Business Application – Acquisition, Development & Implementation

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

Arijit Chakraborty

June 27 , 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

Authority :

- 1. Risk Assessment
- 2. Mandate to perform an IS Audit
- 3. Allocation of resources
- 4. Right to access relevant information, personnel, locations & systems
- 5. Scope or limitations of scope
- 6. Functions to be audited

Applicable IS Audit Standards

- ✓ISACA - COBIT
- ✓NIST
- ✓ISO 27001
- ✓IIA
- ✓ICAI SIA
- ✓ICAI FAIS
- ✓PCI – DSS
- ✓ISO 22301
- ✓COBIT
- ✓ITIL
- ✓ITGI

IS Audit Standards

- 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

SIA- application in IS Audit

- 100 Series: Standards on Key Concepts (New)
- 200 Series: Standards on Internal Audit Management (New)
- 300–400 Series: Standards on the Conduct of Audit Assignments (New)
- **Standards issued up to July 1, 2013**
- SIA 110 - Nature of Assurance
- **SIA 120 - Internal Controls**
- – Define Internal Controls, how they mitigate risk, how viewed - legal angle
- – Explain responsibilities of management & auditors
- – Specify certain requirements which need to be satisfied to be able to provide assurance on Internal Controls.
- SIA 210- Managing the Internal Audit Function
- SIA 220- Conducting Overall Internal Audit Planning

SIA – 14

- **Internal Audit in IT Environment**
