RISKS AND CONTROL WITHIN THE COMPUTERISED INFORMATION SYSTEMS IN THE MILITARY ORGANIZATION

Valentin PÎRVUȚ
"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania
pirvut_v@yahoo.com

ABSTRACT

Within the computerised information system of entities, the auditors have to evaluate both the risks and the control of the system. Thus, there has been a change from an approach focused on the control of the system to an approach focused on the risks to which this is exposed. The shift towards risk evaluation allows for the auditor to notice the efficacy and efficiency of the control exercised over the audited system in a much better manner. The notion of risk in the computerised information system represents the probability of appearance of a failure with negative consequences over the functioning of the system. Regarded as a whole, the computerised information system of entities is exposed to a series of risks. The process of risk management plays a special role in the identification and control of risks.

KEYWORDS: auditor, evaluate, risks, consequences, identification, vulnerabilities

1. Introduction

The notion of risk in the computerised information system represents the probability of appearance of a failure that will have a negative impact on the computerised information resources, as well as on the functioning of the system (Eden, 2003).

Risk management can be defined as being the process of identification of vulnerabilities and threats within an entity, as well as of elaboration of measures meant to minimize their impact over the computerised information resources of the entity (COSO, 2004). According to this definition, the level of total risk can be regarded as a by-product pertaining to threats, vulnerabilities and the value of computerised information means.

This process has to be present at the level of any entity in order to ensure the successful accomplishment of objectives. The entities can, however, transfer, ignore, accept or reduce the risk.

The transfer of risks can be achieved by providing the means mentioned (the computerised information system). Ignoring the risk can lead to significant losses. Accepting the risk can be realised as long as the measures of control are more expensive than the loss itself. Reducing the risk is obtained through the adoption of control procedures of the risk factors.

The inherent risks within computerised information systems can be:

✓ *The business risk. This represents the probability that a certain entity will not attain its business objectives. In order to evaluate this risk, the auditor must investigate the strategic plan of the entity and notice the level of involvement of the* computerised *information resources in achieving the objectives. The factors determining this risk can be both of an internal nature and external to the entity. For example, an internal factor of risk can be the high degree of attrition and the repeated break downs of the electronic devices or equipment used in processing the data, while an external factor can be represented by the emergence of more powerful competitors on the market.*

✓ The auditing risk. This represents the probability that an auditor does not notice an error or fraud in the audited system, thus formulating a wrong opinion. The auditing risk contains several types of risks, as follows:

- the inherent risk – represents the probability that an error or a fraud to be inherently produced due to the nature of the activity taking place in the entity;
- the control risk – represents the probability that an error or a fraud to be produced without being detected or prevented by internal control;
- the detection risk – represents the probability that, through the applied tests, an auditor will not detect an error in the audited system of control.

The level of auditing risk can be regarded as a by-product of these three types: the inherent risk, the control risk and the detection risk respectively.

✓ *The risk of the* computerised *information system. This represents the probability of appearance of errors or frauds due to the inappropriate use of the* computerised *information system. The risk of the* computerised *information system comprises:*

- *the risks at the level of applications and operations in the* computerised *information system;*

– the low security of applications;

– the unauthorized access to the data of the system;

– the introduction of inappropriate or false data;

– the incomplete processing of data;

– doubling the transacted data;

– the late processing of data;

– mal-functioning of the transmission of data;

– the improper or non-existent of separation of functions and responsibilities;

– the faulty analysis and design of applications;

– the incompatibility of the computerised information applications;

– the applications being infected by electronic viruses;

– the inadequate training of users;

– the improper support and maintenance of applications.

✓ The risk that the computerised information system activity continues, which represents the risk associated to the system availability or retrieval. The system availability risk represents the probability that the system becomes not available to the users due to its security (for example, the hackers' DoS type of attack). The system retrieval risk represents the probability that the data and operations of the system cannot be retrieved so that the activity of the entity continues (for example, the non existence of security copies and of retrieval and continuation procedures for the activity lead to an increase in the level of this risk).

2. Evaluation of the Computerised Information System Risks

Both managers and auditors must as correctly as possible assess the risks within the computerised information system of the entity.

The following steps are generally followed for the identification and evaluation of risks:

✓ *identifying the risk factors;*

✓ hierarchization of risk factors according to their importance for the audited system;

✓ determining each risk factor's frequency and duration of appearance;

✓ quantifying and evaluating the level of risk;

✓ programming the audit and the allocation of auditing resources corresponding to the established level of risk.

There is a series of techniques (Munteanu, 2001) for the evaluation and quantification of risks. One of the most known and frequently employed is the technique of scores. This is one of the quantitative methods of risk evaluation. According to this technique, each factor of risk (threats or vulnerabilities) is granted a percentage (importance for the different functions of the entity) and a level of risk. Through the product resulting from the *percentage* and the *level of risk,* the *functioning risk* is determined, while the *risk of the system*, in which the functions are a part, is determined by adding the *risks of the percentages*.

The evaluation of risks is at the same time established through the free judgement of the auditor, founded on his experience and the evidence collected from the audited system.

