INFORMATION SECURITY MANAGEMENT SYSTEM

Gheorghe Mirela

Academia de Studii Economice Bucureşti, Facultatea Contabilitate şi Informatică de Gestiune, Piaţa Romană nr. 6, sector 1, Bucureşti, CP 010374, Email: mirelaghe@gmail.com***, Telefon: 0723858611***

Boldeanu Dana Maria

Academia de Studii Economice Bucureşti, Facultatea Contabilitate şi Informatică de Gestiune, Piaţa Romană nr. 6, sector 1, Bucureşti, CP 010374, Email: danabolde@gmail.com

Information Security Management System plays a critical role to protect the organization and its ability to perform their business mission, not just its IT assets. Risk Management and Risk Assessment are important components of Information Security Management System Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Information and communications technology management and IT security are responsible for ensuring that technology risks are managed appropriately. The research starts with the conceptual framework of the Information Security Management System and provides an analysis of the IT risks management to the level of the financial institutions in Romania.

Key words: information security management system, risk management, risk assessment.

1. Introduction

The acceptation of an Information Security Management System (ISMS) constitutes a strategic decision of an organization, the development and the implementation of such a system being influenced by the needs and the strategic objectives of the entity in case. Practically, this system will assure an adequate and proportional selection of the security measurements to protect the information resources.

The research starts from the conceptual framework of the ISMS based on the requests of standards:

- ISO/IEC 27001(2005) "Information technology - Security techniques - Information security management systems – Requirements" and
- ISO/IEC 17799 "Information technology - Security techniques - Code of practice for information security management".

These standards, recognized also to the level of the Romanian organizations, offer the methodological framework for developing and implementing an efficient security management system to the level of a certain organization. Concomitantly, the ENISA agency (European Network and Information Security Agency), though the Risk Management / Risk Assessment portal (http://enisa.europa.eu/rmra), offers a series of tools and methods for analyzing and assessing IT risks.
The present paper offers also an analysis of implementing IT risks management to the level of the financial institutions in Romania, underlining the most important IT problems pointed out by the respondents in the last year and the most efficient measurements taken by the top management for solving them.

2. The conceptual framework of the Information Security Management System

The information security management system (ISO 27001, 2005) is defined as that part of a global management system, based on a certain approach of the business risk, through which it is establishing, implementing, analyzing, monitoring and improving the security of the information. This system includes organizational structures, politics, planning activities, practices, processes and resources. Information security should be an integral part of the organization's operating and business culture. In ENISA vision, the methodological view of developing an ISMS necessitates the covering of 6 steps (figure 1):

