IOP Conf. Series: Materials Science and Engineering **200** (2017) 012026 doi:10.1088/1757-899X/200/1/012026

Audit in public administration's information systems – External or internal?

D Drljača[1] and B Latinović[2]

[1]Europrojekt centar, Banja Luka, Republic of Srpska, Bosnia and Herzegovina
[2]Pan European University APEIRON Banja Luka, Faculty of Information Technologies, Republic of Srpska, Bosnia and Herzegovina

E-mail: drljacad@gmail.com

Abstract. Audit of the information system, thanks to the increased use of ICT and related cyber-crime, becomes a very important process in modern companies and institutions. It is usual to engage or outsource a third party for independent financial audit. But what about auditing of the information system of public administration institutions? This paper gives an introduction to possible aspects of information system's audit with the aim to discuss possible answer on the question in the title.

1. Introduction

The computer systems and machines are modernising and automate the business process in private (industry) but also in public sector (public administration and institutions). Modern business is not any longer possible without computer systems and Internet-based communication. Traditional (paper-based) information systems become a part of history while computer-based (supported) information systems are more and more in use.

Even the business processes in public administration and institutions introduced this concept and heading fast towards paperless offices. This is important in order to meet expectations from the citizens and business entities since all aspects of living are influenced with the digitalisation.

All of these changes have proven to be positive and usefulness for the overall progress of society, but they are followed by misuse causing fraud and significant problems. Therefore, institutions - especially those dealing with personal and other sensitive data – have to invest additional efforts in protecting such data. Public administration has even more responsibility to do this since their information systems and repositories are overloaded with such kind of information, starting from financial data, personal data up to the data on overall safety and security (such as military data).

Audit of such information systems (IS) can be a really difficult task, from its beginning. But this task is important to be done if we want to secure proper functioning of an IS and protection of data.

This paper will present some aspects of IS audit and will provide insight into the necessity to make it internally.

2. Purpose of IS audit

The audit of information systems (wider than an audit of IT) appeared with the introduction of the information technologies in the accounting systems. During 1960-ies this was known as Electronic Data Processing (EDP) Audit. The increased the use of computers in businesses (as a trigger) resulted with the need for auditors to become more familiar with EDP concepts in business. Business

dictionary defines EDP as the "use of computers in recording, classifying, manipulating and summarising data" [1].

Since mid-1950-ies, many books have been written about EDP, but as the most significant was the works of Richard G. Canning from 1956, titled "Electronic Data Processing for Business and Industry" and Felix Kaufman from 1961 titled "Electronic Data Processing and Audit" [2]. To simplify and to connect it with the public administration we can say that EDP is primarily concerned with the use of computers and IT in basic administrative and accounting functions.

According to Dube and Gulati [3], one of the most important reasons for the establishment of information systems auditing separately from financial is insufficient knowledge of computer that negatively and adversely affects the ability of auditors to carry out the attestation functions. With other words, auditors do not possess sufficient IT skills for adequate attestation of claims.

One of the first definitions of information systems' audit was given in 1998 by Ron Weber [4] that is in use even today. It seems that other scholars favour this definition, so Cangemi sets almost identical one, defining it as the process of collecting and evaluating evidence on the basis of which it can be determined whether the information system keeps the property of the company adequately, maintain the integrity of data, allows you to effectively achieve the set goals, and whether they use available resources efficiently [5].

So, the key phrases are: collecting and evaluating evidence, keeping the property of the entity, maintain data integrity, effective and efficient use of resources. These are the main guidelines for a successful audit. This means that IS audit is becoming more important considering spectrum of controls it has to check and validate against best practices, audit frameworks, and standards.

There were some efforts to improve above mentioned definition of which is good to mention the effort of Panian from Croatia. Namely, Panian intention is to deepen the definition by linking it more closely to the definition of the financial one, adding part of sentence saying "and determining whether the organisation meets the appropriate regulations, rules and conditions" [6].

Taking in the consideration the complexity of IS audit, Piattini considers that IS audit, once being a complement to the financial one, is having own existence and can be considered as a strictly professional discipline [7].

Therefore, it is possible to conclude that IS audit is wider than the financial one and requires a set of specific skills and knowledge of auditor, from both economy and ICT. As such complex process, it also requires specific agreement between the auditor and the client about the confidentiality of audited data and processes.

