



# **Overview of Information System Security & Audit**

## **(Chapter -1 : DISSA Course)**

**Arijit Chakraborty**

*9<sup>th</sup> May 2021*

# 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)***

# 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 & cyber-risks
- 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.

## Chapter 1.1.1. - Information System (IS) Governance

- (a) **Appropriate Strategy for Information System:** Aligning informative strategy with business strategy is quite complicated and critical. The lack of alignment can lead to **mismanagement, inappropriate investments / ineffective implementation** of new system.
- (b) **Laboriousness in Quantifying the Value of Informative System:** This task is necessary during disposals and acquisitions. The **value derived from the impact of IT** should always be known. Else could lead to **improper investment decisions**.
- (c) **Reviewing Existing Informative System Security Controls:** This is done **walking by the best parameters of the industrial standards**. Making recommendations to improve and strengthen Information System controls.
- (d) **Systems and Applications:** An audit to certify that systems and applications are appropriate to the entity's requirements, are **efficient, and are adequately controlled** to ensure valid, reliable, well timed, and secured input, processing and output.
- (e) **Business Application Audits:** Checking upon the limitations, features and application capabilities for establishing the lawfulness in the applicant's logical access controls. Reviewing the **operational adequacy of the application package**,  
Auditing **SLDC process** and testing the performance through different tools.

**f. Information Processing Facilities:** This audit process is conducted for ensuring the timely, accurately and effective processing of the applications under any condition whether **normal or disruptive**.

**g. System Development:** It is an audit to verify that the systems under development **meet the goals of the organization** and to assure that the systems are developed according to generally accepted standards for systems development.

**h. IT and Enterprise Management Architecture:** audit conducted to verify if the **IT management has developed an organizational structure** and procedures for assuring a controlled and efficient environment for IT

**i. Performance Management System:** Measuring and improving IS is a constant challenge. Performance check is conducted for proper management of investment in IT, controlling the technology risks which makes the foundation for improvement.

**k. Regulation and Compliance Frameworks:** Compliance frameworks can be costly and complicated to implement. However, without them, organizations may increase their risk of fines

# Corporate Information Security Policy

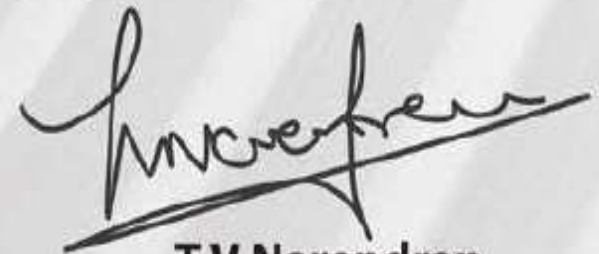
1. **Identify a member of senior management, as Chief Information Security Officer (CISO)**, -designate as a 'Point of Contact', responsible for Co-ordinating security policy compliance efforts & to regularly interact with **Indian Computer Emergency Response Team (CERT)** in Department of Information 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.

# Information Security Risk Management Policy

- This policy shall provide a risk assessment framework as suited to, and as relevant to the business requirement of TSL.
- The information security risks for the identified Information Assets of TSL, covering business operations, vendors, and regulatory and or legal requirements shall be considered for management and mitigation.
- A formal mechanism of conducting Risk Assessments (RA) and execution of the Risk Treatment (RTP) plan shall be developed on all the identified assets of TSL on and off premises and those with the vendors.
- Risk assessment shall consider:
  - The business impact due to the occurrence of the threat,
  - The probability of the occurrence of that threat.
  - Risk Impact Rating which is the product of (Value of Threat x Probability or Likelihood of Occurrence) x Asset Value, will be the criterion used to identify the acceptable level of risk which will be developed and implemented.
  - A Threshold Value based on the outcome of step shall be decided for the purpose of the level above which a mitigating control will be deployed.

