The Information System (IS) Audit Process in a Banking System: Case Studies

Jahangir Khan[1] and Dr. Imran Amin[2]
SZABIST
Karachi, Pakistan

Abstract: *The Information System Audit Process defines the overall procedure of planning; conducting audits of IT environment and IT based business process. The information system audit has different steps to cover the whole audit cycle such as IS Audit Planning, conducting IS audit on the basis of audit phases i.e. defining audit subject, audit objective, scope of audit, Pre-audit planning, audit evidence and data gathering, evaluating test, communication with auditee management and preparation of audit report [S. Anantha Sayana].*

For conducting an effective IS audit, an IS Auditor needs to have a good understanding of professional audit standards, policies, procedures and guidelines such as Control Objective for Information & related Technology (COBIT), Information Systems Audit & Control Association (ISACA), IT Governance Institute (ITGI), ISO 27001 etc. These standards define the control measures that should be complied by the business to prevent its IT based business processes from different threats and cyber crime activities [Lance M. Turcato].

Keywords: *Information System (IS) Audit, Audit Charter, Board Audit Committee, IS Audit Process, IS Audit Phases, Internal Controls, IS Audit Controls*

1. INTRODUCTION

Currently, organizations are highly dependent on the Information Technology for their day-to-day business process. Approximately all the business transactions are perform through digital media , which increase the business and financial risk and organization are showing their more concern to reduce and mitigate these threats [David etal 2006].

As other financial sectors, banking industry are also highly dependents on the operation of information technology. Therefore it is necessary for banks to have a information technology department, which can efficiently handle the operational and financial activities based on the digital medium. Currently, the banking sector providing different online services such as ATM operations, Online fund transfer, mobile banking, credit & debit card operations etc. These all plastic money activities are performing through information system resources available in the banking sector and there is no involvement of physical cash. Therefore, the bank's IT department should ensure that the bank's information system can protect and safeguard the bank's interest [Tommie W. Singleton].

For evaluation and assessment of the IT based business processes, the regulatory bodies as well as professional standards, emphasis to develop an internal audit department within the organization, which periodically review and asses organization's IT based business process and application system running within the organization. The internal audit department then needs to develop their internal audit charter for their policies, procedures and guidelines for their internal auditors. Audit Charter defines the role, responsibilities, scope, authority and accountability of the audit function. It is therefore, necessary for an organization to establish and implement its own Audit Charter, which describes the objective and mission of the audit function [Louis Braiotta, JR.].

2. BACKGROUND INFORMATION

2.1 Auditing

Auditing is a process to conduct, assess and evaluate business entities. Auditing is the process through which an entity such as organization, enterprises, employees, system, project, product etc., can be evaluate and on the basis of this evaluation discrepancies/irregularities can be observed. The main purpose of conducting audit is to improve the operational activities of audit entity and raise the loopholes contained in business process of that system [Gerald Vinten].

2.2 Categorization of Auditing

Auditing can be categorized in different parts, which is based on the domain of audit entity and what areas to be covered in auditing. Therefore, the Auditor can plan the audit according to its category [ISACA, CISA Review Manual]:

There are different categories of auditing are available such as Financial Auditing, Operational Auditing, Management/Administrative Auditing, IS Audit, Integrated Audit, Specialized Audit & Forensic Audit [ISACA, CISA Review Manual].

3. INFORMATION SYSTEM (IS) AUDITING

Information System Audit asses the areas under the domain of Information Technology i.e. weather the Information System & Network Infrastructure of an organization are capable enough to safeguards the information and business assets and provide adequate information system security, having provision of data integrity and provide the assurance of information availability for the smooth functioning of business process [David etal].

The purpose of IS Audit, specially performed by the internal auditors, is to define the loopholes, which can becomes the cause of any fraudulent activity through computer resources, so the IS Auditors should conduct audit for the purpose of improvement in such controls [S. Anantha Sayana].

Different professional Information System Auditing standard has been developed, which provide guidelines through which major controls over business activity can be observed, such as Information Systems Audit & Control Association (ISACA), provides the standard, which deals with the policies, framework, controls and quality of business areas in term of IT framework. Therefore, it is necessary for an IS auditor, to have a thorough knowledge of these standards and analyze an audit in terms of weather these policies, framework, audit controls are properly describe and implemented within the organization to avoid any abnormalities [ISACA, CISA Review Manual].

