ROLE OF INFORMATION SYSTEMS AUDIT TO ENSURE DATA INTEGRITY A CASE STUDY ON SBI AND ICICI BANKS

Mallesha C, Anurag University

ABSTRACT

In the modern business era, Information Systems play a prominent role especially in a sector like Financial Institutions. Extensive use of IT in the banking sector has grown up in recent years through which the banking environment has driven from decentralization to centralization. There is an extreme rise in usage of online banking and computerization leaving less scope to the traditional banking and manual operations through which the risk of losing the data and cyber frauds have also been increased simultaneously. To mitigate these frauds, auditing Information Systems frequently is essential. Data integrity is one of the main objectives of information system audit. It is one such function in which data in systems can be secured by using various controls and also it helps not to get the data manipulated by fraudsters. In this paper, a brief discussion on Data integrity has been dealt and the functioning of Information systems audits concerning Data integrity in both SBI and ICICI banks as per RBI guidelines were also studied, analyzed through a structured questionnaire.

Keyword: Information System Audit, Data Integrity, Reserve Bank of India, Centralization.

INTRODUCTION

Financial institutions are considered the backbone of the country's economy, and information systems share a crucial part of business in today's world. The utilization of IT in the banking industry in India has tremendously grown in the recent decade and most of the banks are converting to technology-based solutions implementation of this technology has left less scope for traditional banking and manual operations. With the impact of information technology, the environment has moved from decentralization to centralization. Bringing of new techniques and various tools to offer customized products based on customer taste is done in banking. It is difficult to measure the influence of computerization but IS audit facilitates evaluation of the use of these IS assets in carrying out banking transactions effectively and efficiently.

All the companies using IT especially banking firms with various external users, applications of e-commerce, employee details are required to maintain IT policies. Banking companies IT policy, therefore, should aim at coding the appropriate data at t h e exact stage in the process of data collection. Companies especially those are in the banking fields heavily rely on e-commerce, wireless networks which are extremely vulnerable to data theft and loss of information. In such circumstances, IS audit helps to verify whether IT policies and procedures are followed or not. It also helps to see that all the transmitted data is secured.

System assessment of IS audit in banks is a vital part of the Financial Inspection of banks. IS audit in banks is still in the initial stage. Different banks have different policy approaches for the conduct of IS audits. Reserve Bank of India (RBI) opined that Computer Security issues did not have more attention from the top management. From the above-said points, it is known that the IS audit in India is still in starting stage and the major problem faced

Citation Information: Mallesha, C. (2022). Role of information systems audit to ensure data integrity a case study on sbi and icici banks. *Academy of Accounting and Financial Studies Journal, 26*(4), 1-13.

by the banking industry is the lack of skilled people for this particular field. In this background, adequacy or otherwise, availability of skilled technical personnel in banks would also be required to be verified by the IS audit.

The IS audit functions are Information Systems Safeguarding, Integrity of Data, Effectiveness of System, Efficiency, Administration, Organization, and Business Continuity Operations. Evaluation of management controls with the help of information technology is known as an audit for information systems. In simple words, it is a type of audit where a firm's IT systems and all other related processes are evaluated. The IS audit focuses mainly on determining risks in Information Systems and in assessing controls to reduce the risks.

Information Systems Audit demanding factors for an organization

1. Cost of organizational data loss
2. Cost of incorrect decision making
3. Computer abuse cost
4. Cost of the hardware, software, and technical personnel
5. Computer error cost
6. Privacy cost
7. Cost of computer use

Three types of Basic Controls are considered by Audit Professionals

Preventive controls: They are designed to prevent an error that is going to occur. The characteristics of these controls are

1. Understanding the asset
2. Estimating probable risk and threats
3. Necessary controls to face those threats

Detective controls: They are designed to detect errors that occur and report. Their characteristics are:

1. Understanding of lawful activities.
2. Reporting unlawful activities.
3. Interaction with preventive control.
4. Checking by the superior

Corrective controls: To reduce or eliminate an error once it is detected. The characteristics are as follows:

1. Identifying the problem and its cause.
2. Impact of threat.
3. Providing solutions for problems.
4. Getting feedback**.**

Importance and protection of Information Systems in Banks

Each bank in India should perform the Audit for Information Systems. These guidelines were given by the Reserve Bank of India (RBI) and the basic aspect of Information Systems is that the risks associated and controls for those risks are periodically evaluated where ever necessary. This can be done with ease with the help of Information Systems (IS) Audit.

