International Journal of Management and Economics
www.managementjournals.net
Online ISSN: 2664-7079
Received: 04-07-2026, Accepted: 04-08-2026, Published: 19-08-2026
Volume 8, Issue 3, 2026, Page No. 7-9

Information system audit-An examination of the organizational management controls

Dr. Vikas Ranjan
Department of Commerce and Business Administration, Lalit Narayan Mithila University, Darbhanga, Bihar, India

Abstract
Information System Audit means an examination of the management controls within an Information Technology infrastructure and business applications. It can be also known as Computer Audits. The objective of this audit is to obtain reasonable assurance that an organisation safeguards its data processing assets, maintains data integrity, and achieve system effectiveness and efficiency. It reviews the performance of company's operational systems. Also, companies are becoming able to evaluate its performance of operations against planned one and validate that objectives pursued by it remain relevant. The Information System Auditor evaluates the control environment and internal controls regarding information system governance structure, general controls, application controls, system development backup and disaster recovery, data integrity and system security.

Keywords: Application security controls, business continuity planning, information system audit, security policy and standards, system development life cycle

Introduction

Information systems auditing or systems audit is an ongoing process of evaluating controls, collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently. Thus, information systems auditing supports traditional audit objectives, attest objectives (those of the external auditor) that focus on asset safeguarding and data integrity, and management objectives (those of the internal auditor) that encompass not only attest objectives but also effectiveness and efficiency objectives.

An information systems audit performed in an organisation is a comprehensive examination of a given targeted system. The audit consists of an evaluation of the components which comprise that system, with examination and testing in the following areas:

- High-level systems architecture review
- Business process mapping (e.g. determining information systems dependency with respect to user business processes)
- End user identity management (e.g. authentication mechanisms, password standards, roles limiting or granting systems functionality)
- Operating systems configurations (e.g. services hardening)
- Application security controls
- Database access controls (e.g. database configuration, account access to the database, rales defined in the database)
- Anti-virus/Anti-malware controls
- Network controls (e.g. running configurations on switches and routers, use of Access control lists, and firewall rules)
- Logging and auditing systems and processes
- IT privileged access control (e.g. System Administrator or root access)
- IT processes in support of the system (e.g. user account reviews, change management)
- Backup/Restore procedures.

Objectives of Information System Audit

During the System audit, the auditors are required to understand and evaluate the overall control environment. The control environment reflects the overall attitude of, awareness of, and actions by the board of directors, management, and others concerning the importance of internal controls in the enterprise.

General objectives of System Auditing are

- Validation of the organizational aspects and administration of the information service function.
- Validation of the controls of the system development life cycle.
- Validation of access controls to installations, terminals, libraries, etc.
- Automation of internal auditing activities.
- Internal training
- Training members of the information service function department.

The Process of Information System Audit

An Information System Audit process includes

1. Obtaining background information,
2. Understanding the controls,
3. Developing the audit plan,
4. Compliance test of controls,
5. Use of analytical review procedures,
6. Preparing summary of evidences,
7. Evaluation, and
8. Giving an opinion.

Checklist on Systems Audit

Management Controls

1. Security Policy and Standards

- Whether the organization has a Security Policy?
- If a security policy exists, it needs to be examined for adequacy in proportion to the risk.

2. Constitution of Steering Committee

The formulation and implementation of a sound security policy should be a team effort, brought into effect **by** a committee in which there is at least one member of the

Board of Directors apart from the Chief Information Officer (CIO) and user HoDs.

3. Business Continuity Planning

The Auditor should examine all such possibilities by which the availability of Computer Systems is threatened with temporary or permanent breakdown. In sensitive areas, even proofing against mob violence/terrorist strikes should be kept in view.

4. Systems Development Methodology

The documentation should be properly cross-indexed. The effect of a change made in the system should be well understood and thorough testing should be done and documented. The System Auditor should get necessary evidence and comment on the lack of proper adherence to procedure.

Operational Controls

1. Monitoring physical assets

- Whether monitoring of physical assets are done in regular intervals?
- Any discrepancy in the data collected and the current data of physical assets are addressed immediately or not?

2. Ensure adequate environmental controls:

- Whether proper facilities of Air-conditioning (dust, temperature & humidity controls), Power Conditioning (Online UPS functioning all the time with backups, proper earthing) are timely reviewed?
- Whether the cable connections/electronic points are functioning properly or not is reviewed on regular intervals?

