DISSA Exam Preparation session

Modules 1 & 2 : DISSA Course)

Arijit Chakraborty

April 23, 2022

Module I: Overview of IS Security & Audit

- Need for IS Audit
- Key drivers for IS & Security controls
- IT Governance, Security Policies and Control
- IT Organisation & Delivery Models
- DevOps
- Risk Assessment, Risk based audit planning
- Applicable Audit Standards
- Pillars of Information Security
- Confidentiality, Integrity, Availability
- ISO / IEC 38500 : IT Governance
- Control & Audit Perspective on each of the above topics

Module 2 = Compliance & Security Framework

- PCI DSS
- NIST Privacy Framework
- ISO 27001 Domains
- COBIT Framework, Maturity Model(CMMI)
- GDPR – EU , Key provisions & challenges
- Personal Data Protection bill (Draft) & Developments : (2020 -2021)
- Information Technology Act, 2008
- IT Act Amendment,
- IT Intermediary Rules & Ethics Guidelines 2021
- ISO / IEC 27018, 27701, 29100 = PII , PIMS
- *CBDC*

Module 3 = Business Continuity & Disaster Recovery

- Business Continuity Management
- Need for BCP , DRP
- Elements of BCP
- ISO / IEC 22301
- Developing a Business Continuity Plan
- Testing Methodology and Checklist-Data communication
- Backups-Vital Records/ Documentation
- IS Audit checklists & reviews

Module 4 = Cyber Security & Cyber Forensics

- Understanding Network Communication
- Network types – bus, ring etc
- IT Hardware – Cables , router, switch , server
- Network Component and Security
- TCP/IP
- Demilitarized Zones (DMZ)
- Common Cyber Attacks
- Vulnerability and Threat Analysis
- Cryptography and Steganography
- Digital Evidence
- Ethical Hacking- concept, process, tools & techniques
- CEH – roles & opportunities

Module 5 = : Business Application-Acquisition, Development & Implementation

- IS Audit Reports – Contents
- Components of Business Application
- Hardware/ Application Acquisition, Business Application Development
- Business Application Implementation/ Post-Implementation
- Application Control – Input, Process, Output
- Understanding Emerging Technologies:
- Block chain & DLT, Cryptocurrency & BTC – operation & process
- RPA,
- AI – DL, ML
- IoT,
- ISS Audit aspects , control checklists & Reporting

Module 6 = CBS Platform & IS Audit In Banking Sector

- Core Banking System- concept, types, operation
- Payment Application – SWIFT, RTGS, IMPS, NEFT, NSS
- Debit/Credit Card, BankNet
- Digital Banking Channel – Phone Banking, Mobile Banking, Net Banking, ATM, Anywhere Banking, Mobile Wallet
- RBI regulation for system security
- IS Audit in CBS Environment – step by step analysis (Finacle code)
- **Module 7 : IT Audit In SAP Environment**
- SAP Basics, Modules, Integration, Technology
- Roles & Authorisation
- SAP Change Management
- SAP AIS, SAP GRC,
- Outline of SAP S/4 HANA (On premise & Cloud)
- IS Audit role in SAP platform

Modules 8 -11 Cloud Computing

- **Mod 8 : Understanding Cloud Computing System**
- Characteristics of Cloud Computing, Types of Cloud Computing
- Cloud Service Models, Major CSP
- Benefit and Risks in Cloud Computing
- **Mod 9 : Adopting the Cloud**
- Key Drivers of Cloud Computing Solutions, Instantaneous provisioning of IT resources
- Tapping into an infinite storage capacity
- Cost- effective pay-as-you-use billing models, Evaluating barriers to Cloud Computing
- Handling sensitive Data-Aspects of Cloud Security
- Assessing Cloud Governance Solutions
- **Mod 10: Calculating the Financial Implications**
- Comparing in-house facilities to the Cloud,
- Estimating Economic Factors Downstream
- Existing DC Cost, Migration cost & TCO
- **Mod 11: Migrating to the Cloud**
- Choosing the right Vendor
- Internal audit & IS Audit role in Migration process

Module 1 - coverage

- IS Audit definition
- Emergence of IS Audit
- Scope & Objectives
- CIA –Triad
- Audit trail, edit log
- Cyber threats
- IS Audit process
- Types of IS Audit
- Important Audit standards
- Key Steps in IS Audit
- Centralised vs Decentralised IS Function
- Staff augmentation
- IT Governance & IS Policy

