IS Compliance and Security Framework
(Module -2 : DISSA Course)

Arijit Chakraborty

15.01.2022

Module 2- Compliance and Security Framework

- SOX
- PCI DSS
- NIST
- SSAE 16
- AT 101
- FEDRAMP
- HIPAA / HITECH
- ISO 27001
- GDPR
- PDP Bill
- IT Act 2000, Amendment 2008, Rules 2021

Recap : Module 1
Critical role of IS Auditor

1. To ensure **Restore of both data and full system is carried out on a regular basis**, so that data integrity can be ensured and the entity can be prepared for any possible disaster
2. To **monitor user or system activity where appropriate**
3. To investigate **security incidents** as when required.
4. Reporting of incidents to regulators

Recap : Module 1

Advantages of Information System Audit

Advantages:

1. Detection of non compliant procedure
2. Continual Improvement
3. Increase in productivity
4. Increased Confidentiality, Integrity & Availability
5. Increased data accuracy, completeness, validity, verifiability and consistency
6. Build a confidence among stakeholders through increase in safe & secure system
7. Compliance to Statutory / Compliance / Legal Requirements

US SOX

Sarbanes-Oxley (SOX)

Why does it exist? The Sarbanes-Oxley Act of 2002 was passed to counteract fraud after accounting scandals at Enron, WorldCom, and Tyco impacted investor trust. These controls are mandatory for public companies.

An an IS team, how will this impact you? There are various security requirements for applications and systems that process financial data. Requirements around access management, general IT controls (ITGCs), and entity-level controls may need to be managed by the IS team.

What types of organizations leverage this framework? Public companies, or companies eyeing a potential initial public offering (IPO).

SOX – Key compliances

- Sarbanes-Oxley Act of 2002 (“SOX”) is a United States federal law enacted on July 30, 2002, which mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud. Among other things, SOX:
- •Established the Public Company Accounting Oversight Board ("PCAOB")
- •Strengthened penalties for corporate fraud
- •Sets **requirements for management to annually state responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting (Section 404a)**
- •Sets **requirements for independent auditor to opine on effectiveness of the Company’s ICFR as of the reporting date (Section 404b)**
- •Establishes **standards of professional conduct for attorneys practicing before the US SEC (Section 307)**
- SOX applies to all public companies in the U.S. and international companies that have registered equity or debt securities with SEC & accounting firms that provide auditing services to them.

PCI DSS – Introduction

Payment **C**ard **I**ndustry, **D**ata **S**ecurity **S**tandard

- Developed by 5 major card brands,
- to address potential areas of vulnerability and
- guide organizations in best practices to maintain the integrity of cardholder data.

PCI DSS

PCI DSS

Why does it exist? The Payment Card Industry Data Security Standard (PCI DSS) exists to protect the security of cardholder data. These controls are mandatory for organizations that process credit card data. The standards are made up of multiple levels, and the extent to which organization interacts with credit card data will determine what level of PCI compliance of organization needs to achieve. For example, banks, merchants, and service providers will be held to higher standards given the nature of the business.

As an IS team, how will this impact you? Aside from enforcing certain procedures and controls based on PCI DSS level, organization may have to complete self-assessment questionnaires, quarterly network scans, and on-site independent security audits.

What types of organizations leverage this framework? Merchants, payment card-issuing banks, processors, developers, and other vendors.

PCI-DSS

- anyone handling payment card details must adhere to:

Payment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandards

- treat payment card details as you would cash
- Treat payment card receipts like you would cash
- Keep payment card data secure and confidential
- Restrict access to card data to “those who need to know"

PCI COMPLIANCE

- **Payment card industry (PCI)** compliance
- mandated by credit card companies to help ensure security of credit card transactions in the payments industry.
- **Payment card industry compliance** refers : *technical and operational standards that businesses follow to secure and protect credit card data provided by cardholders and transmitted through card processing transactions.*
- PCI standards for compliance are developed and managed by the **PCI Security Standards Council**
- PCI-DSS 4.0, latest version released 2021-22.comprehensive set of guidelines aimed at securing systems involved in processing, storage, and transmission of credit card data.

