INFORMATION SYSTEMS AUDITING

Radu Dorin LENGHEL
Miranda Petronella VLAD

Abstract: Financial audit missions have a main role in providing decision makers with more reliable and useful financial information, as well as in improving the internal control system in order to make it adequate to the financial management systems.

IT controls are a significant factor in achieving these goals and in understanding the entity's internal control structure by the auditor. These aspects must be taken into consideration during the entire life cycle of the audit.

Information systems auditing represents the collection of relevant audit evidence in order to determine whether the information systems are secure, maintain the integrity of the processed and stored data, allow the achievement of the entity's objectives and efficiently use information resources.

The audit procedures will provide elements for the foundation of the audit opinion regarding the management of available information resources (data, apps, technologies, facilities, human resources, etc.) towards achieving the entity's goals by ensuring efficiency, confidentiality, integrity, availability, safety and conformity with a frame of reference (standards, good practices, legislation, etc.). The stages of the information systems audit are: audit planning, audit execution, audit report and review.

Keywords: financial audit, information systems auditing, audit planning, audit execution, elaboration of the audit report, etc.

1. Audit planning

Planning is the first stage in the audit's life cycle, its correctness ensuring the efficiency and execution of all the other stages of the audit. Planning supposes gathering information regarding the audited entity and information about its internal control system. Moreover, planning must include an assessment of risks ensuing from the functioning of these systems.

The audit planning is based on an audit strategy that is formulated starting from the definition of the audit's approach and stipulating the elements related to the coordination of the audit mission, the team involved, their responsibilities, the time horizon and the main action directions.

The objective of planning the information systems audit is to gain an understanding of the environment in which the information system functions within the audited entity, to assess the error or fraud risk, to elaborate an efficient approach to the audit through which to collect sufficient and trustworthy evidence in order to formulate an opinion and to assign the

necessary resources for the execution of this activity. Planning activities takes into account the minimization of the audit costs.

Planning the information systems audit must include all the stages necessary for the achievement of the objectives of the audit mission, namely the documentation regarding the audited activity, the programme or system under scrutiny, the establishment of the audit strategy, the establishment of the audit procedures and techniques, the methods of synthesis, analysis and interpretation of the audit evidence, the identification and assessment of risks generated by the supply of electronic services.

At this stage, the auditor gains an understanding of IT operations and controls, and of associated risks. By assessing these risks, the auditor decides which controls are most likely to be effective. In case the controls have a high probability of being effective, and if they are relevant to the objectives of the audit mission, the auditor must determine the nature and volume of audit procedures necessary to confirm hypotheses.

In case the controls do not have a high probability of being effective, the auditor must gain a sufficient understanding of associated control risks in order to formulate adequate associated findings regarding corrective actions.

Moreover, the auditor must determine the nature, extent and volume of necessary tests, in view of choosing the most adequate audit methods, techniques and procedures.

The audit plan provides the general framework for the achievement of the audit objectives in an efficient and pertinent manner. During the audit execution, adjustments of the audit plan are accepted, explained by the appearance of new elements in relation to the initial context assessment that requires the amplification of certain investigations and the application of more detailed audit procedures.

The audit plan contains information regarding the nature, duration and programming of audit procedures, as well as the necessary resources (human, financial, technical, documentary, etc.).

The elaboration of the audit plan focuses on the following directions: defining the coverage area of the audit, describing the way the audit will take place, providing a means of communicating information regarding the audit to the entire personnel involved in the process.

The audit plan of information systems can be updated during the audit mission by the members of the team according to the risks established by the auditors.

Financial auditors must communicate with the audited entity in a constructive manner during the audit mission by organizing meetings or via electronic means.

In order to achieve the objectives set in the audit plan, the financial auditors will elaborate audit procedures for the specific issues of information systems:

assessment of quality management, physical security and environmental controls, information and information system security, system continuity, system change and development management, apps functionality, quality of internal audit regarding the information system, assessment of risks generated by the functioning of the information system. These procedures come with methodological instructions, assessment lists, models and questionnaires, as appropriate.

Audit procedures refer to the procurement of audit evidence, audit evidence analysis and summarizing results.

2. Audit execution

Financial auditors will collect sufficient and adequate audit evidence. In case the evidence is not sufficient and adequate, the financial auditors will extend the collecting procedures with additional thorough tests on the information system.

There will be tests performed on specialized controls for the identification of elements or actions that make up risk factors and an analysis of their impact on the entity's activity will be carried out.

Altering audit evidence can be caused by the existence of some systematic anomalies or errors of the programmes functioning that affect all data processing and lead to false results, difficult to correct through manual procedures, given the great amount of transactions and the complexity of the processing algorithms.

As a result of the automated management of a great amount of data, without human involvement, there is the risk of not detecting some errors for a long time, due to design or update anomalies of certain software components.

Audit procedures will deliver elements for the foundation of the audit opinion regarding the management of available information resources (data, apps, technologies, facilities, human resources, etc.), in order to achieve the entity's objectives by providing efficiency, confidentiality, integrity, availability, safety and compliance with a framework (standards, good practices, legislation, etc.).

Collecting and inventorying audit evidence refer to the elaboration of the electronic or printed data according to scale models, questionnaires and assessment lists, as well as to their set-up and storage. The nature of the audit evidence is dependent on the audit objective and the audit model used.

Even though the audit models can vary as regards the details, they reflect and cover the joint requirement to provide a reasonable assurance that the objectives and criteria imposed within an audit mission (e.g. financial audit) are met.

Obtaining the evidence and registering it in work documents represent essential activities of the audit procedure. The work documents are elaborated as the activities of all the audit's stages take place.

The work documents must be written with accuracy, must be clear and coherent, must be legible and arranged in a certain order, and must refer only to the significant, relevant and useful aspects.

