UNDERSTANDING RISK MANAGEMENT IN SMALL 7 STEPS[25]

Valentin Petru MĂZĂREANU, Ph.D
The Faculty of Economics and Business Administration
"Alexandru Ioan Cuza" University of Iasi

Abstract: Risk management means making steps in order to identify those risks with a highly probability of causing problems to a project, to analyze the probability of loss and the magnitude of loss for each risk and developing composed risks, to classify the risk points identified according to the composed risks they belong to. Risk management problem is quite complex. When such a process is triggered, it must consider several issues in parallel. In this article we detect seven rules (principles) that a risk management department should take into account when deciding to implement a enterprise risk management

JEL classification: D81, M1

Key words: risk management, model, approach, principle

1. Introduction

Risk is an extremely complex phenomenon, and risk management clearly requires combining the rigors of science with art challenges. Science, because risk management should refer to knowledge, the method and methodology, but also art, because someone must feel when to get rid of a certain methodology and borrowing knowledge from other areas of knowledge.

We believe that our approach helps in developing a link between art and science of risk management. This link grows through understanding a set of rules, principles, which, in our opinion, are:

- how risk management works? (analyzing the relationship between asset - vulnerability – risk);
- analyzing the internal and external factors;
- risk analysis in the software development cycle (when appropriate)
- identifying the appropriate timing for risk assessment;
- seeing the boundary between real fact, possible and impossible events (related to risk);
- seeing the limit between threat and opportunity (related to risk);
- seeing risk as a probability event

[25] **Acknowledgements.** The results presents in this paper were obtained in the framework of the postdoctoral school programme financed by the "Dezvoltarea capacității de inovare și creșterea impactului cercetării prin programe postdoctorale POSDRU/89/1.5/S/49944" project.

2. How Risk Management Works? (Analyzing the Relationship Between Asset - Vulnerability – Risk)

First, we can talk about the stake at risk and how important vulnerabilities are in the disaster scenarios taken into account, the result being a way to reduce the resulting risks (Fig. no.1)

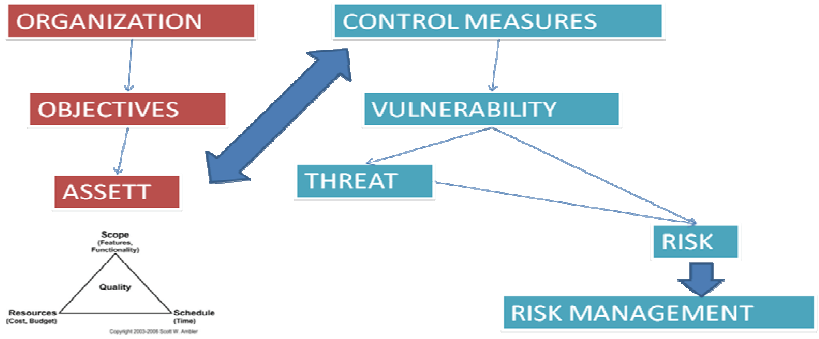


Figure no.1 Risk Management Process

This is an approach proposed also by CLUSIF - Club de L'Information Security Francais in the Mehari methodology (1).

Stake (asset)

The stake is an issue that varies from entity to entity. This should be quantified and classified individually on each business separately. The stakes should be differentiated at by their availability, integrity and confidentiality. The impact of the consequences could be financial or legal or reputational, but all these issues must be examined in relation to the importance for the survival of the organization.

Vulnerabilities

According to ISO 27001 there is the possibility to create a collection (qualitative!) of audit questions as a consequence of good practice. But which one best fits a particular business major stakes in a company? Which one will decrease the potential disaster? Which one will reduce the consequence (impact)? And how could be assessed the correlation between a specific question and a certain effect? Is it possible to group the questions in order to ensure risk reduction? Such a group might bear the name of: security measure.

But this would call for new measures to quantify the contribution of each security measure within a company at reducing the potential (probability, sounds too mathematical) or the impact (consequence) of a disastrous situation.

Risks

At this level a new question arises: how to implement a disaster scenario to such situations? The simplest way would be to have a list of scenarios and some mathematical formulas established between the asset, the vulnerabilities and the risks, given by the security measures laid down in advance.

Also, how to build a security protection to cover the most important scenarios in a very efficient manner? This is achieved by setting the weights of the most important safeguards scenarios.

But as long as there is not a classic pattern of threats in each area and also immediately available statistics, this task may require a considerable research effort. The difficulty may come from the possibility that a significant threat to be overlooked

or accepted by negligence. Worse, it is possible that a significant threat to be intentionally disregarded

3. Analyzing The Internal And External Factors

Second, we must understand that the probability of an event depends on a series of external factors as well as on internal factors of the entity (business/process/project) for which the risk assessment is made. It is essential to know and control as many of these factors as possible.

