ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA" DIN IAŞI
Tomul LIV **Ştiinţe Economice** **2007**

RISK MANAGEMENT AND ANALYSIS: RISK ASSESSMENT (QUALITATIVE AND QUANTITATIVE)

VALENTIN P. MĂZĂREANU*

Abstract

We use to define risk as the possibility of suffering a loss. Starting this, risk management is defined as a business process whose purpose is to ensure that the organization is protected against risks and their effects. In order to prioritize, to develop a response plan and after that to monitor the identified risks we need to asses them. But at this point a question is born: should I choose a qualitative approach or a quantitative one? This paper will make a short overview over the risk evaluation process also proposing a new approach in this direction.

Key words: risk management, risk assessment

1 Introduction

Without going into details regarding the theory of project risk management we present, still, the definition of this concept as it is proposed by the Project Management Institute professionals who, in *The Project Management Body of Knowledge Guide,* [Duncan, W., R., 1996] define risk management as a systematic process of identification, analysis and response to the project risks, process comprising the risk identification, risk quantification, risk response plan, risk response control sub processes.

A closer look to the literature or project risk management standards will make the reader understand that depending on the author of the methodology, the name or the order of these sub-processes is different. Thus, risk identification and risk quantification are sometimes taken together and are called risk assessment or risk analysis; the risk response plan is sometimes met under the name of risk mitigation plan; the risk response plan and the risk control plan are sometimes taken together under the name of risk management plan.

2 Inside Risk Assessment

All the elements of the risk management cycle are important but risk assessment is the headstone for all the other elements.

The problem of risk assessment is an extremely complex one. When a risk assessment process is started, this process has to analyze several aspects in parallel.

First, we can talk about the stake at risk and how important vulnerabilities are in the disaster scenarios taken into account, the outcome being a way to reduce the resulting risks.

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.

* PhD Student, Department of Business Information Systems, Faculty of Economics and Business Administration, "Alexandru Ioan Cuza" University, Iasi, e-mail: vali.mazareanu@feaa.uaic.ro

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 (see business intelligence and data warehouse concepts for understanding how to implement such a data collection system). And when we talk about external factors, it is 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 information systems *(*information viruses, spam, DoS type attacks etc*.)*.

Third, if we come closer to the electronic / mobile business environment and the fact that one of the elements of this environment is the information 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.

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. The corrective action: in this situation is the disaster recovery plan, a component of the business continuity plan. This process is necessary to be applied in the first moments after the unfortunate event took place. (Observation: the opinions differ at this level, some authors regarding the business continuity plan as part of the risk management plan, others, as an independent entity).

Fifth, it also takes an approach on the border of philosophy and mathematics. That is: we have three domains the real, the possible, the impossible. 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.

3 Qualitative vs. Quantitative

When risk assessment is discussed, it can be approached from two directions, two assessment models: the qualitative model and the quantitative model.

The qualitative risk analysis is a process of assessment of the impact of the identified risk factors. Through this process the priorities are determined to solve the potential risk factors, depending on the impact they could have. The definite characteristic of the qualitative model is the use of subjective indexes, such as ordinal hierarchy: low-medium-high, vital-critical-important, bench mark etc.

Through the quantitative risk analysis it is sought to obtain some numerical results that express the probability of each risk factor and its consequences on the objectives of the project, but also the risk on the entire project level. The process uses techniques such as the Monte Carlo method for:

- determining the probability of reaching an objective;
- risk quantification on the entire project's level and determining the additional cost that could be necessary;

- identifying prioritary risk factors through the quantification of their contribution to the risk index on the level of the entire project;
- identifying some realistic changes of cost and activity plan.

The most common formula for evaluating risk exposure is $RE = P \times L$, where:

- RE = risk exposure
- P = risk probability
- L = loss

Starting with probability of occurrence and the amount of lost (impact level) a risk matrix can be developed in order to better understand the risk exposure (see fig. 1).

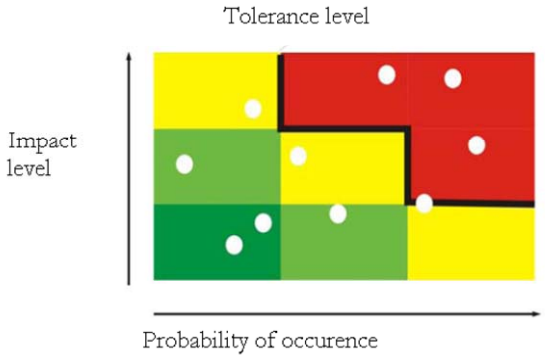

Fig. 1 Quantitative Risk Matrix
(Obs. It is recommended to use a 5 levels matrix, from *very low* to *very high* exposure)

In these analyses the fact that it is sometimes hard to estimate the exact value of this relation must also be considered. The recommendation in these situations is to use all known mathematical methods which could be useful in the situation, but without getting stuck in this type of analysis, and considering personal judgment also. The term „quantitative risk analysis" implies generally the reliance on probability and statistics.

Still, some quantitative decisional methodologies based on risk, such as the game theory, does not require probability knowledge. As Yacov Haimes has mentioned in Risk Modeling, Assessment and Management [Haimes, Y., Y., 1998] here are a few examples of decisional criteria for administrating risk and uncertainty without requesting the involvement of probabilities: maximizing minimum gain (maximin), minimizing maximum loss (minimax or maximin criteria – the pessimistic rule), maximizing maximum gain (maximax – the optimistic rule). There is also a compromise rule: the Hurwitz rule. In this case an α ($0 \leq \alpha \leq 1$) index appears in order to define the optimistic level of the decision maker.