- **IT Environment – Matters to Consider**
- ***Para 3**. 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; and*
- *b. the system of internal control in existence in the entity with regard to:*
- * the flow of authorised, correct and complete data to the processing centre;*
- * the processing, analysis and reporting tasks undertaken in the installation;*
- * the impact of computer-based accounting system on the audit trail that could otherwise be expected to exist in an entirely manual system.*

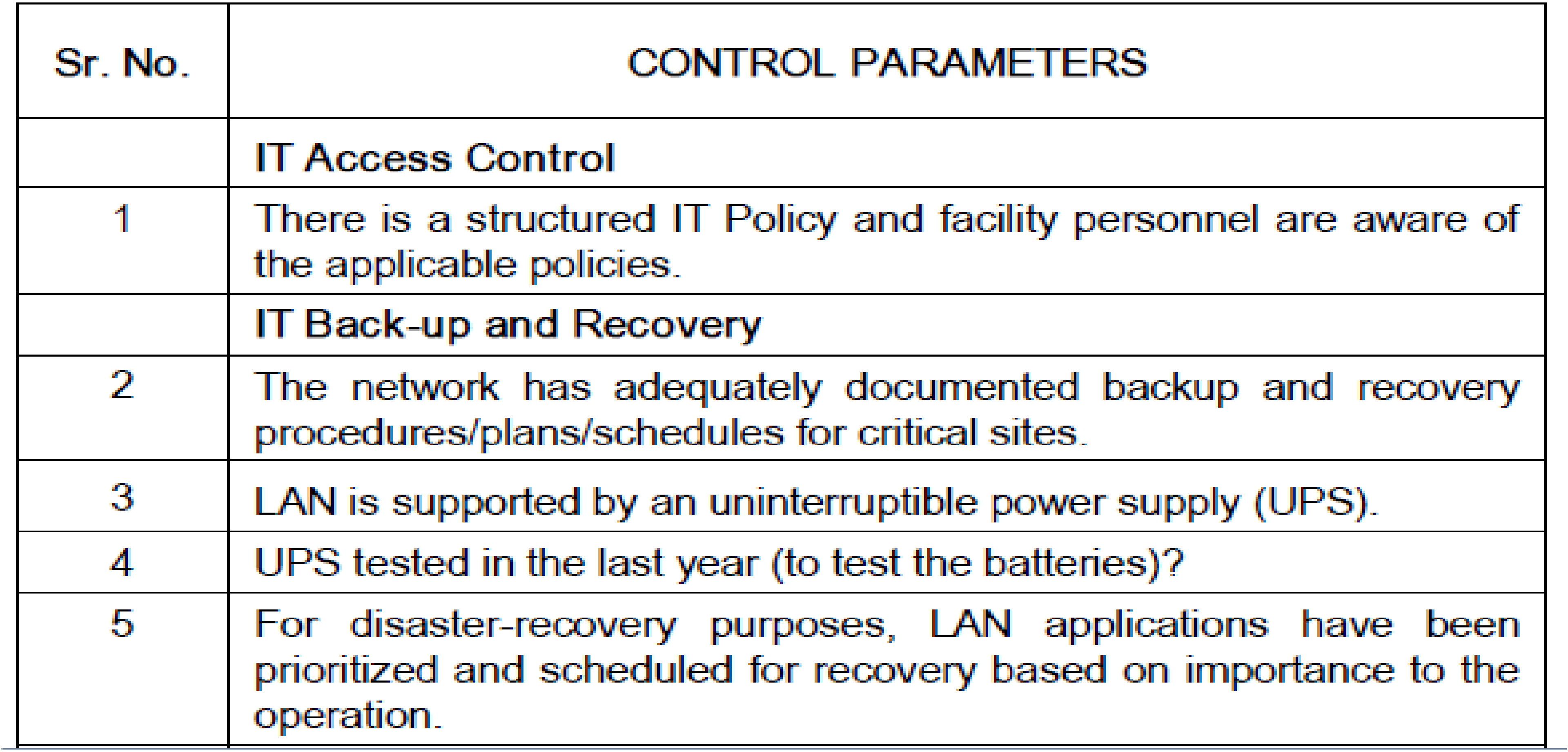
- **Skills and Competence**
- **Para 4**. *The internal auditor should have sufficient knowledge of the information technology systems to plan, direct, supervise, control and review the work performed.*
- *The sufficiency of knowledge would depend on the nature and extent of the IT environment. The internal auditor should consider whether any specialised IT skills are needed in the conduct of the audit, for example, the operating knowledge of a specialised ERP system.*
- ***Specialised skills may be needed,** for example, to:*
- *a) obtain sufficient understanding of the effect of the IT environment on systems, processes, internal control and risk management systems;*
- *b) design and perform appropriate tests of control and substantive procedures; and*
- *c) determine the effect of IT environment on assessment of overall audit risk.*