IS Audit

- **Definition & Key role**
- examination of **management controls** within an IT infrastructure and business applications
- Evaluation of ITGC, AppSec , Migration & adoption, BCP
- IS risks & cyber-risks- assessment & mitigation
- IS Infrastructure, Policy, Config management, benchmarking,
- ISO 27001 compliance, performance measurement

Chap 1: GOVERNANCE, SECURITY POLICIES AND CONTROLS- Role of IS Audit

- IS audit - **collecting & evaluating evidence** to determine whether a computer system could:

(a) **Safeguard its assets** (hardware, software and data) through adoption of adequate security control measures;

(b) **Maintain data integrity;**

(c) **Achieve goals** of the organization effectively; and

(d) **Result in the efficient use** of the available IS resources.

(e) May be performed with a **FS audit, internal audit** etc

IS Security Control objectives : CIA

1. Information is **available and usable when required**, and the systems that provide it can **appropriately resist attacks and recover from failures *(availability)***
2. Information **observed by or disclosed to only those who have a right** to know ***(confidentiality)***
3. Information **protected against unauthorized modification *(integrity)***
4. Business transactions as well as **information exchanges** between organization locations or with partners/ users **can be trusted** (***authenticity* and *non-repudiation***) – (whatsapp chats / media sharing – encrypted)

IS Audit : Key scope & coverage areas

- **1. Systems and Applications**:
- Verify systems & apps :**efficient, adequately controlled to ensure valid, reliable, timely, secure input, processing, output**
- **2. Information Processing Facilities (IPF)**:
- verify that **processing facility is controlled to ensure timely, accurate, and efficient processing** of applications
- **3. Systems Development**:
- verify that **systems under development meet org objectives**
- **4. Management of IT and Enterprise Architecture**:
- verify **IT management developed org structure & procedures**
- ***Control Obj for Info & Tech (COBIT) -*** best practices (ISACA)

IS Audit

- **Key role**
- examination of **management controls** within an IT infrastructure and business applications
- Evaluation of ITGC, SAC , BCP, Migration & adoption
- IS risks & cyber-risks- assessment & mitigation
- IS Infrastructure, Policy, Config management, benchmarking,
- ISO 27001 compliance, performance measurement

COBIT Framework

- ***Control Objectives for Information and related Technology (COBIT)***
- The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992.
- The COBIT Framework states, *"It is management's responsibility to safeguard all the assets of the enterprise.*
- *To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control."*

Key issues for IS Auditors

1. ***Performance measurement*** *- how well is the IT function supporting business requirement?*
2. ***IT control profiling*** *- What IT processes are important? What are the critical success factors for control?*
3. ***Awareness*** *- what are the risks of not achieving the objectives?*
4. ***Benchmarking*** *- what do others do? How can results be measured and compared?*
5. *To ensure* ***data integrity***
6. *To* ***monitor user or system activity where appropriate***
7. *To investigate* ***security incidents*** *as when required.*
8. ***Reporting*** *of incidents to regulators*

IS Audit Review areas

- IS Infrastructure,
- IS Policy
- IT architecture,
- Change management
- Configuration management
- Existing IS Controls –
- physical, logical , environmental, access ,
- Professional judgment on IS risks and cyber-risks that may impact the data integrity
- ISO 27001 compliance

Objectives of IS Audit

- 1. To determine **information and related technological security loopholes** and recommend feasible solution.
- 2. Examining whether **IT processes and IT Resources combine together** to fulfill **intended objectives** to ensure **effectiveness, efficiency , economy, compliance**
- 3. IS auditors **- develop & implement a risk-based IS audit strategy as per IS audit standards, regulatory guidelines** and internal policies
- 4. IS auditors to evaluate **effectiveness of IT governance structure to determine whether IT decisions, directions and performance support entity** 's strategies and objectives.
- 5. IS auditors **evaluate ERM practices to determine - entity's IS-related risks** are properly **managed & secure.**

IS Security Audits may be conducted to:

1. To ensure **integrity, confidentiality and availability of information system(s) and resources.**
2. To investigate **possible security vulnerabilities and incidents** in order to ensure conformance to the entity's security policies.
3. To ensure **software systems deployed conforms** to the entity's software implementation policy
4. To ensure **changes made to any systems** conforms to the entity's Change Control/Change Management policy
5. To ensure **regular Backup of data and business critical system** is taken & preserved.

