# Risk Management for e-Business

Floarea NASTASE, Bucharest, Romania, nastasef@ase.ro
Pavel NASTASE, Bucharest, Romania, nastasep@ase.ro

*In the new Internet economy, risk management plays a critical role to protect the organization and its ability to perform their business mission, not just its IT assets. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The risk management is an important component of a IT security program. Information and communications technology management and IT security are responsible for ensuring that technology risks are managed appropriately. These risks originate from the deployment and use of IT assets in various ways, such as configuring systems incorrectly or gaining access to restricted software.*
***Key words**: risk, e-business, threat, vulnerability.*

## Introduction

***Risk*** is a function of the ***likelihood*** of a given ***threat-source's*** exercising a particular potential ***vulnerability***, and the resulting ***impact*** of that adverse event on the organization (figure 1).

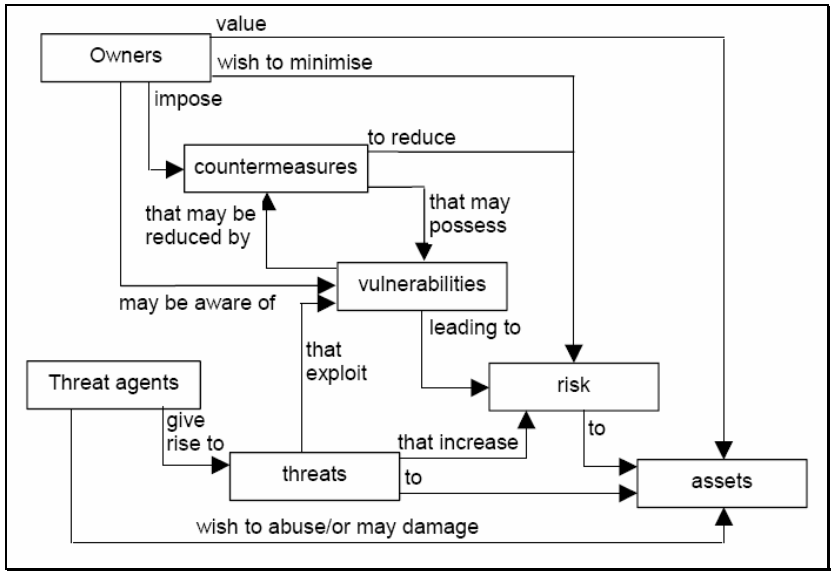


**Figure 1**. Risk context [Source: ISO/IEC 15408-1 Common Criteria]

Information assets are subject to many kinds of threats. Threats can occur from a direct or indirect source, can be from natural (environmental) or human causes (either accidental or deliberate) and it may arise from within an organization or from outside. The impact caused by the unwanted incident may be of a temporary nature or it may be permanent. Vulnerabilities of the asset may be exploited and may lead to undesirable consequences affecting the confidentiality, integrity, availability, accountability, authenticity and/or reliability of information.

The risk categories can help identify and assess the risks, that are poorly managed or not mitigated represent an exposure to the health of the organization. The identification of the risk categories will help to consider where potential events might affect the achievement of e-business objectives. Typical risk categories include: external environment, operational, legal, information, regulatory, human resources, governance, financial, strategic and technology.

## Layered Risk Model

Four levels of risk can be distinguished:

- *Technical risk* - includes viruses, worms,

trojans, backdoors, and other malware as well as hacker attacks plus risks due to hardware attacks.

- *Individual risk* - besides security, individuals greatly value their privacy, which is jeopardized by attacks such as phishing. Other individual risks result from fraud in e-commerce, missing or wrong information, or data manipulation.
- *Business risk* - for businesses, sales and reputation losses are major risks. Companies may never regain their full financial capacity after a computer downtime of several days, and even a company's existence can be threatened as a result of technical incidents.
- *Societal risks* - loss of privacy ("transparent user"), cyber-terrorism, and information warfare are key terms that outline the dangers on the societal level.

They are interrelated and their occurrence is recursive.

