International Journal of Information Technology & Management Information System (IJITMIS)
Volume 6, Issue 2, July-December-2015, pp. 11-20, Article ID: IJITMIS_06_02_002
Available online at http://
http://www.iaeme.com/issue.asp?JType=IJITMIS&VType=6&IType=2
ISSN Print: 0976 – 6405 and ISSN Online: 0976 – 6413
© IAEME Publication

AN EXPOSITION OF MODERN INFORMATION SYSTEM AUDITS

Jinali Gandhi, Umang Shah and Dharmesh Mistry
Computer Engineering, D J Sanghvi College of Engineering, Mumbai, India,

ABSTRACT

There is an ever increasing need for a systemized IT Architecture, in all the business developments in the current hour. The dependency on such architecture is inevitable, as every organization needs safe and secure transaction of data and information. IS Audit here, plays a major role, and it is one of the most prominent methods to maintain the integrity and authenticity of the information databases and transactions. This paper aims to provide an elucidation on the various processes, stages and types of IS audit.

Key words: Audit, Information Systems, Security Audit, Data Integrity, IT Governance.

Cite this Article: Jinali Gandhi, Umang Shah and Dharmesh Mistry. An Exposition of Modern Information System Audits. *International Journal of Information Technology & Management Information System (IJITMIS)*, **6**(2), 2015, pp. 11-20.
http://www.iaeme.com/issue.asp?JType=IJITMIS&VType=6&IType=2

1. INTRODUCTION

An information systems audit is an investigation of the management controls in an IT infrastructure. The assessment of acquired evidence decides if information systems are protecting assets, operating efficiently and maintaining data integrity for accomplishing the organization’s objectives or goals. Such reviews can be done in combination with internal audit, financial statement audit or other kind of attestation engagement. IT audits are also called as “computer audits” and “automated data processing audits [1].

An audit on the level of information security carried on in an organization is called as an information security audit. In the wide scope of auditing information security numerous kinds of audits are there having manifold objectives for diverse audits etc. Usually the controls being audited may be classified as administrative, technical and physical [2]. In an attempt of addressing security risks and revealing how they may be alleviated, this paper presents the importance of information system audit, various tools and techniques used in IS audit, the benefits of it in different domains and more.

2. PROCESS AND TYPES OF IS AUDIT

A typical audit contains various sequential steps.

- Planning an opening conference for discussing the audit timing, objectives, distribution and report format, evaluating the reliability of the business systems and operations and internal controls.
- Discussion of all primary observations with management and discussion of draft audit report and their reactions with management, in case available, earlier to issuing of the ultimate audit report.[3]
- Following up on essential issues upraised in audit reports for determining in case they have been fruitfully resolved. In the opinion of the IT Manager, scope must be clear from the onset of the audit.
- When a scope is determined, a contact for review is provided to an auditor. In many organizations, audit liaison is assigned formally. Frequently, such role fall to a professional of information security, however no expectation is there about audit that it should be somebody in security. By defaulting, it should be IT management chain's highest ranking person, in charge of responsibilities completely involving the systems in the scope of the audit.
- This contact is expected to deliver background information regarding the systems which an auditor may use for planning the audit [4]. Some of the important stages of IS audit are discussed here:

Three major types of audit are internal, external and third party audit. The internal audits are mainly performed by company employees. Agents outside the company mainly perform the external audit and the 3rd party audit is performed by group of experts hired by companies to perform the audit. In all these types following are major stages:

- **General Controls Review**: Review of controls governing development, maintenance and security of the application systems in a given environment: This audit involves reviewing data center, OS, security tool and procedure of controlling program changes.
- **Application Control Review**: Review of controls in application system: involves examining inputs, process and outputs of system data. Communication issues, security, change control and quality issues are examined [5].
- **System Development Review**: This review involves development of new system with evaluation of process and product. General controls in a new application, especially in case of new technical platform or environment are considered.
- **Information Systems Audit activities**: It begins by carrying out plans geared towards integration of Risk Based Audit approach in IS Audit.