Corporate Information Security Policy

1. **Identify a member of senior management, as Chief Information Security Officer (CISO),** -designate as a 'Point of Contact', responsible for Co-ordinating security policy compliance efforts & to regularly interact with **Indian Computer Emergency Response Team (CERT**) in Department of Information Technology (DIT), the nodal agency for cybersecurity.
2. **Prepare information security plan** and implement the security control measures as per IS/ISO/IEC 27001
3. **Carry out periodic IT security risk assessments** and determine acceptable **level of risks**, consistent with criticality of business requirements, **likely impact** on business/functions **& achievement** of organizational goals/objectives.

4. **Periodically test and evaluate the adequacy and effectiveness of technical security control** measures implemented for IT systems and networks. **Test & Evaluation** necessary **after each significant change** to IT system
   - VAPT (both announced as well as unannounced)
   - Application Security Testing, Web Security Testing
5. **Carry out Audit of Information infrastructure on an annual basis** & after **major upgradation/change in IT Infrastructure**, by an independent IT Security Auditing organization.

IS Audits – Engagement types

(i) ***Security, Privacy and Continuity:*** Fundamental controls, such as the **segregation of duties**, are often completely reliant on the strength of technology-based access controls. In a world of global communications networks,

(ii) **security vulnerabilities can be quickly exploited. Well- publicized frauds and scams erode public confidence.(Satyam , PNB, IL& FS)**

(iii) ***IT Internal Audit Services:*** Risk Management through internal audit has been considered as one of the effective techniques .For achieving **highest productivity through Internal Audit, IS Audit specialists with the capability of pointing out** and accessing the business risks to be included

(iv) ***IT Attestation Services:*** In an environment where customers and clients are increasingly affected by a business' IT systems, **extra assurance is often required to satisfy stakeholder expectations.** Reviews offer clients with a **third-party attestation against the organization's internal control objectives.** A formal report including the auditor's opinion is issued to the client at the conclusion of the examination.

iv. IRM in The External Audit:

It is undertaken for evaluating the financial audit risk. Which includes identification of **operational and financial risks** which concluded the finest part of business systems and processes and advise on risk mitigation.

IRM experts integrate technology issues into the audit framework and work as a part of audit's team in accessing the technological component in business issues, risks and strategies.

v. Migration Audits: Reviewing the migration process from legacy systems to state of the art systems like Oracle Applications, SAP.

Banks case – migration to CBS

- **IT Security Audit**
- done to protect entire system from the most common security threats which includes the following:

- ❑ Network vulnerabilities and intrusions
- ❑ Performance problems and flaws in applications
- ❑ Improper alteration or destruction of data (information integrity)
- ❑ Access to confidential data
- ❑ Unauthorized access of the department computers & branches
- ❑ Password disclosure compromise
- ❑ Virus infections
- ❑ Denial of service attacks
- ❑ Open ports, which may be accessed from outsiders (Unrestricted modems & unnecessarily open ports)

IS Security Audits may be conducted to:

1. To ensure integrity, confidentiality and availability of information system(s) and resources.
2. To investigate possible security vulnerabilities and incidents in order to ensure conformance to the entity's security policies.
3. To ensure software systems deployed conforms to the entity's software implementation policy
4. To ensure changes made to any systems conforms to the entity's Change Control/Change Management policy
5. To ensure regular Backup of data and business critical system is taken & preserved.

IS Audit checklist

- A. IT Asset Management
- **b**. IT Service & Facility Management
- **c.** Physical (client/server interface, telecommunication, server, data storage, intranet, internet)
- **d.** & Environmental Security
- **e.** User & Access Management
- **f.** Database Access & Network Security Management
- **g.** Data Center Security
- **h.** Change & Patch Management
- **i.** Problem & Incident Management
- **j.** IT Strategies, IT budget

- **k.** Audit trails &Data Privacy Protection Management
- **l.** IT Service Contract & Agreements and Vendor Management
- **m.** IT Risk Management
- **n.** Data Integrity &Transaction control
- **o.** Data Retention & Disposal
- **p.** System Acquisition, Development Management
- **q.** Business Continuity & Disaster Recovery

Key aspects of an Effective IS Audit Function

Key aspects of an Effective IS Audit Function

Report Writing

Action Taken on Audit Issues

Internal Control Evaluation - Operations, Compliance & Financial Reporting (COSO Framework)