Citation Information: Mallesha, C. (2022). Role of information systems audit to ensure data integrity a case study on sbi and icici banks. *Academy of Accounting and Financial Studies Journal, 26*(4), 1-13.

In recent years the dependence of the banking industry on the computerized environment has been increased rapidly and it has become part of the banking business. Recent developments in the computerization of banks have more impact on audits. Risk management and controls will be efficient if a well-structured audit is performed in the firm.

Collecting and evaluating evidence of the system whether the computer system maintains the integrity of data, safeguarding of information systems, so has to achieve the goals effectively and efficiently by optimum utilization of the resources.

Data Integrity

Data Integrity includes the safeguarding of the information against unauthorized addition, deletion, modification, or alteration. This includes items such as accounting records, backup, documentation, etc. Information Systems are used to capture, store, and process, retrieve and transmit the data securely and efficiently. The emphasis is on the accuracy of the data and its transmission in a secured manner. Data Integrity also implies that during the various phases of electronic processing, various features of the data viz. Accuracy, Confidentiality, Completeness, Up-to-date status, Reliability, Availability, Timeliness, and Effectiveness are not compromised. In other words, data should remain accurate during electronic processing.

The desired features of the data are described hereunder:

Accuracy: Data should be accurate. Inaccurate data may lead to wrong decisions thereby, hindering the business development process.

Confidentiality: Information should not lose its confidentiality. It should be protected from being read or copied by anyone who is not authorized to do so. It also includes protecting the individual pieces of information that may seem harmless by the owner but can be used to infer other confidential information.

Completeness: Data should be complete. Incomplete data loses its significance and importance.

Up-to-date Status: Data should be updated regularly. If the information is not up-to-date, it presents a false picture of the organization.

Reliability: Data should be reliable because all business decisions are taken based on the current database.

Availability: Data should be available when an authorized user needs it. It should be ensured that the information services are unavailable to unauthorized users.

Timeliness: Timeliness of the data is very important because if data is not available when required, the very purpose of maintaining the database gets defeated.

Effectiveness: Information should be effective so that it helps in the process of business development and expansion.

If data integrity is not maintained, an organization loses its true representation. Poor data integrity could lead to the loss of competitive advantage. The corruption of data would affect many users in a networked environment. If the data is valuable to a competitor, its loss may undermine an organization's competitive position.

Data Integrity is the standard element between IS audit and manual audits. All categories of audits including IS audits should evaluate the integrity of data. Management elements related aspects are included as efficiency and effectiveness are involved in IS audit.

Data integrity is defined as the overall accuracy, completeness, and consistency of data. It is also referred to as the safety of data concerning regulatory bodies. It is the process in which all rules, policies, and standards are framed and maintained. The integrity data is said to be secured

Citation Information: Mallesha, C. (2022). Role of information systems audit to ensure data integrity a case study on sbi and icici banks. *Academy of Accounting and Financial Studies Journal, 26*(4), 1-13.

when the information which is stored in the database will stay accurate and reliable no matter how often it is accessed or for how long time it is stored.

Protecting the data from a loss or a data leak would be considered an important aspect of data integrity. To keep your data safe from outside forces with malicious intent, you must first ensure that internal users are handling data correctly. By implementing the appropriate data validation and error checking, you can ensure that sensitive data is never miscategorized or stored incorrectly, thus exposing you to potential risk.

The role of the IS auditors is to protect the organization's assets and required internal controls are used to protect and to see that the information systems data should maintain the data integrity.

Data integrity objectives: It is one of the main objectives of IS Auditing. Maintaining the data integrity of an organization is important and from a business, perspective to enhance the decision-making process, in the market environment.

Controls over Data Integrity and Security

Data integrity: The main objective of data integrity controls is to prevent, detect, and correct errors to ensure that the correct flow is maintained. An organization has to decide what types of controls are to be needed for implementation. Data integrity controls protect data from destroyed or misused data assure the user that the information meets expectations about its quality and integrity.

Data security: Protection of data which is misused, accidental or intentional disclosure. Multiple levels of data security are necessary for an information system environment; they include database protection, data integrity, security of the hardware and software controls, and physical security over the user, and organizational policies.

Aspects of Data Integrity in banks

Following are some of the aspects where the IS auditors should concentrate to maintain the Data Integrity in their banks they are:

1. Data Input Controls
2. Data Processing Controls
3. Purging of Data Files
4. Data Backup
5. Data Restoration
6. Virus Protection

Data Input Controls: The largest number of controls is available at the time of data entry in the system. Data Input Controls are error-prone because the activities involved in data entry are of a routine and monotonous nature. Data entry is also a major area for intentional fraudulent activity. It involves the addition, deletion, modification, or alteration of the input transactions or data. Hence, the IS auditors should minutely evaluate the effectiveness of the data input controls. The use of the scanner and inputs to the system through floppy should be monitored and controlled.

