# Case Study on IS Governance, ERM & IS Audit Process

(Module -1 : DISSA Course)

**Arijit Chakraborty**

***08.01.2022***

# Information Systems Audit

*Introduction:*

- Audit of controls designed & implemented into system to ensure integrity of data processed by the system & maintain proper functionality of system processes.

*Relevance:*

- Provide assurance that IT Systems are adequately protected
- Reduce risk of :
- data tampering,
- data loss or leakage,
- service disruption &
- poor management of IT systems

# IS Audit definition & concepts

- In terms of responding to IS/ IT Risks, Importance of IS Audits includes 2 levels:
- **Level 1** = to Prevent Risks: IT Audits can help companies identify & prevent risks in IT systems that support business, & also help companies audit IT systems avoid possible risks from external environment.
- **Level 2** = to Co-operate with the CISO to effectively manage risks found in the audit and make risk prevention better.

# Goal of IS Audit

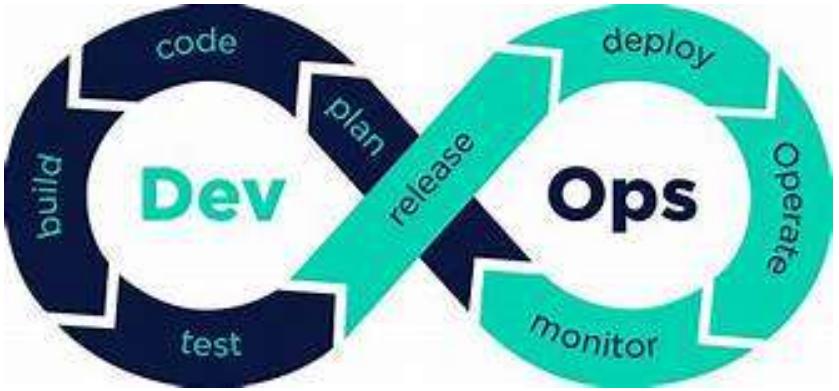
- 1. To determine **information & related technological security loopholes** & recommend feasible solution.
- 2. Examining whether **IT processes & IT Resources combine together** to fulfill the **intended objectives of the organization** to ensure effectiveness, efficiency and economy in its operations while complying with rules.
- 3. IS auditors **should develop & implement a risk-based IS audit strategy in compliance with IS audit standards, regulatory guidelines** & internal policies
- 4. IS auditors **should evaluate effectiveness of IT governance structure to determine whether IT decisions, directions and performance support entity** 's strategies and objectives.
- 5. IS auditors **also evaluate risk management practices to determine whether the entity's IS-related risks are properly managed.**
- IS auditors should conduct audit on overall information and related technological security aspects

# IS Audit in Dev Ops

**DevOps** (**Dev+ Ops** : set of practices **combining software development & IT operations**. ( **Software Dev & Operations)**

