INFORMATION SYSTEMS AUDITING – LEGISLATION AND STANDARDS

Associate Prof. Janka Dimitrova [1]

Associate Prof. Miroslav Andonovski [2]

Associate Prof. Riste Temjanovski [3]

Eftimija Dimitrova[4]

Abstract

The second half of the 20-th and early 21-st century, marked the expansive growth of ICT and software solutions that invaded all spheres of everyday life and work. Effective management of ICT is essential not only for the successful execution of daily activities and processes, but also in achieving the strategic goals of each company. ICT management is not only management costs incurred in doing business operations but also control of their efficiency and security, since advances in technology may result in increased exposure to operational risks. Enterprises should have an adequate system of internal control which is consistent with the nature, complexity and risk profile of operations.

According to the legislation, it is mandatory the establishment of internal audit service as an independent department within the internal organizational structure, and conducting an external audit to verify the information presented in the financial statements. The Internal Audit provides objective and independent assessment of the adequacy and effectiveness of the internal control system, the accuracy of accounting records and financial statements, compliance with internal policies and procedures, and with laws and regulations that are in force, as well as general efficiency operations. As an indispensable part of the operation or the scope of the internal audit is an evaluation of the adequacy and effectiveness of processes and control mechanisms in information systems. Also and the external audits, which are mandatory and are performed annually, among other should provide opinion and assessment of the information security in terms of its compliance with the work and objectives of the company, data protection and established control systems.

Keywords: audit, control, information systems, information technology, management

[1] PhD, associate professor at the Faculty of economics - University Goce Delcev Stip, janka.dimitrova @ugd.edu.mk

[2] PhD, associate professor at the Faculty of economics - Prilep, University ,,Sant Kliment Ohridski" Bitola, miroslav.andonovski@uklo.edu.mk

[3] PhD, associate professor at the Faculty of economics - University Goce Delcev Stip, riste.temjanovski@ugd.edu.mk

[4] student in high school Yahya Kemal Strumica, eftimijadimitrova@yahoo.com

Introduction

Well defined, organized and perfectly executed processes in a modern company are a prerequisite for increased competiveness, reduced costs, strengthening market positions and greater flexibility in changing market conditions. Modern corporate development requires intensive management and optimization of these processes through the introduction of best practices in the field and: development and implementation of management systems for mutual Customer Relationship (CRM), management of business (ERP), Management of supplies (SCM), for managing internal services (Help Desk, call-centre), management of training (e-learning), management of documentation (e-book, Secret Book) and management of communications (IPCC, virtual PBX, call-rec). Today, every business depends on IT because it provides: faster time of delivery, higher quality and cheaper services, the maximum support of business, controlled risk and maximum security. Each developed and dynamic business requires quality IT and use of ITIL (Information Technology Infrastructure Library) as a best practices for managing IT. With the introduction of ITIL, IT and business people can plan together to control the processes together, to remove all obstacles among themselves and have a common goal. Creation and development of corporate IT infrastructure requires previous planning and establishment of a single concept and strategy. It is also a requirement for creation of effective and long-term investment policy, and guarantee compatibility of the programs and the management of information services. The systematic approach provides real achievement of competitive advantages through the application of information technologies.

From a business point of view, information security is one of the most valuable arguments for management with the information systems and secure data storage in the organization. The information` security is considered as a complex of organizational and technical activities which includes:

- Development and implementation of a system of policies, procedures and guidelines for the organization of the process of information services and responsibilities of the different functions and roles of users in the information process
- Training, consulting and technical assistance in support of the policy determined by the level of information security;
- Strengthening the corporate security through the use of modern IT-based methods and technologies such as cryptographic protection, electronic signatures and others.

The three main tenets of which are based the information systems are: confidentiality, integrity and availability and they include:

Confidentiality - The information is available only to those who have authorized access to it.The company is obligated to establish controls that will be used for protection of the information from the unauthorized access.