4. IS AUDIT TASK

The following IS Audit task should be followed by the Audit management [David L. Cannon, Timothy S. Bergmann, Brady Pamplin] [ISACA, CISA Review Manual]:

- In compliance with the audit standards, guidelines and procedures; a risk-based audit strategy should be develop and implement for the Bank.
- For the reasonable assurance, that the IT and business/financial asset of a Bank are save and well protected, an audit plan should be develop.
- To meet the audit plan, conduct IS Audit of various entities of a Bank, in compliance with the IS audit standards, guidelines and procedures.
- Always communicate with key stakeholders of business and communicate up-coming issues, possible risk and audit results.
- Risk management and risk control strategy should be develop and implement within the Bank.

5. KNOWLEDGE STATEMENT OF IS AUDIT

An IS Auditor should have the following knowledge for the batter understanding of the IS audit process areas [David L. Cannon, Timothy S. Bergmann, and Brady Pamplin]:

- An IS auditor should have the knowledge of IS related control and control objective e.g. COBIT.
- An IS auditor should know the information gathering techniques and should know how to preserve evidences.
- An IS auditor should have the knowledge of IS audit standards, guidelines, procedure and policies.
- An IS auditor should have the knowledge of IS auditing techniques and IS auditing practices.
- An IS auditor should have the knowledge of audit risk assessment.
- An IS auditor should know the procedure to gather evidences, which will support the auditor’s observation.
- An IS auditor should know, how to plan and manage audit and audit techniques.
- An IS auditor should know the techniques of communication and reporting.

6. COMPETENCY OF IS AUDITORS

An IS auditor should have a knowledge of the latest Audit tools and techniques and should have proper training to utilize these tools and resources. The high level management should provide the facilities to their internal auditors regarding the access and implementation of new audit techniques and the internal auditors should have a related business test environment, so that auditors can use these resources to find out the loopholes in the existing IT setup of an organization [ISACA, CISA Review Manual].

An IS auditor should have the understanding of, how to conduct and plan an IS audit within stipulated time period and should have the idea how to cover the overall domain of Audit entity. Good understanding of related IS Audit standards, guidelines, procedure and policy e.g. ISACA, COBIT etc, are also necessary of an IS Auditors [Lance M. Turcato].

7. AUDIT CHARTER

Audit Charter defines the role, responsibilities, scope, authority and accountability of the audit function. It is therefore, necessary for an organization to establish and implement its own Audit Charter, which describes the objective and mission of the audit function. The Information System audit charter normally developed as the part of the internal audit charter therefore audit charter defines the role and responsibilities of all entities of audit i.e. internal audit and information system audit [Louis Braiotta, JR.].

In detail, the responsibility of audit function covers the big domain of the IS Audit; for example management's responsibility include mission statement, aim, scope and objective, independence, association with external auditor, success factor, key performance indicators (KPIs) etc [David L. Cannon, Timothy S. Bergmann, Brady Pamplin].

8. IS AUDIT PLANNING

8.1. Short Term IS Audit Planning

In short term audit planning, an organizational internal audit management has to develop a proposed audit plan at the start of the year, which describe that what issues will be covered during the year. The selection of the audit assignment for the year should be based on the major risk areas, which can seriously affect the business operations. The priority can also be given to the areas, which has not been audit so far or last audit period exceed more than two years [Sandra Senft, Frederick Gallegos].

8.2. Long Term IS Audit Planning

Long term audit plan should be based on the future strategy of the organization on the basis of IT infrastructure. The IS Audit management should have the information about the major changes that can be implemented within the organization's IT infrastructure [Frederick Gallegos, Sandra Senft].

8.3. Individual Audit Planning

Beside the short and long term audit planning, an Information System (IS) audit team should also need to plan the audit, assigned to them. First of all, the IS audit team should get a deep understanding of the business processes of the audit entity. For example, if the audit team conducting the information system audit of a financial application system, then they need to have the better understanding of what business activity has been performing through this system [ISACA, CISA Review Manual].

9. INFORMATION SYSTEM (IS) AUDIT PHASE

The information system (IS) auditing has different phases that need to be covered. Here, I am going to describe these phase with two case studies performed during the preparation of this report. Information system audit of two different data centers, Lahore & Karachi, of a commercial bank has been conducted during 22nd to 27th February 2010 & 15th to 20th March 2010, respectively. So each phase has been described here with the examples of case studies:

9.1 Audit Subject

Entity that has to be audited. Every organization has different operational areas that can be audited according to the business domain. The audit subject defines the areas that should be cover during the course of audit [Andrew Hawker] [S. Anantha Sayana].

