ASPECTS OF IT RISK MANAGEMENT FOR A COMPANY

Fratila Laurentiu

Academy of Economic Studies Bucharest, Faculty of Accounting and Management Information Systems, Piata Romana, nr. 6, Bucharest, email: laurentiu_f@yahoo.com, phone: 0765.507.791

Tantau Adrian

Academy of Economic Studies Bucharest, Faculty of Business Administration, Piata Romana, nr. 6, Bucharest, email: ad_tantau@yahoo.com, phone: 0728.201.937

In the computer age, management information system represent an important component for the management of a company, strong linked to the rest of management subsystems. Inside of this subsystem, IT (information technology) is a fundamental element, which allows for a company to survive or to growth on a global market.

IT risk management is a continuous process, integrated in structure and culture of a company, that has as a goal to analyze and to find solution for minimize negative effects and maximize positive effects of risks.

The paper develops these main aspects to analyze risk software and the direction to implement it in a company.

Key words: types of IT risk, risk management, categories and impact of risks, control of risks, reporting systems of risks

Definition of IT risk

In general, risk refers to those factors, both technical and managerial, that are elements to success or a major source of problems on software projects.

From Wikipedia, risk is "a concept that denotes a potential negative impact to an asset or some characteristic of value that may arise from some present process or future event".

The American Heritage Dictionary defines risk as "the possibility of suffering harm or loss".

Risk can be defined using an appropriate definition for the risk, based on two directions: proposal risk and performance risk. Proposal risk referred to those risks inherent in the venture and is associated with the contractor's approach. Performance risks referred to those risks inherent in the proposed approach as is associated with the contractor's track record.

All organizations manage the two groups of risks: financial risks and operational risks.

Operational risk, defined by the Basel II committee of the Bank of International

Settlements is *"the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events"*. In the category of operational risk is included and IT risk.

The types of IT risks using as criteria the business operating conditions that can produce them are:

- Long-term IT risks - result from global circumstances and national and transnational legislation and regulation.
- Medium-term IT risks - result from changes in the market and competition.
- Short-term IT risks - result from interactions with customers, suppliers and partners.
- Ongoing IT risks - arise from the normal use and functionality of processes, systems and networks.

The period of time associated with these types of risks are: years, months, days and hours or minutes, respectively.

Risk management is a process that includes the identification, analysis, planning, tracking, controlling and communication of risk [3]. In the vision of Donald Reefer, risk management can be defined as the process of identifying sources of the problems for the project, analyzing them, quantifying their effects, and implementing plans that counteract their negative effects [6].

Barry Boehm defines the practice of Risk Management in two terms: risk assessment and risk control.

Risk assessment includes:

- risk identification - creating a list of all of the potential dangers that can affect the project;
- risk analysis - assessing the probability of appearance and potential loss of each item listed;
- risk prioritization - ranking the items from most to least dangerous.

Risk control includes:

- risk-management planning – setting the techniques and strategies to mitigate the highest ordered risks;
- risk resolution - implementing the strategies to resolve the high order risks factors;
- risk monitoring - monitoring the effectiveness of the strategies and the changing levels of risk throughout the project

By analysis the software risk, Boehm determines 10 software risk items [1]:

- Personnel Shortfalls;
- Unrealistic schedules and budgets;
- Developing the wrong functions and properties;
- Developing the wrong user interface;
- Gold-plating;
- Continuing stream of requirements changes;
- Shortfalls in externally furnished components;
- Shortfalls in externally performed tasks;
- Real-time performance shortfalls;
- Straining computer-science capabilities.

IT Risk Management methodology – Symantec Corp.

A lot of IT companies proposed different methods to manage the risk. Symantec Corporation is one of these, which propose Symantec Integrated IT Risk Management methodology [10]. This methodology offers to companies the possibility to control of IT risks from threat detection and prevention to the overall strategic direction of the business.

Symantec has developed a five-step process to assist in the management of IT risk, as follows.