***I*ntegrity** - protection of the accuracy and completeness of the information and processing methods. The company is obligated to establish controls that will be used to prevent changing information in unauthorized ways and with unauthorized handling of the systems, which can impair the accuracy, completeness and reliability of information

Availability- the authorized users have access to the information and to the other associated facilities necessary for its presentation, when there is a business need .The company is obligated to establish controls that will apply so that authorized users have access to information and systems when they have a business need.

The audit has a primarily goal to provide independent and objective opinion of the audit committee and senior management, about the risk management, internal control system and corporate management, by measuring and evaluating the effectiveness of these controls and systems in achieving business goals. Therefore, during the implementation of the audit process, special attention is paid to audit to IT systems.

IT systems audit

The IT auditors, are mostly understood only as a technical support to the financial auditors, someone who simply operate with information systems in order and at the request of a conventional audit. The actual presence of information technology has no direct effect to the audit purposes, but it introduces specific questions related to the controls and may require changes in the audit approach. The information technology imposes two special issues for leadership and auditors:

- Computers and network, as well as each other technology, are vulnerable of defects (deterioration, cancellation) *or damage.* Once an organization becomes dependent on the informational technology, consequently the planning of unpredictable events becomes more important than before and according to that sufficient account must be taken for the technical aspect.
- Data and programs that are hold in computer systems are invisible and untouchables (intangible) and can be accessed or be changed without leaving a trace. In similar way the management and the auditors should take special measures to make sure in the authenticity, integrity and confidentiality of data that is recorded on computer.

Accordingly, general accepted control techniques are developed. Audit of informational systems (IS) are editing the valuation of these controls. The various components of the audit of IS should be delimited because they are searching for various level of skills, techniques and time layout; and because they have different contributions to the audit work as a whole. Each of these components is under consideration in a wider scope in the future presentations of this guide.

IT audit implies: control and assessment of the effectiveness and adequacy of the internal control system in the informational system, their compliance with the internal policies and objectives of the organization, and appropriate legislation and best practices (ISO 27001, COBIT, ITIL / ISO 2000) in order to provide safe, effective and efficient IT processes aligned with the company goals.

Greater use of IT and the internet for e-commerce and communication of business entity with consumer, business entity with business entity, business entity with the government and business entity with employee introduces new elements of risk that an entity should cover and the auditor should consider when planning and performing of the audit of the financial statements.

Internet refers to the worldwide network of computers networks, it is a shared public network that enables communication with other entities and individuals worldwide. It is an inter-operative, which means that every computer connected to the Internet can communicate with any other computer connected to the web. The Internet is a public network, unlike private network that allows access only to authorized persons or entities. Using public network introduces special risks that an entity should cover. The growth of e-commerce can have a significant impact on the traditional business environment of the entity. The growth in Internet activity without obligatory attention of the entity relative to these risks may affect the assessment of the risk from the auditor. The threats to the information systems that use the weaknesses of the IT resources to bring the integrity, confidentiality and availability of the processes and services of the

company are changing dynamically and frequently and accumulate very easily and escalate cumulatively for the whole organization.

There are several types of audits:

- Audit of Financial Statements
- Statutory audit
- Compliance Audit
- Audit of internal control systems
- Audit to detect abuses and fraud

But, the IT audit is the one that apply for the implementation of all of the before mentioned types of audit precisely, because IT is present in all segments of the business entities.