The combined utilization of these two techniques is recommended in practice.

The evaluation and quantification of risks in the process of IT auditing has the following results:

✓ efficient determination of the auditing objectives;

✓ efficient allocation of resources for auditing.

3. Control within the Computerised Information System

After identifying and evaluating the risks in the computerised information system, the evaluation and testing of the established controls takes place for the minimization or elimination of risks. The internal control objectives must cover all the functions and activities, no matter if these are performed manually or automatically.

Thus, the auditor must know, identify and test all the types of existent controls.

Within the computerised *information system, as well as at the level of the entire entity, internal control ensures the prevention, detection (identification) and correction of events (problems) caused by the risk factors.*

In order to achieve these objectives, the control can be:

✓ ***preventive***: allows the identification of problems before they appear and affect the activity of the entity. Preventive control of the computerised information system allows for the detection and prevention of errors, omissions or frauds before they take place. For example, the computerised information system preventive control may include: the separation of tasks and responsibilities; the control of the access to the resources in the system (on the basis of personalized accounts through user and password); establishing clear procedures for the introduction of data in the system.

✓ ***detective*:** allows the detection and report of the problems that occur in the system. For example, the computerised information system detective control includes: the validation of entries of data through control characters; the failure messages within the computerised information applications; the procedure for the identification of a double registration in the data base.

✓ ***corrective***: allows for the remedy of a problem or the minimization of the impact of an identified threat through the detective control. For example, the elaboration of procedures for the retrieval of data; establishing the procedures for relaunching the computerised information applications.

The objectives of internal control specific to the computerised information system can be:

✓ ensuring the physical and logical security of the computerised information resources;

✓ ensuring the integrity of the computerised information applications (especially of the accounting management) through:

o verification and authorization of data entries;

o accuracy, integrity and security of data processing's and transactions;

o accuracy, integrity and security of reports;

o integrity of the data bases;

✓ ensuring efficiency of the development or acquisition of computerised information applications, as well as their concordance with the objectives of the enterprise;

✓ ensuring efficacy and efficiency of the system operations and procedures;

✓ ensuring the concordance between the procedures, the system operations respectively, and the legal internal rules and regulations in effect;

✓ ensuring the retrieval of data and continuing the activity in case of disasters or unexpected events.

Taking into account the control objectives, the structure of the computerised information system in an entity and the IFAC – IAPS 1008 standards recommendations (IFAC, 2003), the internal control of the computerised information system can be classified in two categories:

✓ Control of the computerised information system management;

✓ Control of computerised information applications.

The control of the computerised information system management represents the whole set of procedures used to ensure a reasonable level of covering the internal control of the computerised information system (Brândaş, 2003). This type of control has a general character, including the system as a whole. Within this category of control, the auditor must identify, evaluate and test the following:

✓ *Control of the organization of the computerised information system;*

✓ *Control of the design and implementation of the computerised information system;*

✓ *Control of the procedures and the operations in the system;*

✓ *Control of the organization the system security;*

✓ *Control of ensuring the quality of the system.*

The control of the computerised information applications represents the whole set of manually or automatically performed procedures and techniques for the control of entries, processing's and exits of computerised information applications (Brândaş, 2003). This type of control has a specific character and refers to a certain component of the computerised information system. Within this category of control, the auditor must identify, evaluate and test the following:

✓ *Control of entry of data*. This type of control ensures the authenticity, accuracy and integrality of the data introduced in the system, as well as the rejection, correctness or reintroduction of the erroneous data.

Through ***authenticity,*** it is made sure that only the authorized users have access to the introduction of data. This limitation is practically achieved by defining several groups of users within the system, who will have differentiated access to the different modules of data entry. The access is done on the basis of the users' authentification through name and password.

Through ***accuracy***, it is made sure that the introduced data are real, correct and compatible with the processing's in the system. This thing is practically achieved by implementing in the system the verification and validation procedures of the introduced data, such as: validation of codes, validation of the length of the data or the validation of introducing the data during certain intervals. For example, the calculus of the control characters for the codes of the introduced products or goods.

Through ***integrality***, it is made sure that the data were completely introduced, without omissions or doublings. This thing can be achieved through the calculus and comparison of the total of the introduced sums with the totals in the introduced documents.

✓ *Control of processing, data and data files transactions*. This ensures the accuracy and integrality of the processing's and transactions, the integrity of the stored data, according to batches and in real time (online), as well as the correction of the erroneous data.

Ensuring ***accuracy*** in processing and transacting the data is done through procedures of validation for the processings and transactions.

Ensuring ***integrality*** in processing and transacting the data is realised by comparing the entries for transactions in a module with the exits for the transactions in the previous module, as well as the number of transactions and the total of their value. For example, by comparing the number and total of the receipts received at the administration and sent to the accounting office with the number and total of the receipts received at the accounting office and received from the administration.

Ensuring ***integrity*** of the stored data in the data base is achieved through referential integrity, transactional integrity, defining the uniqueness and value constraints, as well as defining the procedures for retrieving the data (backup).