3. ARCHITECTURE AND ACTIVITIES OF IS AUDITS

Auditing information security deals with subjects from appraising data centers' physical security to auditing databases' logical security and emphasizes major components to look for and diverse techniques to audit such areas. A company networks are its devices of information sharing and communication. Conversely, "sharing," information security is attacked daily. Both Individuals outside the company and individuals inside the company, will compromise information security.

Since information is shared through email, network drives and attachments dangers enforced by permitting access are intensified. For minimizing such dangers, companies require to conscious of unauthorized access and take measures to safeguard their resources. The below diagram shows the IS audit architecture.

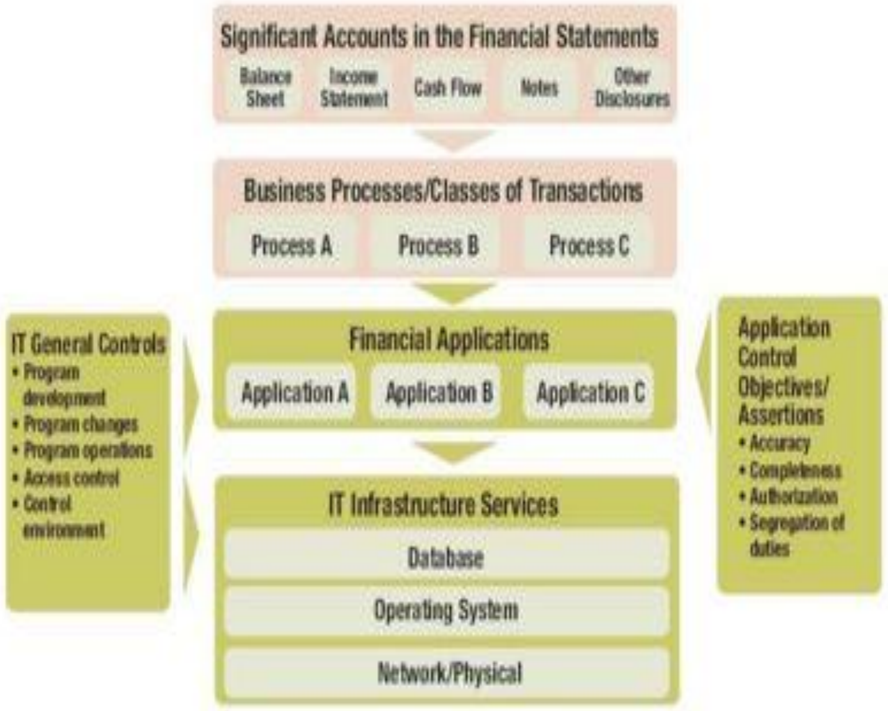

Figure 1 IS Audit Architecture [6]

Some of the significant activities of IS audits are as follows:

3.1 Audit Planning

The audit planning represents the information system complying with audit objectives required by client in compliance with Professional standards and Laws. The main process is firstly, Audit Charter is obtained from client defining purpose, management responsibility and accountability of Information Systems [7]. Audit functions are:

Audit Charter defines mission, goals and objectives of IS Audit. In this stage, Key Performance Indicators and Audit Evaluation process are also defined. Audit Charter must specify Authority given to Information Systems Audit in relation to Risk Assessment to be carried out, specify scope and its limitations, access to client information and functions to be audited and audit expectations [4]. The Audit Charter must delineate assessment of compliance, appraisals, reporting lines and approved actions.

3.2 Risk Assessment and Business Process Analysis

This is the key stage of audit assessment and analysis. It helps in risk evaluation and in relating the cost/benefit evaluation of the control to the identified risk permitting practical choices.