Flash/Exception Reports

Computer Aided Audit Tools (CAAT)

IS Audit scheduling

Key aspects of an Effective IS Audit Function

Additional Qualifications- ISO LA, CEH, PCIDSS

Active Participation in Professional Bodies

Board involvement & commitment in IS Audit & Digital interventions

Integration with Internal Audit / Risk functions

Relevant Auditing Standards

- **9SA 315:** Identifying and Assessing the Risk of Material Misstatements through Understanding the Entity and its Environment which guides the Identification &Assessment.
- **ISA 330:** The Auditor's Response to Assessed Risks elucidates the responses.
- **Conventional Approach :** Get understanding of :

✓ the relevant industry,

✓ legal frameworks,

✓ operations of entity,

✓ governance structure,

✓ financing modes,

✓ selection & application of accounting policies & strategies

1.1.3. Controls

(a) **Deterrent Controls:** Deterrent Controls are designed to deter unauthorised people, internal as well as external, from accessing the information and information systems.

(b) **Preventive Controls:** Preventive Controls prevent the cause of exposure from occurring or at least minimize the probability of the occurrence of unlawful events.

(c) **Detective Controls:** When a cause of exposure has occurred, detective controls report its existence in an effort to arrest further damage or minimize the extent of damage. Detective controls limit the losses, if an unlawful event at all occurs.

(d) **Corrective Controls:** Corrective Controls are designed to help the organization recover from a loss situation. BCP = corrective control. Without corrective controls in place, the organisation will suffer from the risk of loss of business and other losses, due to its inability to recover essential IT based services, information after disaster has taken place.

- IS Auditors will require to ascertain that **adequate control exists to cover each likely unlawful event**.
- TOC : If the unlawful event is covered by a control, the IS auditors will require to evaluate whether the **control is operating effectively**. If more than one control covers an unlawful event (i.e., redundant controls), the IS auditors will require to verify that all these **controls operate effectively.**

Centralized vs Decentralized IT Structures

- **Centralized Structure**: A centralized IT departmental model is one where all **core IT systems and networks are managed by a central organization,** such that all systems can be easily integrated and managed from a single IT central hub.

(a) **Centralized Structure Pros**: Better Budget control, easier governance, better standardization, better alignment across the entire technology portfolio, easier project/workflow integration, more feasible IT management

(b) **Centralized Structure Cons**: may become bureaucratic, business departments may be unhappy

- fighting with other departments to get their tech initiatives prioritized.

- **Decentralized Structure**: A decentralized IT departmental structure is one where the management of critical IT components, system controls and networks is **distributed amongst multiple, different core IT centers** within the overarching enterprise IT infrastructure, allowing different sub-departments and teams to utilize different resources within their own sub-systems/intranets.

(a) **Decentralized Structure Pros**: Individual departments/business units have **more direct control over their tech projects** and priorities; generally decentralized groups can get faster results (less overhead and prioritization fights).

(b) **Decentralized Structure Cons**: Solutions optimized at the department level **often result in inefficiencies at the enterprise level** ("silos" of disconnected data and business processes);

(c) too much departmental independence can **lead to integration challenges** and unnecessarily duplicative systems and data.

Internal vs Outsourced IT Staff

- Businesses may save over 15 to 20 % in costs by outsourcing specific tasks
- COVID era : cost saving

IT roles that are often outsourced to skilled professionals:

- Support Desk
- Network Administrator
- Software Developer
- Software Tester
- Engineer
- Security Analyst
- Systems/Database Engineer

IT Delivery Models

- Developing **in-house** IT capabilities to complete projects or provide services**: costly & risky**, if IT needs **constantly changing**.
- When companies look **for outside help** in fulfilling IT business needs, they consider 2 delivery models:

- **1. Staff Augmentation** - allows organizations **to add staff to their existing teams based on additional skills required**
- **2. Managed Services-** allows it to free up specialist knowledge within organization & focus on **core business activities**.
- IS Auditors : evaluate, advise management on suitable model

Comparing Managed Services to Staff Augmentation

Managed Services (MSP)	Staff Augmentation
Supplier assumes control of all or part of the execution component of IT.	Supplier commits to providing resources of defined capability at a price.
Service Delivery commitments expressed as "Service Levels".	No service delivery commitments.
Committed Scope and Term which ensures accountability.	Limited commitment.
Costs can be tied to quantifiable results.	Pricing tied to hours worked and availability.
Supplier Managed Delivery Model, processes and tools.	Client manages the delivery model (including individual subcontractors); process and tools.
Knowledge must be transferrable according to a contractual commitment.	Knowledge vested in the individual.
Supplier manages the risks of meeting project deadlines, transition and operations.	All delivery risk remains with Business.