In order to obtain the audit evidence, the following audit techniques will be carried out:

- interviews with key persons involved in the project (coordinators, users, system administrators, etc.);
- use of questionnaires and scale models;
- examination of technical, economic, monitoring and reporting documentation: implementation graphs, mail, internal reports, reporting situations, partial reports of the project, lists of documents, usage monitoring documentation, contracts, statistical syntheses, methodologies, standards;
- participation in demonstrations regarding the use of the information system;
- assessment of the portal and electronic services;
- use of audit computer-assisted techniques and tools or other applications.

In the case of financial audit missions that assess the financial-accountancy information system, in order to formulate an opinion regarding the reliability of the information supplied by the information system, the financial auditor will elaborate the assessment lists for testing IT controls specific to the financial-accountancy application, which contains the following application control categories: controls regarding files integrity; controls regarding app security; controls of entry data; controls of data processing; controls of exits; controls regarding the network and the communication; controls of permanent data files.

In case the system does not seem to be sufficiently robust, the auditor must assess the risk of the system malfunction upon the objectives of the financial audit mission.

Within the audited entities, the information systems under assessment are used as support for the assistance of decision, making up IT systems used for the inventory, processing and obtaining of results, operative and synthetic situations at all reporting levels. Therefore, a special category of IT controls refers to the conformity of the information system with the requirements imposed by the legislation.

The legislation requirements include: finance and accountancy legislation; legislation regarding private and personal data protection; legislation regarding the improper use of computers, in the sense of cyber-crimes; financial and banking regulations; legislation regarding intellectual property, etc.

Financial auditors will make an assessment of the information systems and apps by analysing, interpreting and synthesizing the information gathered during the interviews or collected from documents and scale models, questionnaires and assessment lists.

These operations are mainly based on the elaboration and use of synthetic tables, graphic representations, performance indicators, correlation matrixes,

etc. To this effect, computer-based tools and techniques are used on a larger scale.

3. The elaboration of the audit report

The assessment and review of the information system are carried out through the analysis of the findings and their interpretation. According to the impact unconformities have, recommendations are formulated for their reparation and the reduction of risks.

These recommendations reflect the auditor's opinions on the audited entity in terms of the objectives of the audit mission. Synthetically, the findings will refer to the following aspects: the assessment of the information systems complexity, the general assessment of the risks, the assessment of risks for each application, and the auditor's point of view regarding the feasibility of an audit mission based on controls.

The report aims at highlighting the weaknesses of the controls identified by the auditor and informing the audited entity about them through the audit report and the letter that contains the main findings and recommendations. The audit report identifies the domain, objectives, period, planning and coverage of the audited activity.

The audit report is elaborated by the financial auditors for each audit mission and will include the most significant findings, recommendations and conclusions reached during the audit mission regarding the stage and development of the implementation and use of the information systems existent within the audited entity.

The report will also include the auditors' opinion on the nature and weaknesses of the internal control within the audited entity and their possible impact on the entity's activity.

The recommendations in the audit report must not detail the implementation method, which is a responsibility of the audited entity's management. The audit report must be objective and correct, include all the relevant findings even the positive ones, be constructive and present the conclusions and the recommendations formulated by the audit team.

4. Conclusions

Financial audit missions have a core role in providing more reliable and useful financial information to decision makers and in perfecting the internal control system so as it should be congruent with the financial management systems. IT controls are a significant factor in meeting these goals and in understanding the entity's internal control structure. They must be taken into consideration during the entire audit life cycle. The stages of the information system audit are: planning, execution, reporting and reviewing. The audit procedures will provide the elements for the formulation of the audit opinion

regarding the management of available information resources (data, apps, technologies, facilities, human resources, etc.), in view of meeting the entity's goals, by ensuring efficiency, confidentiality, integrity, availability, safety and conformity with a framework (standards, good practices, legislation, etc.).

The financial auditors will make an assessment of the information systems and apps through the analysis, interpretation and synthesis of the information gathered during the interviews or collected from documents and scale models, questionnaires and assessment lists.

These operations are mainly based on the elaboration or use of synthetic tables, graphic representations, performance indicators, correlation matrixes, etc.

To this end, computer-based tools and techniques for the information systems auditing are used on a large scale.

References
1. Oprean, I., Lenghel, R.D., Oprean, D.B, *Auditarea situaţiilor financiare (Auditing financial statements)*, Risoprint Publishing House, Cluj-Napoca, 2015;
2. Lenghel, R.D., *Control şi audit financiar (Control and financial audit)*, Risoprint Publishing House, Cluj-Napoca, 2011;
3. *Manual de reglementări internaţionale de Control al Calităţii, Audit, Revizuire, Alte Servicii de Asigurare şi Servicii Conexe (Manual of international regulations on Quality Control, Audit, Reviewing, Other Assurance Services and Connected Services)*, Volumes 1, 2, CAFR, Bucharest, 2015.

NOTE ON THE AUTHORS
Radu Dorin LENGHEL has a Ph.D. in economy, and is an Associate Professor with the Finance and Accountancy Department at the Faculty of Economic Sciences Cluj-Napoca. He is the author of numerous scientific papers and books in the field of accountancy, control and financial audit. He is currently teaching: *Control and financial audit, Auditing financial statements, Control and internal audit, Accountancy in public institutions, Management accounting.*

Miranda Petronella VLAD has a Ph.D. in cybernetics and economic statistics, and is an Associate Professor with the Finance and Accountancy Department at the Faculty of Economic Sciences Cluj-Napoca. She is the author of numerous scientific papers and books in the field of computer science. She is currently teaching: *Databases, Economic informatics, Information management systems, Decision support information systems, E-commerce.*