IPASJ International Journal of Information Technology (IIJIT)
Web Site: http://www.ipasj.org/IIJIT/IIJIT.htm
A Publisher for Research Motivation ..... Email:editoriijit@ipasj.org
Volume 7, Issue 4, April 2019 ISSN 2321-5976

A Comparative Study of Information Systems Auditing in Indian Context

D M Chudasama[1], L K Sharma[2*],N C Solanki[3]and Priyanka Sharma[4]

[1,4]Raksha Shakti University, Ahmedabad
[2,3]ICMR- National Institute of Occupational Health, Ahmedabad
[*]*Corresponding author*

Abstract

Information Technology has become an inevitable resource to many person in the world, either they know about it or not. With almost millions of people connected to the internet along with the growth of technology. E - Commerce is being thoughtabout by entities of all sorts, be it an individual or an organization. E - Commerce involves using Information Technology to transfer data, which is sometime sensitive, over the internet. The use of the web to transmit sensitive information makes the information progressively vulnerable and subject to undesirable consequences resulting from deficient control. Decreasing this potential is the challenge for Information System Auditing (ISA). There is a huge number of data on both E - Commerce and Information Systems Auditing; information pertaining to an interrelationship between the two subjects has been limited. The different countries follow their own ISA mechanism. In this study, a comparative study is performed in the context of Indian auditing process by considering the ISA process of Germany, Canada and Finland.

Keywords: Information Systems Audits, e-Commerce Audits

1. INTRODUCTION

Information System audit is the examination and evaluation of an organization's information technology infrastructure, policies and operations. IS audit can be considered the process of 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 [1][2]. The audit process includes the four steps or phases. It is described in following subsections.

1.1Strategic Audit Planning

In this phase of the strategic audit planning the preparation of the preliminary assessment, information gathering and understanding the organization are performed. In addition, organizational function and the operating environment, organizational structure, criticality of IT systems, hardware and software used, Nature and extent of Risks affecting the systemsare analyzed. Auditor explores organization publications, annual report and previous audit report, checking long-term strategic plans and talks with key personal to understand the business issues and the key organization facilities [1][7].

1.2Definition of audit objectives and scope

Risk management is an essential requirement of modern IS Audits where security play significant role. It can be defined as a process of identifying risk, assessing risk, and action taken to reduce risk within an acceptable level. The three security goals of any organization are Confidentiality, Integrity and Availability.
An organization damage seem to result from a security failure, taking under consideration the potential consequences of a loss of confidentiality, integrity or handiness of the knowledge and different assets. The realistic probability of such a failure occurring within the lightweight of prevailing threats and vulnerabilities, and therefore the controls presently enforced. The four steps can be used for a risk-based approach to making an audit plan are below.

- The inventory information systems in use at the organization and categories them.
- Determine which of the system impact critical functions or assets.
- Assess what risks affect these systems and the severity of impact on the organization.
- Based on the above assessment decide the audit priority, resources, schedule and frequency

An illustrative list of some of the common audit objectives for an IT audit is as follows:

- Review of the controls of the IT systems to gain assurance about their adequacy and effectiveness.
- Evaluation of the performance of a system or a specific programme.
- Analysis of the security of the IT systems.
- Examine the system development process and the procedures followed at various stages involved therein

The scope of audit is determined before the audit. Determining the scope of the audit is a part of audit planning and addresses such aspects as the period and the number of locations to be covered and the extent of substantive testing depending on risk levels and control weaknesses [8].
The objectives and scope of audit could cover one or combination of the firewall security, physical access security, credentials, security setting, user rights etc. aspects.

1.3 Evidence collection and evaluation

Competent, relevant and reasonable evidence should be obtained to support the auditor's judgement and conclusions regarding the organization, program, activity or function under audit. The required data collection technique is chosen carefully. The sound understanding of techniques and procedures is also necessary for the auditors [9].
The following type of audit evidence is required to consider by the auditor.

