International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

IT Auditing and its Standards

Dr D S Kushwaha[1], Ankur Singh[2]

[1]Director (R&D), SR Institute of Management& Technology, Lucknow-226201 (India)
Email ID: *drkushwaha[at]rediffmail.cm*

[2]Research Scholar, SR Institute of Management& Technology, Lucknow-226201 (India)

Abstract: ***Information Systems Audit is the process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allows organizational goals to be achieved effectively and uses the resources efficiently.The IT Auditor should see that not only adequate internal controls exist in the system but they also wok effectively to ensure results and achieve objectives. Internal controls should be commensurate with the risk assessed so as to reduce the impact of identified risks to acceptable levels. IT Auditors need to evaluate the adequacy of internal controls in computer systems to mitigate the risk of loss due to errors, fraud and other acts and disasters or incidents that cause the system to be unavailable***

Keywords: IT Auditing, Information System, data integrity, risk assessment, System Availability

1. Introduction

The use of computers and computer based information systems have pervaded deep and wide in every modern day organization. An organization must exercise control over these computer based information systems because the cost of errors and irregularities that may arise in these systems can be high and can even challenge the very existence of the organization. An organizations ability to survive can be severely undermined through corruption or destruction of its database; decision making errors caused by poor-quality information systems; losses incurred through computer abuses; loss of computer assets and their control on how the computers are used within the organization. Therefore managements across the world have deployed specialized auditors to audit their information systems to find out gaps between declared policies and actual use and shortcomings in the information system design and usage.

Information Systems Audit is the process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allows organizational goals to be achieved effectively and uses the resources efficiently. The IS Auditor should see that not only adequate internal controls exist in the system but they also wok effectively to ensure results and achieve objectives. Internal controls should be commensurate with the risk assessed so as to reduce the impact of identified risks to acceptable levels. IT Auditors need to evaluate the adequacy of internal controls in computer systems to mitigate the risk of loss due to errors, fraud and other acts and disasters or incidents that cause the system to be unavailable

Auditing Standards for Auditing Information Systems

The specialized nature of Information Systems auditing and the professional skills and credibility necessary to perform such audits, require standards that would apply specifically to IS auditing. Standards, procedures and guidelines have been issued by various institutions, which discuss the way the auditor should go about auditing Information Systems. In line with such developments Supreme Audit Institution of India has declared a mission to adopt and evolve standards, guidelines and best practices for auditing in a computerized environment. This will lend credibility and clarity in conducting audit in computerized environment.

The framework for the IS Auditing Standards provides multiple levels of guidance. ***Standards*** provide a framework for all audits and auditors and define the mandatory requirements of the audit. They are broad statement of auditors' responsibilities and ensure that auditors have the competence, integrity, objectivity and independence in planning, conducting and reporting on their work. ***Guidelines*** provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure. ***Procedures*** provide examples of procedures an IS auditor might follow in an audit engagement. It provides information on how to meet the standards when performing IS auditing work, but do not set requirements. The objective of the IS Auditing Guidelines and Procedures is to provide further information on how to comply with the IS Auditing Standards.

While conducting Information System Audit the auditor should consider the issues of confidentiality, integrity and availability (CIA) and his work should be guided by international or respective national standards. These may include INTOSAI Auditing Standards, International Federation of Accountants (IFAC) Auditing Standards, International standards of professional audit institutions such as Information Systems Audit and Control Association (ISACA) and Institute of Internal auditors (IIA) and national auditing standards of SAI member countries.

Information Systems Audit and Control Association (ISACA) has laid down the following generic requirements for IS audit which are applicable to all categories of IS audits –

1) The ***responsibility, authority and accountability*** of the information systems audit function are to be appropriately documented in an audit.
2) The information systems auditor is to be ***independent*** of the auditee in attitude and appearance.
3) The information systems auditor is to ***adhere to the 'Code of Professional Ethics'. Due professional care***

and observance of applicable professional auditing standards are to be exercised.