- develop awareness of IT risks – implies understanding all defined main elements of the IT risk;
- quantify business impacts – implies to quantify and measure the impact of all categories of IT risk over all stages of the business and identified the main risks for critical business;
- design solution – implies to find/create the appropriate solutions to manage the identified risks;
- align IT/business value and implement solution – implies to implement the designed solution to mitigate the identified risks, especially for the critical stages of business;
- build and manage unified capability – implies to manage the risks in the general line of management of the company, at all levels of decisions.

Categories of IT risks

The failure of the company in management of IT risk is generate by difficulties in one of the following directions: security, availability, performance or compliance.

Risk Category	Source	Potential Impact
Security ***Compromise of information,*** ***confidence in it and technology and processes for managing it***	- External attacks - Malicious code - Physical destruction - Inappropriate access - Disgruntled employees - Proliferation of platform and messaging types	- Corruption of information - External fraud - Identity theft - Theft of financial assets - Damage to reputation and brand - Damage to assets
Availability ***Failure or delay in delivering IT processes or information needed for business transactions and operations***	- Hardware failures - Network outages - Poor change management processes - Data center failures - Force majeure	- Abandoned transactions and lost sales - Reduced customer, partner, employee confidence - Interruption or delay of business critical processes - Reduced IT staff productivity
Performance ***Slow or inefficient operation of IT processes supporting business transactions*** ***and operations***	- Poor system architectures - Network congestion - Inefficient code - Inadequate capacity	- Reduced client satisfaction - Reduced client or partner loyalty - Reduced user productivity - Interruption or delay of business critical process - Lost IT productivity
Compliance ***Penalties, fines and loss of reputation from failure to comply with laws and regulations, or consequences of noncompliance*** ***with IT policies***	- Regulations unique to each jurisdiction, including: • Graham-Leach-Bliley Act • EU Data Protection Directive • Health Insurance Portability and Accountability Act (HIPAA) • Sarbanes-Oxley Act - Legal actions - Internal IT safeguards supporting compliance - Inadequate third-party compliance standards - Expansion from central to end-point compliance	- Damage to reputation - Breach of client confidentiality - Litigation - Executive productivity

Table 1: Categories of IT Risk, with examples of the sources and potential impacts associated with each (source: [11]).

For IT applications, these categories of IT risks can be refine in more categories. Thus, appears two new categories: recoverability risk and scalability risk.

The term of IT recoverability risk defines the activities of creating and testing IT backup solutions, in ways that minimize the risk. Known as a “disaster recovery”, recoverability takes two forms: backup and recovery tests. If backup implies to realize copies on different removable media and store them outside the affected area of an anticipated disaster, the recovery tests implies to restore the data and apply logs against that data to bring them to consistency at a particular point in time up to the last transaction in the logs.

In practice, the both forms are used together. Thus, is eliminated the danger that bugs or human error have corrupted the backups

Scalability for IT risks can be evaluated from two perspectives [5]:

- the ability to have an acceptable response time under increased load on the same system;
- the ability to have an acceptable response time under increased load when using more hardware or software resources.

Thus, we can conclude on a large definition of scalability, as the ability to utilize additional resources efficiently in order to maintain a required response time.

