THE IT AUDIT – A MAJOR REQUIREMENT FOR THE MANAGEMENT QUALITY AND SUCCESS IN THE EUROPEAN BUSINESS CONTEXT

Ivan Ion

ASE Bucureşti, Piața Romană 6, 0744502345, ionivan@ase.ro

Surcel Traian

ASE Bucureşti Piața Romană 6, 0728884615, *tsurcel@ase.ro*

Amancei Cristian

ASE Bucureşti Piața Romană 6 0740181433 *cristian.amancei@ie.ase.ro*

A requirement for the improvement of the quality management for the Romanian companies that are integrated in the European environment is represented by the development of an informational partnership between the actors involved in the company network. This partnership must be characterized by credibility, conformity, performance and security. The IT&C system represent the hardware and software support of this partnership, and the IT audit is the process that certify it's conformity. In the audit process, the main accent is on the security audit due to the importance of the vulnerabilities, threats and IT risk analysis. The list of measures that are proposed at the end of the audit to company management should be incorporated in the company security policy, that is the starting point for the ISMS – Information Security Management System, part of the company general management system. The implementation of the Business Continuity and Disaster Recovery Plan is one of the most important measures in order to increase the confidence level of the business partners and to provide safe environment for business continuance.

Key words: Management, IT&C Systems, IT Audit, ISMS, Security Policy, Business Continuity, Disaster Recovery Plan.

1. Management, informational partnership and IT audit

In the space of business environment extended at European level, between the multiple requests of a quality management, it retrieves the necessity of increasing of the competitivity together with enhancing of the cohesion and cooperation between of the actors integrated in the company's business network logistics chains.

The business relations between suppliers, producers, outsourcing companies, transporters up to the final customer, the consumer, should be based on an informational partnership characterized by *credibility, conformity, performance* and *security*.

Credibility refers to the confidence in the results and reports provided by the company. The Sarbanes-Oxley Act, adopted in audit, states and straightness this mandatory condition for running out the normal economical processes.

Conformity refers to legislation, standards and norms conformity regarding the application of the best practices in the company's business activity.

Performance is regarded as the effectiveness and efficiency of the activity performed in the logistics system of the company.

Security refers to the plurality of the four attributes: information confidentiality, integrity, availability and no repudiation.

The IT&C systems provides the hardware and software support for the informational partnership between the company and the business network members developed by it. The IT audit certifies the quality of the informatics system and by this, the managerial quality of the electronic information.

The Romanian companies, members of the European economic environment are now obliged to approach the IT systems audit according to the international standards, the most used of them being CobiT developed

by ITGI/ISACA. In accordance to this, the BSI certification – British Standard 7799 for Information Security can be obtained.

The relationship between the management quality and the information security is important and it has three coordinates which illustrates the economic dimension of the information security. This three coordinates are: consolidation of the management capacity to protect the company structure and resources; development of the management ability to guarantee the business integrity and efficiency; assurance of a stable economic environment and continuity of the company business activity.

The IT audit, according to the CobiT standard, performs a control examination of the IT entity. The audit, as it is presented by ISACA - International System Audit Control Association, is a process that is used for evaluation of the audit evidence, in order to determine if the physical protection of the IT&C assets (controls from the CobiT standard) and the management measures by which the data integrity is insured, leads to an efficient utilization of the company resources and carrying out the company goals.

2. Types of IT audit

Analyzing different methodologies and opinions of various authors, we consider that the audit missions performed in practice correspond to a complex typology. For this typology we recommend four criteria for structuring: the audit organization mode, the moment of the audit, the audit scope and the audit area it covers.

Regarding the audit organization mode, the *way* the audit activity is organized, it can be differentiate the *intern audit and the extern audit*. The intern audit represents an evaluation or an organized monitoring made by a company's own department, while the extern audit is performed by an independent auditor organization.

Regarding the moment when the audit is performed, it can be differentiate the *preventive audit and the corrective audit*. The preventive audit is defined as an examination of the operations made before they are effectively done, having the advantage that it can prevent a loss before it appears. The corrective audit is defined as an examination of the way the operations are made. It can lead to loss recovery; it can prevent the same mistakes to be repeated in the future thru establishing responsibilities for the guilty persons.

When establishing the scope of the audit, we can differentiate three audit categories: the conformity audit, the attestation audit and the performance audit.