4) The information systems auditor is to be ***technically competent, having the skills and knowledge*** necessary to perform the auditor's work and has to maintain technical competence through ***continuing professional education.***
5) The information systems auditor is to ***plan*** his work to address the audit objectives.
6) Information systems audit staff is to be ***appropriately supervised*** so as to ensure that audit objectives and applicable professional auditing standards are met. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of ***sufficient, reliable, relevant and useful evidence***.
7) The information systems auditor is to provide a ***report***, in an appropriate form, to intended recipients upon the completion of audit work.
8) The information systems auditor follow-up action timely taken on ***previous relevant findings.***
9) SAI India has adopted COBIT as a source of best practice guidance. The COBIT framework gives an IS Auditor an understanding of business objectives, best practices and recommends a commonly understood and well-respected standard reference. It includes ***Control Objectives, Control Practices and Audit Guidelines, which*** provides guidance for each control area on how to obtain an understanding, evaluate each control, assess compliance, and substantiate the risk of controls not being met.

Information Systems Security and Audit

Organizations in all sectors of the economy depend upon information systems and communications networks, and share common requirements to protect sensitive information. Organizations and professional bodies' work towards establishing secure information technology systems for protecting the integrity, confidentiality, reliability, and availability of information.

Defining security and audit

Information Systems Security Audit is an independent review and examination of system records, activities and related documents to determine the adequacy of system controls, ensure compliance with established security policy and approved operational procedures, detect breaches in security so as to verify whether data integrity is maintained, assets are safeguarded, organizational goals are achieved effectively and resources are used efficiently. Security audit is a systematic, measurable technical assessment of how security policies are built into the information systems.

Professionalism and credibility play a very important role in the auditor's performance of Information Systems Security Audit. He should have full knowledge of the organization and its various functions, at times with considerable inside information. The three fundamental features of an Information System that gets tested in course of security audit are assessment of confidentiality, availability and integrity of the information systems assets. The principle screening variables are various conceivable physical and logical security threats.

The purpose of any audit will be essentially to examine three basic compliances in terms of Confidentiality, Integrity and Availability (CIA) –

- Confidentiality concerns the protection of sensitive information from unauthorized disclosure. Keeping in view the level of sensitivity of the data the stringency of controls over its access should be determined.
- Integrity refers to 'the accuracy and completeness of the information as well as to its validity in accordance with business values and expectations. It is an important audit objective as it provides assurance to the management as well as the users that the information can be relied and trusted upon. It also includes reliability, which refers to degree of consistency of the system to function.
- Availability relates to information and information systems being available and operational when they are needed. It also concerns safeguarding of necessary resources and associated capabilities. This implies that the organization has measures in place to ensure business continuity and timely recovery can be made in case of disasters.

Why is security audit important?

An organization is always subjected to a set of risks in every business and project initiative it undertakes. These include Business Risk, Strategic Risk, Operational Risk and Risk of legal non-compliance. The information systems, while they play significant role in the strategic initiatives of organizations (be it an ERP in a large auto company or be it an e-governance initiative) are also subjected to these risks. Threats can be internal or external to the organization on one hand and a result of some slippage or deliberate intrusion on the other. Thus besides safeguarding the information system, a Security Audit protects the organization's overall interests.

Standardizing security audit-an initiatives so far

Institutions and professional bodies all over the world have issued various guidelines and best practices regarding Information System Security from time to time.

British Standards (BS 7799) provides guidelines to organizations to identify, manage and minimize the range of threats to which information is regularly subjected. These include internal threats, external threats, accidents, malicious actions and industrial sabotage.

International Organization for Standardization (ISO/IEC 17799) guidelines state that the management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

Centre for Internet Security (CIS) Has a mission to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls. CIS benchmarks support high level standards that deal with the "Why, Who, When, and Where" aspects of IT security by detailing "How" to secure an ever widening array of workstations, servers, network devices, and software applications in terms of technology specific controls.

Generally Accepted System Security Principles (GASSP) (which is sponsored by the International Information Security Foundation (I^2SF) promotes good practice and provide the authoritative point of reference and legal reference for information security principles, practices and opinions.

National Institute of Standards and Technology (NIST) has published guidelines to provide a standardized approach for assessing the effectiveness of the management, operational, and technical security controls in an information system and for determining the business or mission risk to an agency's operations and assets brought about by the operation of that system. Under the Computer Security Act of 1987 (P.L. 100-235), the Computer Security Division of the Information Technology Laboratory (ITL) develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. The **NIST IPsec Project** is concerned with providing authentication, integrity and confidentiality security services at the Internet (IP) Layer, for both the current IP protocol (IPv4) and the next generation IP protocol (IPv6).

Commonly Accepted Security Practices & Recommendations (CASPR) provides advice about how to use technologies, products, and methodologies to secure the IT environment, through papers written and vetted by a community of experts.