- ***Para 5*** *: 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.*
- *8. When the IT systems are significant,* ***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 risks and the internal control characteristics in IT environments include :*
- *a.* ***Lack of transaction trails****: Some IT systems are designed so that a complete transaction trail that is useful for audit purposes might exist for only a short period of time or only in computer readable form.*
- *Where a complex application system performs a large number of processing steps, there may not be a complete trail. Accordingly, errors embedded in an application's program logic may be difficult to detect on a timely basis by manual (user) procedures.*

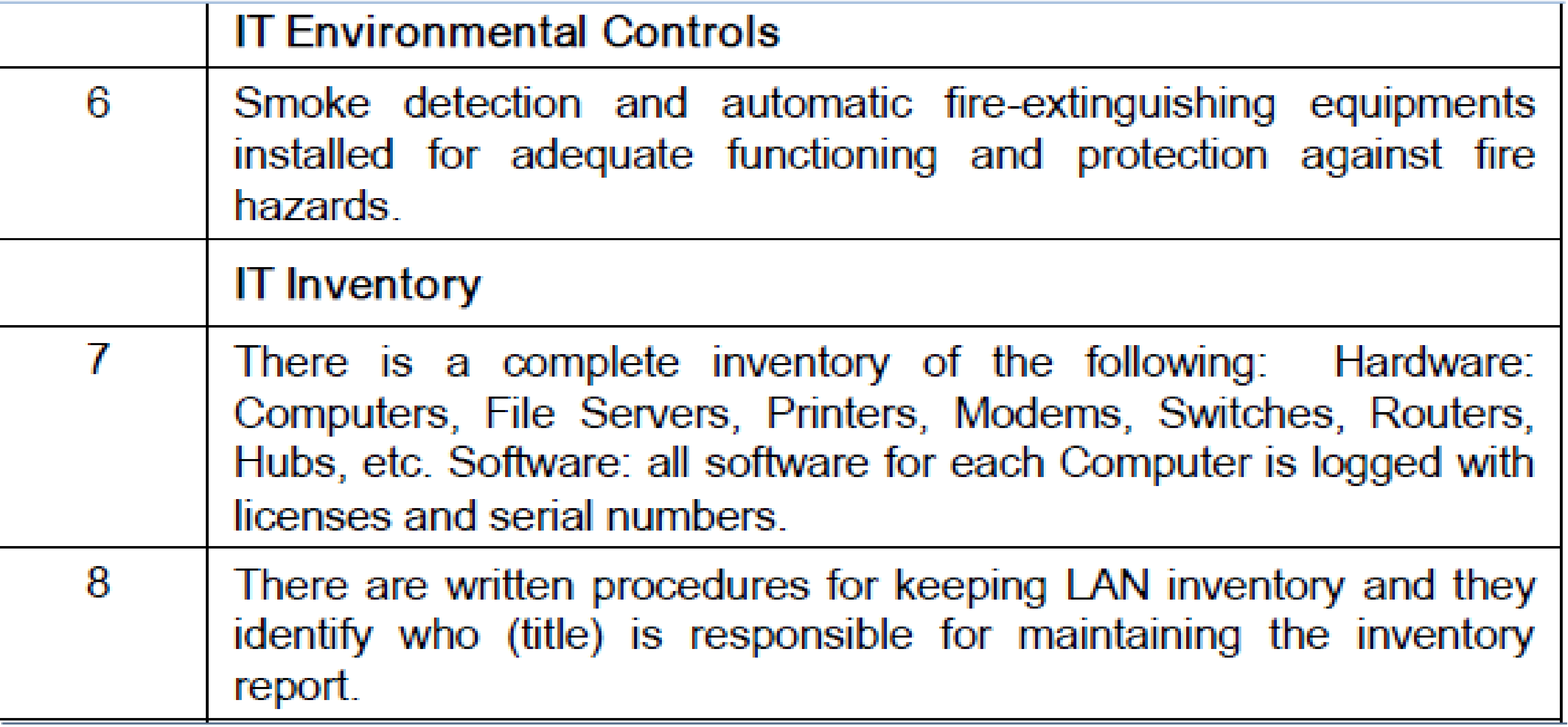
- ***b. Uniform processing of transactions****: Computer processing uniformly processes like transactions with the same processing instructions.*
- *Thus, the clerical errors ordinarily associated with manual processing are virtually eliminated. Conversely, programming errors (or other systemic errors in hardware or software) will ordinarily result in all transactions being processed incorrectly.*
- ***c. Lack of segregation of functions****: Many control procedures that would ordinarily be performed by separate individuals in manual systems may become concentrated in a IT environment. Thus, 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****: The potential for human error in the 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. Also, the 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. In addition, decreased human involvement in handling transactions processed by computer information systems can reduce the potential for observing errors and irregularities. Errors or irregularities occurring during the design or modification of application programs or systems software can remain undetected for long periods of time.*

- ***Review of Information Technology Environment***
- ***Para 14.***
- *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, if any;*
- *d) **General controls like segregation of duties**, physical access records, logical access controls;*
- *e) **Application controls** like input, output, processing controls;*
- *f) **Excerpts from the IT policy** of the entity relating to business continuity planning, crisis management and disaster recovery procedures.*

SIA 14 – Key IS Controls



Sr. No.	CONTROL PARAMETERS
	IT Access Control
1	There is a structured IT Policy and facility personnel are aware of the applicable policies.
	IT Back-up and Recovery
2	The network has adequately documented backup and recovery procedures/plans/schedules for critical sites.
3	LAN is supported by an uninterruptible power supply (UPS).
4	UPS tested in the last year (to test the batteries)?
5	For disaster-recovery purposes, LAN applications have been prioritized and scheduled for recovery based on importance to the operation.



	IT Environmental Controls
6	Smoke detection and automatic fire-extinguishing equipments installed for adequate functioning and protection against fire hazards.
	IT Inventory
7	There is a complete inventory of the following: Hardware: Computers, File Servers, Printers, Modems, Switches, Routers, Hubs, etc. Software: all software for each Computer is logged with licenses and serial numbers.
8	There are written procedures for keeping LAN inventory and they identify who (title) is responsible for maintaining the inventory report.