Data Processing Controls: The application system processes the data online on a day-to-day basis. The IS auditors are concerned about the Data Processing Controls. They should examine that only designated/authorized officers perform a start-of-day operation. The day- end

Citation Information: Mallesha, C. (2022). Role of information systems audit to ensure data integrity a case study on sbi and icici banks. *Academy of Accounting and Financial Studies Journal, 26*(4), 1-13.

process should be completed with the generation of the prescribed reports. It is also required that proper record is maintained in respect of the corrections made in the database under authentication.

Purging of Data Files: It is pruning of the data files of the identified past period for which it is no more necessary to store the data in the current system. Before undertaking the purging activity, it is necessary to take a backup of the full data directory. The purging of the static data or master particulars is never taken. The IS auditors should examine that the purged data backup media is stacked in chronological order for easy tracing and also is in safe custody. A manual record of purging activity should also be maintained. Access to the purged data should be restricted and controlled to ensure the integrity of the purged data.

Data Backup: Data backup is an essential aspect of all computer operations. Some commonly used computer media include hard disks, floppy disks, tape cartridges, CD- ROMs, DVD ROMs, etc. Off-site back-ups are taken on floppies or tape cartridges, while on-site back-up is taken on hard disks. Back-up is one of the measures of business continuity planning and is also required for archiving old records.

The backups must be taken regularly. One set of backups requires being stored off-site. The backups have to be tested periodically by restoring the data therefrom. The backup media have to be verified periodically for readability. Backup media should be properly labeled and numbered. This is a very important area and requires proper attention.

Restoration of Data: It is defined as downloading of data afresh from magnetic media, in case of a crash of the system, irrecoverable corruption, or loss of data, for going back online. Backup is taken at a particular point of time like the beginning of day operations, end of day operations, etc. Thus, the restoration of data is dependent on the magnetic media and the data stored thereon. Restoration of the data is required in the event of major corruption of data. In the event of a virus attack or destruction of a server or the computer site, the only option is to fall back upon the restoration option. Restoration of data helps to obtain a position of data as of a particular date, to establish whether any data tampering has taken place. It assists in conducting system audits as of the previous date and generates ledgers of previous years. Transactions of the purged period can also be retrieved.

Virus Protection: A computer virus is a program that is self-replicating and can corrupt or destroy data irretrievably. It resembles biological viruses in behaviour. It may have a dormancy period and get activated on a certain date. It is potentially disastrous. Anti-virus software is available and is capable of countering against known viruses, malicious programs. Anti-virus software is updated by the manufacturers regularly to counter against the new viruses coming up. It is necessary to keep the anti-virus software updated at all times. All extraneous floppies and other media should be checked/scanned for viruses before use.

REVIEW OF LITERATURE

"*Information Security specialists generally consider DiD as the best way to improve an organization's security posture. Of today's IT audit framework, none are customized to fit the needs of SMIFI's when considering the DiD theory. SMIFI should develop an IT audit framework based on the DiD theory, regulatory controls, organizational controls, and industry standards. Future research includes developing a holistic IT Audit framework specifically designed for SMEIFI's*" (Lovaas & Wagner, 2012).

"*Factors affecting on IT audit quality is a business environment, entity activities and risks, which can be to mystification for auditors in condition, auditors haven't enough known.*

Citation Information: Mallesha, C. (2022). Role of information systems audit to ensure data integrity a case study on sbi and icici banks. *Academy of Accounting and Financial Studies Journal, 26*(4), 1-13.

But in a condition that auditors have sufficient knowledge, it may be helping the entity's auditors to improve the quality of audit work" (Yeghaneh et al. 2015).

"*The formalization of the IT audit adaptable to all types of organizations, based on both theoretical and practitioners. In the future, this research can be completed with more empirical work. Primarily could be observed at real organizations if their actual IT AM process/architecture is performed"* (Rosário et al., 2013).

"*IT audit guidance and issue of IT audit object are the top three topics most widely used in research issues in IT audit. While the issue of the IT audit process and the issue of IT auditor are in the bottom two with a relatively small number of occurrences. For issues of IT, audit process, and IT auditor, the trend of its emergence has only been in the last few years, because the current amount of literature support in IT audit is still very limited, so it is very open for researchers to research in the field of IT audit to help IT audit practice from the theoretical side, and especially deeper review of modern IT audit*" (Aditya et al., 2018).

