory requirements.

The goal here is to protect the organization, its vendors, customers, partners, from the resulting effect of the intentional or accidental damage. Also to protect the integrity of the data and availability of the systems for the continuity of the business.

Cybersecurity policy is not easy to understand. They become useless if the employee, customers or stakeholders are unable to understand and follow. So it is very important to have a good cybersecurity policy in place.

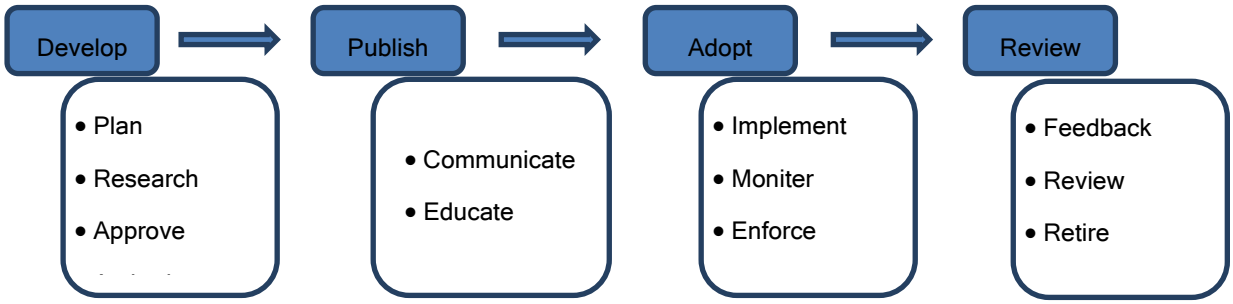

Figure 4.1 Cyber Security Policy Life Cycle

4.4 CYBER SECURITY REGULATIONS IN INDIA

Currently INDIA has the Information Act, 2000 and then it was revised in 2008 again. The Information Technology (Amendment) Bill, 2008 amended a number of sections that were related to digital data, electronic devices, and cybercrimes.

The Government approved a framework to enhance security in Indian cyberspace for cybersecurity with the National Security Council Secretariat functioning as the nodal agency.

The National Cyber Security Policy, 2013 was developed to build secure and resilient cyberspace for India's citizens and businesses.

The Ministry of Electronics and Information Technology said that the policy aims to protect information and the information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

Additionally, the Indian Computer Emergency Response Team (CERT-In) is responsible for incident responses including analysis, forecasts, and alerts on cybersecurity issues and breaches.

As the INDIA is moving towards digitization government has become more strict in the banking and financial sectors. As to provide security to the transactions and payments for the customers of banks is a must.

Due to the recent cyber-attacks on banks in India has left everyone worried. Such as Pune based Cosmos Bank recently saw a massive security breach where Rs 94 crore was siphoned off. In a similar incident, about $2 million was stolen from City

Union Bank through a cyber-attack. The Union Bank of India also fell prey to a hacking attempt and lost around $171 million, though they managed to recover it.

Taking into the account for the essential need to secure from cyber-attacks, Reserve Bank of India(RBI) which is the central regulatory and monitoring authority for controlling operations of banks in India. RBI has issued multiple circulars such as RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16 and circular RBI/2018-19/63, DCBS.CO.PCB.Cir.No. 1/18.01.000/2018-19, Dated 19th October 2018 for Urban Co-operative Banks for Cybersecurity Compliance.

All Urban Co-operative Banks are required to comply with the various guidelines prescribed and submit the report of Cyber Security Compliance after framing all the required policies and implementation of Cyber Security Controls.

Let us take look into the details given by RBI from both the circulars.

Cyber-security Policy: Banks has to immediately put in place the cybersecurity policy which contains a strategy that how the bank is dealing with the cyber threats and what is the readiness of the current defensive measures. Also to provide details regarding proper incident response and recovery framework. This policy needs to be approved from the board of members who are appointed by the RBI.

Also as per the RBI Cybersecurity policy should be different from the IT security policy of the bank.