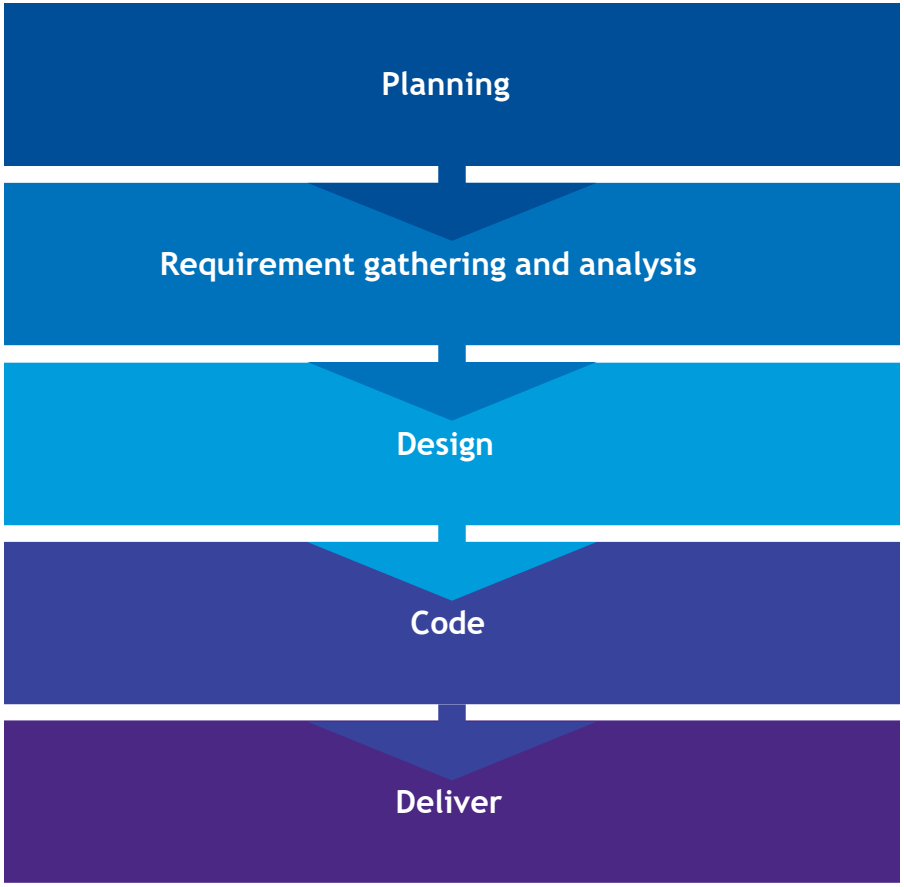
**DevOps –**

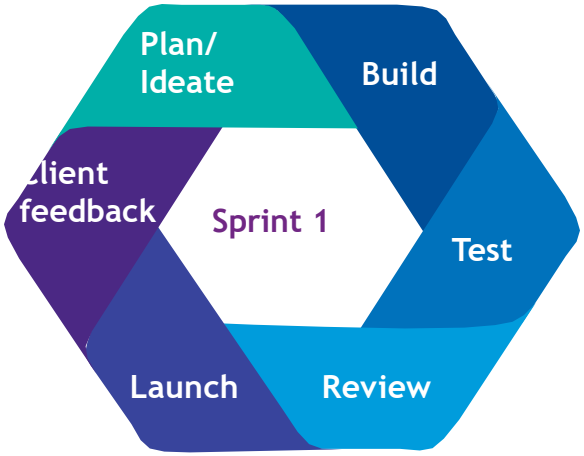
- complementary to ‘’Agile approach’’
- Inspired by –’’The Toyota Way’’
- PDCA Cycle of Lean & Deming




1. **Plan**
2. **Coding – code development & review, source code management tools**
3. **Building**
4. **Testing**
5. **Releasing – change management, release approvals**
6. **Deploy**
7. **Operate & Configure – infrastructure configuration and management**
8. **Monitoring – applications performance monitoring**

# Software development : Waterfall model  vs Agile Model




**Key Agile principles :**

- Customer satisfaction
- Periodic delivery of working software
- Good design, simplicity,
- attention to detail
- Consistent development  pace
- Interaction, motivation & metrics

# 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

# IS Audit Review : 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 current system).

# IS Auditors & Cloud computing

- **Cloud computing** : **Internet-based computing = provides shared computer processing resources & data to computers**
- Enables **global, on-demand access to shared pool of configurable computing resources (e.g. computer networks, servers, storage, applications & services),** = can be rapidly provisioned & released with minimal management effort.
- Provide users = **various capabilities to store & process their data in either privately owned or third-party DC** may be located far from user

# **Cloud Computing** ( DISSA= 20 %)

**Cloud Service Models**

- IS Auditors to advise :
- 1. single or multi-cloud strategy
- 2. Concentration risk mitigation ,
- 3. extent of 3rd party reliance

# Why Auditing Standards are Important in IS Audit

- Auditing Standards are mandatory to be by followed by IS Audit practitioners under the direction issued by ISACA / IIA / ICAI / ICMAI (GN)
- Standards = important for **Quality Control**
- Uniformity, comparison, best practices ( Eg OWASP, ISO,NIST, ,SoX, AES)
- If not complied :
- IS Auditor shall be held guilty of Professional misconduct & negligence

# Key Audit pronouncements ( made applicable / modified for IS Audit) – IFAC ( IAASB)

- **ISA 200** : General Principles and Responsibility
- ***ISA 210:*** *Agreeing the Terms of Audit Engagements*
- ***ISA 250:*** *Consideration of Laws and Regulations in an Audit*
- ***ISA 300:*** *Planning an Audit*
- ***ISA 315:*** *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity & Environment*
- ***ISA 402:*** *Audit Considerations Relating to an Entity Using a Service Organisation*

