Business Application – Acquisition, Development & Implementation

(Module - 5 : DISSA Course) **Part 1**

Arijit Chakraborty

March 06, 2021

Audit Charter, Audit Policy to include IS Audit

- Audit Charter / Policy = document, guides & directs activities of IS audit function.
- Charter = documented to contain **clear description** of its mandate, purpose, responsibility, authority & accountability of relevant members or officials in IS Audit (-IS Auditors, management & Audit Committee)
- IS Auditor - have to determine **how to achieve implementation of applicable IS Audit standards**, use professional judgment in their application, & prepared to justify any departure there from.

IS Audit Policy

- Clearly address - responsibility, authority & accountability of IS auditor.
- 1. Mission Statement
- 2. Scope or Coverage
- 3. Audit Methodology
- 4. Objectives
- 5. Independence
- 6. Relationship with External Audit
- 7. Auditee's Requirements
- 8. Critical Success Factors
- 9. Key Performance Indicators
- 10. Other Measures of Performance
- 11. Providing Assurance on Control Environment
- 12. Reviewing Controls on Confidentiality, Integrity & Availability of Data or Systems

IS Audit Standards

- **Challenge of SINGLE uniform standard- ‘’One size fits all’**
- The Institute of Chartered Accountants of India (ICAI), in March 2009, published **"Standard on Internal Audit (SIA) 14 : Internal Audit in an Information Technology Environment**" covering requirements of planning stage, which IA should follow.
- IIA = guidance on defining IS Audit Universe, through the guide issued on **"Management of IS Auditing" under the "Global Technology Audit Guide" series**.

IIA GTAG

- IIA issued Global Technology Audit Guide (GTAG).
- GTAG 1: Information Technology Controls
- GTAG 2: Change and Patch Management Controls: Critical for Organizational Success
- GTAG 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment
- GTAG 4: Management of IT Auditing
- GTAG 5: Managing and Auditing Privacy Risks
- GTAG 6: Managing and Auditing IT Vulnerabilities
- GTAG 7: Information Technology Outsourcing
- GTAG 8: Auditing Application Controls
- GTAG 9: Identity and Access Management

IASB (ICAI) & SIA

- **Introduction of SIA:**
- The Internal Audit Standard Board, issued Standards on Internal Audit.
- SIAs establish **uniform evaluation criteria, methods, processes, and practices.**
- The Standards form the basis **for conducting all internal audit activity.**
- SIA **= only recommendatory** & not notified.
- Standards on Internal Audits is applicable for all internal audits beginning on or after a date to be notified by the Council of the Institute.
- CIA – IASB
- **SIA – Standard setting process –**

1. Draft –
2. Peer reviewed draft-
3. ED – Circulation

- Public comments - Law Enforcement Agencies, Corporates, Banks & stakeholders

1. Regulators – RBI, SEBI, IRDAI, CBDT, NABARD, NHB, MCA, MoF, CAG, CERT, EOW, ED
2. Definitive Standard with SIA Numbering
3. Technical guides, AG, IG issued
4. Feedback from CA Members in using SIA

Interviewing Key Personnel

- Information System Auditor conducts meetings & interviews each Dept. / Unit Head, to know–
- To understand employee's awareness towards organization's IS policies and procedures
- Reporting Hierarchy & relationship to understand implementation of SOD (Segregation Of Duties) control
- To gain knowledge of process & flow of data / transactions in organization
- ***Interviewer :*** *be flexible & modify questions, or sequence*

IS Auditor – Responsibilities

- a. scope of auditing assignment is defined clearly by auditee
- b**. IS auditing carried out strictly in accordance with T&C**
- c. all applicable **codes of conduct & auditing standards** adhered to
- d. contract between IS Auditor & Auditee **expressly permits access** to system for Auditor & representatives of client, if need be, during audit
- e. **responsibility of client data**, preserved by auditing organization, remains **with auditing organization**.
- f. after sign off of engagement, if the client's data is retained **by auditing organisation, must be encrypted & access must only be provided on "Need to Know" basis.**

- g. auditing organization **should not share client’s data** without explicit written permission from auditee.
- h. **audit outcome & related matters** should only be communicated to specified Point of Contact **(POC)** of auditee organization.
- i. IS audit report should only be shared **using secure methods such as use of passwords, encryption** etc.
- j. **Non-Disclosure Agreement (NDA)** signed with auditee before commencement of project & legally enforceable.
- **CONFIDENTIALITY**
- IS Auditor **ensure - employees, agents & sub- contractors keep confidential all information in whatever form** which is obtained, produced or derived from or related to carrying out of its obligations
- IS Auditor shall, upon termination (for whatever reason), comply with requests from Client **to return all documents & materials provided under or in relation to Auditor empanelment** & **refrain from advertisement or making claims regarding status of empanelment**

Contents of Engagement Letter

- The form & content of Engagement Letters vary from one engagement to another, but they generally include :
- **A. Clauses concerning the nature of engagement :**
- • The objective of the engagement, including a brief on the **nature of the background, concerns and allegations.(eg – in cyber fraud)**
- • **Scope of coverage** - including reference to applicable legislation, regulations, or pronouncements of professional bodies or any limitations.
- • **Nature and form of deliverables**, intended use and distribution of the report to be issued.
- • **List of entities,** functions, geographical regions, or sites to be covered.
- Unresolved conflicts of interest, if any.
- • **Project timeline and milestones**.
- • Any special requirement, such as the **need to testify** to competent authorities.

- **B. Clauses concerning the responsibilities of the Stakeholders:**
- • Provision of unrestricted access to records, documentation and other information required in connection with the engagement.
- • Access to key personnel and officials.
- • Assistance in Third Party Verifications and such particulars.
- • Safeguards in use of Tools, techniques and Methods.
- • Specific logistical requirement, arrangements regarding planning and performance of the engagement.
- • Arrangements concerning the involvement of other professionals and technical experts in some aspects of the engagement (if any – eg CEH / VAPT Professional, ISO 22301 / 27001 Certified LA)

- **Responsibility**

✓ Scope, Objectives

✓ Independence

✓ Risk assessment

✓ Specific auditee requirements, Deliverables

- **Authority**

✓ Right of access to information, personnel, locations and systems

✓ Scope or any limitations of scope

✓ Evidence of agreement to the terms and conditions of engagement

- **Accountability**

✓ Intended recipients of reports

✓ Auditee rights

✓ Quality reviews

✓ Agreed completion dates

✓ Agreed budgets/fees if available

Guidance on executing IS Audit

1. Refining understanding of business process & IT environment
2. - Refining scope & identifying internal controls
3. - Testing Control Design
4. - Testing the outcome of the control objectives
5. - Collecting audit evidence
6. - Documenting test results
7. - Concluding tests performed
8. - Considering use of audit accelerators

- 9. Considering use of Computer-Aided Automated Tools (CAATs)
- 10. Considering work of others
- 11. Considering third-party review by service providers