PCI SCOPE – PPT Approach

- PCI Scope : environment that must meet the 12 requirements stated within **PCI Data Security Standard (DSS)**. The scope is a combination of **people, processes, and technologies** that interact with or could otherwise impact the security of **cardholder data (CHD).**

- **INTERNAL SYSTEMS AND NETWORKS**
- Whatever **assets store, process, or transmit payment card data** are "**in scope" for PCI Compliance.** Any system component that stores or processes or transmits payment card information are considered as a part of CDE (cardholder data environment)

- The PCI DSS security requirements **apply to all entities involved in the payment car process including merchants, processors, issuers, and service providers**.

- It applied to **all system components included in or connected to the CDE**.

- CDE = people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data.

- December, 2016, PCI Security Standards Council (SSC) released a **supplemental guide for scoping and network segmentation**

PCI-DSS

- **Device (PCs, Laptops, Mobiles, etc.) Settings**
- **All devices MUST:**
  - Have automatic updates enabled for operating system updates
  - Run a virus checker which is automatically updated
  - Be kept fully up-to-date with all software updates for all software installed on the machine
  - Be Entity owned and not personally owned by a member of staff
  - Log anti-virus messages centrally and keep those logs for at least one year
  - Chip and Pin devices must ONLY be used on the correct secure network
- **Devices (PCs, Laptops, Mobiles, etc.):**
  - Must NOT run any peer to peer software
  - Must NOT be used for browsing websites commonly associated with malware, especially pornographic sites or sites that provide illegal software/ apps download / movies etc.

PCI DSS Requirements

Goals	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 & 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 IS Policy	12. Maintain a policy that addresses information security for all personnel.

Restrict physical access to CHD

1. Periodically inspect all credit card devices for tampering or substitution.
2. Never allow direct physical access to the credit card device, without supervisor approval.
3. Be aware of suspicious behavior.
4. Immediately report tampering or evidence of “skimming” or any breach to supervisor.

IS Audit review areas :

- Never allow access to credit card terminals without supervisor approval.

- Always verify with your supervisor the identity of any third-party claiming to be repair or service personnel.

- Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).

Requirements for Compliance

1. Assess CHD environment for compliance with the PCI DSS.
2. Complete Self-Assessment Questionnaire (SAQ) according to the instructions in Self Assessment Questionnaire Instructions and Guidelines.
3. Complete the Attestation of Compliance in its entirety.
4. Submit SAQ & Attestation of Compliance, along with any other requested documentation, to payment brand

- May also include
  - ✓Regular network or web site scanning by an Approved Scanning Vendor
  - ✓Report on Compliance by a Qualified Security Auditor & Assessor (only needed by very largest companies)

PCI DSS – India

- RBI, NPCI join the PCI Security Standards
- *“Digital payments have become a way of life in India in 2020-21, due to the pandemic. As a result, the country becomes an increasingly attractive target for cybercriminals and security of cardholder data must be a top priority. Today’s discussion brings together expertise from top leaders across the industry to address the biggest challenges facing data security in India.”*
- **- Nitin Bhatnagar, Associate Director – India, PCI SSC**
- *. “2020 will be remembered not only for the pandemic, but also as the year of India’s digital transformation. We have observed people adapting to and adopting the means of working from home, collaborating virtually, e-governance, online transactions. Unfortunately, we have also witnessed an exponential rise in the number of cyber-attacks in the country,”*
- **- Lt. General (Dr) Rajesh Pant, India’s National Cybersecurity Coordinator**

PCI Security Standards Council India Forum

- The India Forum brings together representatives from regional businesses, industry groups and government to discuss payment security challenges and solutions for organizations in India and globally.
- It provides a venue for Indian organizations involved in PCI SSC to share their experiences and insights and highlight opportunities for regional companies to participate in the development of PCI Security Standards and programs in 2021-22.