## *SIA – 14*

## The Institute of Chartered Accountants of India

## *INTERNAL AUDIT IN AN INFORMATION TECHNOLOGY ENVIRONMENT*

- The purpose of this Standard on Internal Audit (SIA) is to establish standards on procedures to be followed when an internal audit is conducted in an information technology (IT) environment.
- An IT technology environment exists when one or more computer(s) of any type or size is (are) involved in the processing of financial information, including quantitative data, and other types of information processing whether those computers are operated by the entity or by a third party.
- An IT system is a system that uses technology to capture, classify, summarize and report data in a meaningful manner to interested users, including an enterprise resource planning (ERP) system
- **( SIA 14 may be used / modified for use in IS Audit)**

# Scope & Objectives

- The overall objective and scope of an internal audit does not change in an IT environment. However, the use of a computer **changes** the processing, storage, retrieval and communication of financial information and the interplay of processes, systems and control procedures.
- This may affect the internal control systems employed by the entity. Accordingly, an IT environment may affect:
- a) the procedures followed by the internal auditor in obtaining a sufficient understanding of the processes, systems and internal control system;
- and
- b) the auditor's review of the entity's risk management and continuity systems.

# IT Environment – Matters to Consider

- The internal auditor should consider the effect of an IT environment on the internal audit engagement, *inter alia:*
- a. the extent to which the IT environment is used to record, compile, process and analyse information
- b. the system of internal control in existence in the entity with regard to:
- • the flow of authorised, correct and complete data to processing centre;
- • the processing, analysis and reporting tasks undertaken in the installation; and
- • the impact of computer-based accounting system on the audit trail that could otherwise be expected to exist in an entirely manual system

# Need of Specialised skills

- If specialized skills are needed, the internal auditor should seek the assistance of a technical expert possessing such skills, who may either be :

❑ the internal auditor's staff or

❑ an outside professional.

- If the use of such a professional is planned, the internal auditor should, in accordance with SIA16*, "*Using the Work of an Expert", obtain* = sufficient appropriate evidence that the work performed by the expert is adequate for the purposes of the internal audit.

# Internal / IS Audit Planning

- The internal auditor should obtain an understanding of the :
- systems, processes,
- control environment,
- risk-response activities &
- internal control systems sufficient to plan the internal audit and to determine the nature, timing and extent of the audit procedures, in accordance with SIA 1*, "Planning an Internal Audit". Such an understanding would* help the internal auditor to develop an effective audit approach.
- In planning the portions of the internal audit which may be affected by the IT environment, the internal auditor should obtain an understanding of the significance and complexity of IT activities and availability of the data for use in the internal audit.

- This understanding would include such matters as:
- i) IT infrastructure [hardware, operating system(s), etc., and application software(s)] used by the entity including changes, if any, therein since last audit.
- ii) the significance and complexity of computerised processing in each significant application. An application *may be considered to be complex* when, for example:
- a) the volume and materiality of transactions is such that users would find it difficult to identify and correct errors in processing.
- b) the computer automatically generates material transactions or entries directly to another application.
- c) the computer performs complicated computations of financial information and/or automatically generates material transactions or entries that cannot be (or are not) validated independently.

- d) transactions are exchanged electronically with other organisations [as in electronic data interchange (EDI) systems] without manual review for propriety or reasonableness.
- iii) determination of the organisational structure of the client's IT activities and the extent of concentration or distribution of computer processing throughout the entity, particularly, as they may affect segregation of duties.
- iv) determination of the availability of data. Source documents, computer files, and other evidential matter that may be required by the internal auditor may exist for only a short period or only in machine-readable form.
- IT systems may generate reports that might be useful in performing substantive tests (particularly analytical procedures).

# IT Environment

- ***When the IT systems are significant, the internal auditor should also obtain an understanding of the IT environment and whether it influences the assessment of inherent and control risks***
- The nature of the risks and the internal control characteristics in IT environments include the following
- **a. *Lack of transaction trails*** - errors embedded in an application's program logic may be difficult to detect on a timely basis by manual (user) procedures
- **b. *Uniform processing of transactions*** - programming errors (or other systemic errors in hardware or software) will ordinarily result in all transactions being processed incorrectly.
- **c. *Lack of segregation of functions***
- an individual who has access to computer programs, processing or data may be in a position to perform incompatible functions