- Risk Treatment Plan shall consider all the aspects of Risk Treatment such as (Mitigation, Acceptance, Transfer and Avoidance).
- The execution, development and implementation of a Risk Assessment and Risk Treatment Plans shall be responsibility of the Information Security Organization as defined in the Information Security Organization Policy.
- TSL shall develop and or deploy adequate and sufficient controls to ensure that information security risks are reduced to an acceptable level commensurate with the risk appetite of the organization and any residual risk(s) thereof shall be acceptable to TSL after the application of supplementary controls.
- The Risk Assessment and Risk Treatment shall be reviewed periodically, should there be major changes to the business, organizational structure and regulatory landscape which will impact the information security posture of TSL.
- The effectiveness of the Risk Assessment and Risk Treatment approach shall be measured through the development of appropriate metrics, which will be reviewed periodically to ensure their relevance and adequacy.
- Any exception to this policy shall be managed by a formal process.



**T V Narendran**  
CEO & Managing Director

**Date :** November 1, 2017

# Information Security Asset Classification Policy

- Any asset which has a business value is to be considered as an information asset. This will include, but not be restricted to; information in digital and non digital format, portable media, network infrastructure devices (servers, routers, switches, modems, tape drives, storage devices, load balancers, ids, ips, firewalls), applications, services, desktops , laptops and mobile computing and communication devices, utilities such as power generation, conditioning and distribution equipment and air-conditioning equipment amongst others.
- Valuation of information assets shall take into account the Business Impact Parameters such as (Financial, Operational, Regulatory/Compliance, Competitive and Legal); should they be compromised in any manner.
- A score shall be assigned for each of the Business Impact Parameters against Business Impact Criteria such as HIGH, MEDIUM and LOW comprising point scale of 5, 2 and 0.5 respectively, to arrive at the Risk Impact Class.

- Risk Impact Class shall be categorised as CRITICAL, SIGNIFICANT, MODERATE AND NEGLIGIBLE. The Risk Impact Class (RIC) will lead to the classification of the Information Asset.
- All Information generated or in existence shall be clearly identified and an Information Asset Classification (IAC) template shall be drawn up by respective Department Implementer (DI). The IAC shall only be effective after approval from the authorized signatories.
- Labelling methods in pursuant to the classification modality shall be adopted.
- Retention Limits shall be defined for every category of the identified information asset in consonance with the requisite business, regulatory and legal requirements.
- The term 'owner' for an information asset is an individual or department which has a management approval and hence responsibility for controlling the production, development, maintenance, use and security of an asset. Owners shall set the security requirements for information assets and shall be responsible for communicating those requirements to all the custodians.
- Custodians shall be those who are the authorized employees/departments who shall have the custody of the Information Asset.
- There shall be a formal review mechanism to ensure that the listing of all Information Assets along with their valuation and classification is current, accurate and relevant.
- In order to measure the effectiveness of the process of the maintenance of the inventory of the Information Assets, stakeholders shall be evaluated against the metrics which have been defined. Corresponding actions and records shall form as supporting elements of the compliance process.
- Any exception shall be managed through a formal process.

A handwritten signature in black ink, appearing to read 'Anurag', is located in the bottom right corner of the page. The signature is stylized and written over a horizontal line.

# 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

## ***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.**

# 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, organisation will suffer from 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 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

# Key stakeholders of DevOps

- ❑ Product management
- ❑ QA
- ❑ Internal Audit
- ❑ IT Operations
- ❑ IS Security

- **IS Auditors Role:**
  - 1. evaluate DevOps strategy
  - 2. guide management to secure DevOps process
  - 3. Audit of Change management : access controls, SOD, Customer satisfaction etc
  - 4. Evaluate DevOps metrics & performance

# DevOps goals & metrics

## Goals of DevOps

- Improved deployment frequency;
- Faster time to market;
- Lower failure rate of new releases;
- Shortened lead time between fixes;
- Faster mean time to recovery (in the event of a new release crashing or otherwise disabling the current system).

# 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

# Thank You

**Arijit Chakraborty**