Bureau of Indian Standards (BIS) describes Information Security Policy as one of the main responsibilities of the management of an organization and thus is a pointer to the roles and functions of the auditor. It talks about identifying all business critical information and evaluating their existing classification, risk assessment, reviewing the security controls to mitigate the risks and suggesting improvements in the Information Security Management System.

Legal Enactments

In 1996, United Nations Commission on International Trade Law (UNCITRAL) adopted ***Model Law on Electronic Commerce***. The Model Law facilitates the use of modern means of communications and storage of information, such as electronic data interchange (EDI), electronic mail and telecopy, with or without the use of paper-based concepts such as "writing", "signature" or "original". The General Assembly of the United Nations by resolution on 30th January 1997 adopted the Model Law on Electronic Commerce. This resolution recommended inter alia that all States should give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information.

In India the IT Act 2000 has provided legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies.

Standards for Auditing Information Systems Security

In addition the generic auditing standards to be followed while auditing an Information Systems, guidelines, practices or benchmarks are necessary to specifically address issues relating to audit of Information Systems Security. We will discuss this issue in respect of three distinct domains of Information System Security viz. Operations System Security, Telecommunication System or Networking Security and Access Control Security which are the sub-themes in this seminar.

1) Operational Systems Security

Operational Systems Security Audit is a process to evaluate the security features of an information system in an organization. This includes examining the internal controls within the system and to what extent are they effective in achieving the objectives of safeguarding of assets and of data integrity and availability. These controls could be preventive, detective, corrective or response-based in nature. The following specific areas come under the scope of a comprehensive security audit of the operational system – Organizational Security, Asset classification and control, Physical and Environmental Security, Personnel security, System Development and Maintenance, Business Continuity Management policies and Compliance to legal framework. The auditor should examine the following issues in respect of procedures and policies laid down by the organization –

a. ***Organizational security*** –Auditor should check that the management has defined a security policy and is committed to implementation of the same, continuously improve upon its effectiveness, spreading awareness among the users and ensuring availability of resources. He should examine how clearly and appropriately the mission statement defines the purpose and goals of the policy to preserve the confidentiality, integrity and availability of computing resources. He should see that–

- The comprehensive security policy approved by the management is in place, documented and communicated to and understood by all concerned.
- It defines clearly the responsibilities of the members of the organizations.
- The policy is reviewed regularly and amended if required with appropriate authorization.
- The procedures are documented and followed as laid down.
- Adequate controls are in place to ensure the security of organization information processing facilities and assets either accessed by third parties or outsourced.
- The policies and procedures are having their intended effect and the confidentiality, integrity and availability of the system and data are maintained and assets are safeguarded.

b. ***Asset classification and control*** – Auditor should examine the classification system adopted to maintain appropriate protection of organizational assets both physical and logical. These models classify the assets and

information into various levels, which describes that who will be allowed access to what resource classifications. For e.g. in military circles, it is common for information to be classified into five levels viz. top secret, secret, confidential, restricted and unclassified and accordingly their information also mirror the principles which are in practice. Access information at each level is decided as per the need- to-know principle. The level of controls required, determines how elaborate a classification should be.

Similarly with reference to the network where there are multiple users, at multiple destinations, including those outside the organization, the IS auditor should examine whether the terminals or network elements are classified appropriately, say for example a company deploys an IP system, with what rationale the network contents are classified as unclassified, shared, company only and confidential. There can be alternative classification systems. The auditor would need to map these classifications with segregation of duties, creation of users, access levels as defined by the organization. The auditor should study the following issues:

- Inventory of all the assets is maintained and is kept up to date – both hardcopy as well as electronically.
- The database of the information assets is maintained along with the designated owner of the asset.
- Classified information is labeled, stored and handled strictly in accordance with the classification level assigned to that information.

c. ***Personnel Security*** – The auditor should satisfy himself with respect to the organization's policy to include security roles in job description, making it binding on the employees and steps taken to make them aware of threats and concerns. He should examine the comprehensiveness of the policy, whether it addresses the issue of violations of the security policy by the employees. He should make an attempt to address the following issues:

- Is there a formal system for reporting and taking preventive and remedial actions in place, which works towards minimizing the damage from such incidents? Are the users following a formal incident response mechanism?
- Is there an Acceptable Use Policy for IT resources and are users complying with the same?
- Is there a mechanism in place to defend the system against techno-vandalism?
- What are the steps taken to make the users aware of the threats and safeguards to the information system and the required remedial measures?