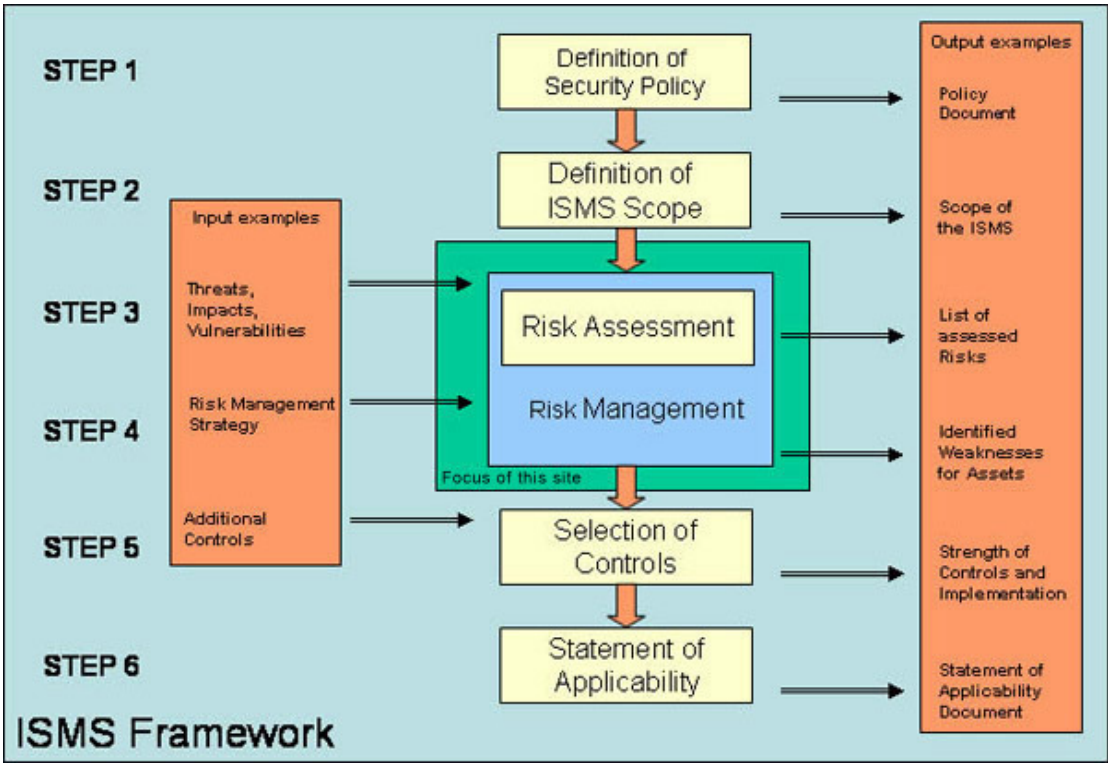

Figure 1. The steps of process developing of the information security management system (Source: http://www.enisa.europa.eu)

1. Definition of Security Policy,
2. Definition of ISMS Scope,
3. Risk Assessment (as part of Risk Management),
4. Risk Management,
5. Selection of Appropriate Controls and
6. Statement of Applicability

Steps 3 and 4, the Risk Assessment and Management process, comprise the heart of the ISMS and are the processes that "transform" on one hand the rules and guidelines of security policy and the targets; and on the other to transform objectives of ISMS into specific plans for the implementation of controls and mechanisms that aim at minimizing threats and vulnerabilities.

The processes and activities related to the steps 5 and 6 do not concern information risks. They are rather related to the operative actions required for the technical implementation, maintenance and control of security measurements. Appropriate controls may either be derived from existing sets of controls or mechanisms, usually included in information security standards and guidelines, or the outcome of a combination or adaptation of proposed controls to the specific organizational requirements or operational characteristics.

In both cases, step 6 is the documented mapping of the identified risks, applied to the specific organization with the technical implementation of security mechanisms the organization has decided to deploy.

Finally, although the ISMS is a recurring process as a whole, in most of the types of organizations mentioned above, steps 1 and 2 recur on a longer cycle than steps 3, 4, 5 and 6. This is mainly because the establishment of a security policy and the definition of the ISMS scope are more often management and strategic issues while the Risk Management process is an everyday operational concern.

Risk Management and Risk Assessment are major components of Information Security Management System (ISMS). Risk management can be defined as "the process of identifying vulnerabilities and threats within the framework of an organization, as well as producing some measurements to minimize their impact over the informational resources". This process of the risk management includes some basic processes, as we can see in the figure below (figure 2):

1. *Risk Assessment* requires the covering of three steps: risk identification, risk analysis and risk evaluation. Every organization is continuously exposed to an endless number of new or changing threats and vulnerabilities that may affect its operation or the fulfillment of its objectives. Identification, analysis and evaluation of these threats and vulnerabilities are the only way to understand and measure the impact of the risk involved and hence to decide on the appropriate measures and controls to manage them.

   7.

2. *Risk Treatment* is the process of selecting and implementing of measures to modify risk. Risk treatment measures can include avoiding, optimizing, transferring or retaining risk. The measures (i.e. security measurements) can be selected out of sets of security measurements that are used within the Information Security Management System (ISMS) of the organization.

   8.

3. *Monitor and Review* is a process for measuring the efficiency and effectiveness of the risk management of the organization processes is the establishment of an ongoing monitor and review process. This process makes sure that the specified management action plans remain relevant and updated.

   9.

4. *Risks Communication, Awareness & Consulting* means a process to exchange or share information about risk between the decision-maker and other stakeholders inside and outside an organization. The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk.