Risk is the likelihood of an act happening that has an adversative influence on the organization and its information systems. Risk may be the possibility, which a given threat will exploit. Risk is the possibility of an act or event occurring that would have an adverse effect on the organization and its information systems. Risk can also be the potential that a specific threat exploiting susceptibilities of an asset or group of assets in causing damage to the assets. Normally, it is measured by possibility of occurrence and a combination of effect. [8]

Various organizations are shifting to an audit approach that is risk-based and can be adapted for developing and improving the constant audit process. Such approach is used for assessing risk and assisting an IS auditor’s decision of performing substantive testing or compliance testing. In such approach, IS auditors also rely on operational and internal controls and also knowledge of the organization [2]. Quantifying risk’s process is known as Risk Assessment. It is beneficial in making decisions like: The business fields to be audited, the timing extent and nature of audit procedures and the amount or resources that are assigned to an audit.

3.3 Performance of Audit Work

While performing Audit Work, Audit Standards of the Information Systems need us to offer supervision, documenting audit work and collecting audit evidence. This objective is accomplished through the establishment of an Internal review Process where another senior person reviews the work of one person. The organizations acquire adequate, relevant and reliable evidence to be acquired through Recompilation, confirmation, Observation, Inspection and Inquiry of calculations. Based on the identification of risky fields and on our assessment of risk, we go forward in developing an Audit Plan and Audit Program. The Audit Plan will comprehend the nature, aims, timing and the extent of resources needed [9].

Data Origination controls refer to controls established for preparing and authorizing data that is entered into an application. The assessment contains review of Transaction ID codes, Alternate documents, User procedures and manuals, Cross reference indices and Special purpose forms. In the data capture process; it will contain a review of separation of duties and authorization procedures [10].

Controls associated with Transaction numbering, Transmission controls, Batch serial numbering, Logs analysis, Processing and a review of turnaround and transmittal documents are controls related to Input preparation controls. Transaction security, batch proofing and balancing, monitoring corrections, Processing schedules and Review of Error messages are involved in Transmission controls [8]. Processing controls since it undertakes processing phase inclusive of Data Storage and Retrieval and Relational Database Controls ensures integrity of data. Output controls procedures contain procedures about records retention, processing output errors, distribution and reconciliation.

3.4 Reporting

On performing the audit test, the Information Systems Auditors is needed to produce and correct

Report communicating the outcomes of the IS Audit. An IS Audit report must recognize proposed organization, recipients and limitations on circulation. It should state conclusions, findings, and limitations and qualifications.

4. APPLICATION DOMAINS

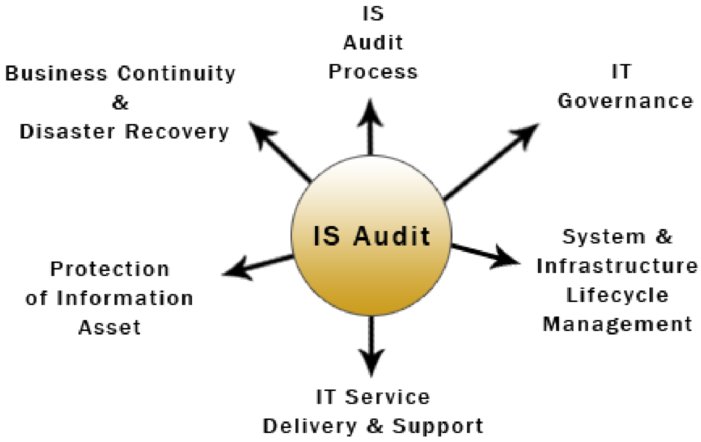
IS Audit Process
Business Continuity & Disaster Recovery
IT Governance
IS Audit
Protection of Information Asset
System & Infrastructure Lifecycle Management
IT Service Delivery & Support

Figure 2 Domains of IS Audit

4.1. Banking Industry

Recently several IT dependent companies are there which depend on the Information Technology for operating their business e.g. Banking Company. Here, IT plays a big role of company containing the application workflow instead of utilizing paper request form, using application control that is quite dependable or executing the banking application to help the organization by making use of an application: One of the most significant roles of the IT Audit is auditing over essential system for supporting the financial auditing or supporting the particular regulations announced e.g. SOX [11]

4.2. Healthcare

Healthcare is one of the modern domains that required IS audit. In a seamless world, access controls only would guarantee security and privacy of electronic protected health information. Conversely, complexities of modern healthcare environment make it is highly challenging to restrict access to the minimum information needed by members of workforce to perform their jobs. In community-based hospitals and smaller organizations, employees do manifold functions, every one of which needs different levels of access [10]

Devoid of having access to particular portions of employees ‘effectiveness, each patient’s health record might be meaningfully inhibited. It is essential for organizations to develop security audits with associated procedures and policies for holding the members of the employees responsible for their actions while opening ePHI via the electronic health record.