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 confidence among stakeholders through increase in safe & secure system
7. Compliance to Statutory / Compliance / Legal Requirements

The 5 domains of IT governance

- **ITGI** : IT Governance Institute (a division of ISACA) breaks down IT governance into 5 domains:

1. Value delivery
2. Strategic alignment
3. Performance management
4. Resource management
5. Risk management

IT governance frameworks and models

1. King reports of corporate governance (versions I to IV).
2. ISO/IEC 31000:2018 (risk management).
3. ISO/IEC 27001:2013 (information security).
4. Business continuity management and disaster recovery.

Governance of Enterprise IT (GEIT):

- GEIT = domains of Corporate governance
- GEIT = system in which all stakeholders, including BoD, senior management, and departments provide input into the decision-making process.
- GEIT = responsibility of BoD and executive management.
- **Purposes of GEIT are:**
  - to direct IT endeavors to ensure that IT performance meets the objectives of aligning IT with the enterprise's objectives and the realization of promised benefits
  - enable the enterprise by exploiting opportunities and maximizing benefits
  - IT resources should be used responsibly, and IT-related risk should be managed Appropriately
- Key element of GEIT = *alignment of business and IT, leading to the achievement of business value.*

ISO 38500 –international IT Governance Standard

- Sets out principles, definitions and a high-level framework that organisations of all types and sizes can use to better align their use of IT with organisational decisions, and meet their legal, regulatory and ethical obligations.
- ISO/IEC 38500:2015 is applicable **to all organizations**, including public and private companies, government entities, and not-for-profit organizations. ISO/IEC 38500:2015 is applicable to organizations **of all sizes** from the smallest to the largest, regardless of the extent of their use of IT.

ISO 38500

- ISO/IEC 38500 = guiding principles for members of governing bodies of organizations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, and acceptable use of IT within their organizations.
- *seeks to establish that IT is the entire executive management team's responsibility, and not just dependant on the CISO*
- *Addresses = responsibility of appraising IT proposals, scrutinizing current projects and providing guidelines for improved IT policies*
- *ISO 38500's objective = to provide a framework of principles that directors can use when evaluating, directing and monitoring the use of IT in their organizations*
- *ISO 38500 places strong emphasis on corporate governance*
- ISO 38500 standard expects directors to provide a set of IT principles and oversee the implementation (which includes approvals)

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

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.

Key Components of SOX

- **Certification**
- •CEOs and CFO must certify periodic SEC reports (both 10Q and 10K)
- **Corporate governance**
- •Independent Audit Committee directly responsible for appointment, pre-approval, compensation, and oversight of the public accounting firm, including the resolution of disagreements between management and the auditor regarding financial reporting
- **Potential Criminal Penalties**
- •Each periodic report containing FS filed with SEC shall be accompanied by a written certification by the CEO and CFO:
- –Information must present fairly, in all material respects, the financial condition and results of operations of the issue
- •Certifying statements that do not comply with the requirements may result in up to 10 years in prison and/or up to $5 million fine
- **Complaints and Anonymous Tips**
- •The Audit Committee must have procedures for the receipt of complaints regarding questionable accounting, auditing or internal control
- •Complaints must be anonymous and confidential

ISO 27001

•ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system (ISMS).

•An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

•It is used for maintaining and improving an information security management system.

ISO 27001 – 2022 Version

- The information security management standard ISO 27001 and its code of practice ISO 27002 were last updated in 2013
- However, a new iteration of ISO 27002 was published earlier this year in February 2022, and a revised version of ISO 27001 is likely to be published in October 2022.

Change in ISO 27001:2022

- A key segment of ISO 27001, which consists of clauses 4 to 10 remain roughly the same and has been advised that few changes are being made.
- These clauses will still include : scope, interested parties, context, information security policy, risk management, resources, training & awareness, communication, document control, monitoring and measurement, internal audit, management review, and corrective actions.
- Number of controls has decreased from 114 to 93 and are placed in 4 sections instead of the prior 14.
- There are 11 new controls, while none of the controls were deleted, and many controls were merged.