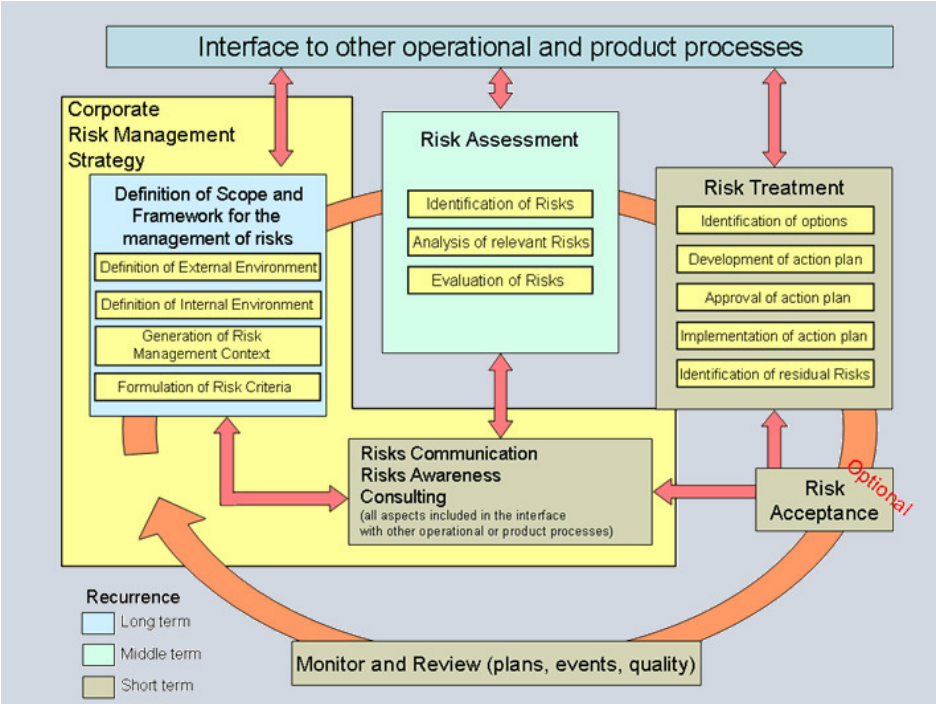

Figure 2. Risk Management Process

(Source: http://www.enisa.europa.eu)

5. *Risk acceptance* is the decision to accept a risk by the responsible management of the organization. For each risk area, the options are:
   a) reduce: lower the risk through controls, or technology;
   b) transfer: offload the risk by placing it on some other entity;
   c) accept: decide the risk is acceptable based on the benefit;
   d) ignore: choose not to reduce, transfer or accept the risk - this is equivalent to accepting the risk, but without due diligence.

3. The analysis of the IT risk management to the level of Romanian's financial institutions

To the level of financial institutions in Romania, the European requests for Basel II implementation have had major implications in the governance way of the information technologies. For many information systems in the banks is absolutely necessary an architectural rethinking which will allow a consolidated and, also, flexible approach of the market, as well as the selling of some complex products and financial services adequate to the permanent change of the economic environment. Basel II involves a bigger responsibility in the well functioning of the banks informatics systems both for the IT department and for the management of the bank.

In our research, the analysis of the IT risk management has been based on the data gathered from a number of 30 subjects (financial institutions) through a questionnaire. The gathered information allowed us to point us the following:

- the most severe IT problems distinguished by the respondents in the last year,
- the most efficient measurements taken into consideration by the top management for resolving the pointed out problems.

As we can notice also in figure no. 3 the most severe IT problems pointed out in the last period (year 2007) have been bonded by the personnel (staff problems 24%) and high cost of IT with low improvement of ROI (19%). We can also mention between stringent problems serious IT operational incidents and low IT performances (both with 13%).