Case Study 1:
Audit Subject: Information System (IS) Audit of Regional Data Centre Lahore

Case Study 2:
Audit Subject: Information System (IS) Audit of Regional Data Centre Karachi

9.2 Audit Objective

The Objective of the Audit is to achieve the particular goal and to identify areas that need to be improved. The main objective of audit is to reduce the possibility of business risk and analyze all sensitive business areas. After identification of the major risk areas, the auditor has to check weather required controls has been placed and followed properly or not. If the required control has not been implemented or implemented but not followed can be result of any abnormality and the auditor has to mentioned this risk in the audit report so they irregularity can be rectified and the chances of fraudulent activity can be minimize [Sandra Senft, Frederick Gallegos].

Case Study 1:
Audit Objective
The Primary Objective of this audit assignment is to access and minimize the IT/business risk associated with the implementation of technology in the banking operations and to establish IT governance, best practices and ensure the effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability of the information and technology employed by the bank. The audit team will specifically check the compliance of following areas during the audit period.

Provision for the creation of the user IDs with respective rights for branches
Management of Dormant User IDs of branches and RDC
Trouble shooting management of the RDC for branches
Support provided to region for generating different MIS reports
Server room maintenance and security controls features i.e humidity controls etc
Segregation of duties, Leave record maintenance,
Effectiveness of Dispatch of Statement of Accounts
BCP /DRP, Effectiveness of Communication Channels Utilization and security features
Compliance of SBP guidelines on ATM operations
ATM downtime management
TNA and training of the staff, Maintenance of office discipline
Review of system values, Application level security and administrator controls
Management of Hardware / old IT equipments, Management of Antivirus.

Case Study 2:
Audit Objective (Same as case study 1)

9.3 Audit Scope

Audit scope define the period as well as the domain of the audit entity that should be cover during the course of audit and if the subject audit integrated with other operational areas then that areas can also partly covered. Although, auditors has the authority to review any sort of operational areas at any time, but it is recommended that the auditor should not go beyond the audit scope. The scope of the audit i.e period and domain, will also help for the auditor to make him secure such if any fraud commented before or after the audit period or the fraud not relates to the domain of audit area [S. Anantha Sayana].

Case Study 1:
Audit Scope

The period of audit will range from the **last audit date to 20th Feb 2010** and will cover all the operational area of data centre and support provided to branches, comes under data centre jurisdiction.

Case Study 2:
Audit Objective

The period of audit will range from the **last audit date to 13th April 2010** and will cover all the operational area of data centre and support provided to branches comes under data centre jurisdiction.

9.4 Pre-Audit Planning

In a Pre-Audit planning, the audit team has to discuss the operational and technical areas of the entity that has to be audited, before starting audit. To cover the technical aspect of any system the auditor has to again the complete knowledge of business process of that area. On the basis of discussion between audit team, pre-inspection data should be developed and requested from the auditee management [ISACA, CISA Review Manual].

Case Study 1:
Pre-Audit Planning

- Audit Period: 22nd to 27th February 2010
- Pre-Audit Meeting between Audit Team Members: 17th February 2010
  (Discuss different operational Areas of Regional Data Centre such as online branches operational activities, offline branches operational activities, ATM operations, Server Machine Security Controls, Physical Access Control etc)
- Requirement of Pre-Inspection Data from Data Centre

Case Study 2:
Audit Objective

- Audit Period: 15th to 20th March 2010
- Pre-Audit Meeting between Audit Team Members: 10th March 2010
  (Discuss different operational Areas of Regional Data Centre such as online branches operational activities, offline branches operational activities, ATM operations, Server Machine Security Controls, Physical Access Control etc)

- Requirement of Pre-Inspection Data from Data Centre

9.5 Audit Evidence & data gathering procedures

The pre-Inspection data required from the auditee management should include all related documentations, policies, operational & technical manuals and guidelines. Through these resources the auditor is able to assess, whether the operational activities are performing on the basis of policies, procedures and guidelines. If any deviation between the operational activity and available documentation, then the auditor mentions this irregularity in its report and these documents should be use for the purpose of evidence [Sandra Senft, Frederick Gallegos].

Case Study 1:

This phase defines the 1st part of audit, where auditors have to collect all the information mentioned in the pre-inspection data.