"*The selection of a set of security techniques must be done according to the potential risks. But to provide proper and effective protection to the organization as- sets, the security system (measures) must be as- assessed. An internal or external security audit is one of the best ways to determine security efficiency. Many security audit standards specify procedures that should be followed to ensure that IT resources are adequately safeguarded. With still high losses due to inadequate IS security, a security audit must be considered by any organization*" (Suduc et al., 2010).

"*There is an agreement between workers in internal auditing departments about the impact of the characteristics of technological environment for information systems on the operational control risks. There is a positive impact of using information technology on the independence and privacy of internal auditing in Islamic banks operating in Jordan in the shadow of globalization. Improving the currently available accounting system in the Jordanian Islamic banks to feed sufficient information to all parties involved in the auditing process*" (Al-Refaee & Saim, 2013).

"*There is a significant statistical relationship between general controls of information systems auditing and information systems performance. The general controls of information systems auditing have a significant statistical impact on information systems performance*" (ALraja & Alomian 2013).

"*There is no protected Information System in the Banking sector or any other sector. However, through the process of experimentation and improvement on the existing systems, we may come to the point where it will be extremely difficult for a potential hacker to acquire access to the personal accounts of different users. Further research is focusing on inserting the personal biometric characteristics of an individual to have access to his data. In this way, it will be very difficult for a potential hacker to invade the accounts of users because the biometric characteristics of every individual are unique*" (Thomas Chatzigagios, 2018).

"*In practice, banks adopted three types of control measures: physical controls which expected to prevent unauthorized individuals from gaining access to a company's facilities; access controls which expected to restrict unauthorized individuals from using information resources; and communications controls (also called network controls) which expected to secure the movement of data across networks. One key step in developing a secure network is to conduct a risk assessment. This assigns levels of risk to various threats to network security by comparing the nature of the threats to the controls designed to reduce them. It is done by developing a control spreadsheet and then rating the importance of each risk. To be sure, that*

Citation Information: Mallesha, C. (2022). Role of information systems audit to ensure data integrity a case study on sbi and icici banks. *Academy of Accounting and Financial Studies Journal, 26*(4), 1-13.

the data communication network and microcomputer workstations have the necessary controls and that these controls offer adequate protection, it is best to build a control spreadsheet" (Bawaneh, 2018).

"*Banks should have the general inspection and revision over their infrastructures. In other words, in the vulnerability section, they should improve their infrastructure in the area of hardware, software, network, and communication. In the threat domain, banks should increase the external inspection and recognize the external factors that cause disorder in security and minimize these threats by observing and controlling the information and network and all users would be able to have necessary pieces of training on banks sites and portals. In this process, a very important point is that all bank staff and experts should support performing correction and improvement strategies from the beginning. Eventually, it is suggested that research be conducted on different methods of banks security development and staff's organizational performance liability in the future by the researchers. As a matter of fact, due to allocating the lowest score to manpower for security in the final weighing, it would be great to research manpower and its role in information system security*" (Shokouhyar, et al, 2018).

"*The IS audit must be scheduled to allow the audit plan to consider the IS audit's findings. IS audit also needs to be heavily involved in the financial audit of entities where significant changes to existing IS, or the implementation of new IS, have occurred. The adoption of CAATs in support of the financial audit will in practice also support efficiency and effectiveness in undertaking the financial audit. The results indicate that application control reviews are rarely undertaken, but equally indicate that application control reviews are undertaken as systems increase in risk, complexity, and materiality. I.S. audit methodologies in practice must set out the criteria for undertaking application control reviews to ensure the effectiveness and efficiency of the financial audit*" (Axelsen et al., 2011).

"*Concerning the information security and IT audit system implemented by the banks to protect information from threats, the study found that the systems included information security policy, information security organization, asset, and human resource security, information access control, and IT audit systems. Largely all these systems were implemented by the selected banks. About the challenges of the banks in managing threats to information system, the study found that; high cost of investing information security controls, and the unpredictable nature of information security threats were identified as the main challenges*" (Sylvester Hatsu, 2015).

A system within the company will not be able to run properly if the components inside do not work well together. Discipline, accuracy, accuracy, and speed are needed in every officer both at the branch and head office. On the branch side in submitting data or documents in the TPS system the approval level can be more concise or there is a handover as a temporary person in charge of the branch manager is not in place, so that import officers at the central office can more quickly obtain data or documents from the branch or not too close to the cut off time (Saleh & Sari., 2020).