Current State Assessment (As per RBI Cyber Security Framework)

1. Current State Security Assessment (CSSA)

    a. An interactive workshop to assess your current and desired state

    b. Security assessments that assess the current security landscape in your organization

    c. Recommendations for improvement

    d. The development of a security roadmap based on business and technology initiatives

2. CSSA - Value Proposition

    a. Org level view of data security control strengths and weaknesses

b. Understand business and technology risks

c. Identify critical, necessary and good-to-have controls

Drafting of Policies & Procedures & Implementation of Cyber Security Controls (As per RBI Cyber Security Framework)

Implementation

a. Security policies and procedures drafting & review
b. Risk assessment
c. Documentation structured storage and taxonomy
d. Compliance with RBI guidelines
e. Security Awareness Training

Implementation and Management of CSOC (As per RBI Cyber Security Framework): Continuous surveillance and real-time analysis were required as it helps in taking actions faster when attacked from outside. New guidelines would require banks to implement 24*7 real-time based surveillance.

Cyber Crisis Management Plan: The RBI circular calls for the establishment of a Cyber Crisis Management Plan to address the full lifecycle of detection, response, containment, and recovery. CCMP should address the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment. Banks need to take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond/recover/ contain the fallout.

Readiness Check/Audit to make sure that the RBI Cyber Security Framework has been successfully implemented.

National Cyber Security Policy, 2013: National Cyber Security Policy is a policy framework by Department of Electronics and Information technology (DeitY).

It aims at protecting public & private infrastructure from cyber attacks. It also intends to safeguard critical information such as personal information, financial & banking information, and sovereign data. Let us look into the details.

1. Set up of a 24×7 National Critical Information Infrastructure Protection Centre (NCIIPC) for obtaining strategic information regarding threats to ICT infrastructure,

creating scenarios for a response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.

2. Creation of a task force consisting of 5,00,000 cybersecurity professionals in the next five years through capacity building, skill development, and training.

3. Provision for fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cybersecurity.

4. Designation of CERT-In as the national nodal agency to coordinate cybersecurity-related matters and have the local (state) CERT bodies to coordinate at the respective levels.

5. All organizations to designate a CISO and allocate security budget.

6. Use of Open Standards for Cyber Security.

7. Development of a dynamic legal framework to address cybersecurity challenges (Note: The National Cyber Security Policy 2013 does not have any mention of the IT Act 2000)

8. Encouragement of wider use of Public Key Infrastructure (PKI) for government services.

9. Engagement of infosec professionals/organizations to assist e-Governance initiatives, establish Centers of Excellence, cyber security concept labs for awareness and skill development through PPP – a common theme across all initiatives mentioned in this policy.

10. Apart from the common theme of PPP across the cybersecurity initiatives, the policy frequently mentions of developing an infrastructure for evaluating and certifying trustworthy ICT security products.

4.5 CYBERSECURITY REGULATIONS IN OTHER COUNTRIES

Below are the major regulations entities in the European Union(EU)

European Union Agency for Network and Information Security(ENISA): An agency was initially organized by the regulation number 460/2004 of the European Parliament and of the Council of 10 March 2004 for the sole

purpose of raising information and security awareness for all the operations within the EU. ENISA currently runs under the regulation number 526/2013 which is the latest one. Their website has all the details related to the current policies, regulations and other cybersecurity related information. https://www.enisa.europa.eu.

EU General Data Protection Regulations(GDPR): It is created to maintain a single standard for the data protection among all the member states in the EU.

4.6 CYBERSECURITY POLICY FRAMEWORK

Now we will learn different cybersecurity policy framework for different business functions and understand how they are important.

Health Insurance Portability and Accountability Act(HIPAA): HIPAA was first enacted in 1996. HIPAA was established as a standard to protect the individuals' electronic personal health information(ePHI). To fulfill this U.S. Department of Health and Human Services(HHS) published the HIPAA Privacy Rule and HIPAA Security Rule.

Privacy rule deals with the standards set for the privacy of individually identifiable health information. Security Rule takes care of security standards for protecting health information that is in the electronic form. Security Rule’s goal is to secure individuals ePHI.

The components which are covers in this are allowed to adopt new technologies and to improve the quality and efficiency of patients care. It has been into light due to greater risk and data breaches in the healthcare sector.

Purpose of HIPAA:

It has two main purposes: to provide continuous health insurance coverage for workers who lose or change their job and to reduce the administrative burdens and cost of healthcare by standardizing the electronic transmission of administrative and financial transactions.

HHS expanded the act when it put the HIPAA omnibus rule in place in 2013 to implement modifications to HIPAA in accordance with guidelines set in 2009 by the Health Information Technology for Economic and Clinical Health (HITECH) Act.

The omnibus rule also increased penalties for HIPAA compliance violations to a maximum of $1.5 million per incident.