Organizations should do security audits using the audit logs and the audit trails which provide a back-end view of system use. Logs and audit trails record major activities, revealing system threads of transactions and access modifications [8].

4.3. Telecom

An AT&T key switch failed because of a procedural error and two software errors, causing communications then switch to become encumbered and making customers making use of credit cards incapable of accessing their funds for eighteen hours. In another event in 1998, a communication satellite entered into an uncontrollable rotation triggering pager communications systems wide-reaching to be "useless", and companies using such technology for the transaction and verification of E-account were incapable of processing credit card information for twenty four hours, in this way initiating their customers in order to pay cash for their dealings [7]. The interruption of paging services produced severe impact on services offered by private as well as governmental organizations that rest on this communication

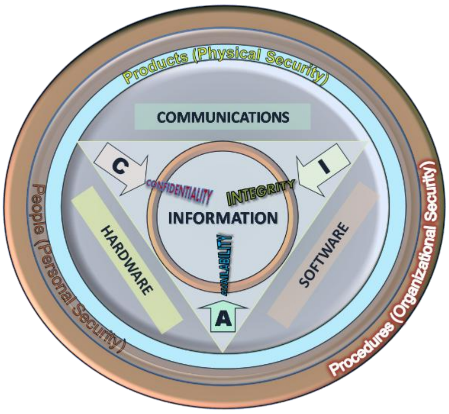
Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
People (Personal Security)
HARDWARE
AVAILABILITY
SOFTWARE
A
Procedures (Organizational Security)

Figure 3 Information Security Audit [6]

Today, telecom organizations function in a dynamic universal multi-enterprise environment having team-oriented place and collaboration very strict needs on the telecommunications network. Such systems' design is complex and management may be quite difficult. Organizations are essentially reliant on timely flow of precise information [12]. A decent way of viewing how strict the network needs are is to study them in connection with telecommunications service. Maybe, two instances of the world's reliance on IT come as an outcome of two described events in the past wherein IT failure obstructed world communications and commerce.

5. NEED OF AN IS AUDIT

The significance of the information security is to guarantee data availability, integrity and confidentiality.

Confidentiality of data refers to the protection of information from revelation to unauthorized parties. Information like personal information, bank account statements, and trade secrets must be kept confidential and private. Protection of this information is a key part of information security. Therefore, an information systems audit would guarantee that the data of the organization is stored confidentially, that integrity of data is guaranteed and at all times data is available for authorized users [13]. An Information systems audit refers to an auditing of IT systems, operations, management and associated procedures of an organization.

The IT auditors may be engaged from the preliminary design and the installation of information systems for ensuring that the three constituents of information security (availability, confidentiality and integrity) will be fulfilled to. Hence, the roles of IT auditors may be summarized as taking part in developing high risk systems, offering technical support for other auditors and offering services of IT risk consultancy [14]. The fundamental fields of an IT audit scope may be summarized as: standards and organization policy, the organization with its management of physical environment wherein the computers operate, facilities of computer, planning of contingency, the functioning of system software, end-user access, the review of user applications and the applications system development process.

As per the analysis and study conducted, it is highly recommended that every organization consider IS audit as a crucial aspect of business process. It is suggested that company that ventures into the new markets must observe that an audit is beneficial in building public reputation and confidence. Supposing a company is establishing itself in a new market, and the head of the business determines that cutting prices is priority. Then the head of the business moves ahead and selects the cut-rate information systems to be installed [3].