"*Digital transformation is a good opportunity for IT audit to play a more positive role and contribute to the development of business and organizations. Defining the IT audit universe and IT audit characteristics becomes a key element in driving the changing role of IT audit to become more relevant, forward-looking, and risk-focused. In addition, the high demand for qualified IT auditors, as well as the need to adapt specifically to existing IT audit frameworks, will be an interesting issue for further research to support the effectiveness of modern IT audit in the era of digital transformation*" (Aditya & Menzelthe, 2019).

Citation Information: Mallesha, C. (2022). Role of information systems audit to ensure data integrity a case study on sbi and icici banks. *Academy of Accounting and Financial Studies Journal, 26*(4), 1-13.

"*In the process of determining the IT audit guidance, there are many considerations. Thus, with the side-by-side comparison of the various IT audit guidance, it can be clearly described the functions and uses of each IT audit guidance. An IT auditor needs to understand the IT audit guidance needed in the IT audit process and their suitability with the objectives of the IT audit to be carried out. Therefore, the auditor's expectations of IT audit guidance can be relevant according to the needs and objectives of the IT audit*" (Aditya & Menzelthe, 2019).

"*The need for execution to perform the audit task that should be able to optimize the use of work experience owned to detect if there are irregularities in the implementation of activities. The need to improve the quality of audits by improving the auditor's competence by increasing the knowledge of the auditor in terms of scholarship with further education level, and always active in following the development of accounting scholarship and also attending various supporting training to improve information systems Audit quality and supply chain*" (Nur Zeina, 2018).

"*The role of IS auditors in this arena is dwindling due to the increased complexity of IT environments and the continuous reliance on the specialized external consultant for assurance in this area. In application auditing, the role of IS auditors is lessening as well due to the proliferation of applications all over the organization and the sensible shift of this responsibility to operations and financial auditors. CA is also emerging in the arena of application auditing as a factor that is easing up the drift of application audits from IS auditors to operations auditors. In IT management audit, the role of IS auditors is getting more significant due to the importance of IT management practices in providing the basis of assurance for any IT environment. Furthermore, the emergence of some management practices like IT governance, proactive involvement of IS auditors in IS projects, and outsourcing is giving more opportunities to IS auditors to contribute value to their organizations*" (Munir Majdalawieh, 2009; Sari & Susanto, 2018).

"*The conceptual approach concerning information systems security was based on ISO standards. This is a new strategy and there aren't constructive research studies addressing this approach. This fact is specially related to the lack of a standard model to manage and audit information system security and by the fact that each organization performs the information system security management according to its objectives, activities, structure, and its particular view of risks. We will accomplish the proof of concept, through the instantiation of the conceptual framework within an organization*" (Pereira & Santos, 2010).

THE OBJECTIVE OF THE STUDY

The basic objective of the study is to examine the mechanism prevailing in SBI and ICICI banks in respect of Data Integrity of Information Systems using IS Audit.

METHODOLOGY OF THE STUDY

The method used for the data collection, tools, and techniques of analysis are as follows:

Sources of data: The data for the study is collected from primary sources and secondary sources. They are:

Primary data: The Bank Managers perceptions on Information Systems Audit are collected through a structured questionnaire and personal interviews.

Secondary data: The Reserve Bank of India Circulars and Reports of committees, Annual reports and IS Audit Reports of SBI and ICICI banks form the main basis for analysis

Citation Information: Mallesha, C. (2022). Role of information systems audit to ensure data integrity a case study on sbi and icici banks. *Academy of Accounting and Financial Studies Journal, 26*(4), 1-13.

and interpretations. Reports, Books, and Journals of IDRBT, ISACA, ICAI, and IBA have been used to obtain the data that is needed for the study. Research studies conducted by individuals, Institutions, business dailies, and other journals are considered for the study. Online studies on IS Audit and websites, eBooks, e-Journals also helped in filling the information gaps.

Sample Size

The study is devoted to public sector and private sector banks. Since all the banks operate in the same market adhering to guidelines issued by the Reserve Bank of India, it was considered appropriate to select a leading bank from both public and private sectors. The State Bank of India from the public sector and ICICI Bank from the private sector are selected for closer analysis for the present study. Both the banks are leading banks in the public and private sectors.

A questionnaire has been prepared and administered to bank managers of SBI (192) and ICICI (62), data was collected from the bank managers about their perceptions on implementation of Information Systems Audit in their respective bank branches, Greater Hyderabad Municipal Corporation (GHMC), Telangana State.