The HHS Office for Civil Rights (OCR), which enforces HIPAA, issued guidance in 2016 clarifying that cloud service providers and other business associates of healthcare organizations are covered by the HIPAA privacy, security, and breach notification rules.

HIPAA violations can prove quite costly for healthcare organizations. In addition to the notification costs, healthcare organizations can encounter fines after HIPAA audits mandated by the HITECH Act which is conducted by the Office for Civil Rights. Providers could also face criminal penalties from violations of HIPAA privacy and security rules.

OCR undertook its first round of HIPAA audits of healthcare organizations in 2012 and 2013. Those pilot audits carried no fines or penalties.

A considerably wider, formal round of desk and in-person audits of about 200 healthcare-covered entities and business associates began in 2016 and continued into 2017. These audits were expected to carry fines or corrective plans.

OCR further strengthened the HIPAA security rule in 2016 by releasing a crosswalk between aspects of the National Institute of Standards and Technology's Cybersecurity Framework to identify cybersecurity gaps and align HIPAA with national cybersecurity standards.

Organizations can lower their risk of regulatory action through HIPAA compliance training programs. OCR has six educational programs on complying with privacy and security rules.

A number of consultancies and training groups offer programs, as well. Healthcare providers may also choose to create their own training programs, which often encompass each organization's current HIPAA privacy and security policies, mobile device management processes and other applicable guidelines.

What is considered protected health information under HIPAA?

- A patient's name, address, birth date, and Social Security number.
- An individual's physical or mental health condition.
- Any care provided to an individual.
- Information concerning the payment for the care provided to the individual that identifies the patient, or information for which there is a reasonable basis to believe could be used to identify the patient.

HIPAA contains five different sections or title which are listed below.

TITLE 1: HIPAA Insurance Reform

Title 1 provides health insurance coverage to individuals who lose jobs. It also provides group health plans coverage to individuals with specific disease and pre-existing conditions from setting lifetime coverage limits:

TITLE 2: HIPAA Administrative Simplification

Title 2 directs U.S. Department of Healthcare and Human Services(HHS) to establish security standards for processing the electronic healthcare transactions. It also requires for Healthcare organizations to implement secure electronic access to health data and to remain in compliance with privacy regulations standards set by HHS.

TITLE 3: Tax Related Health Provisions

Provides guidelines for the tax-related provisions for medical care.

TITLE 4: Application and Enforcement of Group Health Plan Requirements

Provides health insurance reform. Also, it has provisions for individuals who have pre-existing medical conditions and those seeking continued coverage.

TITLE 5: Revenue Offsets:

It includes provisions for company-owned life insurance and the treatment of those who lose their U.S. citizenship for income tax purpose.

We will see more details regarding Title 2 as is more related to our context and requirements. Title 2 includes many other compliance requirements which are mentioned below:

National Provider Identifier Standard: Each healthcare entity, including individuals, employers, health plans, and healthcare providers, must have a 10 digit unique national provider number(NPI).

Transactions and Code Set Standard: Healthcare organizations must follow a standardized mechanism for electronic data interchange (EDI) in order to submit and process insurance claims.

HIPAA Privacy Rule: Officially known as the Standards for Privacy of Individually Identifiable Health Information, this rule establishes national standards to protect patient health information.

HIPAA Security Rule: The Security Standards for the Protection of Electronic Protected Health Information sets standards for patient data security.

HIPAA Enforcement Rule: This rule establishes guidelines for investigations into HIPAA compliance violations.

National Institute of Standard and Technology(NIST): President of the United States issued an Executive Order to improve the nations critical infrastructure which was directed to NIST.

NIST has worked with different stakeholders and created a framework with the collaboration between industry, government. The Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. We will follow the details present in the actual source of the NIST publication under the article No: NIST.CSWP.04162018 for critical infrastructure.

Components of the Framework: Cybersecurity framework consists of three main components: The Core, Implementation Tier, and Profiles.

Framework Core provides desired activities and outcomes using a common taxonomy which is easy to understand. The Core guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization’s existing cybersecurity and risk management processes.

The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

Identify: Develop the understanding to manage cybersecurity risk to systems, assets, data, and capabilities. To identify the business context, and core functional areas of the business are fundamental of this framework. Categories within this Function include Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.

Protect: Develop and implement appropriate safeguards to ensure the delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Categories within this Function include Identity Management and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.

Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables the timely discovery of cybersecurity events. Categories within this Function include Anomalies and Events, Security Continuous Monitoring, and Detection Processes.

Respond: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Categories within this Function include Response Planning, Communications, Analysis, Mitigation, and Improvements.

Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include Recovery Planning, Improvements, and Communications.

Figure 4.2 NIST Framework, Source: NIST Article: NIST.CSWP.04162018

The Framework Implementation Tiers assist organizations by providing context on how an organization views cybersecurity risk management. The Tiers guide organizations to consider the appropriate level of rigor for their cybersecurity program and are often used as a communication tool to discuss risk appetite, mission priority, and budget.

Framework Profiles are an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.

How to use Framework:

An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Using the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

There are different sections present different ways in which organizations can use the Framework.

- Review Current Cybersecurity Practices
- Establish and improve a cybersecurity program
- Communicate cybersecurity requirements with stakeholders
- Buying decisions
- Identify opportunity for new or revised informative references
- Methodology to protect, privacy and civil liberties

Check Your Progress 1

1. Which is the most import data privacy and protection law in European Union?
2. Which function is responsible to timely identify any cyber threat according to NIST?
3. Which framework is responsible for security healthcare data of patients?

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 4.1 Function and Category Unique Identifier, Source: NIST Article NIST.CSWP.04162018

ISO/IEC 27000-series: It is also known as the 'ISMS Family of Standards' or 'ISO27K' for short comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The series provides best practice recommendations on information security management - the management of information risks through information security controls - within the context of an overall Information security management system (ISMS).

It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information risks, then treat them (typically using information security controls) according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information risk and security, the ISMS concept incorporates continuous feedback and improvement activities to respond to changes in the threats, vulnerabilities or impacts of incidents. There are many documents in the ISO 27000 series and many others which are still under development.

- ISO/IEC 27000: Information security management systems. Overview and vocabulary.
- ISO/IEC 27001: Information technology Security Techniques. Information security management systems requirements. The 2013 release of the standard specifies an information security management system in the same formalized, structured and succinct manner as other ISO standards specify other kinds of management systems.
- ISO/IEC 27002: Code of practice for information security controls. Essentially a detailed catalog of information security controls that might be managed through the ISMS.
- ISO/IEC 27003: Information security management system implementation guidance
- ISO/IEC 27004: Information security management. Monitoring, measurement, analysis, and evaluation.
- ISO/IEC 27005: Information security risk management.
- ISO/IEC 27006: Requirements for bodies providing audit and certification of information security management systems.
- ISO/IEC 27007: Guidelines for information security management systems auditing (focused on auditing the management system).

We will look at the ISO/IEC 27001:2013 which is: Information technology Security Techniques.

ISO/IEC 27001 specifies a management system that is intended to bring information security under management control and gives specific requirements. Organizations that meet the requirements may be certified by an accredited certification body following successful completion of an audit.

Most organizations have a number of information security controls. However, without an information security management system (ISMS), controls tend to be somewhat disorganized and disjointed, having been implemented often as point solutions to specific situations or simply as a matter of convention. Security controls in operation typically address certain aspects of IT or data security specifically; leaving non-IT information assets (such as paperwork and proprietary knowledge) less protected on the whole.

Moreover, business continuity planning and physical security may be managed quite independently of IT or information security while Human Resources practices may make little reference to the need to define and assign information security roles and responsibilities throughout the organization.

ISO/IEC 27001 requires that management: Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts.

Design and implement a comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address risks that are deemed unacceptable and adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis. ISO/IEC 27001 is designed to cover much more than just IT.

Security Controls will be tested as part of certification to ISO/IEC 27001 which is dependent on the certification auditor. Management determines the scope of the ISMS for certification purposes and may limit it to, say, a single business unit or location.

This International Standard adopts the Plan-Do-Check-Act (PDCA) model, which is applied to construct and setup ISMS processes in an organization. It provides a robust model for implementing the principles of governing risk assessment, security design and implementation, security management, and reassessment.