The conformity audit certifies the responsibility regarding the transactions and the reports made based on the respective transactions. The attestation audit refers to the credibility of the final statements, attesting or not, if they present a fair view of the company and the transactions it realizes. The performance audit examines the performance in relation to the economic inputs and the outputs by analyzing the resource allocation under the economic efficiency principles.

The area covered by the IT audit are that the most important criteria. Regarding this criterion, the members of the audit team can handle the following segments of issues: *systems and applications, information processing environments, development systems, IT management and the Client/Server architecture*.

All these five audit segments focus on auditing the information security and refer to the following aspects: the physical security of the data centers and the logical security of the databases, the networks security and the applications security.

3. Risk analysis

The management – audit relation is best reflected by the management's responsibilities in the company regarding defining, implementing and monitoring of the internal controls that assure the decision processes feedback in the company.

The most significant problem regarding these controls refers to the analysis and risk management, especially due to the fact that the Internet contributes to an internationalization of threats and consequently to the risk exposure. IT risk is evident through its own components: threats, vulnerabilities and impact. The threats exploit the vulnerabilities of a system causing by its impact losses and managerial difficulties.Generally speaking, the risks associated to an information system regard:

- the physical security risk, regarding the existence of the security, detection and fire alarm systems, protection systems against tension fall-down, robbery, natural catastrophes, physical protection of the memory devices;
- the communication risk that may arise from connecting to the public network and it needs a firewall, antivirus protection, utilization of encoding techniques and the virtual private networks – VPN;
- the risk regarding the data and transactions integrity;
- the access risk regarding assurance of the information and network confidentiality, data and database integrity and their availability. The passwords management, monitoring and incidents resolving report is considered;
- the risk regarding the information system documentation and the personnel risk;
- the unpredictable situations risk management (the availability risk) is the risk associated to natural dangers, disasters, system fall-dawn that may lead to irrevocable data losses, in the absence of activity monitoring procedures and disasters recovery plans.

Only inventorying the risks is not sufficient, the IT audit should also contain a risk evaluation, the impact of the risks, from point of view of the losses they may cause. In practice, it operates with quantitative and qualitative methods to evaluate the respective losses.