The total number of respondents selected for the study from both the SBI and ICICI banks is 192 and 62 out of the 124 (65%) from SBI and 36(58%) from ICICI bank managers have responded Tables 1 and 2.

Table 1
SAMPLE SIZE AND RESPONSE RATE

S. No.	Name of the Bank	Sample Size	Responses	Response Rate
1.	SBI	192	124	65%
2.	ICICI	62	36	58%
Total		254	160	63%

Source: Field Survey

Table 2
RELIABILITY STATISTICS RESULTS

Correlation Between Forms		0.744
Spearman-Brown Coefficient	Equal Length	0.853
	Unequal Length	0.853
Guttmann Split-Half Coefficient		0.847

Source: SPSS generated values

Concerning Bank Managers, a total of 82 items are considered for the study. By applying Cronbach's Alpha through SPSS, the value obtained is .847. Since, the value is higher than 0.7000, it is concluded that the items considered for the data collection have relatively high internal consistency.

Statistical Tools

The data collected through the questionnaire from primary sources have been processed in tune with the objectives set. While processing the data and testing hypothesis Statistical Package for Social Sciences (SPSS) has been used. Hypotheses are formulated and processed by employing appropriate statistical tools such as Chi-Square Test to draw meaningful conclusions; t-Test and Grade Point Average (GPA) have been used for testing whether there is a significant

Citation Information: Mallesha, C. (2022). Role of information systems audit to ensure data integrity a case study on sbi and icici banks. *Academy of Accounting and Financial Studies Journal, 26*(4), 1-13.

difference between the banks. Bar Diagrams have been used to present the data simply, for better understanding.

To study and analyze the Data Integrity in SBI and ICICI banks as per Information Systems Audit requirements the researcher collected the perceptions of banks managers of both the banks regards to Data Integrity in their respective branches.

To solicit the opinions of the bank managers 39 parameters are taken into account. By framing hypothesis and sub-hypotheses and with the help of Chi-square test, t-test and grade point average were used to find out whether there is any significant difference in SBI and ICICI banks with regards to Data Integrity.

A structured questionnaire containing multichotomous, dichotomous, open-ended, and closed-ended questions is administered to critically examine the views of Bank Managers on the implementation of Information Systems and Information Systems (IS) Audit in Banks. The Public and Private Banks SBI, ICICI Bank managers of Greater Hyderabad Municipal Corporation were selected for the study. Out of 192 branches of SBI, 62 branches of ICICI, 124 (65%) and 36 (58%) responded in SBI and ICICI respectively.

RESULTS

Perceptions of Bank Managers of SBI and ICICI Banks were tested using the following Hypothesis of the Study:

Thirty-nine Sub-Hypotheses of Data Integrity were tested using the Chi-Square test from the perceptions of bank managers of both SBI and ICICI banks. The Chi-Square Test results are given below Table 3:

Table 3
CHI-SQUARE TEST RESULTS

S. No	Sub-Hypotheses(Parameters)	Sig. Value	Table Value	Null Hypothesis Accept / Reject	Better performing Bank
1	Availability of scanned signature's history in system	0.15	0.05	Accept	SBI
2	Entry of cheque books stock in the system	0.4	0.05	Accept	ICICI
3	Entering and confirming the cheque books which are issued in system by daily basis	0.24	0.05	Accept	ICICI
4	Checking whether the entered data of various accounts is correct and accurate	0.005	0.05	Reject	SBI
5	Start of day process being done by authorized persons	0.046	0.05	Reject	ICICI
6	Taking corrective action on the error messages which are displayed on screen by the operating staff	0.127	0.05	Accept	ICICI
7	Cancellation of entries only by appropriate authority	0.013	0.05	Reject	SBI
8	Generation of reports at day end process	0.068	0.05	Accept	ICICI
9	Maintaining a record on corrections done in database under authentication	0.001	0.05	Reject	SBI
10	Recording and maintaining purging activity in the register	0.332	0.05	Accept	SBI
12	Maintaining a proper and safe custody of purged backup media	0.041	0.05	Reject	SBI
13	Restricting the access to purged data	0.254	0.05	Accept	SBI
1	Labeling and maintaining the operating system,	0.105	0.05	Accept	ICICI

Citation Information: Mallesha, C. (2022). Role of information systems audit to ensure data integrity a case study on sbi and icici banks. *Academy of Accounting and Financial Studies Journal, 26*(4), 1-13.