However, these risks can be identified and remediated by detecting vulnerabilities, assessing their potential impact, and when warranted, deploying corrective measures (figure 2). Vulnerability management is the processes and technologies that an organization employs to identify, assess, and remediate IT vulnerabilities — weaknesses or exposures in IT assets or processes that may lead to a business risk (such as failure to maintain integrity of financial reporting or a loss of revenue or productivity) or security risk (such as violations of confidentiality, integrity, or availability of data).

*Interface to other processes*. The interfaces of risk management with other relevant security and operational processes have to be identified, including product evaluations, Information Security Management Systems (ISMS), security controls deployment, incident handling, business continuity planning and operational processes.

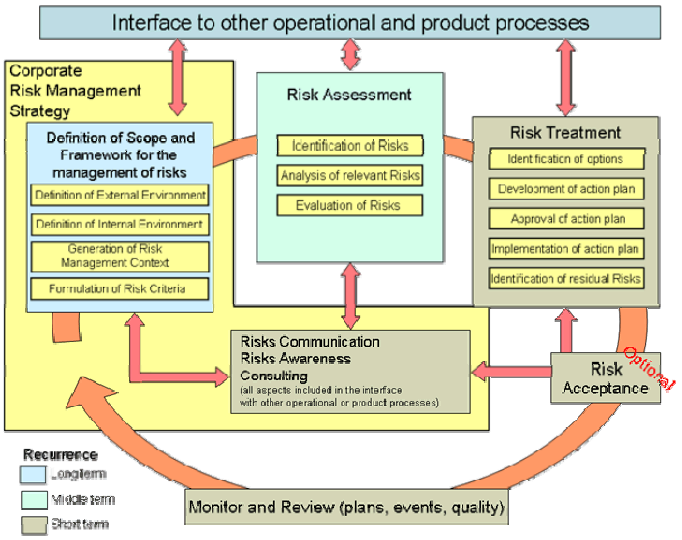


**Figure 2.** Risk Management Process [Source: **http://www.enisa.europa.eu**]

**The Risk Management Process**

*Definition of Scope*. Process for the establishment of global parameters for the performance of risk management within an organization. Within the definition of scope for risk management, both internal and external factors have to be taken into account. In order to define an efficient framework for the management of risks it is important to:

- understand the background of the organization and its risks (e.g. its core processes, valuable assets, competitive areas etc.);
- evaluate the Risk Management activities being undertaken so far;
- develop a structure for the Risk Management initiatives and controls (countermeasures, security controls etc.) to follow.

*Risk Assessment*. A scientific and technologically based process consisting of three steps, risk identification, risk analysis and risk evaluation.

*Risk Treatment*. Process of selection and implementation of measures to modify risk. Risk treatment measures can include avoiding, optimizing, transferring or retaining risk.

*Monitor and Review*. A process for measuring the efficiency and effectiveness of the organization's risk management 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. This process also implements control activities including re-evaluation of the scope and compliance with decisions. Continuous monitoring encompasses the processes that management puts in place to ensure that the policies, procedures, and business processes are operating effectively. It addresses management's responsibility to assess the adequacy and effectiveness of controls. This involves identifying the control objectives and assurance assertions and establishing automated tests to highlight transactions that fail to comply with the relevant control objectives and assurance assertions. Many of the techniques of continuous monitoring of controls by management are similar to those that may be performed in continuous auditing by the internal audit department.

*Risks Communication, Awareness & Consulting*. 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.

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

Information and Communications Technology (ICT) has become vastly important, but the consistent increase of security threats calls for an integrated, multivendor approach to security management. Figure 3 show ICT security incidents in European Enterprises that had an impact on the business, all organizations having experienced such an incident.

New forms of security attacks constantly emerge, and organizations must address the business risks arising from these security issues: viruses, worms, trojan horse, port scanning, denial of service attacks, remote administration, sniffers, spoofing, intrusion.