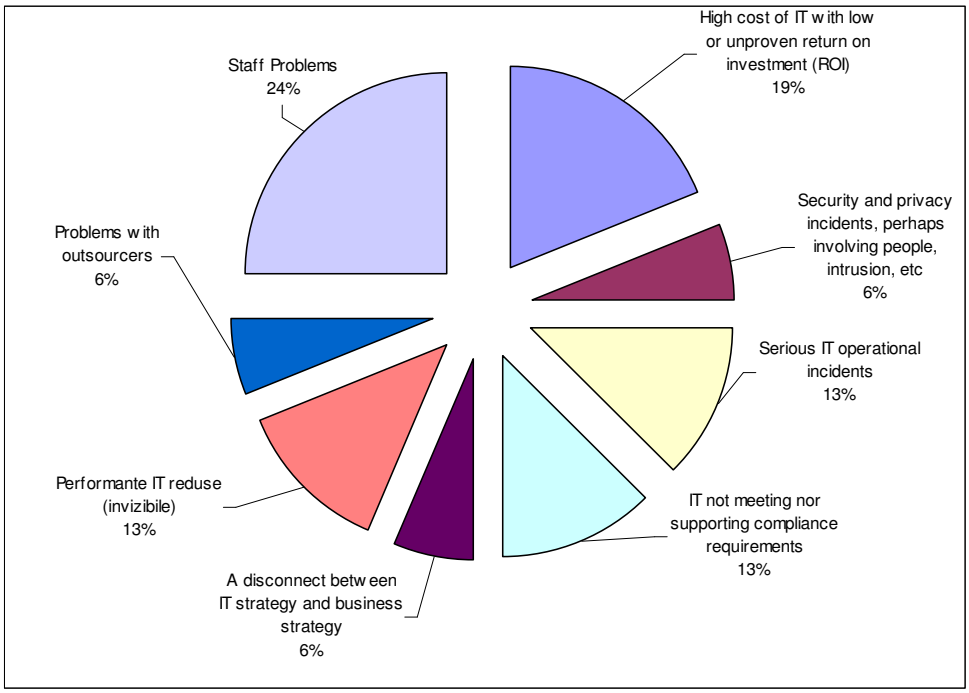

Figure 3. The most serious IT problems pointed out in the last year

The most efficient measurements taken into consideration by the management for resolving their problems have been the following: the alignment between IT strategy and overall strategy and a more efficient IT risk management.

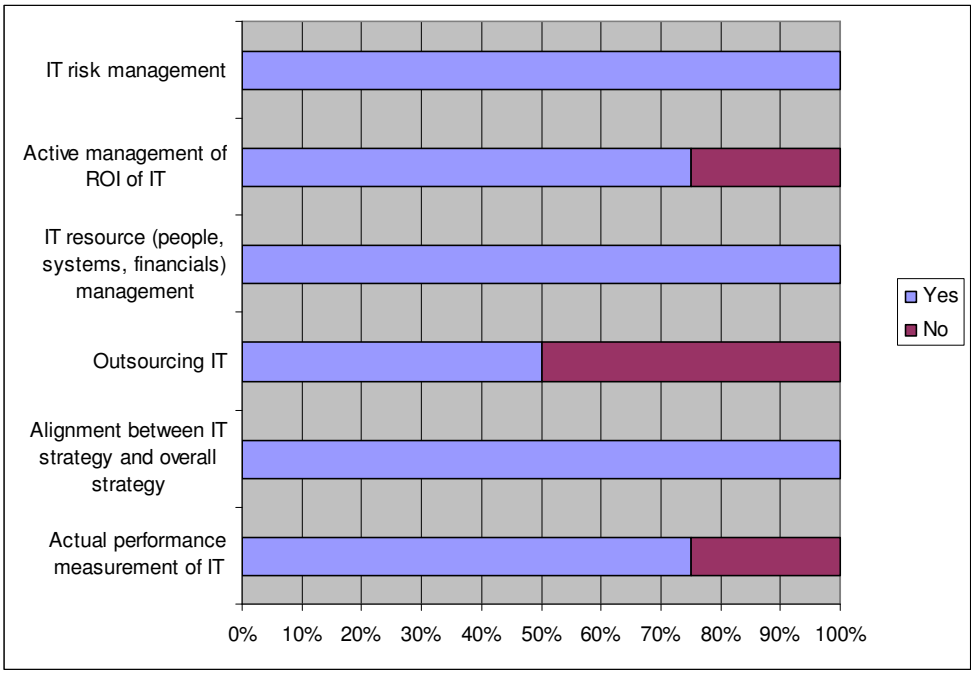

Figure 4. The most efficient measurements taken into consideration by the management for issuing pointed out problems

In conclusion, although the last years have been remarked through rapid changes to the level of informational architecture of the Romanian financial institutions, which implicated major investments, the efficiency of the IT management risks is valuated and the real issues in the area aimed more the human side than the technical one.

4. Conclusions

Therefore the establishment, maintenance and continuous update of ISMS provide a strong indication that a company is using a systematic approach for the identification, assessment and management of information security risks. Furthermore such a company will be capable of successfully addressing information confidentiality, integrity and availability requirements which in turn have implications for:

- business continuity;
- minimization of damages and losses;
- competitive edge;
- profitability and cash-flow;
- respected organization image;
- legal compliance.

References

1. ENISA (European Network and Information Security Agency), “Risk Management /Risk Assessment “ (available on-line at http://www.enisa.europa.eu/rmra)
2. ISO/IEC 17799 (2005) “Information technology - Security techniques - Code of practice for information security management”.
3. ISO/IEC 27001(2005) “Information technology - Security techniques - Information security management systems – Requirements”.

4. NIST, “Risk Management Guide for Information Technology Systems NIST Special Publication 800-30”; available on-line at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
5. Pradhan P.L. and Meher P.K. (2004), “Risk Assessment on IT Infrastructure”, available on-line at http://www.infosecwriters.com/text_resources
6. Symantec (2007), “IT Risk Management Report. Trends through December 2006”, Volume 1, Published February, 2007.
7. Symantec (2008), “IT Risk Management Report2, Myths and Realities”, Volume 2, Published January, 2008.