The installation process cannot consider several IT controls resulting in to a system which is susceptible to tampering. In case an incident takes place and is stated in the news, such company risks losing any customers and its reputation it might have earned. Managing the incidents of negative security in the news is very much expensive when compared to their prevention in the initial stage [5]. Losing on your reputation implies competitors gaining bigger profit margins and customer base.

Thus it is recommended that, an information systems audit is significant for it provides assurance that the systems of IT are sufficiently protected, offer trustworthy information to users, and are suitably handled in order to accomplish their envisioned benefits. Besides, it diminishes the risks of leakage or data loss, poor handling of IT systems and disruption and data tempering.

6. BENEFITS OF IS AUDIT

Today in business community, IT security auditors have gained popularity since their work enhances value to an organization. Generally, internal audit departments of firms have a constituent of IT auditing that is used with a clear perception over its role in an organization. Conversely, the broader business community requires understanding IT auditing’s function so as to comprehend the full benefit. Particularly, IT auditing involves a wide range of IT processing and communication substructures like operating systems, software applications, web services, security systems, disaster recovery planning, client-server systems and networks, telecom infrastructure, databases and change management procedures [10]. The standard auditing begins with recognizing risks. After this, evaluating controls’ design takes place. Lastly, auditors test the efficacy of controls. Experienced and expert auditors certainly enhance value at every phase of the audit. IT security firms can enhance value of an organization, and a precondition to enhance value is depth and quality of a technical audit [9]. Value is added by IT audits in following various ways:

Also, risk planning and implementation of an IT audit includes evaluation and identification of IT risks in every organization. Generally, IT audit is inclusive of risks associated with availability, integrity and confidentiality of information technology processes and infrastructure. Certain added risks include reliability, proficiency and efficacy of IT if risks are evaluated, there may be clear idea regarding the path to be taken for transferring the risk via insurance, to lessen the risks through controls [9].

Strengthen controls: After assessment of risks, controls may be identified and assessed. Poorly designed controls may be redesigned. Various frameworks may be used by the auditors like Committee of Sponsoring Organization and COBIT of the Tread way Commission background to gain assurance on the efficacy of operations, the trustworthiness of financial reporting, the agreement with relevant laws and regulations and comply with regulations [4]. Different regulations at the state and central levels contain particular needs for the information security. A significant role is by the IT auditor in guaranteeing that all the particular needs are fulfilled, risks are evaluated and controls are executed. IT audit also improves IT Governance. In any company, board of directors and executives has the responsibility of IT Governance. It contains processes, leadership and organizational structures that ensure that IT of organization extends and sustains the objectives and strategies of that organization.

7. TOOLS AND TECHNIQUES USED IN IS AUDIT

7.1 Utility Tool

One of the famous tool is the utility tool. Utility Tools are single purpose tools that can be either innate to the operating system or available freely. Utility tools need a manual approach, although often they are contained in customized scripts. Utility tools are available freely and are focused tightly for definite tasks make them more proficient. Manual testing is time consuming for a large audit and can generate unpredictable results, dependent on auditor’s skill [3].

7.2 COBIT

COBIT is one of the renowned frameworks highly used for audit purpose. This tool supports the company managers bring existing gap between business risks and control requirements. COBIT contains an integration of various frameworks which govern the models, measure the outputs of processes and monitor activities, in the form of a single tool. It together defines the processes and its results, objectives, measures of the performance and also the activities [11].

7.3 Power Tool

Power Tool is another famous tool. Multifunction utilities envisioned modernizing and automating the process of auditing. Although some are open source packages, several are commercial products having custom susceptibility databases. Automated tools against a database scan vulnerabilities against databases. Alerts can be tied into tools of help desk monitoring. In several cases, scanning tool may be combined with a firewall station. Several commercial scanners generate brilliant reports explain exposures and connected risk [15]. In their databases, scanners merely check for susceptibilities that must be recent. Several scanners are sold on the number of susceptibility checks done. A computer program does not have intuition and merely works as programed. A scanner is unable to assess risk precisely.

