Received: 07-12-2023
Accepted: 17-01-2024

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Research on Information Technology Audits in Vietnam

Tat Thanh Doan
University of Labour and Social Affairs, Hanoi, Vietnam

Corresponding Author: **Tat Thanh Doan**

Abstract

In the continuous development of technology and the 4.0 industrial revolution, information technology audit is a new type of audit but is developing rapidly. In Vietnam, although the concept of information technology audit is still quite new, it is initially implemented in businesses with a high level of information technology application such as commercial banks. This article studies the current status of information technology audits at some Vietnamese commercial banks, thereby evaluating the results achieved, as well as the limitations that need to be overcome of this audit activity.

Keywords: Financial Statement Audit, Information Technology, Independent Audit

Introduction

Currently, financial statement auditing is familiar and plays an important role in making financial information transparent. With the development of information technology, in many modern business models, processes are performed automatically and business data, as well as accounting data, are stored and processed through information systems. Extremely modern and complex information. Therefore, the information system itself becomes an important object of audit.

In Vietnam, research on auditing in commercial banks often focuses on traditional auditing areas such as financial statement auditing, credit operations auditing, and internal auditing. This article uses the case study method at two banks: Vietnam Investment and Development Joint Stock Commercial Bank (BIDV), Military Joint Stock Commercial Bank (MB).

Concepts and goals of information technology audit

An information technology audit is the process of collecting and evaluating evidence to determine whether an information system has been designed to maintain data integrity, protect assets, and enable organizational goals. achieve efficiency and optimal use of resources.

The overall objective of an information technology audit is to evaluate the information system of the audited organization to determine the timeliness, accuracy, completeness and reliability of information outputs, as well as ensuring data confidentiality, integrity, availability and reliability, as well as compliance with relevant legal and regulatory requirements. Therefore, information technology audits can be performed by the State Audit, independent audit or internal audit. This study evaluates the current state of information technology auditing at commercial banks from the perspective of internal audit.

Current status of information technology audit at Vietnamese commercial banks

Information technology audit at BIDV

At BIDV, the information technology auditing department belongs to the Supervision and Compliance division under the Executive Board. This department is responsible for checking and monitoring information technology activities in the bank, and is the second layer of control in COSO's 3-layer model.

The main contents within the scope of information technology audit at BIDV include:

- Evaluate the internal control system for the implementation of the bank's information technology projects, the control of management and use of computers and information technology equipment at the units, and the actual situation. Currently monitors and controls information technology activities and the effectiveness of internal control systems in information technology applications at units.

- Risk assessment: Unauthorized access to important information; Inconsistency between changes in major strategies and information systems; Providing incomplete or inaccurate information; Technical problems cause transactions to stall or data to be lost...
- Auditing the operation of information technology systems, including: Auditing the operations of the Information Technology Center; Auditing the operation and security of information technology infrastructure; Auditing compliance with processes, legal regulations, as well as BIDV regulations such as: AS400 server operation and maintenance process, SIBS system operation and maintenance process, core banking system of BIDV, maintenance process of hardware, software, WAN/LAN...

- Auditing outsourcing resources.

It can be seen that the content of information technology audit at BIDV closely follows the regulations in Circular No. 18/2018/TT-NHNN of the State Bank regulating the safety and security of information systems at banks.

İnformation technology audit process at BIDV follows the following 3-step process:

- Planning audits, performing audits and reporting.
- During the audit implementation stage, information technology auditors at BIDV use all testing methods to check according to archived records and actual implementation process.
- During the reporting phase, the results of the audit process provide post-audit assessments and suggestions for remediation. Assessments and recommendations are required to be reported and re-examined as an independent inspection, or integrated into the following inspection depending on the level of recommendation.

Information technology audit at MB

At MB, the information technology audit department consists of 5 employees and 1 expert, belonging to the Internal Audit Agency, under the Board of Directors, belonging to the 3rd layer of defense in the model of 3 lines of defense of the auditor. internal control. The second layer of defense is the Inspection - Internal Control Division and the unit in charge of operating the information technology system at MB, as well as establishing the first layer of defense, the Information Technology Division. The content of information technology audit at MB is determined on the basis of risks, including risks related to information technology activities and risks related to components of information technology systems.

Information technology audit content is based on risks related to information technology system components including the following 3 groups: Users; Information technology officer; hardware, software and connectivity infrastructure. These audit contents are considered the "vertical" and "horizontal" axes that constitute all content related to information technology in MB.