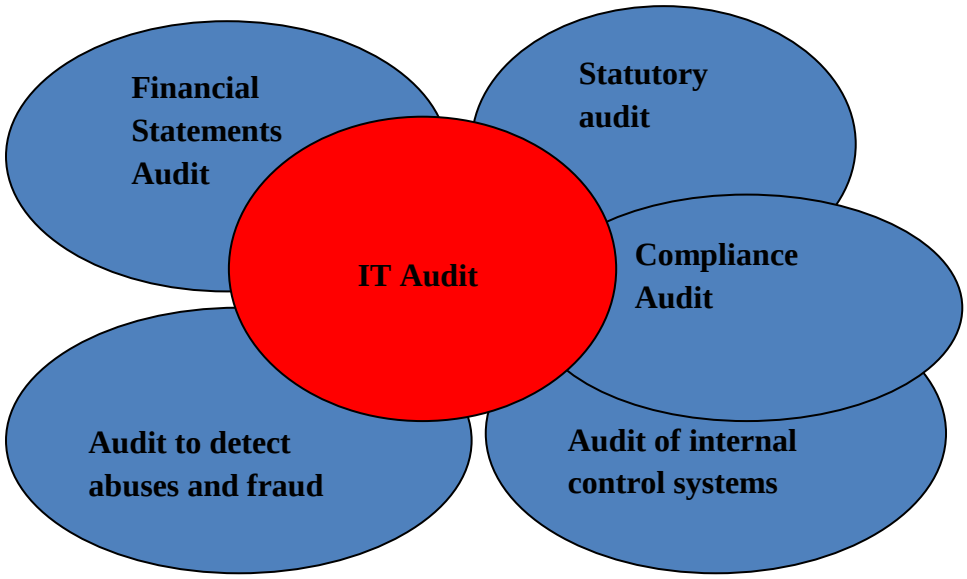

Figure1. Types of audit

According to *Implementation Standard 1210.A3,* the internal auditors must have sufficient knowledge of the key Information-technology risks and controls and about the available technology-based audit techniques to perform their work. However, all internal auditors are expected to have expert knowledge as it has an internal auditor whose primary responsibility is an IT audit.

The Audit of IT processes and IT systems implies check on:

- The safety and the IT systems (network, operating system, database application)
- Development of applications and running projects
- The authorization (rights) to access IT resources
- Back up
- The existence of unauthorized intrusions and using systems
- Introduced protection against viruses and other malicious programs
- Physical Security
- The relationships with IT suppliers
- Protection of the privacy
- Compliance with the legislation
- Plans for Continuity in the working restoration from disaster
- Applied controls.....

The implementation of fast efficient and effective audit of IT systems goes through the following four stages.

Phase I - planning and preparation of audit program

Phase I I - performing the audit, interviews, observations, review of procedures, testing, verification of system configurations and placement

Phase III - publishing reports and

Phase IV - Monitoring

The primary reason IT auditor should perform a preliminary study in the initial planning phase of the audit engagement is:

- For understanding the process.
- Because of the compliance with the auditing standards
- For identification of the control environment
- For developing a plan for testing

Enterprise *Resource Planning (ERP)* – are business information systems I.e. commercial application systems designed for support of operations in the organizations. They include standard business processes in every organization such as material operations, accounting, human resources, payroll, procurement, billing and so on. These application systems can be adapted and execute specific functions for certain types of organizations / industries such as banks, insurance companies, telecom, healthcare, public administration.

Key controls who may need to be implemented by the IT auditor:

- Input controls - check at data entry
- Output controls - reports
- Data transfer / alignment between systems (Batch controls)
- Segregation of duties
- Maintenance of the application system
- The right to use (license)
- Right to functional changes (source code)
- Training and education for use
- Inspection / testing errors (bugs, backdoors)