Nevertheless, it is also obvious that IS audit is becoming more and more important part of usual business practices, especially for entities dealing with e-commerce, or providing e-services such as public administration. Therefore, IS auditor should not be seen as a person of whom organisation should be afraid of, but as a business partner willing to help and to assist in overcoming problems. Therefore, the role of IS auditor crucially differs from the role of the traditional financial auditor (see below Table 1). The overall holistic approach in IS audit requires new skills and more important – new way of thinking and approaching clients as business partners.

Table 1. The role of IS auditor against financial auditor

IS auditor	Financial auditor
To prevent misuse or fraud	To detect misuse or fraud
To act as a partner in the team	To punish as authority
To act as risk preventing manager	To act as evaluator and auditor
To focus on business process	To focus on audit findings

3. Types and aspects of audit

In order to have better insight into the issue of the audit, it is necessary to see different types and aspects of the audit process. In a literature, it is possible to find different definitions and aspects of audit in the company. This often depends on the aspect and point of view. But, summarising experiences from the different literature sources, a possible classification of audit types is given in Figure 1 below.

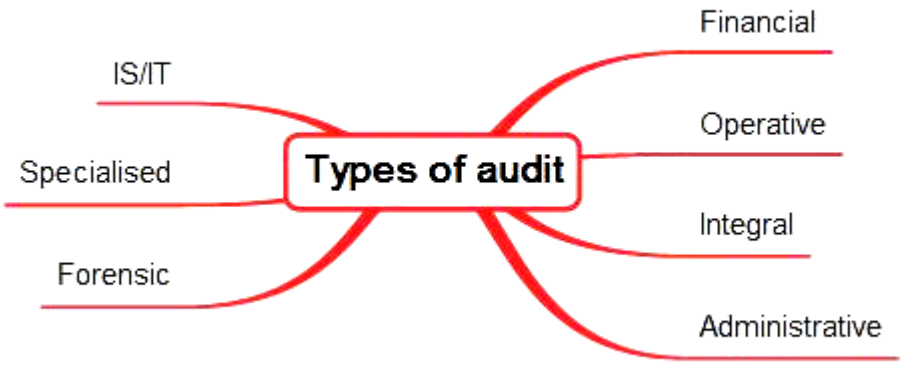

Figure 1. Types of audit in the institution (author)

The most common type of audit is **the financial audit**. The purpose of this audit is to evaluate the validity of financial reports. It relates to the integrity and reliability of financial information. This audit in public administration institutions is obligatory by law and is performed usually by contracted auditing company such as PricewaterhouseCoopers, Deloitte etc. Also, it can be done by authorised independent and licensed auditor under the condition that there is no conflict of interest and auditor is not an employee of the institution auditing.

Operating audit has a purpose evaluating the structure of internal controls of given process or work area. An example of this type of audit is the audit of application controls and logical security systems. This is a specific and targeted audit.

Integral audit combines both – financial and operative audits. The integral audit, in essence, is implemented to evaluate organisational goals related to the financial information, preserving of property, efficiency and harmonisation with overall goals of the audited institution.

Administrative audit aims to evaluate issues related to the efficiency of operative productivity within the organisation or institution. An administrative audit can be agreed even as the part of more complex reviews and audit.

IS audit aims to collect and to evaluate evidences to determine if the information system and related resources adequately preserves the organisation's assets, maintain integrity and availability of the data and the system itself, provide relevant and reliable information, achieve the business aims of the organisation with effective and efficient use of resources and have internal controls. This should assure achievement of business, organisational and control aims and that the unwanted events will be discovered, prevented and/or corrected.

Specialised audit presents a specific type of targeted audit. It is about the larger number of specialised audits delivered or undertaken by the third parties. Given business often and in large depends on services from the external service provider, the demand for this kind of audit is growing.

Forensic audit is a special case of the IS audit. Its task is to detect, publish and follow-up of threats and fraud. The primary purpose of this audit is to collect forensic evidence for eventual court processes and procedures.