In each information technology audit, the implementation process at MB is similar to the process of performing a normal audit, including the following 3 stages: (i) Audit planning; (ii) Perform audit; (iii) Report.

Information technology audit specialists collect necessary information from inspection reports, reports outsourced by MB to evaluate, internal reports... to create a detailed plan including objectives and key audit contents. According to the assessment of information technology auditors at MB, the more detailed the audit plan, the easier the implementation process and the closer it sticks to the goal.

One of the most important contents in this stage is building a risk profile. Risks are identified “vertical” and “horizontal”. In addition, in the audit planning stage, auditors also determine control objectives, current control measures, risk levels and effects on information systems.

Normally, information technology auditors at MB take 3-5 days to complete the risk profile before performing the audit, including time to add comments from observing information on the system. Or write some commands for testing. Fieldwork time fluctuates between topics, usually 10-15 days for small topics, 30-45 days for large topics. In fact, information technology audit activities at MB have only been implemented for one year. Because this is a very new activity at MB, the audits are following the vertical axis, not the horizontal axis of the system, and are planned to be deployed in the following years.

Reports and recommendations are the products of each audit, given by auditors with the goal of perfecting the risk management framework in the bank, ensuring comprehensive management of key information technology risks. confidence in MB Bank's operations according to good practices and international practices of the Basel Committee, COSO, and ISO.

Evaluate the current status of information technology audits at BIDV and MB

From the current status of information technology audits at BIDV and MB, it shows similarities and differences in aspects of implementation departments, audit content, and audit processes. Specifically:

Regarding the implementation department: At BIDV, the information technology auditing department belongs to the Supervision and Compliance Division, under the Executive Board, while at MB this department belongs to internal audit under the management of the Board of Supervisors. With this structure, at BIDV, information technology audit belongs to the 2nd line of defense, while at MB this department belongs to the 3rd line of defense in COSO's 3-line of defense model. However, one of the audit contents identified by BIDV is to evaluate the internal control system on the implementation of supervision and control of information technology activities at the unit, as well as the effectiveness of the system. Internal control system in information technology application at the unit, proving that this is the function of the third line of defense. Thus, the information technology audit department at BIDV is located in the Supervision and Compliance Division. defense is not reasonable.

Regarding audit content: It can be seen that each bank has a different way of determining audit subjects and content. BIDV relies mainly on regulations on information system management in banking according to Circular No. 18/2018/TT-NHNN of the State Bank to propose audit topics, while MB has its own way. risk-based approach. BIDV's approach has the advantage of being easy to evaluate the system's compliance with the law, however, the audit content is widely determined, making it difficult to synthesize, analyze, and find information. out the cause. MB's approach is more modern, applying ISACA's guidelines on identifying and classifying risks, thereby determining audit content and topics. This will help banks build a complete and logical risk profile, making it easier for audit planning and root cause assessment. However, this method also requires more time and qualifications of staff.

Regarding the audit process: Although it is explained into different steps, in general, the audit process of both banks includes the main steps, which are audit planning, audit performance and reporting.

Results achieved and existing, limited

Evaluating information technology audit activities, it can be seen that commercial banks have achieved some initial results, specifically: Information technology audit activities receive close attention from the Board of Directors. and units throughout the system; The audit system and process have been built and are increasingly perfected; The information technology audit team has been formed and is increasingly improving its capacity and qualifications; Information technology audit has contributed to improving the quality of risk management and operational quality at the bank.

Besides the advantages, according to the assessment of officials directly performing information technology audits at commercial banks, there are still difficulties and problems such as: The scope of the audit is too wide, causing difficulties for determining the focus and possibly missing risks. Banks are often confused in choosing methods and tools to assess risk; The information technology field frequently changes both in technology and system architecture, causing audit activities to constantly change, causing pressure on time, effort and reducing management efficiency; Human resources for information technology auditing are lacking and weak.

Conclude

To strengthen information technology audits in Vietnamese commercial banks to meet increasing requirements for quality, safety, and security of banking information technology systems, solutions are needed. synchronized from the State Bank, commercial banks and Banking Association. Only then will information technology audit fully promote its role as the last line of defense in preventing, detecting and handling risks in commercial banks, thereby increasing management efficiency and effectiveness. bank's operational efficiency.

References

1. Joint Stock Commercial Bank for Investment and Development of Vietnam, Annual Report, 2022.
2. Military Commercial Joint Stock Bank, Annual Report, 2022.