Audit data gathering:

- Gather all the policy document such a user/operational manual, Organizational chart of data centre, job description of data centre employees etc
- Collect a copy of all MIS reports generated by the data centre such as ATM down time report, Audit log reports, system values, user list etc
- Data centre physical access security
- Server Room Physical Access Security
- Detail of IT equipment
- Detail of all software applications supported by Data Centre Lahore.
- List of employees who have left the Data Centre during the last two years.
- Details of Training provided to the staff during last two years.
- Detailed of all user IDs / Profiles for logging on to server machine.
- Maintenance of log and fault reporting procedure followed in case of Computer Hardware and Software.
- Backup/ Contingency procedures & policies being followed at Data Centre Lahore.
- Backup tape movement log and its review procedure / evidence.
- Steps taken by the RDC to physical secure Data tapes/storage media.
- Procedure to be adopted in case of backup restoration or backup tapes testing procedure.
- Network Diagrams including Internal network of Data Centre, External links to other Data Centers, Head Office, online branches, ATMs etc.
- Different security policy related to Anti Virus, Network Security etc.
- Last year Internal IS Audit Report of the Data Centre.
- External Audit Report of the RDC during last 5 years, if any.
- A photocopy of **approved** Mandatory leave plan for 2009/2010.
- Detail of Fraud / Enquiry (if any) during last two years.
- List of all Projects / Software (Implemented, Partially Implemented, Pilot & Pipelined) in 2009/2010
- Documents related to Email IDs i-e request to create, enable, disable or delete, amend accordingly from branches / controlling offices.
- File maintained for User Change/Amendments Requests from end users for changing / amendments in different applications / software.
- Details of Internet connection (if any) at RDC.

Case Study 2:
Audit data gathering: (Same As Case Study 1)

9.6 Procedures for evaluating test/review result

The auditor should also review its observation and test conduct during the course of audit and should ensure that the proper evidence is available for the support of your observations [Frederick Gallegos, Sandra Senft].

Case Study 1:
Procedures for evaluating test/review result

On the basis of data and information collected in data gathering phase, from data centre Lahore, the audit team members raise the following issues:

- Unapproved Organizational Chart
- Weak physical security of data centre
- Non-wearing of ID cards by staff
- Non-Avaiblity of digital lock in server room
- Non-availability of humidity and temperature controller
- Non-availbility of smoke detector
- segregation of duties
- training not provided to staff
- Non availability of IDS/IPS
- Non availability of encryptors
- Sharing of Administrative Password
- Sharing of primary partition
- Non availability of security policy
- No availability of disaster recovery & contingency plan
- No availability of Backup policy

Case Study 2:

Approximately same irregularities has been observed, while conducting the IS audit of data centre Karachi.

9.7 Procedures for communication

During the course of the audit the auditor should also present its findings/observations to the auditee management for their comments and response. This procedure will also helpful for the auditors to ensure that his/her observation is fine and there is no contradiction between auditors and auditee managements. Normally, the findings that has been raised by the auditors, discussed with the auditee management to know the management response against that observations [S. Anantha Sayana].

Case Study 1:
Procedures for communication

A meeting has been conducted with the auditee management of data center Lahore at the 5th day of audit period and all major irregularities has been presented and discussed with the auditee management. The auditee management tried to clear their position against observation raised by the auditors. Some of the observations are omitted after the satisfactory clarification of auditee management.

Case Study 2:
Procedures for communication

The same meeting has been arranged with the auditee management on the last day of the audit period and major finding has been discussed with auditee management. Auditee management accept all the finding raise by the auditors.

9.8 Audit report preparation

The auditor should also prepare its report during the course of audit and present to the auditee management. The draft audit report should also discuss with the auditee management at the end of audit and if possible, take management comment on the audit observations. It is recommended that the draft audit report should be submitted and discussed with auditee management at the end of audit but if it is not possible, then the draft report can be submitted to auditee management after some days as well [S. Anantha Sayana].

Case Study 1:
Audit report preparation

During the course of the information system audit of regional data centre the auditors prepared a Draft IS Audit Report comprising all finding observed during course of audit. At the end of the audit assignment the draft audit report has been presented to the auditee management for their comments against each observations at the same time, but the auditee management requested that they will furnish the management comment within three days.

An exit meeting letter has also been presented by the auditors to the auditee management about the final discussion and then duly signed by the auditee management members and audit team members.

