**HCL CORPORATION PRIVATE LIMITED**
CIN: U74120DL2008PTC183849
A 9, Sector 3, Noida, 201301, U.P, India
Tel: +91 120 3667180
Registered Office: 806, Siddhartha, 96, Nehru Place, New Delhi – 110019
www.hcl.com

# INFORMATION SYSTEMS AUDIT

**(Approved in the Board dated 8th January, 2024)**

Information Systems Audit is a managerial, technical and organisational process to ensure proper utilization of Information Technology and systems to strategically align with the overall mission and goal of organisation. Information Systems Audit should not be viewed as controlling procedure, but as a means of leveraging maximum return on investments from IT investment and better dissemination of Information resources to the stakeholders.

Information systems form the backbone of all decision support systems with senior management relying heavily on the outputs, reports and business intelligence generated by the Management Information Systems. The task of Information Systems Audit ("ISA") is to ensure that authentic, qualitative information is made available to all the stakeholders at all times. ISA also encompasses the domain of software development environment, IT enabled services and software products. ISA is a solution to ensure that the procedures, controls and practices are pursued religiously. The defining role of IT is in knowledge management, knowledge sharing and information transparency.

## Background

ISA is a technical, managerial process undertaken by independent auditing experts in IT and systems to verify and validate the systems and technologies in an organisation. The objective of ISA is to align the IT strategy of the organisation with the overall business goals and mission.

ISA is more a necessity than a milestone review in IT deployment. ISA has to be carried out at every stage of the technology life cycle in the organisation. The need for auditing financial systems became more pronounced due to the risk involved in operations.

Information flow and its impact on the organisation's value chain make IT an enabler to business. Senior Managers in the organisation are accountable for the substantial business expenditures in IT infrastructure. The significant rise in usage of IT in business has created a need for communication controls, securing knowledge assets and intellectual property and disaster planning. Electronic Data Processing (EDP) process auditing provides for above controls through systematic verification and validation procedures.

The audit function in information systems is an extension of the testing phase of the software development life cycle. Software verification is the process of knowing "Is the software built right ?" while the software validation is the process of

answering the question, "Is it the right software product ?". Verification and validation of software during development stages of software has become an important requirement for achieving process maturity, and better software reliability. The question is "What happens after the software is delivered ?". It is a fact that all software will undergo a change through periodic maintenance.

An independent IS auditor will work in conjunction with the organisational goals to ascertain the management and control of IT in the organisation. IT security manager will formulate and implement the security protocols, provide authorization and control to safeguard data, passwords, and system operations to prevent unauthorised access to computer systems. This facilitates better co-ordination, control and greater commitment.

**OBJECTIVE**

The objective of the IS Audit is to provide an insight on the effectiveness of controls that are in place to ensure confidentiality, integrity and availability of the organization's IT infrastructure. IS Audit shall identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local and wide area networks, physical and information security, telecommunications etc.

**Coverage**: IS Audit should cover effectiveness of policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address deficiencies and follow-up. IS Audit should also evaluate the effectiveness of business continuity planning, disaster recovery set up and ensure that Business Continuity Plan is effectively implemented in the organization. During the process of IS Audit, due importance shall be given to compliance of all the applicable legal and statutory requirements.

## Information Systems Auditor

The function of the IS Auditor is to survey and scrutinize computer systems with the objective of assuring hardware, software, data integrity and efficiency and effectiveness of IT infrastructure in an organisation. The key is to establish controls and control objectives for each business process. Controls are formalized to eliminate errors and irregularities. Data loss is a major IS risk facing an organisation. It is beneficial for an organisation to allow the auditors to be involved in IS planning, development and implementation. The internal audit function increases internal controls over the systems thus improving system performance and quality. The auditor involvement in software life cycle development was identified during three phases; design, milestone reviews and system operations. The verification and validation are done through walkthroughs and inspections to check for any errors. Periodic reliability checks and inspections need to be conducted on the deployed systems. The IS auditor should prepare detailed test cases, simulate worst case scenarios, disaster recovery plans, mock-drills for

IT staff and train the personnel in the art of verification and validation. The IS auditors should be well qualified and should be certified by some authorised professional body e.g. ISACA.