- ISO 27002:2022 lists 93 controls rather than ISO 27002:2013's 114.

  These **controls are grouped into 4 'themes' rather than 14 clauses.**
- **They are:**
  - People (8 controls)
  - Organisational (37 controls)
  - Technological (34 controls)
  - Physical (14 controls)
- **The completely new controls are:**
  - Threat intelligence
  - Information security for use of cloud services
  - ICT readiness for business continuity
  - Physical security monitoring
  - Configuration management
  - Information deletion
  - Data masking
  - Data leakage prevention
  - Monitoring activities
  - Web filtering
  - Secure coding

5 Attributes

The controls now have 5 types of 'attribute' to make them easier to categorise:

1. Control type (preventive, detective, corrective)
2. Information security properties (confidentiality, integrity, availability)
3. Cybersecurity concepts (identify, protect, detect, respond, recover)
4. Operational capabilities (governance, asset management, etc.)
5. Security domains (governance and ecosystem, protection, defence, resilience)

PCI DSS

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**

- The Payment Card Industry Data Security Standard (PCI DSS) exists to protect **security of cardholder data.**
- Mandatory for organizations that process credit card data.
- For example, banks, merchants, processors and service providers
- **IS Auditor role**

✓ enforcing certain procedures and controls based on PCI DSS level,
✓ complete self-assessment questionnaires,
✓ quarterly network scans, and
✓ on-site independent security audits.

12 REQUIREMENTS OF PCI DSS

- Requirements by the **PCI SSC** : both operational and technical,
- **Core focus** = always to **protect cardholder data.**

1. **Install and maintain a firewall configuration to protect cardholder data** -

Configuration rules to be **reviewed bi-annually** & ensure **no insecure access rules** which can allow access to CDE.

2. **Do not use vendor-supplied defaults for system passwords and other security parameters-**

Most of O/S & devices come with **factory default setting such as usernames, passwords**, & insecure configuration parameters. Default usernames and passwords **simple to guess,** even published on Internet. Such default passwords & security parameters **are not permissible per this requirement**

3. **Protect stored cardholder data**

4. **Encrypt transmission of cardholder data across open, public networks-**

secure card data when it is transmitted over open or public network (e.g. Internet, Bluetooth, GSM, CDMA, GPRS).

PCI DSS

5. **Use and regularly update anti-virus software or programs-**

anti-virus or anti-malware programs , anti-virus mechanisms to be always active, generating auditable logs.

- 6. **Develop and maintain secure systems and applications** = areas :
  - Operating systems
  - Firewalls, Routers, Switches
  - Application software
  - Databases
  - POS terminals

7. **Restrict access to cardholder data by business need to know**

8. **Assign a unique ID to each person with computer access-** should not use shared/group user and passwords

9. **Restrict physical access to cardholder data-**

*use of **video cameras/electronic access control to monitor entry** and exit doors of physical locations such as data centre. Recordings or access logs of personnel movement to be **detailed for minimum 90 days***

10. **Track and monitor all access to network resources and cardholder data-** *all the systems must have **correct audit policy set** & **send logs to centralized syslog server,** logs must be reviewed **at least daily to look for anomalies**, & suspicious activities*.

Security Information and Event Monitoring tools (SIEM), can help to log system and network activities, monitor logs and alert of suspicious activity

11. . **Regularly test security systems and processes**

- ✓ **Wireless analyser scan** to detect & identify **all authorized and unauthorized wireless access points on a quarterly basis.**

- ✓ **All external IPs and domains exposed in the CDE** are required to be scanned by a PCI **Approved Scanning Vendor** (ASV) at **least quarterly.**

- ✓ **Internal vulnerability scan** must be conducted **at least quarterly.**

- ✓ All external IPs and domains must go through exhaustive **Application penetration test** and **Network penetration test at least yearly or after any significant change.**

- ✓ **5. File monitoring is a necessity**. The system should perform file comparisons **each week to detect** changes that may have otherwise gone unnoticed.

12. **Maintain a policy that addresses information security for all personnel -** SOP:

- ✓ An annual, formal risk assessment that identifies critical assets, threats, and vulnerabilities.

- ✓ User awareness training

- ✓ Employee background checks

- ✓ Incident management