Following and ***correcting the erroneous data*** in the proceedings and transactions of data is realised through registering the errors and correcting them in some log files.

✓ *Control of exits of data and information,* by which it is made sure that the exits in the system are real, correct, integral, secured and delivered in time to the users and corresponding decisional factors (authenticated). The control procedures for the exits include the following: authorization for generating exits; comparing the totals in the reports with the totals in the transactions (for example, comparing the turnovers in the balance sheet with the totals calculated in the log); authorization for the distribution of exits (only authenticated users must benefit from the exits in the system); verification of the receipt of exits to the authenticated beneficiaries. The generation and distribution of exits must also be registered in the log by means of log files.

The evaluation of risks and of the computerised information system control is a dynamic process in a permanent transformation due to the rapid evolution of the technology of information. Thus, besides the aspects mentioned above, there is a series of risks and particularized control systems for the computerised information systems of electronic trade, electronic banking, ATM, e-finance and others. The auditor must take into consideration the general framework of risk evaluation and control implementation and functioning, the risks and the particularized control systems for the computerised information systems, as well the ones mentioned above.

The major implications that the computerised information systems exert over the control and the auditing of enterprises have led to the elaboration by professional or governmental associations of sets of standards with regard to the processes for the evaluation of the risks and for the implementation of internal control in the informatics system. The most important standards regarding the risks and control of the computerised information systems will be further mentioned.

4. Standards regarding the Treatment of Risks and the Control in the Informatics Systems

The most complete standards, guides and procedures regarding the evaluation of risks and the implementation of control of the ***computerised*** information systems are drawn up by **I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation (ISACA)**.**

Thus, the **IT Governance Institute (ITGI, 2000) institute (founded by ISACF** – **I**nformation **S**ystems **A**udit and **C**ontrol **F**oundation) conceived and published a collection of standards on defining and implementing the objectives of control in the *computerised* information system.

These standards have been reunited under the name of **CobiT (C**ontrol **Ob**jectives for **I**nformation and related **T**echnology), representing the most powerful instrument and working framework for implementing and auditing control within the accounting management computerised information systems. It is directed towards the computerised information systems management, internal control departments, auditors and owners especially (shareholders or associates) who use the technology of information in doing business, in order to ensure confidentiality, integrity and availability of the data and information.

CobiT contains the following documents ***(ITGI, 2000)***:

✓ general presentation (Executive Summary);

✓ working framework (Framework);

✓ control objectives (Control Objectives);

✓ management guide lines (Management Guidelines);

✓ audit guide lines (Audit Guidelines).

✓ implementation instruments (Implementation Tool Set).

The ***IFAC body also brings several regulations through ISA*** and ***IAPS*** about the evaluation of risks, control and auditing in the accounting management computerised information systems, as follows (IFAC, 2003):

✓ *ISA – 400*: regulates the evaluation of risks and internal control;

✓ *ISA – 401*: regulates the process of auditing in the computerised information systems;

✓ *IAPS – 1008*: regulates the evaluation of risks and internal control within the computerised information systems.

In addition to these bodies, several other national or international professional associations refer through their standards to the evaluation of risks, control and auditing in the computerised information systems.

At an international level, the most frequently used standards regarding the auditing of the computerised information systems are elaborated by the two large ISACA and IFAC professional associations. The auditor must know these standards and use them throughout the auditing process.

5. Conclusions

The key to success in the field of auditing is that of recognizing that it can have a greater value if it makes analyses that go beyond the traditional financial problems and focuses on points of interest for a larger public. The auditing methodology, which corresponded to the industrial age, is not sufficiently developed for the informational era, when the assets are untouchable, trade is electronic, markets are global and the rhythm of change is increasingly faster. The internet plays a more and more important role in spreading the information, financial or of any other nature, thus modifying the international boundaries of information, generating expectancies on the timely reporting of updated information. The success of the mission of auditing will increasingly depend on diversifying the auditors' basic knowledge that should go beyond the traditional financial analysis towards new fields, such as the technology of information, the measuring of the non financial performance and the general management.

REFERENCES

Brândaş, C. (2003). Necesitatea şi conţinutul auditului sistemelor informaţionale. *Revista de Audit Financiar nr. 3/2003.*

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise Risk Management Framework*. Retrieved from: http://www.coso.org/documents/coso_erm_executivesummary.pdf.

Eden, A. (2003). Riscurile de audit în condiţiile utilizării sistemelor informatice de prelucrare a datelor. *Revista de Audit Financiar nr. 2/2003*.

Information Systems Audit and Control Association. (2004). *CISA Review Manual.* Rolling Meadows. Retrived from: http://www.isaca.org.

International Federation of Accountants. (2003). *International Standards on Auditing (ISA)*. Retrieved from: https://www.iaasb.org/clarity-center/clarified-standards.

IT Governance Institute. (2000). *CobiT, 3rd Edition.* Rolling Meadows, Illinois: Information Systems Audit and Control Foundation.

Munteanu, A. (2001). *Auditul Sistemelor Informaţionale Contabile – cadrul general.* Iaşi: Polirom, p. 13.