- **d. *Potential for errors and irregularities***
- 1. potential for human error in development, maintenance and execution of computer information systems ***may be greater*** than in manual systems, partially because of the level of detail inherent in these activities.
- 2. Potential for individuals to gain unauthorised access to data or to alter data without visible evidence may be greater in IT than in manual systems.
- 3. Decreased human involvement in handling transactions processed by computer information systems can reduce the potential for observing errors and irregularities.
- 4. Errors or irregularities occurring during the design or modification of application programs or systems software can remain undetected for long periods of time

- **e. *Initiation or execution of transactions*** – *IT* systems may include the capability to initiate or cause the execution of certain types of transactions, automatically. The authorisation of these transactions or procedures may not be documented in the same way as that in a manual system
- **g. *Potential for increased management supervision***: *IT systems can offer* management a variety of analytical tools that may be used to review and supervise the operations of the entity. The availability of these analytical tools, if used, may serve to enhance the entire internal control structure

# Review of IT Environment

- The internal auditor should review the robustness of the IT environment and consider any weakness or deficiency in the design and operation of any IT control within the entity, by reviewing:
- a) System Audit reports of the entity, conducted by independent Information System auditors;
- b) Reports of system breaches, unsuccessful login attempts, passwords compromised and other exception reports;
- c) Reports of network failures, virus attacks and threats to perimeter security,
- d) General controls like segregation of duties, physical access records, logical access controls;
- e) Application controls like input, output, processing and run-to run controls;
- f) Excerpts from the IT policy of the entity relating to business continuity planning, crisis management and disaster recovery procedures.

# Case Discussion : LIC – IT Infrastructure & Risk Governance

- **1964** : introduction of computers in LIC.
- Unit Record Machines introduced in late 1950's phased out in 1980's and replaced by Microprocessors based computers in Branch and DO for Back Office Computerization.
- **1990 s** : Standardization of Hardware and Software. Standard Computer Packages developed & implemented for Ordinary & Salary Savings Scheme (SSS) Policies.
- **FRONT END OPERATIONS**
- **July 1995** : LIC started On Line Service to Policyholders & Agents through Computer.
- *Enabled* : policyholders to receive immediate policy status report , prompt acceptance of their premium and get Revival Quotation

# ERM & IS Policy – LICI

- **Enterprise Risk Management** (ERM) Concept launched- 2017
- **Description of the Risk Management Architecture (RMR)**
- LIC funds are invested in asset classes in line with the IRDAI (Investment) Regulations 2016 and are exposed to *various risks like market risk, credit risk, interest rate risk, liquidity risk , IS Risk and counterparty risk*
- A robust *Risk Management Structure is required to continuously monitor, measure and mitigate these risks* emanating from such a diverse exposure in the financial markets.
- The investment risks are systematically identified and SOP implemented
- In line with the IRDAI Guidelines, Corporation has constituted the Risk Management Committee of the Board (RMCB).

# BoD Role

- Board of Directors provide overall guidance on Risk Management & IS function which includes :

✓ providing necessary oversight on key risks & measures,

✓ approving Risk Management Policy & Risk Management Strategy,

✓ Risk Appetite statement,

✓ Annual Asset Liability Management (ALM) Policy

✓ IS & Business Continuity Plan of LIC

- The Corporation is committed to having a *continuous organizational focus on Risk Management and has a Risk Management Policy covering areas :*

- *Risk Vision,*
- *Risk Governance,*
- *Risk Identification,*
- *Risk Measurement,*
- *Risk Monitoring &*
- *Risk Reporting*

- Developments across the economic sectors and companies are continuously tracked, through equity research & economic scenario reports to enable Investment Operations Department to take investment decisions in primary/ secondary equity markets

- ***DISSA Exam : Points to remember:***

1. Most important function of IS management in outsourcing practices is – monitoring the outsourcing provider's performance
2. Enterprise **cannot outsource** accountability for IT security policy. Accountability **always lies with senior management/ BoD**
3. When IT outsourcing service provided in another country, major concern for the IS auditor is – legal jurisdiction can be questioned
4. Clause in outsourcing contract to help in improving service levels & minimize costs is – Gain-sharing performance bonuses = *group bonus in which entire entity workforce shares as a result of improving productivity above a certain level & decreasing rejects / rework.*
5. Type of IS Controls – P,D,C
6. IT Resource management – Out /Insourcing , Cen/ decentralised , etc
7. Contents of IS Policy
8. IT Governance & ERM
9. ITIL , IT Delivery Models
10. Applicable Standards – ISO 38500, COBIT, ISO 27001
11. Role of CISO & Deliverables