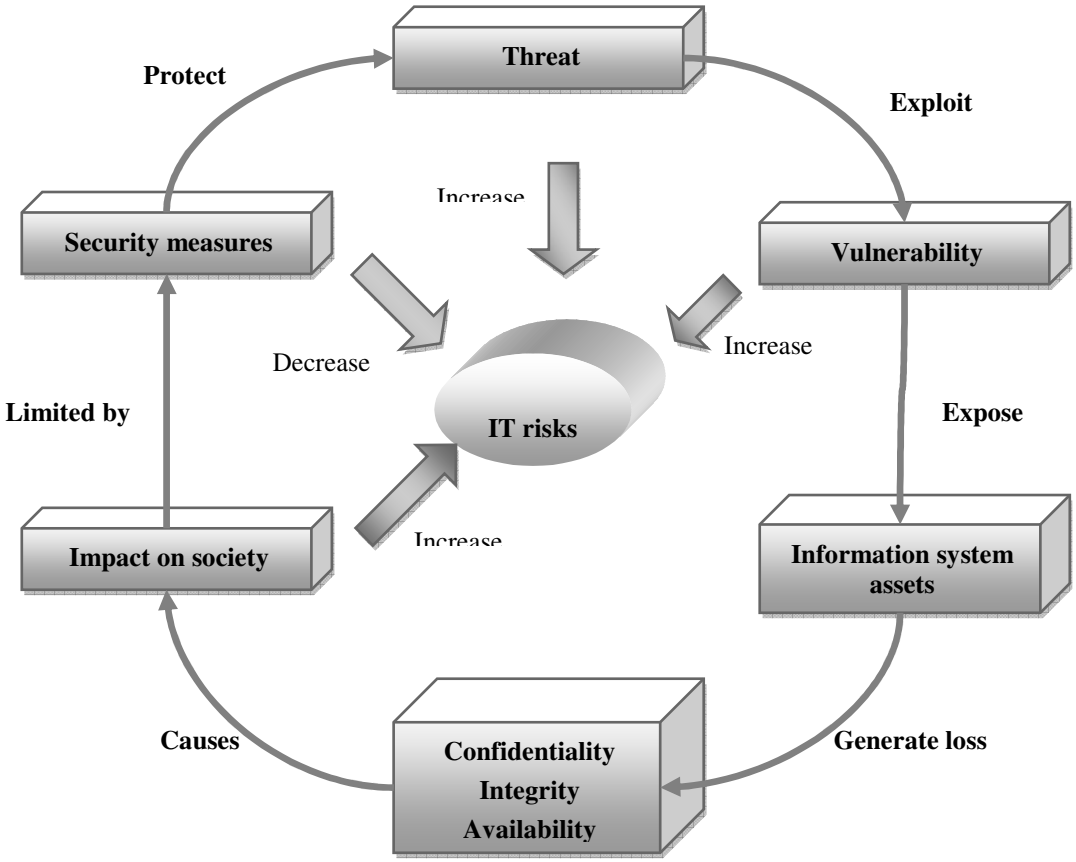

Fig. 1 IT risk components

4. Business Continuity and Disaster Recovery Plan

The most important measure recommended from the IT auditors to the company management, in order to lift up the partner level of trust and ensure the success undisturbed by the incidents. The principal reason for a company to develop a Business Continuity and Disaster Recovery Plan is the assurance of the company ability to operate efficient in the case of severe disruption of the normal operations. The severe disruption can appear from different sources:

- Natural disasters (fires, flows, earthquakes etc.);
- Equipment or processes fall-down (disks, programs, databases etc.);
- operating errors, sabotage;
- Terrorism or premeditated informatics criminality acts (for example, "denial of service" actions, hacking, viruses, worms, etc.);

The prevention of such events is not possible, but it is important to resume as fast as possible the essential operations of IT&C system. We should differentiate the loss prevention plans from the disasters recovery plans.

The loss prevention plans focus on minimizing the organizations exposure to the elements that may threat the normal operations. They basically contain activities planned on a regular basis like backups, authentication and authorization in the system, scanning for viruses and monitoring of the system usage.

The disasters recovery plans focus on a set of actions that must be realized by an organization in order to restore the normal services and operations in case of a serious loss. Generally, such plan will not describe the actions for every type of possible disaster, but it would search for common elements of the possible disasters, like information losing, personnel losing, equipment losing, the loss of access to information or facilities.

Conclusions

The projection into practice of these major requirements of a quality management in the European context means the implementation of a special component dedicated to the information security, called ISMS - Information Security Management System, in the informatics system of a company. The IT&C audit will focus on this system, without the resource consumption that is realized today for the classic IT audit.

ISMS is the frame for establishing, operating, monitoring, reviewing and developing controls and measures for assuring the information security in the context of an IT governance into an organization. ISMS become an organic component of the IT system and, as a consequence, a part of the general management system of the organization. ISMS is presented in ISO/CEI 17799 – 2000 standard, that has been taken over and adopted in Romania also by ASRO as an Information Technology Standard – practice code for the information security management SE ISO/CEI 17799 : 2004.

The security policy represents the central element of the ISMS. The security policy is made of a set of measures accepted by the management of the company, which states clear, but flexible rules that determine the standard operations and technologies required in order to assure the security. The security policy represents a document that states the main requirements or rules that must be known and implemented for assuring the security.

Audit certification, by obtaining the BSI Certificate awarded by the UK Accreditation Services – UKAS, even on-line, regarding the way an organization deals with the information security, respectively the control objectives, the security measures, the information security politics, procedures and processes, become a basic condition of an efficient management at European standards for the Romanian companies.

Bibliography

1. Mikhael Feleker, "Analysis of FFIEC Guidance, Technologies and Decisions on
2. Authentication, Information Control Systems Journal", Vol. 6, 2007, pp. 52-57;
3. Office of Government Commerce ITIL Lifecycle Publication Suite, version 3, 2007;
4. ISO/IEC 17799:2005 "Information technology - Security techniques - Code of Practice for information security management";

5. ISO/IEC 27001:2005 “Information technology -- Security techniques – Information Security management systems – requirements”;
6. Traian Surcel, Cristian Amancei, “The Information Security Management System
7. Development and Audit “, in the Proceedings of the Eight International Conference on Informatics in Economy, Editura ASE, Bucharest 2007;
8. Traian Surcel, “Auditul şi managementul sistemelor informatice“, The Proceedings of the 2006 International Conference on Commerce”, Editura ASE, Bucharest 2006;
9. Tejus Trivedi, ” If Compliance Is So Critical, Why Are We Still Failing Audits? How to Minimize Failure and Make the Audit Process Easier Things to Consider when an
10. Organizational Learning”, Information Control Systems Journal, Vol. 5, 2007, pag. 37-42.