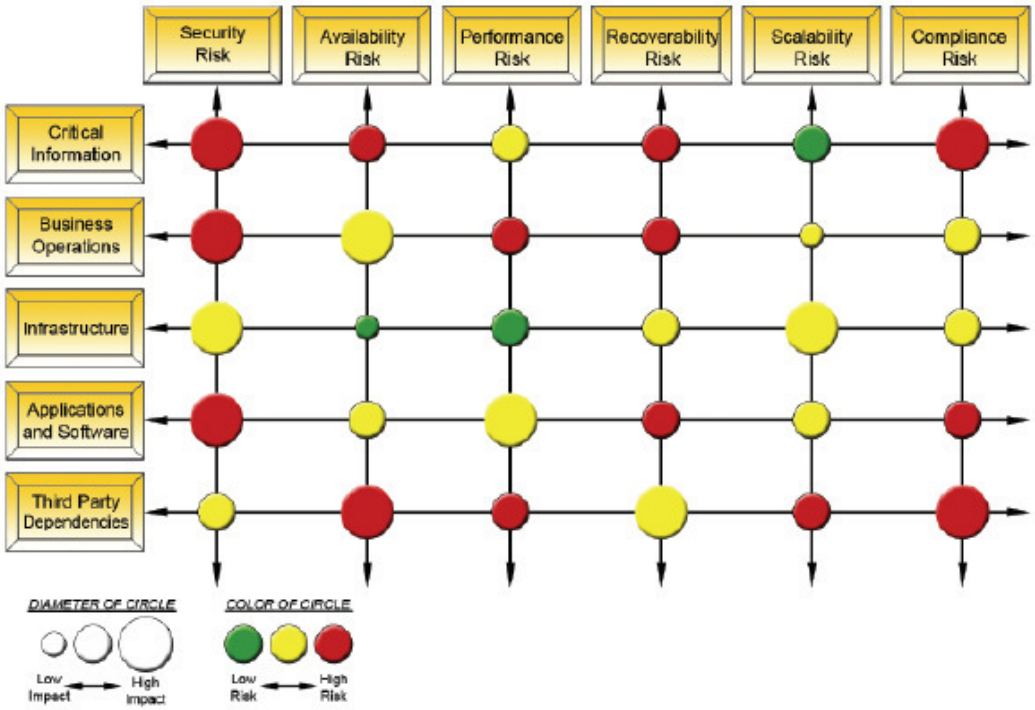

Figure 1. Level of Risk and Impact are critical facets of evaluation that should be considered when analyzing a portfolio of IT focus areas (source: [4]).

Control of IT risks

The problem of control of IT risk is very important for a company. The control will be treated over three visions: threats, vulnerabilities and impact.

These implies following aspects:

- Controls that will detect threats and issues in good time and will anticipate or prevent them where necessary and appropriate
- Controls that will enable vulnerabilities to be fixed and system weaknesses resolved
- Controls to manage the impact of any issues or threats that have succeeded in exploiting vulnerabilities or unresolved weaknesses

The responsibility for IT risk control belong to all departments of company, from the departments of IT services to the departments of Business Organization.

For the IT departments, the main activities to manage the risks are: detection and prevention, vulnerability fixing and response and recovery.

For the departments of business organization, the main activities to manage the risks are: strategic detection, program management and risk analysis.

The responsibilities of the employees for the largest organizations are shown in the table 2.

Control → / Role ↓	Detection and Prevention	Vulnerability Fixing	Response and Recovery	Risk Analysis	Program Management	Strategic Detection
Information Technology	x	x	x	x	x	x
Information Security	x	x	x	x	x	x
Audit and Compliance	x	x	x	x	x	x
Human Resources	x	x	x	x	x	x
Finance			x	x	x	x
Unit Management			x	x	x	x
Chief Information Security Officer			x	x	x	x
Legal Team				x	x	x
Chief Information Officer				x	x	x
Chief HR Officer					x	x
Chief Finance Officer					x	x
Chief Auditor						x
Chief Legal Officer						x
Chief Executive Officer						x

Table 2: Responsibilities in relation to IT risk management (source: [10]).

A performing reporting system implies three levels of reporting, as is shown in figure 3.

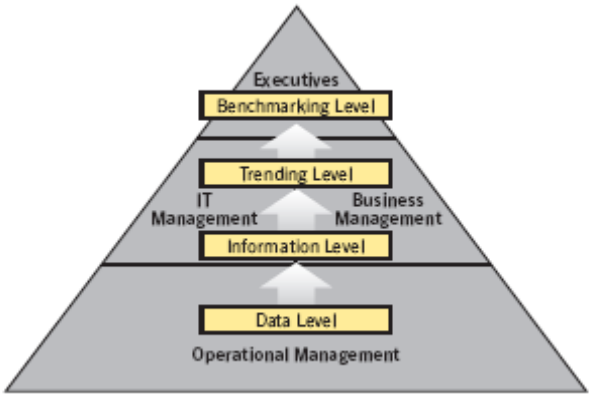

Figure 3: Reporting levels in relation to communities of practice (source: [10]).