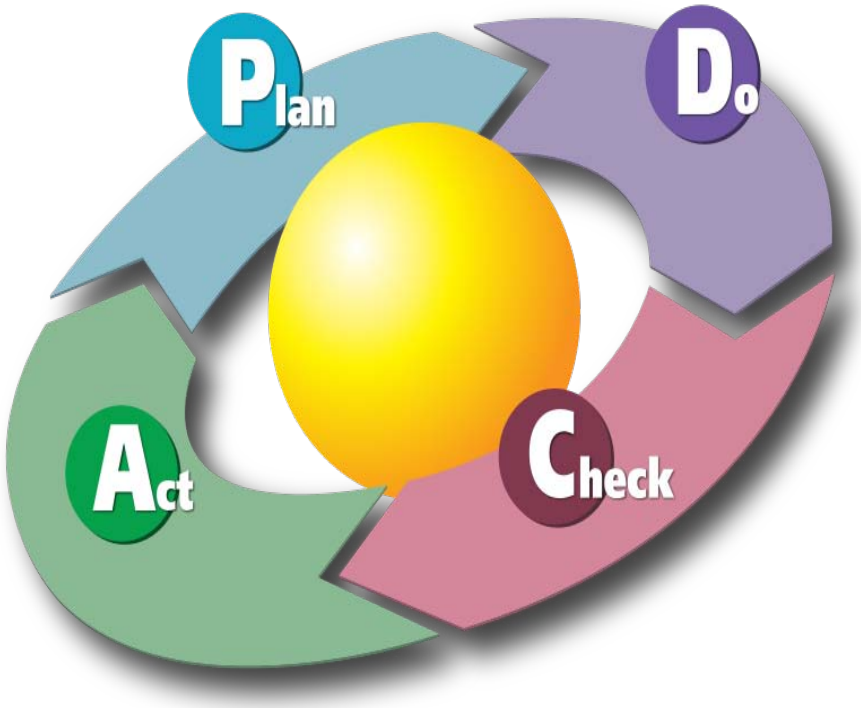

Figure 4.2 PDCS Cycle Source: Wikipedia.org

Plan (establishing the ISMS): To establish the policy, the ISMS objectives, processes, and procedures related to risk management and the improvement of information security to provide results in line with the global policies and objectives of the organization.

Do (implementing and workings of the ISMS): Implement ISMS policy, controls, processes and procedures.

Check (monitoring and review of the ISMS): Assess and measure the performances of the processes against the policy, objectives and practical experience and report results to management.

Act (update and improvement of the ISMS): Conduct an internal audit and undertake corrective and preventive actions, based on the audit results and take management review.

Payment Card Industry(PCI) Security Standards: The PCI security council provides a robust set of standards and supporting materials to enhance the security for payment card data security. Which includes specifications, tools, supporting resources which ensures the safe handling of cardholder information. The key to this is the PCI Data Security Standard(DSS). It provides and robust and actionable framework for payment card data security process. Which includes prevention, detection, and response to any security incident. Below is a high-level overview of the 12 PCI DSS requirements.

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and

	processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Table 14.2 PCI DSS Requirements and Testing Procedures

Source:www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

This above table of PCI Data Security Standard shows the requirements and Security Assessment procedures combines the 12 PCI DSS requirements and corresponding testing procedures into a security assessment tool. It is designed for use during PCI DSS compliance assessments as part of an entity's validation process.

Check Your Progress 2

1. What are the 4 phase of CCMP?

2. ISO standard which is used for Information Security and Risk Management is _____

3. Which section is respoble to secure electronic healthcare data?

PCI DSS is applicable to all who are involved in payment card processing such as merchants, service providers processors, issuers, acquirers. Also to them who are part of storing, processing or transmitting the payment card data.

Sensitive data of card holder which is defined as Account Data which further includes:

Cardholder Data includes:

- Permanent Account Number(PAN)
- Cardholder Name
- Expiry Date
- Service Code

Sensitive Authentication Data:

- Magnetic chip data or data stored on the chip.
- CVV2/CID/CAV2
- PIN

4.7LET US SUM UP

A security framework is a combination of different terminology used which provides guidance on topics related to information systems security and regarding its planning, implementation, management, auditing, review process. In this chapter, we have seen multiple frameworks which are used for different business functions and are followed to achieve the best security practices. We have National Cybersecurity Policy, 2013 from the Indian context. GDPR which is an important data privacy law in the European Union. Also, we have seen HIPAA which is used in the healthcare industry to process and store patients data and to achieve robust security control over the patient's electronic healthcare data. At last, we have seen NIST, ISO/IEC standards and PCI DSS standards.

4.8CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1

1. GDPR

2. Detect Phase

3. HIPAA

Check Your Progress 2

1. 4 phase of CCMP are Detection, Response, Recovery, Containment.

2. ISO 270005

3. Title 2 Administrative Simplification