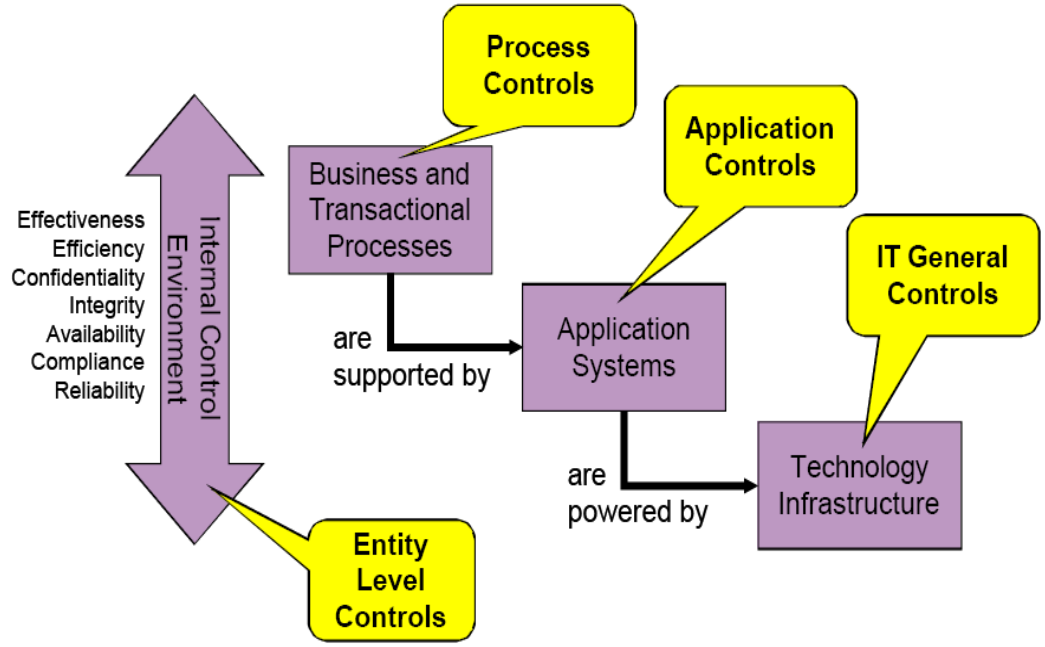

Figure2. The system of internal controls

Primary responsibility of the IT auditor against the inappropriate segregation of duties is:

- To force implementation of adequate segregation of duties
- To inform the management about the risks resulting from inadequate segregation.
- To participate in the definition of the roles and responsibilities of employees in order to establish a proper segregation of duties
- Simply to document the identified deficiencies related to the segregation of duties

Legal framework, standards, procedures and policies

The Internal Audit and external auditors with regard to IT has to follow professional standards for performing this type of audit, such as Standards for the professional practice of internal auditing issued by the Institute of Internal Auditors (IIA), or standards issued by the Information System Audit and Control association (ISACA), as well as the local legislation and policies, procedures / guidelines established by the entity itself.

- **Standards** are processing the independence, ethics, professional skills, powers, performing audit and quality control audit. The standards define the activities presented as rules and restrictions, that will ensure the achievement of defined objectives with the policy information security.
- **Politics** is the starting point (constitution) for IT, it gives tone and character of the structure and the expectations of IT systems
- **The Guidelines / Procedures** contain detailed operational steps for the use of information systems

The practice shows that not always in advance can be predicted the emergence of different situations, this causes other employees to act different and make decisions in the use of IT. To allow unified approach establishment of policies and procedures is made that employees will use during operation of IT systems.

Planning and providing auditing staff of IS

Because today there are only a limited number of features that are executed without a computer support each auditor needs to know how presence of computers affect of valuation of the interval controls. Training programs should reflect these general requirements. To become specialists for Information Systems Audit, the Auditors need additional training. On the other side professionals IS are not trained to evaluate the controls to the extent that the auditors are trained (to a degree that would have paralleled with the auditors). Because of that an account must be taken the staff which need to specialize for audit of IS to gain and to maintain suitable circuit of knowledge how for IS so and for audit. For that there is a special training which can provide this.

Very often the specialist for audit of IS representing a finite resource whose use must be focused on the points where this resource is from the greatest benefit. In these circumstances, the specialists for IS need that be invited only in case when for the goals of the audit and the complexity of the information systems, the expertise of these specialists is necessary. The general auditors can be trained to use computer supported audit techniques (CSAT), without having to become experts for IS.

Planning and use of specialists

Safety standards and control of the information systems are perfect. Too high level of control (over the technical possibilities) is too expensive and usually inefficient. The set of controls in place should reflect the purpose and benefits of each system, and normally it is a combination of technical and manual (handheld) procedures. Effective controls over computer data processing can be found in the instructions for inspection of processing that are intended to the users of applications or in control procedures used by management of the user. According to it, the information systems should not be examined separately, but as part of general audit of overall administrative or financial function. Only by this way the auditor can real estimates appropriate control standard and evaluate the interaction of technical controls and controls on the user.

In the planning stage, you need to collect information on which base the areas and scope of the audit of IS to be performed will be determined. In this phase it would be useful to consult the auditor for IS that will help in deciding the priorities of the audit. In particular, it should adopt a decision on whether it is necessary to check the general controls, and the extent to which the sustained computer supported audit techniques (CSAT) should be used. Because both mentioned techniques require the need of using specialists that represent expensive solution, it can be necessary to apply strict priorities in using of auditors for IS.