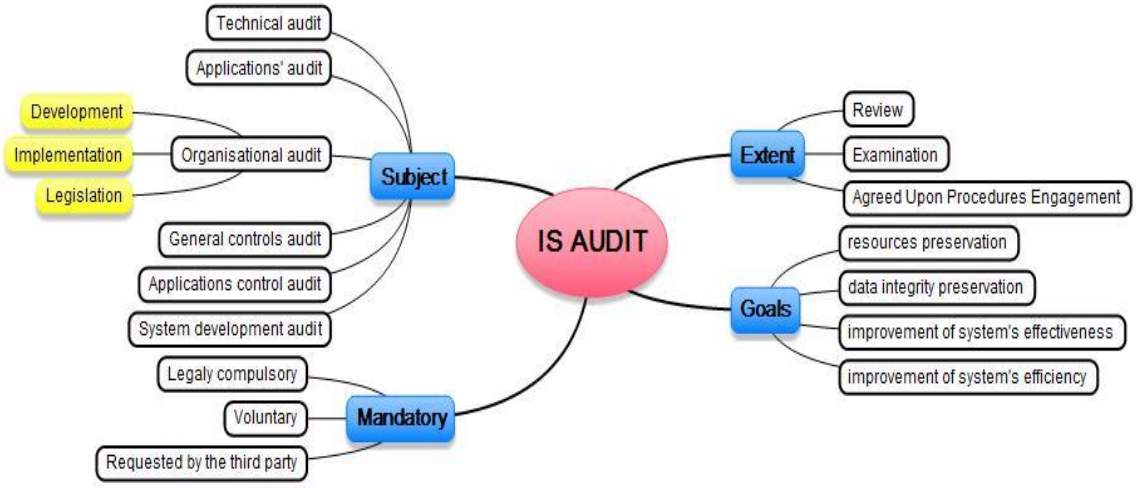

Figure 2. Aspects of IS audit in the institution (author)

4. External or internal?

Having in mind variety of aspects and points of interests for audit, it is very interesting to decide whether this audit should be outsourced and contracted by external audit company? This is a very important issue that requires determination and reasoning of the CEO or Management Board, which are in charge to make a decision on the audit. This is a very important issue especially for public administration organisations and their decision-making bodies having in mind that sensitivity of data being analysed.

The audit process can be organised internally and externally depending primary on the decision from top management and on the volume of the audit.

The audit of an information system can be a part of the internal audit. It can also function as a separate or integrated audit together with the financial audit. Integration with the financial audit should provide more assurances related to the IT linked controls for financial auditors. It is up to the management of the institution to decide on the modality for implementation of the audit before making Audit Charter. But it has to be strictly defined in the purpose of the audit – either the audit of IS functionalities, or audit of IS in the function of support for financial audit, or audit in the function of business operations improvement.

The Audit Charter (the programme of the audit) has to include the decision on which type of IS audit shall be implemented. It also must have a clear statement from the management of objectives and aim of the audit as well as delegated authorities for implementation of the audit. Besides these more general, the management should make a decision on volume of the audit – which can be defined together with the assistance of auditing authority or audit implementing company.

As results of the audit will be used for more tactical and strategic decision-making process and at the operative level used for implementation of corrective measures, these Terms of References for Audit should be approved by the senior manager or owners of the company or in some cases an audit board (if present).

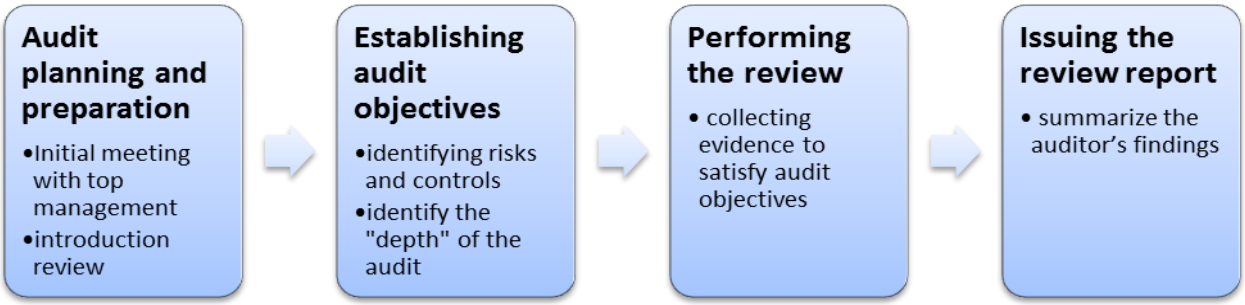

Figure 3. Usual steps in IS audit in the institution (author)

The IS audit is very complex and wider than a financial one. Therefore, IS auditor should be a technically complete person, with sufficient skills and knowledge needed for implementation of IS audit. IS auditors have to update and review their competencies and knowledge due to the large and fast changes in the field of information technologies, communication technologies, but also in the overall area of information system components. For IS auditor, it is important to understand the processes and if they are harmonised with best worldwide practices. However, it is necessary also to know the legal framework for business operations in the company or the institution. There are two main lines related to familiarity with the legal framework: one is to know legal aspects related solely to the audit of information systems and the other one is to know legal aspects of the topic of the audit, which is more specific and more precise.