- Observed process and existence of physical items
- Documentary audit evidence (including electronic records)
- Analysis (including IT enabled analysis)
- Physical evidence is obtained by observation

1.4 Documentation and reporting

The documentation and reporting is an important feature for the future reference. Auditors should adequately document the audit evidence in working papers, including the basis and extent of the planning, work performed and the findings of the audit documentation [10]. The draft and final reports of the audit should form part of the audit documentation. The auditors should record the following documents:

- The planning and preparation of the audit scope and objectives
- The audit programme
- The evidence collected based on which conclusions are arrived at
- All work papers, including general file pertaining to the organization and system
- Observations as the auditor monitored the performance of work. The observations may include the place and time, the reason for observation and the people involved.
- Reports and data obtained from the system directly by the auditor or provided by the audited staff. The auditor should ensure that these reports carry the source of the report, the date and time and the conditions covered.
- At various points in the documentation, the auditor may add his comments and clarifications on the concerns, doubts and need for additional information. The auditor should come back to these comments later and add remarks and references on how and where these were resolved.

2. LIST OF REVIEW POINTS

The information technology is a leading industry in India and the usage of information technology in public and private sector is gradually increasing. Hence, the systematic and effective information system audit is becoming essential in present scenario. The comparative study ofthe ISA process in India [2], Germany [3], Canada [4] andFinland [5] [6] is performed and the pro and cons of these auditing processes is explored. The 10 important components namely a hardware review evaluates the structures, software evaluations cover, documentation covers the details, a system environment review entails, security examines, software security examination explores, hardware security examination, assess of risk of the server going, to down, network hardware instruments, network configuration are considered.

2.1 Hardware Review evaluates the structures

It evaluates the insight into the structures of a variety of various devices and components. It makes too easy of the audits. The comparative analysis of different review points is shown in the Table -1.

IPASJ International Journal of Information Technology (IIJIT)
Web Site: http://www.ipasj.org/IIJIT/IIJIT.htm
A Publisher for Research Motivation .....
Email:editoriijit@ipasj.org
Volume 7, Issue 4, April 2019
ISSN 2321-5976

TABLE 1: A HARDWARE REVIEW EVALUATES THE STRUCTURES

REVIEW POINT	INDIA	GERMANY	CANADA	FINLAND
THE SYSTEM FILESERVERS	YES	YES	YES	YES
WORKSTATION / NETWORK HUBS	YES	YES	YES	YES
MAINTAIN INVENTORY CHART OF HARDWARE	NO	YES	YES	NO
POWER SUPPLIES AND AIR CONDITIONING	NO	YES	YES	NO
COMMUNICATION DEVICES	YES	YES	YES	YES
DESKTOP/ LAPTOPS / PRINTER	YES	YES	YES	YES
MAINTAIN IT EQUIPMENT AND SERVICES	YES	YES	YES	YES
PERIPHERAL	YES	YES	YES	YES
CABLING	YES	NO	NO	YES

2.2 Software evaluations

It is covered up all required parts of the software like installed operating systems, required application or not, user polices with vendors [1]. Software evaluation parameters are shown in Table 2.

TABLE 2: SOFTWARE EVALUATIONS COVER

REVIEW POINT	INDIA	GERMANY	CANADA	FINLAND
OPERATING SYSTEMS	NO	YES	NO	NO
CRITICAL APPLICATIONS	YES	YES	YES	YES
LICENSING	YES	YES	YES	YES
UPGRADE POLICIES	YES	YES	YES	YES
USER TRAINING	YES	YES	YES	YES
STANDARDIZATION AND MORE	YES	YES	YES	YES

2.3 Documentation covers and details

It is to cover up all parts of systems components, user polices and disaster recovery plans of the organizations. The documentation cover is explored during audit process is shown in Table 3.

TABLE 3: DOCUMENTATION COVERS THE DETAILS

REVIEW POINT	INDIA	GERMANY	CANADA	FINLAND
SYSTEM COMPONENTS	YES	YES	YES	YES
LOG FILES	YES	YES	NO	YES
DISASTER RECOVERY PLANS	YES	NO	YES	NO
USER POLICES	YES	YES	YES	YES

2.4 System environment review entails

An auditor function has auditing organization well trained; which keep all necessary document before him/her going[1][4]. Table 4 shows the different review points.