4	hardware, software and printer				
	Availability of user manuals of the application software and other end-user packages for guidance	0.055	0.05	Accept	ICICI
	Back up of data is done without fail on regular intervals and it is available as per requirement	0.037	0.05	Reject	ICICI
	Backup copies are having proper storage procedures and facilities in place	0.055	0.05	Accept	ICICI
	Availability of offsite storage of backup data	0.001	0.05	Reject	SBI
	Periodic verification of back up media for readability	0.001	0.05	Reject	SBI
20	Backup media is provided with Physical and fire protection	0.001	0.05	Reject	SBI
21	Instructions for restoration of backup data are compiled well	0.008	0.05	Reject	SBI
22	Is verification of data integrity done after completion of restoration	0.15	0.05	Accept	SBI
	Date, time, reason and size of restoration are recorded while restoration work is done	0.059	0.05	Accept	ICICI
	After disruption is there any alternate source to resume business activity within shortest possible time	0.055	0.05	Accept	ICICI
	Backup of software and data available for restoration purpose	0.069	0.05	Accept	ICICI
	Does audit trail report generate the user ID of the operator and the official for any addition / modification / deletion of the transaction data effected in the database	0	0.05	Reject	SBI
27	Generation of audit trail report done daily and verification, scrutinization of entries is done.	0.029	0.05	Reject	SBI
28	Scrutinizing the cancelled entries and recording the reasons for cancellation	0.004	0.05	Reject	SBI
29	Availability of updated authorized version of OS and anti-virus	0.02	0.05	Reject	ICICI
30	Computerized operations use the software which has legally licensed copies	0.001	0.05	Reject	SBI
31	Approval from higher department and controlling office is given to make the changes to the application software	0.005	0.05	Reject	SBI
32	Is the Information Systems Audit & Security Policy framed in strict compliance with Reserve Bank of India guidelines	0.391	0.05	Accept	SBI
33	Is the Staff aware of existence of Information Systems Audit & Security Policy	0.109	0.05	Accept	ICICI
	Are banks audited as per the checklist designed in the Information Systems Audit & Security Policy	0.569	0.05	Accept	SBI
35	Is Information Systems Audit good enough to prevent frauds in the banks	0.845	0.05	Accept	SBI
	Does Information Systems Audit facilitate detection of software deficiencies in preventing financial loss to the bank	0.589	0.05	Accept	SBI
37	Does the bank have good Disaster Recovery System to continue customer operations in case of failure of existing systems	0.008	0.05	Reject	ICICI
38	Does the Bank receive complaints from customers with regard to leakage of Information	0.001	0.05	Reject	SBI
3	Does the Bank receive complaints from customers	0.001	0.05	Reject	SBI

Citation Information: Mallesha, C. (2022). Role of information systems audit to ensure data integrity a case study on sbi and icici banks. *Academy of Accounting and Financial Studies Journal, 26*(4), 1-13.

9	with regard to internet banking frauds				
40	What is the periodicity of Information Systems Audit	0.035	0.05	Reject	ICICI

DISCUSSION ON RESULTS AND INTERPRETATION

H_0: *There is no significant difference with regard to Data Integrity between SBI and ICICI Banks*

Table 4
DATA INTEGRITY T-TEST RESULTS

BANKS	N	Mean	Std. Deviation	t	P	df	Table Value
SBI	124	45.3306	2.62794	-1.797	.074	158	1.9751
ICICI	36	46.1944	2.20155				

The calculated t-value-1.797 is less than the table value of 1.9751 and the calculated p-value is 0.074, is greater than table value of 0.05 Table 4. The null hypothesis is therefore accept indicating that there is no significant difference in SBI and ICICI banks with respect in maintaining Data Integrity.

Mean is calculated on the preference i.e. first preference-1, second preference-2 likewise, therefore least Mean value is considered as better performing bank. The calculated mean value of SBI is 45.3306 and that of ICICI Bank is 46.1944 which are greater than that of SBI, thus better performing bank can be stated to be SBI with regards in maintaining Data Integrity.

Grade Point Average

Grade Point Average is calculated in order to verify whether ICICI is better than SBI. The GPA of SBI is 2.84 whereas that of ICICI is 2.82 which is clearly indicated that SBI is marginally better off as compared to SBI in maintaining Data Integrity.

CONCLUSION

In computerized information systems, most of the business processes are automated. Organizations are increasingly relying on Information Technology (IT) for information and transaction processing. Technology has impacted what can be done in business in terms of information as a business enabler. It has increased the ability to capture, store, analyze and process tremendous amounts of data and information by empowering the business decision-maker. There are 4 types of controls based on the category of the objective of controls viz. 1. Preventive 2. Detective 3. Corrective 4. Compensatory.