Organizational Controls

- Whether the roles, responsibilities and duties of User Departments and IT Department are defined?
- The CIO should have three repartees- one for taking care of the development team, one for ensuring Information System / IT Centre security and another for managing the facilities (i.e., operations and maintenance of hardware), OS, database administration, vendor management, service providers etc.

Application Controls

Whether each of the Computer Systems and subsystems must have its own set of controls for Inputs, processing & outputs. Processing controls should also ensure checks for legal compliance:

- Provision for annual health check-up and medical facilities has also been made which enhances labour productivity and increases life expectancy.
- Statutory provision has been made for the first time to issue appointment letter to every employee of the establishment which leads to formalized contract of employment that increases job security and enables a worker to claim statutory benefits such as minimum wages, social security etc.
- Provision of Re-skilling Fund for skill development of workers.
- The gig worker and the platform worker have been defined for the purpose of formulating schemes to provide social security benefits. Social security schemes can be formulated from the contribution of aggregators, and the other sources con include funds from the Central and State Governments.
- A worker engaged under Fixed Term Employment (FTE) is entitled for all the benefits which are available to permanent employees and has also been made eligible for gratuity if he renders service for a period of one year.
- Every worker is entitled to annual leave with wages after working for 180 days in comparison to 240 days (at present). Provision for encashment of leave on demand by a worker while in service at the end of calendar year.
- Applicability of Employees' Provident Fund has been extended to all industries as against scheduled industries at present.

The Information System Auditor

The Digital Revolution is transforming the traditional ways of doing business, necessitating realignment of profession to leverage the multiplier of digital-technology enhanced efficiency, scale and speed, effectiveness agility and giving access to newer markets. In view of the rapid technological changes, it is imperative for Information System Auditors to adapt, be innovative in aiding organisations to improve its control environment and strengthen governance of IT Risks.
The responsibilities of an Information System Auditor include

- Evaluate risk, document processes & systems in Flow Chart
- Form & Design audit programs
- Review to ensure high quality deliverables & minimum review iterations.
- Apply audit lessons to reduce recurring review comments
- Draft written reports and audit findings and present the same to the management
- Suggest enhancement in controls, policies & procedures
- Follow-up on client execution of management actions
- Demonstrate project management skills
- Manage audits to meet target dates within budgeted hours
- manage multiple projects
- Communicate hurdles & status of projects to Audit services management
- Manage technology governance methodologies & frameworks
- Assess technology risk and accordingly develop audit plans
- Measure control requirements and compliance
- Oversee and report status of audit remediation activities
- Handle completion of corrective actions
- Innovate control automation to minimize compliance cost
- Guide on emerging operational, legal & regulatory compliance matters

The Information System Auditor has to adhere following 7 principles:

1. Integrity,
2. Fair Presentation,
3. Due Professional Care,
4. Confidentiality,
5. Independence,
6. Evidence-based approach, and
7. Risk-based approach.

Conclusion

Information System Audit aims to verify the security controls and evaluate the risk of information systems within the infrastructure of the organization. The audit approach to information systems is based on preventive protection against risks and the occurrence of any kind of loss to the organization. This makes it possible to address all potential weaknesses or omissions of controls and to determine whether this could lead to significant non-compliance with regulatory requirements.

Many organizations, no matter their size or scope of operation, have come to realize the importance of using Information Technology to stay ahead in the current global scenario. Companies have invested in Information Systems because they recognize the numerous benefits IT can bring to their operations. Management should realize the need to ensure IT systems are reliable, secure and invulnerable to computer attacks. The importance of information security is to ensure data confidentiality, integrity and availability. Hence, we may conclude that Information System Audit is critical for every organisation.

References

1. Doshi H, Patel H. The Beginner's Guide to Information System Audit. Notion Press, Chennai, 2022.
2. Mehta AM. Auditing Information Systems- A Practical Approach. Conestoga Open Learning, Kitchener, 2024.
3. Namuduri K. Information Systems Auditing- Going Beyond Compliance. International Journal of Auditing Technology,2013:1(1):45-51.
4. Shah S. Information System Audit-Role of CMAs. The Management Accountant,2021:56(9):45-47.
5. Weber R. Information Systems Control and Audit. Pearson Education India, Noida, 2002.
6. www.cag.gov.in
7. www.iibf.org.in
8. www.isaca.org
9. www.issai.org