TABLE 4: A SYSTEM ENVIRONMENT REVIEW ENTAILS

REVIEW POINT	INDIA	GERMANY	CANADA	FINLAND
CRITICAL SYSTEM FUNCTIONS	YES	YES	YES	YES
MANAGEMENT ATTITUDES	YES	YES	YES	YES
TRAINING POLICIES	YES	YES	YES	YES
KEY TECHNOLOGY PERSONNEL	YES	YES	YES	YES
INFORMATION SYSTEM BUDGETING	NO	NO	YES	YES
OBTAIN COPIES OF PAST SECURITY AUDITS	NO	YES	YES	NO

2.5 Security examination

It is examination of the all access point of hardware, checking the entirepassword, determine all the internal controls, identify the key application and back of systems [10]. Table 5 shows comparative chart of security examination followed by the selected country.

TABLE 5: SECURITY EXAMINES

REVIEW POINT	INDIA	GERMANY	CANADA	FINLAND
ACCESS CONTROLS	YES	YES	YES	YES
PASSWORD	YES	YES	YES	YES
INTERNAL CONTROLS ON KEY APPLICATIONS	NO	YES	YES	NO
BACKUP SYSTEMS	NO	YES	YES	YES

2.6 Hardware security examination

Hardware security is given the protection on attached physical device and installed software on the hardware of computer systems. It is attached device used to scan a system and monitor network traffic [1]. Table 6 shows comparative chart of hardware security examination followed by the selected country.

TABLE 6: HARDWARE SECURITY EXAMINATION

REVIEW POINT	INDIA	GERMANY	CANADA	FINLAND
FILESERVER INTEGRITY	YES	YES	YES	YES
HARD DRIVE SPACE	NO	YES	YES	NO
AMOUNT OF RAM	NO	YES	YES	NO
PROCESSOR SPEED	NO	YES	YES	NO
DRIVE PARTITION INFORMATION	NO	YES	YES	NO
OPERATING SYSTEM VERSIONS	NO	YES	YES	YES

2.7 Software security examination

It is very critical phase of the examination because software security auditing is necessary for the conditions under which privileged and powerful software is authorized for use. Determine the extent to which safeguards for the abuse of this software is used including inventory control, physical access control, logical access control, and the establishment of resource limits and the use of monitoring mechanisms [5]. The parameter for the software security examination adopted by the selected country is summarized in the Table 7.

TABLE 7: SOFTWARE SECURITY EXAMINATION EXPLORES

REVIEW POINT	INDIA	GERMANY	CANADA	FINLAND
CRITICAL APPLICATIONS	YES	YES	YES	YES
NUMBER OF LICENSED CONCURRENT USERS	YES	YES	YES	YES
VERSION LEVELS	YES	YES	YES	YES
INTERACTION WITH OTHER APPLICATIONS	NO	YES	YES	YES
WHERE AND HOW APPLICATIONS ARE EXECUTED	NO	YES	YES	YES
INPUT AND OUTPUT CONTROLS	YES	YES	YES	YES
DATABASE STRUCTURE	YES	YES	YES	YES
LEVEL AND TYPE OF SUPPORT BY THE SOFTWARE VENDOR	YES	NO	NO	NO
VIRUS SCANNING	NO	NO	YES	NO

2.8 Assess of risk of the server

This kind of auditing is more beneficial to company or organization against slowserver by providinga faster server to user step to more improvement and making speedy to user [3][4]. The server assess point is shown in the Table 8.

TABLE 8: ASSESS OF RISK OF THE SERVER BREAK DOWN

REVIEW POINT	INDIA	GERMANY	CANADA	FINLAND
DOES THE SERVER HAVE ENOUGH CAPACITY?	NO	YES	NO	YES
IS THE PERFORMANCE ADEQUATE FOR THE ENVIRONMENT?	YES	YES	NO	YES
SHOULD THE OPERATING SYSTEM BE UPGRADED TO THE LATEST SERVICE RELEASE?	NO	YES	NO	YES
ARE THERE ANY INCOMPATIBLE ELEMENTS EMBEDDED IN THE SYSTEM?	NO	YES	NO	YES
IS DATA STORAGE OPTIMIZED FOR ACCESS SPEED AND END-USER EASE OF USE?	NO	YES	NO	YES

2.9 Network hardware instruments

It audits the instrument of the network established in organizationlike necessary, unnecessary, working and non-working instruments and how many of them are involve in network[1][2]. The audit points are shown in the Table 9.