The internal factors include historical data from within the entity, collected in time, as it is necessary to keep a record of all processed data, no matter if for the moment it is thought that the data will not be useful in the future.

One way to achieve this without affecting the operational environment is appealing to data warehousing technology and decision support systems. Without going into technical details we mention only that the data warehouse is a way of storing data and creating information, a topic-oriented database, integrated, nonvolatile, other (sensitive) over time, which support management decisions. And decision support system is in a simple definition, the layer of data presentation from the data warehouse. In fact it is much more than a presentation layer: the decision support system extending itself from extracting data from data warehouse to present these data to the decision maker, including sophisticated reporting tools, tools, OLAP (Online Analytical Processing) and Data Mining.

And when we talk about external factors, we are talking about those factors undergoing STEEP analyses (Social, Technological, Economic, Environmental, Political), factors that cannot be controlled but that could be anticipated. Here are also included the events from the company's activity, such as natural disasters or terrorist attacks, attacks against informational systems (informational viruses, spam, DoS type attacks etc.).

In order to evaluate these factors one may choose to study the statistical data available from various sources including the FBI (eg CSI FBI Survey) or various international information security experts centers such as CERT (Computer Emergency Response Team), the Software Engineering Institute or CERIS (Centre of Expertise and Response to Security Incidents).

But this data gives only a vague estimate of the probability of occurrence and impact generated by such an occurrence. Such an approach is justified such as "always be prepared for the worst."

4. Risk Analysis In The Software Development Cycle

Third, if we come closer to the electronic business environment and the fact that one of the elements of this environment is the informational system, we must not ignore the software risk, which represents the combination between the probabilities of occurrence and the loss caused by an unwanted result which affects the project, the process or the software product.

Each software system is unique with its own set of risks. There are many software risks but fewer consequences that we want to avoid. Perhaps because of this software risk is often discussed in terms of potential cost, timing and technical consequences.

In software development business the risk management has a different behavior; because in this case the accent falls more on the process of development and

ensuring the integrity of the process and less on the final product. Although at first glance seem similar, there should be no confusion between risk management and quality management (Roy, 2004): the quality assurance is a process that will minimize the chances of the project to deviate from a set of rules originally established and risk management deals with the identification of components that could go wrong and their impact on project analysis.

5. Identifying The Appropriate Timing For Risk Assessment

Fourth, the moment suitable to launch a risk assessment process must be identified. We thus differentiate between a corrective action and a preventive action. Risk assessment is a preventive action, so it is necessary to take place before the unfortunate event (Fig. no. 2).

An example of a corrective action plan is the disaster recovery, a component of business continuity plan (Obs. at this level the opinions are divided; some authors take business continuity plan as part of the risk management plan, others refer to this plan as an independent entity).

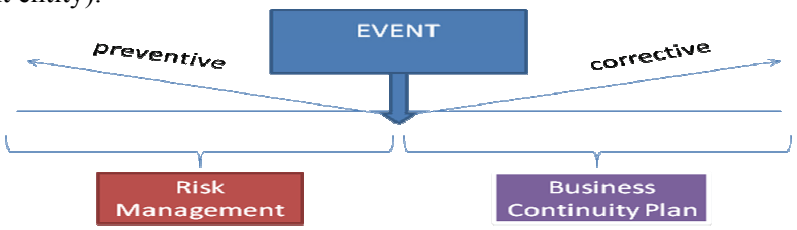


Figure no. 2 The Appropriate Timing For Risk Assessment

6. Seeing The Boundary Between Real Fact, Possible And Impossible Events

Fifth, it also takes an approach on the border of philosophy and mathematics (Măzăreanu, 2010). That is: we have three domains the real, the possible, the impossible (Fig. no. 3).

Figure no. 3 The Boundary Between Real Fact, Possible And Impossible Events

The problem of risk management is in the realm of the possible. The possible is what can be but is not. The main characteristic of the possible is defined through relation to the human being. This characteristic is called probability. It gives the chance of a scientific approach to a border domain between real and impossible. The probability reported to man has two manifestations: chance and risk. Chance is favorable to man, risk is unfavorable.

Scientifically, the approach of this matter can only be a calculation of the probability of an event or of its passing from the possible to the real. So we could

assume that it is useless to approach the matter as a risk of something occurring, but only as probability.

As a result a formula to determine the probability for an unfortunate event to occur is necessary.