d. ***Physical and Environmental Security*** – The auditor should examine whether the steps taken by the organization adequately prevent unauthorized physical access and interference to the business premises and information assets and prevent loss, damage or theft. To satisfy himself of the adequacy of procedures in this respect, the auditor should see the following issues:

- The equipments are maintained in accordance with the documented procedures.
- Secured areas are created with restricted physical access and guidelines are given to conduct activities in these area.
- Logs of entry and exit are maintained in the system.
- Adequate steps are taken to secure equipments at other related sites.
- The equipments at site are protected from natural disasters like fire, flood, earthquakes etc. and man-made disasters like terrorist attacks, power problems etc.
- Necessary facilities like air-conditioning, dust-free environment are in place for smooth functioning of the system.
- The equipments are supported by appropriate maintenance facilities from qualified engineers.

e. ***Communications and Operations Management*** – Controls should be in place to secure all the three stages of data communication viz. assembly, dispatch and retrieval of the data in a network. The auditor should see if a multi-layered security model consisting of some or all of the following: border router filtering, firewalls, intrusion detection systems, domain based security system, host protection, cryptography, physical security, incidence response, defined standards and active monitoring and testing. Security standards would cover examining operating systems, system software, servers, database, personnel, application software, networking protocol etc.

f. ***System Development and Maintenance*** – Auditor should examine the extent to which the security is embedded in the system during development of system and support processes should be verified. Well-documented change control procedures should also be in place for smooth maintenance of the application system. Stringent controls are in place in respect of outsourced software development and facility management.

g. ***Business Continuity Management*** – The auditor should review the disaster recovery plan implemented by an organization to reduce the disruption caused by security failures to an acceptable level. It should be time tested and include clearly laid down preventive steps and recovery controls. This area of audit addresses identification and reduction of risks associated, limiting the consequences and ensuring timely resumption of essential operations. Disaster recovery plans for network failures should be tested in advance and updated periodically. Key personnel should be identified, who would be accessible at the time of any eventuality. All the users should also be aware of the plan and their respective duties.

h. ***Compliance*** – The auditor should check the organizations' compliance to various applicable statutory, mandatory and contractual requirements concerning design, operation, use and management of Information Systems including intellectual property rights, use of licensed versions of all software in use along with the operating systems, safeguarding and protection of organizational records and data, prevention of misuse of information processing facilities, collection of evidence for legal action and regulation of cryptographic controls. It should also be checked whether organization performs regular checks for technical compliance with security implementation

standards and the provisions of the Information Technology Act.

2) Telecommunication Or Networking Security

The network systems encompass various communication network elements and protocols deployed to carry data and information between various users and sites of the information system. As the world becomes more networked and so are the organizations, there is an increasing threat from intruders in the network who can damage the information system, at times beyond repair. Thus an Information Systems Auditor needs to find out the breaches in the security policy, which compromise the Confidentiality, Integrity and Availability (CIA) of network security domain thereby affecting the network performance.

In order to ensure that CIA triad is preserved the auditor should look into the following issues:

Confidentiality

1) A clear description of the security attributes of all network services and protocols used by the organization is clearly laid down.
2) Routing controls exist to ensure that information flows across various nodes of the network do not breach the access control policy of the application.
3) The network layout and architecture and its interface with other external networks are approved by the competent authority.
4) A policy on Network Trust Relationship exists and only approved and authorized networks exchange information.
5) Connections to non-trusted networks are denied by firewall.
6) Communication between two trusted networks is within the scope of approved VPN policy.
7) VPN clients use encrypted VPN tunnels to ensure the privacy and integrity of the data passing over the public network.
8) Cryptographic controls are exercised in compliance with the IT Act enacted in the country. Approved and standard encryptions are applied to protect the confidentiality of sensitive or critical information. Digital signatures are applied to protect the authenticity and integrity of electronic information. Key management system based on an agreed set of standards, procedures and methods is used to support the use of cryptographic techniques.
9) In case of remote locations access is subject to user and node authentication, access to diagnostic ports is securely controlled, controls are there in place to segregate groups of information service and users.