9	Unused equipment is properly and securely stored.
	IT Operations
10	LAN administrator has a backup person.
11	LAN administrator monitors the LAN response time, disk storage space, and LAN utilization.
12	LAN administrator is experienced and familiar with operation of the LAN facility.
	IT Physical Security
13	Alarms installed at all potential entry and exist points of sensitive areas.
	IT Service Agreements
14	Vendor reliability considered before purchasing LAN hardware and software.
15	Service log maintained to document vendor support servicing.
16	LAN hardware and software purchase contracts include statements regarding vendor support and licensing.
	IT Virus Protection Policy
17	The level of virus protection established on servers and workstations is determined and the monitoring of infection are being done by IT administration. Virus Application should be updated on a monthly basis. Laptops if issued should be ensured to have secured internet access.

ICAI - FAIS : Application in IS Audit

- FAIS NO. 210: ENGAGEMENT OBJECTIVES
- FAIS NO. 220: ENGAGEMENT ACCEPTANCE & APPOINTMENT – **Consideration of engagement factors**
- *(a) Nature of engagement and its primary purpose;*
- *(b) Scope of the engagement and any limitations imposed;*
- *(c) Key stakeholders, their relationships and any conflict of interest;*
- *(d) Execution challenges - access to systems and availability of information;*
- *(e) Requirement and availability of necessary skills and expertise;*
- *(f) Nature and form of deliverables;*
- *(g) Intended users (both primary and secondary); and*
- *(h) Fees and costs.*

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.**

Quality Assurance Process

Information System Auditor ensure - Auditee is aware about other requirements of Auditors –

1. Availability of respective staff
2. Physical Access to Facility
3. Conference Room to be booked for Auditors
4. Telephone & Internet Arrangement
5. Access to different IS applications as a GUEST User

- IS Auditor = consider quality assurance process (e.g., interviews, customer satisfaction surveys, or assignment performance surveys)

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)

- **C. Clauses concerning responsibilities of IS Auditor & team**
- • Engagement team composition in terms of qualification,
- seniority, experience and involvement in the engagement.
- • Confidentiality and limitations in sharing workpapers, such as for Testimony, Quality control, or Peer Review purposes.
- • Form of reports or other communication of results of the engagement.
- • Details of any letters or special reports the Professional needs to issue.
- **D. Clauses concerning other matters:**
- • Billing and payments – Fee basis & billing/payment arrangements.
- • Any restriction of the IS / Cyber forensic professional's liability when such possibility exists.
- • Termination of Engagement or Situations that may warrant withdrawal from Engagement.

MODEL NON-DISCLOSURE AGREEMENT (NDA)

- THIS NON-DISCLOSURE AGREEMENT is made on this …….. day (date) of ………… (Year)
- By and between

- ***In case of Central Government Ministry/ Departments #/State Government Departments***
- President of India/Governor of (name of state) acting through …………………………….. (Name, Designation) of …………………….. (Name of Ministry/ Department) address …………………… hereinafter referred to as "Auditee"which expression shall unless repugnant to the context or meaning thereof ,include its successors and assigns)of the first part.
- ***# In case of Autonomous Societies/ Not-for-profit companies/ Public sector Undertakings/Private sector***
- …………………………. (Name of Company/ Society) incorporated /registered under the Companies Act,1956/2013/ the societies registration Act,1860 having its registered/corporate office at …………………… (hereinafter referred to as "Auditee" which expression shall unless repugnant to the context or meaning thereof, includes its successors, administrators and permitted assigns) of the first part .