7. Seeing The Limit Between Threat And Opportunity

This approach opens a new topic. Given that risk is defined as a future and uncertain event, able to affect the project objectives (in terms of human, material, financial, technical or in terms of scheduling) why to look at this event only its catastrophic side? (Fig. no. 4)

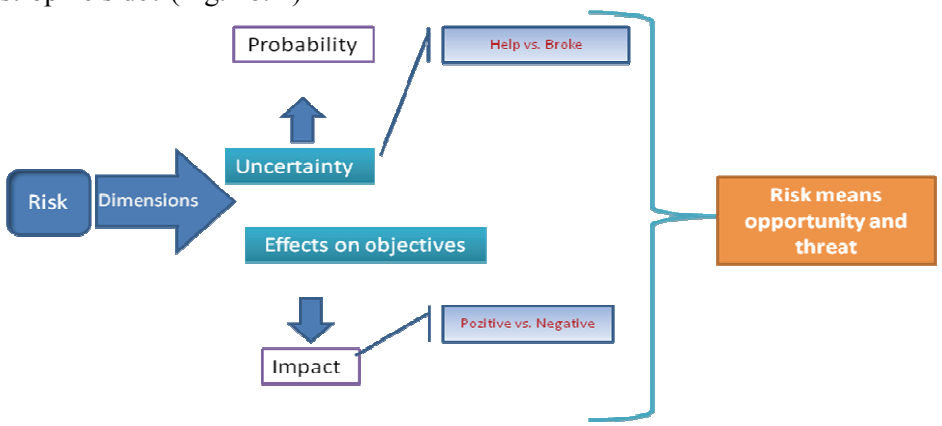
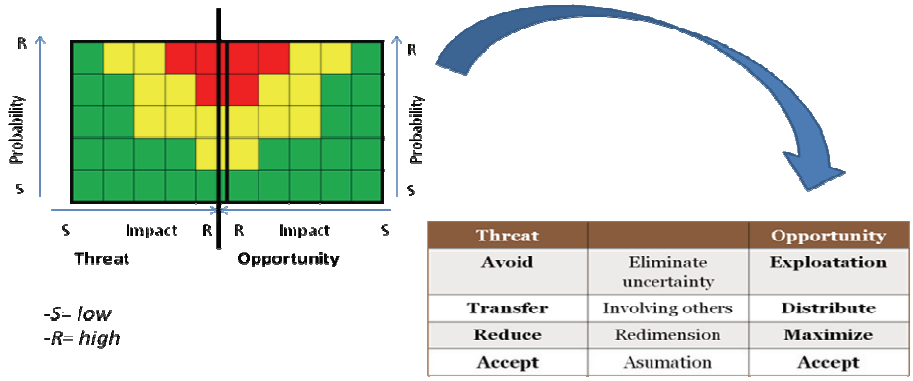


Figure no. 4 Understanding the new approach



Threat		Opportunity
Avoid	Eliminate uncertainty	Exploatation
Transfer	Involving others	Distribute
Reduce	Redimension	Maximize
Accept	Asumation	Accept

Figure no. 5 The New Approach

As long as we relate the risk to uncertainty and to impact on the objectives, as well this event could be considered an opportunity. Under these conditions the generally risk approach need to be changed (Fig. no. 5).

8. Seeing Risk As A Probability Event

It should be understood that risk is a probabilistic event: it is possible to occur, it is possible that it may not appear. Moreover, it is known that human ability to estimate the likelihood of an event is quite poor and take a number of factors, including (Leach, 2000):

- mathematical factors (eg. failure to understand how the probabilities may combine, inability to work with numbers of greater value);
- errors of representation;
- error of judgment (eg. The dependency on a first decision, the tendency to trust a first impression, the tendency to not deviate too much from a first impression).

For this reason, there are optimistic tends to not see the risks involved in a project or that these risks would not occur. Such attitudes can lead to big problems if the risk materializes, and risks in large projects are inevitable

9. Conclusions

It is clear that the risk varies from situation to situation, whether speaking of an activity, project, or the entire business process. Consequently, the risk response plan differs. It is clear why the risk management and the risk manager are strictly required for a successful activity in the business and the organizational structures especially in the organizations that are lead through projects management.

If the management level decides that the risk management will be run by complying with a standard or by adjustment and adaptation to standards, methods, methodologies and laws (this is another debate about which approach is more appropriate), in this paper the emphasis is on the risk manager (the risk management team). Because if the manager fails to understand the risk factors listed above, the whole process of risk management, whether standardized or adapted, is subject to failure.

Note

(1) The Mehari methodology may be found on CLUSIF website (https://www.clusif.asso.fr/fr/clusi/).

The Romanian translation of the Mehari methodology may be found on http://www.managementul-riscurilor.ro, a Romanian website dedicated to risk management.

REFERENCES

1. Leach, L.P. Critical Chain Project Management, Ed. Artech House, Boston, 2000
2. Măzăreanu, P.V Economia Digitală şi Managementul Riscurilor, Ed. Tehnopress, Iaşi, 2010
3. Roy, G.G. A Risk Management Framework for Software Engineering Practice, Proceeding of the 2004 Australian Software Engineering Conference (ASWEC'04), IEEE Computer Society, 2004