7.4 NMAP

Nmap is another service scanning and network tool of selection for majority security professionals. Scanners can check only vulnerabilities in current database. They are marketed based on number of vulnerability checks being performed and this not necessarily an indication of its effectiveness. Many times vulnerabilities may be misdiagnosed. As scanners cannot assess risk accurately, it remains job of auditors [11].

7.5 HPING

Hping expands ping functionality by offering capability of creating custom IP packets for testing security controls. It enables sending arbitrary packets and manipulating IP fields with port scanning capabilities and enables auditor set up listening mode for display of packets returning and matching specific patterns. This helps for testing security controls like firewalls and in intrusion detection and prevention.

7.6 Nessus

Nessus is a vulnerability scanner that identifies known vulnerabilities in OS, applications and networking. Version 4 has expanded functionalities, as it was an open source project introduced 10 years ago. With this version it is now a closed source product, which is owned by Tenable Network Security. This is still available free for the home users for scanning personal devices. For other uses, professional paid license is necessary. The professional feed offers access to new updates and many features like compliance checks support for SCAP protocol, ability to load as virtual appliance and support from Tenable [4].

8. CONCLUSION

Today, overtime hardware and software systems in an organization gets upgraded and with that increases the vulnerabilities that arises. Latest and updated solutions shall be kept on developed for the same. The findings from this study illustrate that an organization must invest regularly in developing complex models for security to have a safe system. It shall be a regular task and not just occasional. Security policy is not just an individual problem but shall be thought of on a global level. One must understand that the weakest link represents the entire system and shall be periodically updated and thus IS audit plays a very important role in multiple domains.

REFERENCES

[1] P. Năstase, Study Regarding Information Systems Audit for E-business, Audit Financiar, 2015, p90-99.

[2] C. BRANDAS, Integrated Approach Model of Risk, Control and Auditing of Accounting Information Systems. Informatica Economica., 2013 , p87-95.

[3] J. Beveridge, A New Practical Guide On Information Systems Auditing. COBIT Focus, 2015, p1-3.

[4] A.M. Suduc, Audit for Information Systems Security. Informatica Economica, 2010, p43-48.

[5] M. K. Wright, Auditor Independence and Internal Information Systems Audit Quality. Business Studies Journal, 2012, p63-83.

[6] Autocons, IT Auditing. Retrieved from http://www.autocons.net/, 2015.

[7] R.E. Cascarino, Auditor's Guide to Information Systems Auditing (New York: Routledge, 2007).

[8] M. Piattini, Auditing Information Systems (London: Cenage Learning, 1999).

[9] G. P. Schneider, Discussion of determinants of information systems audit involvement in EDI systems development. Journal of Information Systems. 2000, p129-132.

[10] Mr. Navanath Jadhav and Mrs. L. Laxmi, Privacy-Preserving Public Auditing For Secure Cloud Storage, *International Journal of Computer Engineering & Technology*, 5(7), 2014, pp. 36 – 42.

[11] V. Hingarh, Understanding and Conducting Information Systems Auditing (London: Sage, 2013).

[12] J. C. Bedard, Information Systems Risk and Audit Planning. International Journal of Auditing, 2005, 12-43.

[13] Eminenceways, Information Systems Audit. Retrieved from http://eminenceways.azurewebsites.net, 2014.

[14] J. J. Champlain, Auditing Information Systems. (London: Sage, 2003).

[15] C. Carnaghan, Discussion of an Analysis of the Group Dynamics Surrounding Internal Control Assessment in Information Systems Audit and Assurance Domains. Journal of Information Systems, 2000, 43-89.

[16] B. Conway, the Information System Audit: A Control Technique for Managers. Management Review, 2000, 22-89.

[17] Dr. Sonali Dasgupta. Improve Energy Efficiency of Electrical System by Energy Audit (Data Logging), *International Journal of Electronics and Communication Engineering & Technology*, **3**(3), 2014, pp. 240 – 245.

[18] Ali Sami Azeez, Public Auditing In Secure Cloud Storage, *International Journal of Computer Engineering & Technology*, 5(3), 2014, pp. 174 - 183.