A Hypothesis that there is no significant difference in SBI and ICICI bank about Data Integrity is formulated with 39 parameters (Sub-Hypotheses), t-Test, Chi-Square test, and GPA (Grade Point Average) was used to analyze the perceptions of bank managers.

REFERENCES

Aditya, B.R., & Menzelthe, Y. (2019). IT Audit Guidance: Side by Side Comparison. *In IOP Conference Series: Materials Science and Engineering, 662*(2), 022055).

Aditya, B.R., Ferdiana, R., & Santosa, P.I. (2018). Toward Modern IT audit-current issues and literature review. *In 2018 4th International Conference on Science and Technology (ICST),* 1-6.

Citation Information: Mallesha, C. (2022). Role of information systems audit to ensure data integrity a case study on sbi and icici banks. *Academy of Accounting and Financial Studies Journal, 26*(4), 1-13.

Aditya, B.R., Hartanto, R., & Nugroho, L.E. (2018). The role of IT audit in the era of digital transformation. *In IOP Conference Series: Materials Science and Engineering, 407*(1), 012164.

ALraja, M.N., & Alomian, N.R. (2013). The Effect of General Controls of Information System Auditing in the Performance of Information Systems: Field Study. *Interdisciplinary Journal of Contemporary Research In Business, 5*(3), 356-370.

Al-Refaee, K., & Saim, A. (2013). The effect of using information technology increasing the efficiency of internal auditing systems in Islamic Bank operating in Jordan. *Research Journal of Finance and Accounting, 4*(9), 2222-2847.

Axelsen, M., Coram, P., Green, P., & Ridley, G. (2011). Examining the role of IS audit in the public sector. *Pacific Asia Conference on Information Systems, United States of America*.

Bawaneh, S. (2018). Securing Information Technology for Banks and Accounting Information Systems. *International Journal of Applied Engineering Research, 13*(6), 3291-3300.

Lovaas, P., & Wagner, S. (2012). IT audit challenges for small and medium-sized financial institutions. *In Annual symposium on information assurance & secure knowledge management*, 16-22.

Munir Majdalawieh, I.Z. (2009). Paradigm shift in information systems auditing. *Managerial Auditing Journal*, 352-367.

Pereira, T.S.M., & Santos, H. (2010). A Conceptual Framework to Manage and Audit Information Systems Security. *Semana de Engenharia*.

Rosário, T., Pereira, R., & Silva, M.M.D. (2013). IT audit management architecture and process model. *In International Conference on Business Information Systems*, 187-198.

Saleh, M.H., & Sari, A. (2020). Audit on Information System Function in Import Transactions Process PT. Bank Rakyat Indonesia (Persero). *In Annual International Conference on Accounting Research (AICAR) 2019*, 15-18.

Sari, N.Z., & Susanto, A. (2018). The effect of auditor competency and work experience on information systems audit quality and supply chain (case study: Indonesian Bank). *International Journal of Supply Chain Management (IJSCM), 7*(5), 732-747.

Shokouhyar, S., Panahifar, F., Karimisefat, A., & Nezafatbakhsh, M. (2018). An information system risk assessment model: a case study in online banking system. *International Journal of Electronic Security and Digital Forensics, 10*(1), 39-60.

Suduc, A.M., Bîzoi, M., & Filip, F.G. (2010). Audit for information systems security. Informatica Economica, 14(1), 43.

Sylvester Hatsu, M.B. (2015). An examination of the extent of implementation of the information security system and IT audit system in Ghananian Banks. *Journal of Information Engineering and Applications*, 33-42.

Thomas Chatzigagios, D.I. (2018). Protection of the Information Systems in the Banking Sector. Journal of International Scientific Publications, 314-319.

Yeghaneh, Y.H., Zangiabadi, M., & Firozabadi, S.D. (2015). Factors affecting information technology audit quality. *Journal of Investment and Management, 4*(5), 196-203.

Received: 28-Jan-2022, Manuscript No. AAFSJ-22-11023; **Editor assigned:** 31-Jan-2022, PreQC No. AAFSJ-22-11023(PQ); **Reviewed:** 14-Feb-2022, QC No. AAFSJ-22-11023; **Revised:** 03-May-2022, Manuscript No. AAFSJ-22-11023(R); **Published:** 10-May-2022

Citation Information: Mallesha, C. (2022). Role of information systems audit to ensure data integrity a case study on sbi and icici banks. *Academy of Accounting and Financial Studies Journal, 26*(4), 1-13.