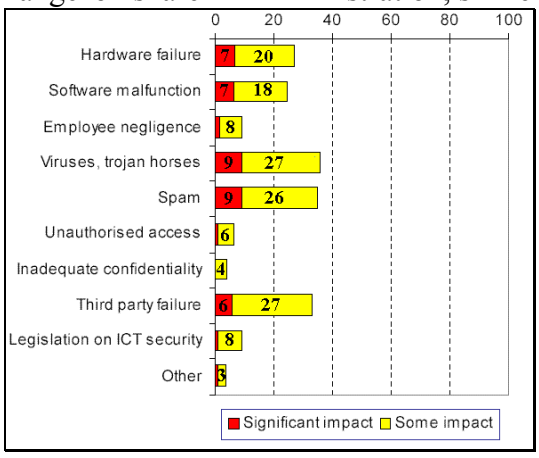


**Figure 3.** ICT security incidents in European Enterprises **[**Source: e-Business W@tch]

## Standards and legislation

Standards for risk analysis, security controls and management can significantly reduce the cost to enterprises of proper security policy implementation. Standardization here can reduce the decision load on management to acceptable levels for smaller enterprises. The adoption of standards by software and service suppliers will increase competition and market size, reducing the cost of solutions to

customer enterprises as economies of scale are passed on.

The **AS/NZS 4360** is the only internationally accepted risk management standard. The Standard provides a generic guide for establishing and implementing the risk management process involving identification, analysis, assessment, treatment and continuous risk monitoring.

The **COBIT** (Control Objectives for Information and Related Technology) framework was released in 1996 and updated in 1998 and 2000 by the Information Systems Audit and Control Foundation (ISACF) in response to the need for a reference framework for security and control in information technology. In 2000, the IT Governance Institute and ISACF developed the Management Guidelines for COBIT. These guidelines respond to a need by Management for control and measurability of IT, for the purpose of ensuring that IT activities achieve business objectives.

The **COSO** (Committee of Sponsoring Organisations of the Treadway Commission) framework was developed to help management better control their business activities. An internationally recognized standard, it provides a starting point for the individual assessment of internal control and applies a consistent approach to the review of business entities. *Enterprise Risk Management* (ERM) – *Integrated Framework* encourages internal auditors to approach their activities from the way management runs a business: control environment, risk assessment, information and communication, and risk monitoring.

**ISO 17799** (in full: ISO/IEC 17799:2005) is a risk management code of practice framework for Information Systems security developed by the International Organization for Standardization.

The **Sarbanes-Oxley Act** of 2002 requires that SEC-registered annual reports need to contain an "Internal Control Report".

**Conclusions**

Risk management tools provide benefit to an organization through better understanding of the operational environment, improved monitoring of the effectiveness of controls and a more robust response to compliance auditors. There is the danger however that they detract from the skills and experience of the corporate Risk Managers and business unit managers. The use of these tools within an organization must be clearly understood and the roles and areas of responsibilities for the various individuals defined ensuring the output is accurate and accepted. Like other security controls, a risk management tool will not be effective unless it is used and maintained properly. It is worth spending the time at the outset to determine exactly what is needed and following the accepted approach for application testing and procurement. This can be a major expense so the return on investment must be clearly demonstrated. This is only possible through a well-structured, well-managed and well-understood process.

**References**

[1] Pauline Bowen, Joan Hash, Mark Wilson, Nadya Bartol, Gina Jamaldinian, ***Information Security Handbook***: *A Guide for Managers*, NIST, 2006

[2] NIST Special Publication 800-30, ***Risk Management Guide for Information Technology Systems***, January 2002

[3] Fl. Nastase, P. Nastase, ***Security Controls to Protect Information Systems***, 2006, Proceedings of the 3rd International Conference - Economy and Transformation Management, Editura Universităţii de Vest, Timişoara

[4] P. Nastase, Fl. Nastase, R. Sova, ***IT Audit Trends within Framework of Balkan Countries***, The Balkan Countries' 1st International Conference on Accounting and Auditing (BCAA), 8-9 March 2007, Edirne- Turkey

[5] Buecker, J. Destro, ***Enterprise Security Architecture***, 2006, IBM Redbooks

[6] *** http://www.isaca.org

[7] *** http://www.enisa.europa.eu