## Systems Development Audit

The first step of audit control is to establish management controls. The exercise starts with study and evaluation of existing systems, concept and operations, feasibility study and information flow. The audit personnel will have to get involved in the requirements gathering stage to verify the system functions. The checklists can be prepared according to the IEEE (Institute of Electrical and Electronics Engineers) standards for Software Requirement Specifications. The auditor can also verify management make or buy decisions for IT acquisition and development. The assessment of software process maturity of third-party vendors can be standardised based on the CMM (Capability Maturity Models) process maturity questionnaire. The application controls form the major operational audit procedures involving, program management, testing of input controls, interfaces and data control limits.

## Capability Maturity Models (CMM)

CMM is a process maturity framework that helps software developers to evaluate their software-delivery capability. Importance of CMM in software process management cannot be restricted to design and development of software. IS auditors can borrow the process maturity questionnaires to evaluate vendors and internal development processes. CMM framework identifies five levels of maturity for software development organization that are Initial, Repeatable, Defined, Managed and Optimized. The strong relationships between CMM and ISA can be identified strongly at Software Quality Management, Defect Prevention and Technology Change Management. The IS Auditor should ask questions modelled on following lines :

- Does the organisation follow a plan for managing technology changes ?
- Are new technology evaluated to determine their effect on quality and productivity ?
- Are improvements continually made to the organisation's standard software process and the projects defined software processes ?
- Does the project conduct casual analysis meetings to identify common causes of defects ?
- Is the process capability of the organisation's standard software process known in quantitative terms ?

## Corporate Governance

It is true that ISA has institutionalized the process of IT governance. There are numerous ethical issues that have been unanswered. Some ethical issues in IS

deployment can unsettle the future of corporate governance.

A financial institution uses higher bit of encryption key against allowed 128-bit encryption keys and not willing to disclose the key to the government agencies.

The Company shall refer to guidance issued by Professional bodies like ISACA, IIA, ICAI in this regard. ICAI has published "Standard on Internal Audit (SIA) 14: Internal Audit in an Information Technology Environment" on the subject.

The Company shall adopt an IS Audit framework duly approved by their Board. Further, the Company shall have adequately skilled personnel in Audit Committee who can understand the results of the IS Audit.

**Personnel** – IS Audit may be conducted by an internal team of the Company. In case of inadequate internal skills, the Company may appoint an outside agency having enough expertise in area of IT/IS audit for the purpose. There should be a right mix of skills and understanding of legal and regulatory requirements so as to assess the efficacy of the framework vis-à-vis these standards. IS Auditors should act independently of Company Management both in attitude and appearance. In case of engagement of external professional service providers, independence and accountability issues may be properly addressed.

**Periodicity** - The periodicity of IS audit should ideally be based on the size and operations of the Company but may be conducted at least once in a year. IS Audit shall be undertaken preferably prior to the statutory audit so that IS audit reports are available to the statutory auditors well in time for examination and for incorporating comments, if any, in the audit reports.

**Reporting** – The reporting framework shall be to the Board or a Committee of the Board viz. Audit Committee of the Board (ACB)

**Compliance** – The Company's management is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during IS Audit. Responsibilities for compliance/sustenance of compliance, reporting lines, timelines for submission of compliance, authority for accepting compliance should be clearly delineated in the framework. The framework may provide for an audit-mode access for auditors/ inspecting/ regulatory authorities.

**Computer-Assisted Audit Techniques (CAATs):** The Company shall adopt a proper mix of manual techniques and CAATs for conducting IS Audit. CAATs may be used in critical areas (such as detection of revenue leakage, treasury functions, assessing impact of control weaknesses, monitoring customer transactions under AML requirements and generally in areas where a large volume of transactions are reported) particularly for critical functions or processes having financial/regulatory/legal implications.

## Conclusion

Information Systems Audit is a specialized task that has to be performed by any organisation that uses IT and systems. The performance of these systems is proportional to the performance of the organization, and any failure will result in loss of stakeholders. IS Audits should be formalized and performed with rigor. It is time when organisation accept the need for audit and control of their IT infrastructure. Institutionalization of ISA and implementation in the organisation is required. The organisation can take lead in creating benchmarks for IT audits.

_____X_____