- And
- Name incorporated/registered under the…….. Name of the Act having its registered/corporate office at ………………(herein referred to as “Auditor” which expression shall unless repugnant to the context or meaning thereof ,includes its successors, assignors, administrators, liquidators and receivers)of the second part
- Both Auditor and Auditee have given their irrevocable consent to fully comply the ______Guidelines thereof without any reservations.
- **NOW, THEREFORE, in consideration of the foregoing and the covenants and agreements contained herein, the parties agree as follows:**
- 1. **Definitions. :** “Confidential Information” shall include ; ______
- **2. Protection of Confidential Information. With respect to any Confidential Information disclosed to it or to which it has access, Auditor affirms that it shall:**
- (a) Use the Confidential Information as necessary only in connection with scope of audit and in accordance with the terms and conditions contained herein;

- (b) Maintain the Confidential Information in strict confidence and take all reasonable steps to enforce the confidentiality obligations imposed hereunder, but in no event take less care with the Confidential Information that the parties take to protect the confidentiality of its own proprietary and confidential information and that of its other clients;
- (c) Not to make or retain copy of any details of products and/or services, prototypes, business or marketing plans, Client lists, Proposals developed by or originating from Auditee or any of the prospective clients of Auditee.
- (d) Not to make or retain copy of any details of results of any information security audits, tests, analysis, extracts or usages carried out by the Auditor in connection with the Auditee's products and/or services, IT infrastructure, etc. without the express written consent of Auditee.
- (e) Return to the auditee, or destroy, at auditee's discretion, any and all Confidential Information disclosed in a printed form or other permanent record, or in any other tangible form (including without limitation, all copies, notes, extracts, analyses, studies, summaries, records and reproductions thereof) immediately on (i) expiration or termination ofthis agreement, or (ii) the request of Auditee therefor.

- (f) Not to send Auditee’s audit information or data and/or any such Confidential Information at any time outside India for the purpose of storage, processing, analysis or handling without express written consent of the Auditee
- (g) Not to discuss with any member of public, media, press, any or any other person about the nature of arrangement entered between Auditor and Auditee or nature of services to be provided by Auditor to Auditee.
- (h) Make sure that all the employees and/or consultants engaged to undertake any audit on its behalf have signed the mandatory non-disclosure agreement.

- **3. Onus.**
- Auditor shall have the burden of proving that any disclosure or use inconsistent with the terms and conditions hereof falls within any of the foregoing exceptions.
- **4. Remedies.**
- Auditor affirms that damages from such disclosure or use by it may be impossible to measure accurately; and injury sustained by Auditee / its clients may be impossible to calculate and compensate fully.
- In addition Auditor shall compensate the Auditee for the loss or damages caused to the auditee actual and liquidated damages which may be demanded by Auditee.
- Liquidated damages not to exceed the Contract value.
- Auditee shall be entitled to recover all costs of litigation including attorneys' fees which it or they may incur in connection with defending its interests and enforcement of contractual rights arising due to breach of this agreement by Auditor.
- **5. Need to Know.**
- Auditor shall restrict disclosure of such Confidential Information to its employees and/or consultants with a need to know .
- No information relating to auditee shall be hosted or taken outside the country in any circumstances

- **6. Authority.**
- The parties represent and warrant that they have all necessary authority and power to enter into this Agreement and perform their obligations hereunder.
- **7. Governing Law –** dispute
- **8. Binding Agreement**
- **9. Amendments**
- **10. Non-solicitation -**
- Auditor shall not solicit or attempt to solicit Auditee’s employees and/or consultants, for the purpose of hiring/contract (2 or 3years)
- **11. Term of agreement**
- IN WITNESS HEREOF, and intending to be legally bound, the parties have executed this Agreement to make it effective from the date and year first written above.
- **(AUDITEE)   (AUDITOR)**
- WITNESSES:
- 1.   2

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

IS Audit periodicity

- Process, Site audit, outsourcing activities, Compliance to IT ACT - **Once in a year**
- Application Controls Audit - **Once in a year**
- Network Audit - **Once in a year**
- Firewall Rule base Review/Audit - **Half Yearly**
- Penetration Testing - **Quarterly**
- Vulnerability Assessment & Core Firewall, Router & Switch - **Half Yearly**
- Database Audit **- Once in a year**
- Migration Audit (One Time)
- Cyber Security Framework(One Time)

Using Work of Others- SA 620

- IS Auditors should, where appropriate, consider using work of other experts for audit
- ii. They should assess, and then be satisfied with:

❑ professional qualifications,

❑ competencies,

❑ relevant experience, resources,

❑ independence and

❑ quality control processes, prior to engagement

- IS Auditors to determine & conclude whether:
- the work of experts is adequate & competent to enable them to conclude on current audit objectives.
- Such conclusion should be documented
- IS Auditor's views, relevance & comments on adopting expert's report should form a part of IS Auditor's Report

SOC Testing(service org)

- User manual
- - System overview
- - Technical manuals
- - Contract or service-level agreement between entity and organisation
- - Reports by service organisation, internal auditors, or regulatory authorities, on service organisation controls
- - Reports by an auditor of the organisation (service auditor), including management letters
- IS Auditors may use a service auditor to perform procedures such as tests of controls at service organisation, or substantive procedures on the entity's IS operations, served by a service organisation.

Draft Report & Follow-up

- Professional bodies like ISACA, IIA, ICAI have issued guidance
- *Reporting and follow-up entails following activities or steps :*

1. - Drafting audit summary and memorandum
2. - Discussing findings with management
3. - Finalising and submitting reports
4. - Reviewing the Actions taken report
5. - Undertaking follow-up procedures
6. - Archiving documents

- **Evidences and Documentation**
- - **Detailed review of working paper** prepared by less experienced member of the IS Audit team, by a more experienced member, who did not participate in the preparation of such working paper

ASM

- **Audit Summary and Memorandum :**
- **An IS Auditor should perform audits** or reviews of control procedures and form a conclusion about, and reporting on, the design and operating effectiveness of the control procedures based on the identified criteria.
- **The conclusion for an audit** is expressed as a positive expression of opinion and provides a high level of assurance.
- **The conclusion for a review** is expressed as a statement of negative assurance and provides only a moderate level of assurance.

SA 560 – Subsequent Events

- Events sometimes occur, **subsequent to point in time or period of time of the subject matter being tested, but prior to the date of the IS Auditor's report**, that have a material effect on the subject matter -- require adjustment or disclosure in presentation of subject matter or assertion.
- **Update Audit Summary Memorandum**
- Conclusion about specific risk
- The result of subsequent reviews and conclusion

IS Audit Progress status Report

- **a. Audit Plan** & proposed vs actual progress in Cyber Audit **-** weekly basis.
- b. **Dates and Locat**ions of Proposed and Actual Cyber Audit exercise.
- c. **Summary of Cyber Audit findings**, identification tests & results of tests.
- d. **Analysis of vulnerabilities and issues of concern** of Cyber Security needs to be reported on **a weekly basis**.

IS Audit Report

- IS Auditors should review & assess conclusions drawn from evidence obtained as basis for forming an opinion on effectiveness of control procedures based on identified criteria.
- **Major findings identified during an audit** = definite time line indicated for remedial actions, these should be followed up intensively and compliance should be confirmed
- **ATR**
- After reporting of findings & recommendations, IS Auditors should request and evaluate relevant information to conclude whether appropriate action taken by management in timely manner
- **Follow-up Procedures**

IS Audit Report coverage

- Description of **scope of audit**, including :
- > Identification or description of area of activity
- > Criteria used as a **basis for IS Auditor's conclusion**
- > A statement that **maintenance of effective internal control structure, including control procedures for area of activity, is <u>the responsibility of management</u>**
- - A statement that **IS Auditors have conducted the engagement to express an opinion on the effectiveness of control**

IS Audit Report content format

1. Identification of auditee (Address & contact information)
2. Dates and Location(s) of audit – IS Audit period
3. Terms of reference (as agreed between auditee and auditor), including standard for IS audit, if any
4. IS Audit plan
5. Explicit reference to key auditee organisation documents (by date or version) including policy and procedure documents
6. Additional mandatory or voluntary standards applicable to auditee
7. Summary of IS audit findings including identification tests, tools used and results of tests performed
8. Risks associated with Gaps, deficiencies, vulnerabilities and Analysis of the same.
9. Detailed report of network, application audit including VAPT with recommendations and suggestions.
10. Summary of audit findings including identification tests, tools used, results of tests performed during IS Audit and recommendations for corrective action.
11. Personnel involved in the audit