In terms of the general objectives of the audi , the following factors should be taken into account:

- the extent to which the relevant function uses computer processing of data or data stored in the computer;
- in which range the user, with their controls, including and the control procedures of management, has confirmed that there is a required level of accuracy of data and processing to the extent necessary for the function;
- complexity of computer data processing, particularly the degree to which function (specific application) use data generated with computer programs (by difference from data that are manually recorded, sorted or analyzed by the application);
- the size of installations (computer center): For example, just by itself may not be possible to have good general controls because it does not have enough staff to provide enough separation of duties. This will be the case, for example, if It is unable to make full separation of duties among developers, operators and the administration which has access to the application;
- sensitivity of the data and obligations for protection of data;
- any kind of special difficulties in managing / audit verification. In elderly or modestly designed systems there may be problems, for example in monitoring of the basic details for data that are included in a set, or in getting assurance that the totals include all relevant transactions. This will increase the need of the auditor to use the CSAT access, simply for determining that the data is correct.

When with application of alternative compensating controls that are implemented by the end- user (including and the control procedures of the management of the user) to prove the accuracy of the data and their processing, to the extent that satisfy in terms of downloaded audit, verification of technical general controls as part of the audit mayt be unnecessary. In such a case, however, the general auditor should get a report from a third party (Internal Audit Specialist) or to cover the questionnaire for management with IS by himself.

Conclusion

The Information technology and the software solutions entered in all aspects of management and are essential not only for the successful execution of the daily activities and processes, but also for achieving the strategic goals of each company .From the proper functioning of IT depend the proper execution of workflows but and the accurate records of business transactions and preparation of financial statements that are a source of information for many stakeholders. The information security is the most valuable argument for managing the information systems and the safe data conservation in the organization and includes the three basic tenets upon which the information systems are based - confidentiality, integrity and availability.

The audit of IT systems is essential for completion of the whole audit process and issuing an objective opinion. Auditors of IT are commonly understood only as a technical support to the financial auditors, someone who simply operate with information systems in order and at the request of the conventional audit. IT audit is that applicable in the implementation of all of the before mentioned types of audit because IT is present in all segments of the business entities. The internal audit and external auditors with regard to IT has to follow the professional standards to perform this type of audit. Very often the specialist for audit of IS representing a finite resource whose use must be focused on the points where this resource is from greatest benefit.

Bibliography

1. Adams R.: *Auditing* - ACCA, Association of Chartered Certified Accountants, Longman, 1989.
2. Adams Roger: *Audit Risk, Current Issues in Auditing*, Accounting & Finance Series, Paul Charman Publishing Ltd., London, 1991.
3. Andrenj D. Chembers, Beorges M. Selin, Beralt Vinten: *Internal Auditi*, Pitman Publishing, London, 1993.
4. Aceski Dr. Blagoja, Trajkoski Dr. Branko: *Internal and external audit*, Faculty of Economics-Prilep, 2004
5. Bozhinovska Lazarevska Dr. Zorica: *Auditi*, Faculty of Economics, Skopje, 2011
6. Dimitrova Janka, *Audit - theoretical and practical aspects*, Gotse Delchev University, Faculty of Economics, Stip , 2013 .
7. Dimitrova Janka, *Internal audit*, Gotse Delchev University, Faculty of Economics, Stip, 2015 .
8. Dimitrova Janka, *State audit*, Gotse Delchev University, Faculty of Economics, Stip, 2016 .
9. Dan, Gaz M., NJazne C. Alderman, Alan J. NJinters: *Audit*, The Druden Press, Forth NJorth, 1996.
10. *International Standards on Auditing* (translated from English), Committee on Auditing Standards.
11. *International Financial Reporting Standards (IFRS)*
12. Stanoevski Dr. Stanoil: *Control and Audit*, Faculty of Economics Skopje, 1998.
13. Audit Law,
14. Law on Internal Audit
14. Law on State Audit
15. Company Law