TABLE 9: NETWORK HARDWARE INSTRUMENTS

REVIEW POINT	INDIA	GERMANY	CANADA	FINLAND
SWITCH	YES	YES	YES	YES
HUBS	YES	YES	YES	YES
PROXY SERVER	YES	YES	YES	YES
ROUTER	YES	YES	YES	YES

2.10 Network configuration

Configuration management of network is adequately controlled and managed appropriately [3][4]. The audit points regarding network configuration are shown in the Table 10.

TABLE 10: NETWORK CONFIGURATION

REVIEW POINT	INDIA	GERMANY	CANADA	FINLAND
IP ADDRESS	YES	YES	YES	YES
REMOTE ACCESS	YES	YES	YES	YES
UNIQUE CREDENTIALS	NO	YES	YES	NO
SNMP CONFIGURED	NO	YES	YES	NO
BACKUP / RESTORE	NO	YES	YES	YES
VULNERABILITY	NO	YES	YES	YES
FIREWALL	YES	YES	YES	YES
LAN/WAN	YES	YES	YES	YES
PREMISES DEVICES AND HUBS	YES	YES	YES	YES
DISABLED PORTS	YES	YES	YES	YES
EXPLICIT PERMITS	YES	YES	YES	YES
IMPLICIT DENIES LOGGING AND ALERTS	YES	YES	YES	YES
ROUTING PROTOCOLS	YES	YES	YES	YES
HARDWARE CONFIGURATION ARE DULY AUTHORIZED	NO	NO	YES	YES

3. DISCUSSION

India audit system follows the hardware review point of views the system file server, workstation/network hubs, communication devices, desktop / laptops / printer, cabling, peripheral and maintaining its equipment and services. However, India audit system is not maintaining an inventory chart of hardware and also power supplies and air conditioning and Canada and Germany follows these things. This two point is more important of the hardware evaluates the structure because hardware inventory which is helpful of stokes maintain ace and helpful for when require any emergence any equipment so it is knowledge of which place is necessary or which place is not necessary.

India audit system checks the critical applications, licensing, upgrade polices, user training and standardization during the audits. This type of similarity follows the Canada and Finland. However, India audit system cannot check the operating systems in ISA. This thing is only checked in the Germany. The operating system is important for security purpose and incorporate in audit checking is necessary.

Documentation Covers the details follow the all point's system components, log files, Disaster recovery plans and user policies. India and Canada only check the Disaster recovery plans, but Germany and Finland do not check this point. Canada is not using the log files. Log files are useful for the records either events that occur in an operating system or other software runs, or messages between different users of a communication software.

India audit system follows the points of critical system functions, management attitudes, training polices, key technology personnel. However, it does not follow information system budgeting and obtain copies of past security audits this thing only apply Canada. Germany does not maintain information system budgeting during audits. Finland

mention budgeting and audit completion in 60 days. Nevertheless, Finland does not contain copies of past security audits. For India require these two points because this is easy to audit process and fast and less expensive. India audit system is not providing the budgeting and time duration for completion of audits so it is process become and long and expensive and wastage more money.

India audit system follows the two points in the mention table access controls and password. India audit system does not follow internal controls on key applications and backup systems. However, Germany and Canada follows these points because backup systems helps for the company or any organization etc. for future data recover and internal controls key application help to hall system to manage to easy.

India audit system audits fileserver integrity, but Canada and Germany audited all points of the mention in the Table 6.

A review auditing point mentioned in the Table 6 is necessary because from the list of all operational information technology systems, networks and applications, review several of varying size and complexity. In the IT documentation, mention the hardware security settings. Mentioned system managers checking all default settings hall the system initialization. Mention the basis of the hardware security settings of reviewed.