Usually, the quantitative analysis follows the qualitative analysis, but the two processes can be done simultaneously. The growing or decreasing tendencies indicate the necessity to increase or decrease the risk management actions.

As Hal Tipton and Micki Krause noted in Handbook of Information Security Management [Tipton, H. & Krause, M., 1998], whether we choose the quantitative assessment, whether we try a qualitative assessment, the elements that need to be considered (if we recall the *„Divide et Impera"* adage) are:

- *tangible or intangible asset value* (the value of these assets is determined, usually, in terms of cost required for replacing them)
- *threat frequency* (the threat defines an event whose would lead to an unwanted impact.) existence
- *threat exposure factor* (this factor represents a measure of the magnitude of loss or the impact on the value of an asset.)

- *safeguard effectiveness* (this term represents the degree to which a safeguard manages to effectively minimize a vulnerability and to reduce the risks of associated loss.)
- *safeguard cost* (safeguards are often described as controls or countermeasures and we can talk here about the practice of the cost/benefit analysis.)
- *uncertainty* (this term characterizes the degree, expressed in percentages of trust in the value of any element of the risk assessment process)

4 A new approach to risk assessment: human factor consideration

The elements presented before do, in truth, perform a risk assessment, but more through risk „*behavior*" (the exterior event with devastating potential, the financial damages it causes etc.). For this reason, we think that other elements can also be considered in risk assessment, such as:

- the professionalism of the assessment team / trust granted to the human factor ;
- the time available to make the assessment ;
- the moment of risk identification in the system's life cycle (analysis, project, implementing, testing, effective functioning etc.);
- the necessary cost for assessment and adopting the risk response plan – acceptance, avoidance or transfer. ("Is the assessment still worth if it generates a cost higher than the damage that would be generated in the case of a risk occurrence?");
- the STEEP factors (social, technological, economical, environmental, political).

We reveal on this opportunity another factor which should be considered in the assessment of risk generated by the human component - the psychological factor. And we don't necessarily mean by that abilities, skill (ability consolidated through habit) or intelligence (analytical, synthetic, pragmatic, and theoretical). We consider personality, character, creativity (when required), and temperament to be important. This is not the first time man is being analyzed. We mention the risk centers technique (human – technical – information – market – financial), the P^2I^2 formula (people – processes – infrastructure – implementation) or the cause-effect diagram (fishbone diagram or Ishikawa diagram) where the analysis of the human factor is one of the important elements.

Still, the main idea of this section of the paper proposes a different approach: the project's predisposition to risk starting from the human factor. Let's remember that when the famous Golden Gate bridge was built in San Francisco, Joseph Strauss, the founder of this project, a symphony in steel as it is called by John Bernard McGloin, professor at the University of San Francisco, dismissed one of his best workers because he, so confident of himself, refused to follow the required work protection measures (e.g. wearing a protective helmet, ensuring himself with safety wires). Or more recently, talking about Google's human resources policy, Eric Schmidt (CEO Google) and Hal Varian (professor at Berkeley and consultant for Google) highlighted the fact that, in a project, it is almost fatal to have in a team an intelligent but inflexible person. Exactly for this reason the combination of recommendations „*he is the most clever person I have ever met*" and „*I would never want to work with this person again*" represents a bad solution for Google [Schmidt, E. & Varian, H., 2005].

Let us take for example temperament. Without going into such an analysis for the moment, we mention that temperament is a form of manifestation of personality under the aspect of energy, quickness, regularity and intensity of the psychic processes. It is the dynamic side of personality with influence on the character. The temperament is influenced by aspects of genetics, experience, chemical substances in the body at a certain point. Closely connected with temperament is the attitude towards risk.

Each person has a natural preference towards risk, preference which depends on one's own temperament. By knowing a person's preference towards risk, we can anticipate which choices they are going to make. And the attitude towards risk can be of three types:

- risk averse: It shows a conservatory attitude towards risk, with preference for safe results.
- risk seeking: it shows a liberal attitude towards risk, with preference for speculative results.
- risk neutral: It shows an impartial attitude towards risk, with preference for future results.

All these psychological aspects are subjects to be discussed in a more detailed paper, but there is a saying that can sustain our approach; and that saying is: to err is human ("*errare humanum est*", Cicero)

5 Conclusions

Risk assessment is commonly defined starting with two elements: *the probability of risk to occur* and *the potentially lost in case of risk occurring*. These helps defining *risk exposure*. Some of the authors propose the extension of these elements to: *the value of asset, thereat frequency, threat exposure factors, safeguard effectiveness, safeguard cost* and *uncertainty*.

In our opinion all the elements mentioned above are important but, as presented in the paper, we propose another extension: *the human factor* (considering all the aspects related to it: professionalism, skills and abilities, psychological factors), the most incontrollable part of every system.

If all these elements are evaluated starting from a high-medium-low type criteria, the assessment will be qualitative.

To the degree to which each of these elements is quantified into independent objective indexes such as the monetary value of replacing the value of the asset or the annual occurrence rate for the frequency of the threat, risk assessment becomes predominantly quantitative.

If all the six elements we have mentioned above (including the psychological factors we have referred to) are quantified through objective independent indexes, risk assessment is fully quantitative, undergoing a series of statistic analyses.

References

Duncan, W., R., *A Guide to the Project Management Body of Knowledge,* Project Risk Management, Project Risk Management, Upper Darby, 1996

Haimes, Y., Y., *Risk Modeling, Assessment and Management*, John Wiley & Sons, Inc., New York, 1998

Schmidt, E., Varian, H., "Google-Ten Golden Rules"*, Newsweek*, December 2005

Tipton, H., Krause, M., *Handbook of Information Security Management*, CRC Press LLC, 1998