Case Study 2:
Audit report preparation

In regional data centre Karachi, the draft audit report has been submitted on the last day of the audit and the same report has been discussed with auditee management. The auditee management provide their comments against each observation. A copy of draft audit report comprising management comment has also taken by the auditors for their record.

10. Internal Controls

Internal controls are strategy, develop and implemented by the organization, to reduce major risk. The main objective of internal control is to safeguard the organization’s business interest by implementation of preventive, detective and corrective control measures. Internal control provides reasonable assurance to the high level management that the organizational business process comply the policies and guidelines provided by the regulatory body and professional standards [Sandra Senft, Frederick Gallegos].

Information System (IS) Internal Controls can be classified into three major categories:

- IS Preventive Controls
- IS Detective Controls
- IS Corrective Controls

11. IS Audit Controls

An Information System (IS) auditor needs to cover different areas during the course of IS audit assignments. This is also the responsibility of an IS auditor to review and analyze the general as well as physical controls when performing an IS Audit. Although, these general & physical controls having no issues of IT but these controls can be directly affect the operation of information systems and can be the cause of any illegal activity. The following are major control areas that need to be covered during the course of information system auditing [Frederick Gallegos, Sandra Senft]:

- General control
- Organizational control
- Continuity of Operations
- Operating Systems Platform security
- Network Security
- Application Level Security & Controls

12. Conclusion & Discussion

The information system audit process is the evaluation and assessment of the IT based business processes, the regulatory bodies as well as professional standards, emphasis to develop an internal audit department within the organization, which periodically review and asses organization’s IT based business process and application system running within the organization [S. Anantha Sayana].

Furthermore, for more effective review of IS internal control, organization need to conduct external audit from independent audit firm. At the end of audit, the audit team present and discuss draft audit report with the auditee management, which contain the information related to audit entity and audit findings/observation. The audit management then explain their concern about the finding raised during the audit assignment and these management comments will then incorporated in the audit report [Sandra Senft, Frederick Gallegos].

During the completion of this report, I have conducted the information system audit of two data centers Lahore & Karachi of a leading commercial bank. The duration of audit assignment was one week for each data centre.

Complete life cycle, which I have mentioned in my report has been carried out during the course of auditing the regional data centre Lahore and Karachi. Phases of information system auditing has also described according to case studies.

13. References

[1] David L. Cannon, Timothy S. Bergmann, Brady Pamplin “CISA-Certified Information Systems Auditor ™ Study Guide”, 2006
[2] Gerald Vinten, “Current Issues in External and Internal Auditing”, 2004
[3] Alan Calder, Steve Watkins “IT GOVERNANCE - A MANAGER’S GUIDE TO DATA SECURITY AND BS 7799/ISO 17799 3rd Edition”, 2005
[4] Andrew Hawker, “Security in Information Systems : A Guide for Business & Accounting”, 2000
[5] Christopher L. T. Brown, “Computer Evidence: Collection and Preservation”, 2005
[6] Ken Doughty, “Best Practices, Volume 15: Business Continuity Planning: Protecting Your Organization's Life”, 2000
[7] Louis Braiotta, JR., “THE AUDIT COMMITTEE HANDBOOK Fourth Edition”, 2004
[8] ISACA, Certified Information System Auditors (CISA) Review Manual – 2008
[9] Sandra Senft, Frederick Gallegos, “Information Technology Control and Audit” 3rd Ed – 2009
[10] Frederick Gallegos, Sandra Senft “Information technology control and audit” 2nd Edition – 2004
[11] Lance M. Turcato, “Integrating COBIT® into the IT Audit Process” (Planning, Scope Development, Practices) – 2006
[12] IT Audit Monograph Series # 1 “Information Technology Audit”, General Principles
[13] Fred Gallegos, “IT Audit Independence: What Does It Mean?”, Volume 6, 2003
[14] S. Anantha Sayana, CISA, CIA, “The IS Audit Process” Information Systems Control Journal, Volume 1, 2002
[15] Tommie W. Singleton, Ph.D., CISA, CITP, CMA, CPA, “What Every IT Auditor Should Know About Scoping an IT Audit” Volume 4, 2009
[16] Tommie W. Singleton, Ph.D., CISA, CITP, CMA, CPA, “IT and Privacy Audits” Volume 5, 2009
[17] S. Anantha Sayana, “Approach to Auditing Network Security”, Volume 5, 2003