India audit system audits critical applications, number of licensed concurrent users, version levels, input and output controls, database structure, level and type of support by the software vendor. India is only country audited level and type of support by the software vendor. Virus scanning auditing is performed in Canada. India audit system lacks some auditing point in mention Table 7 like interaction with other applications (this information gives how many application connected with us), where and how applications are executed (this information necessary for security purpose) and virus scanning (safety against the virus – you are not scanning network so easily enter the virus and destroy the network and also some virus through leaks the information).

India audit system audits the performance adequate for the environment. Germany and Finland follows all the point mention in the Table 8. Indian Auditor does not take a risk of the when sever break down, they do not check the sever have enough capacity, operating system is latest or upgraded, if any incompatible element has embedded in the system, and storage data optimized for access speed and end-user ease of use. This type of auditing gives more benefits to the company or organization because sever going to down how to take against step to more improvement and making speedy to the user.

All four countries audits switch, hubs, proxy server, and router in the Network Hardware Instruments as per mentioned in the Table 9.

India audit system follows IP Address, remote access, firewall, LAN/WAN, premises devices and hubs, disabled ports, explicitly permits, implicitly denies logging and alerts, routing protocols checking during network configuration audits. Only Canada follows the all points mentioned in the Table 10. India and Finland do not use the unique credentials, SNMP configured points checking in the audits. Unique credentials give the situation where my employer has a support contract with a vendor for an application and SNMP configured gives the information about the an application- layer protocol that provides a message format for communication between managers and agents. India audit system does not check the hardware configuration that is duly authorized; this checking is performed in Canada and Finland.

4. CONCLUSION

Audits should have necessary and sufficient observations to support the conclusions reached to support each audit objective. The process of dividing the audit into component parts does not remove the need to make conclusions in relation to the overall audit objectives. The planning decisions have identified the audit issues. Audit evidence has been gathered and performance in the critical areas has been assessed against each of the criteria. Actual performance has been found to be satisfactory or deviations from the standards are known. Further examination of the deviations from satisfactory results of best practices has led to the development of observations. In this study, we compared the ISA process of India, Germany, Canada and Finland and the pro and cons are identified. It is also discussed that were lacking the Indian audit system and how it can be upgraded. The framework of effective information system audit process will be proposed in future work and it will be able to handle the all lacking points in the Indian audit system.

References

[1] H Botha and J A Boon, “The information Audit: Principle and Guidelines”, Libri 53, pp. 23-38, 2003.
[2] Manual of Information Technology Audit, Office of the Comptroller and Auditor General of India, Vol 1 & 2, 2014.
[3] Information security audit (IS audit) - A guideline for IS audits based on IT-Grundschutz - German Federal Office for Information Security 2008 – Version 1.0
[4] National Audit Office of Finland - Auditor General Manual - Finland Registry no. 23/01/2015

[5] Coordinated Audit of Information Technology Security (with Shared Services Canada), Govt of Canada. https://www.canada.ca/en/treasury-board-secretariat/corporate/reports/coordinated-audit-information-technology-security.html [Last access on 14/04/2019]

[6] Katakari 2015, Information Security Audit tool for authorities, the national security audit criteria, Finland, 2015. ISBN: 978-951-25-2778-6

[7] H J Wagner, "Information System Auditing and Electronic Commerce", Thesis, University of Illinosi at Springfield, Illinois, 2001.

[8] M A AKablan, "A Suggested Integrated Framework to Foundation: the Libyan Institute of Internal Auditors: A Pilot Study", Scientific Journal of University of Benghazi, 31(1), pp 34-61, 2018.

[9] M Alles and M A Vasarhelyi, "Adopting continuous auditing", Managerial Auditing Journal, 30(2), pp. 176-204, 2015, doi: 10.1108/MAJ-08-2014-1080

[10] Y D Li, "A Comparative Study about Internal Auditing Approach between Germany and China", Journal of Modern Accounting and Auditing, pp. 71-75, 2006.