Integrity

1) A firewall policy in tune the departmental Security policy is in place. Firewall are procured from standard vendors and configured as per the organizational policy.
2) Automatic terminal identification is in place to authenticate connections, access to information services use a secure log-on process, users have a unique ID for their own use so that activities can be traced back to them, password management system is strictly followed, use of system utility programmes should be restricted and controlled, inactivate terminal time-out facility exist along with restrictions on connection time.
3) Industry standard routers are used.
4) Reports to the intrusion detection systems are analyzed and remedial actions are taken.
5) The server is protected from unauthorized intrusion and malicious programs using firewall and anti-virus programs.
6) Non-repudiation services are used for important communications.
7) Procedures for incidence response are in place, which are indicative of an organization's preparedness to deal with threat situations.
8) The audit should see that a well-defined policy on use of network services exist and users have access to services for which they have been authorized.

Availability

1) Fault tolerance for data availability is identified keeping in view the criticality of the information.
2) Regular exercises are undertaken to make relevant personnel familiar with the computer incidents and breaches in security.
3) Back-ups are taken as per the laid down policy by the designated officials, periodically tested and record of the test is maintained. Back-ups are taken in more than one sets and kept at a safe and secure place.
4) Operational network logs are maintained, analyzed and remedial action is taken.
5) All servers, firewalls, routers and other mission critical workstations units have back-up power supply.

Access Security

Access Security encompasses control on access to information, prevention of unauthorized access to information systems, unauthorized user & computer access, protection of network services, detection of unauthorized activities and providing security during computing and teleworking processes. Audit of access security would require an auditor to see whether the organization has defined and documented business requirements for access control and an access control policy for restricted access. Auditor should review the user access and information access management in the organization in great detail to assess the adequacy of controls. The access controls should be defined in the application at the time of its development and tested. In case of a third party maintenance or facility management the access should be defined in a way so as not to compromise the CIA of data.

In order to ensure that CIA triad is preserved the auditor should look into the following issues:

Confidentiality

1) A password policy should be designed keeping in view the criticality of the application. It should contain parameters such as composition of user ID and password, frequency of changing the password, minimum password length, etc. The auditor should attempt to seek answers to following questions:
   - Are the users' IDs unique and only one per user?
   - Are passwords difficult to crack?
   - Are there access control lists (ACLs) in place on network devices to control that has access to shared data?
   - Are there audit logs to record who is accessing data?

- Are the audit logs reviewed?
- Are the system-generated passwords stored in the system?
- Are the password generated algorithms protected?
- Is there any limit for consecutive unsuccessful attempts to log-on?
- Is there a unique combination for user ID and password for a user?
- Are the users informed and asked to follow good security practices in selection and use of passwords
- A formal procedure for registration of a user is in place.

2) The allocation and use of privileges is restricted and controlled.
3) A formal policy and documented procedure for allotment of user ID is in place.
4) The usage rights are reviewed at regular intervals and revised, if necessary.
5) Un-attended equipment is sufficiently protected.

Integrity
While reviewing the Application Controls the auditor should satisfy himself in respect of input data validation, data processing validation, message authentication, output data validation.

Availability
Physical and Logical Access Security – The auditor should verify the adequacy of controls for physical security of information system installations. He should also review the logical security access controls, which include classification of users and their level of access on the basis of segregation of duties, password policy and validations controls.

2. Case Study and Example

SAI India has in recent times taken up IT reviews of important applications implemented in various departments of the Central as well as State Governments on priority basis. Audit's main concern has been to critically examine these systems to ensure that the national and international best practices, standards, procedures are being followed and to find out the impact of these initiatives on governance in general. A few case studies and interesting cases, highlighted in the print media, have been placed in the appendix. These case studies bring out various security lapses, which have been observed in course of audit.

3. Conclusion

Information system security has gained importance with increase in use of Computer Systems and proliferation of Internet. IS auditors have to play an important role given the strategic importance of information systems. Various institutions have attempted and framed elaborate guidelines and standard practices to be adopted while conducting a security audit. We have tried to capture the important issues that would form the basic premise of any security audit standard to protect the confidentiality, integrity, reliability and availability of information systems.

References

[1] 6th ASOSAI Research Project, IT Audit Guidelines
[2] IS 15150 2002 issued by Bureau of Indian Standards
[3] Information Systems Security Hand book for Indian Audit and Accounts Department, Office of the Comptroller and Auditor General of India, December 2003
[4] Information Systems Control and Audit, Ron Weber
[5] Information Security Policies made easy, Charles Cresson Wood