In the planning phase, the auditor must be aware of the complete area that is under examination. This may include (but also not limit to) understanding and knowing of different business practices and functions that are in direct relation with the topic of the audit. However, for IS auditor is necessary to learn about the type of information system, supporting technologies and many other things.

If implemented as a part of the internal audit, the management should make all necessary efforts to make this audit as independent as possible. However, a hint of subjectivity will always be presented in such audit. Internal auditors are responsible to the audit board or to the top management and owners. The aims of internal audit should be aligned with the mission of the organisation or institution and should be based on the short- and long-term plans for the audit process. The aim of short-term audit plans is to plan a specific arrangement with known initial point and end with concrete goals. While on the other hand, long-term plans for audit deal with guidelines and definition of resources for efficient audit implementation. As in the financial audit, in the core of IS audit is also evaluation of related risks. Figure 4 shows usual steps in IS audit in the institutions or organisations.

It is obvious that even the most objective persons from the institution or organisation can be subjective in evaluating the IS and its functionalities. The internal auditor will be very skillful to evaluate the status of the technology and processes due to working experience and affiliation, while external auditor may blindly follow the instructions from frameworks and standards and not specifically experienced in the field.

The internal auditor will pay less attention to the achievement of customer satisfaction, while the external will look exactly to this and the two opinions may be very different. The internal auditor

might focus more on security aspects of IS, while external can focus easily on overall functioning as independent one, especially when dealing with communication and information flow.

From the safety aspect, the internal auditor is more desirable one since all the knowledge and data are staying "in the house" unlike the external auditor. The organisation may perceive external auditor as a potential point for "leaking of information" and as security problem despite signed confidentiality agreements. From the other hand, if not providing quality access to data and information to the external auditor may cause false interpretation of the collected data and also mistrust from the auditor on its skills and independent view.

However, the quality of data collected and opinion presented is mostly in the interest of the organisation or the institution. Therefore, this is always an open and ongoing issue in the planning phase of the IS audit process.

Figure 4. Usual steps in IS audit in the institution (author)

5. Conclusion

The audit of IS becomes more important for business operations regardless the size and the functionalities of the IS, especially in those dealing with sensitive data and with a large number of clients. The primary interest of the audit is security and safety of the IS, but there should be considered many other controls influencing IS role in the business processes.

Public administration IS are very sensitive to any kind of audit due to the importance of data. Although there are no legal requirements for IS audit in public administration in Bosnia and Herzegovina, this should be enforced in legislation such as it is a case in the banking sector.

Also, there is an ongoing dilemma - who should perform this audit? Should it be internal auditor or external? What do we get by engaging and paying external one? Do we really need these services and will this external auditor possess sufficient knowledge and skills to do it better than our internal auditor? Do we have a skilful internal auditor, since this audit is completely different from the financial one?

There are just some of questions that should be clear in minds of those making a final decision on implementation of the IS audit in the organisation or institution. One should consider all benefits and all potential risks in the implementation of the IS audit. IS including related IT, is not only a tool for

business operations but is a crucial element of each business and should be kept and maintained with more care and with more attention.

References

[1] ***Business dictionary 2016 *Electronic Data Processing*, available at http://www.businessdictionary.com/definition/electronic-data-processing-EDP.html, accessed on 21.10.2016
[2] Wayne S B 1965 *Auditing with the Computer*, University of California Press
[3] Dube D P and Gulati V P 2005 *Information System Audit and Assurance*, Tata McGraw-Hill, New Delhi
[4] Weber R 1988 *EDP Auditing--Conceptual Foundations and Practice*, McGraw-Hill, 1988
[5] Cangemi M P 2000 *Managing the Audit Function: A Corporate Audit Department Procedures Guide 3rd ed.*, John Wiley & Sons, New York, USA
[6] Panian Ž 2001 *Kontrola i revizija informacijskih sustava*, Sinergija, Zagreb, Croatia
[7] Piattini M 2000 *Auditing Information Systems*, Idea Group Publishing, USA/UK