The primary information is data about the everyday issues that arise at each of control layers. Form the middle reporting model, data are processing as information about importance of the aspects taken into account and transformed in trending information. At the highest level, information are used to formulate strategic directions by benchmarking the organization's risk, both internally and externally.

We can make a connection between the four levels of reporting (data, information, trending and benchmarking levels) with their specific control layers and risk performance indicators as is shown in table 3.

Control layer	Report Level	Risk Performance Indicators
Strategic Direction	Benchmark	Monthly risk index
Program Management	Benchmark	Month-on-month change in effectiveness of risk-reduction program
	Trend	Monthly trend in progress of implementing risk-reduction program
	Information	Weekly progress in implementing risk-reduction program
Risk Analysis	Benchmark	Index of month-on-month change in percent of applications at critical risk
	Trend	Monthly trend in number of applications at critical risk
	Information	Weekly progress in assessment of applications
Response and Recovery	Benchmark	Month-on-month change in downtime of applications
	Trend	Monthly trend in response to incidents affecting applications
	Information	Weekly report on response to incidents affecting applications
	Data	Weekly report on number of incidents affecting applications
Vulnerability Fixing	Benchmark	Month-on-month effectiveness in deployment of patches
	Trend	Monthly trend in deployment of patches
	Information	Weekly report on number of patches deployed
	Data	Weekly report on number of vulnerabilities
Threat Detection and Prevention	Benchmark	Month-on-month risk from software threats
	Trend	Monthly trend in speed of deployment of definition files
	Information	Time between vendor release of definition files and deployment
	Data	Names and frequency of software issues

Table 3: Key performance indicators for reporting levels across the risk control spectrum (source: [10]).

Conclusions

Now a days, each company use computers equipments in every stage that suppose processing data. An effective and efficient using of IT is a key factor that differentiating successful firms from their less successful counterparts. Many companies understood the possibilities to exploit IT capabilities and made high IT investments without deriving any benefits from IT. But using a new IT system implies appearance of risks that must be managed and mitigated in order to control the evolution of business in the established limits. As a bigger company or more complexity activity, IT risk factors can occur.

Using a performance IT risk management, the company must take into account the risk in every stage of the application development cycle in order to realize a significant improvement in their processes of design, develop, test and maintain the integrity of the applications.

In the same time, there are positive effects in two directions: on one hand, a normalize development of the business/applications and maintenance the costs in the settlement limits, on the other hand, the raising the quality and the competitiveness of the business/applications.

Bibliography:

1. Boehm, R., "Software Risk Management: Principles and Practices", IEEE Software, Vol. 8, No. 1, January 1991
2. Jones, C., J., "Minimizing the Risks of Software", 1998
3. Higuera, R., Haimes, Y., "Software Risk Management" – Technical report, Carnegie Mellon University, Pittsburgh USA, 1996
4. Kapuria, S., "Addressing IT Risks of Software Applications: A Risk Management Strategy", Symantec Corporation, 2006, available at www.symantec.com
5. Makedonov, Y., "Scalability is a rather ambiguous term", 2006, available at http://www.softwaretestconsulting.com
6. Reifer, R.,"Software Management, Fourth Edition", IEEE Computer Society Press, 1993.
7. Van Scoy, R., "Software Development Risk: Opportunity, Not Problem", Pittsburgh, Software Engineering Institute, Carnegie Mellon University, 1992
8. Young, P., Use of Earned Value Management to Mitigate Software Development Risk", George Mason University, USA, 1997
9. Department of the Air Force, Software Technology Support Center, Guidelines for Successful Acquisition and Management of Software-Intensive Systems: Weapon Systems, Command and Control Systems, Management Information Systems, Condensed Version, 2003
10. Integrated IT Risk Management, Symantec Corporation, 2007, available at www.symantec.com
11. IT Risk management report, Symantec Corporation, 2007, available at www.symantec.com