УДК 004.056:006

IDENTIFICATION OF RISKS, THEIR ANALYSIS AND EVALUATION

Kupreeva G.
Belorussian National Technical University
Minsk, Belarus

Every organization is continuously exposed to an endless number of new or changing threats and vulnerabilities that may affect its operation or the fulfillment of its objectives. Identification, analysis and evaluation of these threats and vulnerabilities are the only way to understand and measure the impact of the risk involved and hence to decide on the appropriate measures and controls to manage them. It has to be noted, that Risk Assessment is a process that in many cases is not (at least not adequately) performed, even if Risk Management is implemented.

For insurance companies, the performance of Risk Assessments is in general of significant importance and in particular concerning IT risks for current and potential customers.

This is the phase where threats, vulnerabilities and the associated risks are identified. This process has to be systematic and comprehensive enough to ensure that no risk is unwittingly excluded. It is very important that during this stage all risks are identified and recorded, regardless of the fact that some of them may already be known and likely controlled by the organization.

The first step is to generate a comprehensive list of sources of threats, risks and events that might have an impact on the achievement of each of the objectives as identified in the Definition of Scope and Framework. These events might prevent, degrade, delay or enhance the achievement of those objectives.

In general, a risk can be related to or characterized by

- it’s origin (e.g. threat agents like hostile employees or employees not properly trained, competitors, governments etc.);
- a certain activity, event or incident (i.e. threat) (e.g. unauthorized dissemination of confidential data, competitor deploys a new marketing policy, new or revised data protection regulations, an extensive power failure);
- its consequences, results or impact (e.g. service unavailability, loss or increase of market/profits, increase in regulation increase or decrease in competitiveness, penalties, etc.);
- a specific reason for its occurrence (e.g. system design error, human intervention, prediction or failure to predict competitor activity);
- protective mechanisms and controls (together with their possible lack of effectiveness) (e.g. access control and detection systems, policies, security training, market research and surveillance of market);
- time and place of occurrence (e.g. during extreme environmental conditions there is a flood in the computer room).

Good quality information and thorough knowledge of the organization and its internal and external environment are very important in identifying risks. Historical information about this or similar organizations (competitors or not) may also prove very useful as they can lead to safe predictions about current and evolving issues that have not yet faced by the organization.

Identifying what may happen is rarely sufficient. The fact that there are many ways an event can occur makes it important to study all possible and significant causes and scenarios. Methods and tools used to identify risks and their occurrence include checklists, judgments based on experience and records, flow charts, brainstorming, systems analysis, scenario analysis and systems engineering techniques.

In selecting a risk identification methodology, the following techniques should be considered:

- team-based brainstorming where workshops can prove effective in building commitment and making use of different experiences;
- structured techniques such as flow charting, system design review, systems analysis, Hazard and Operability studies, and operational modeling;
- for less clearly defined situations, such as the identification of strategic risks, processes with a more general structure such as ‘what-if’ and scenario analysis could be used.

Risk analysis is the phase where the level of the risk and its nature are assessed and understood. This information is the first input to decision makers on whether risks need to be treated or not and what is the most appropriate and cost-effective risk treatment methodology.

Risk analysis involves:

- thorough examination of the risk sources;
- their positive and negative consequences;
- the likelihood that those consequences may occur and the factors that affect them;
- assessment of any existing controls or processes that tend to minimize negative risks or enhance positive risks (these controls may derive from a wider set of standards, controls or good practices selected according to a an applicability statement and may also come from previous risk treatment activities).

The level of risk can be estimated by using statistical analysis and calculations combining impact and likelihood. Any formulas and methods for combining them must be consistent with the criteria defined when establishing the Risk Management context. This is because an event may have multiple consequences and affect different objectives, therefore consequences and likelihood need to be combined to calculate the level of risk. If no reliable or statistically reliable and relevant past data is available (kept for e.g. an incident database), other estimates may be made as long as they are appropriately communicated and approved by the decision makers.

Information used to estimate impact and likelihood usually comes from:

- past experience or data and records (e.g. incident reporting),
- reliable practices, international standards or guidelines,
- market research and analysis;
- experiments and prototypes;
- economic, engineering or other models;
- specialist and expert advice.

Risk analysis techniques include:

- interviews with experts in the area of interest and questionnaires;
- use of existing models and simulations.

Risk analysis may vary in detail according to the risk, the purpose of the analysis, and the required protection level of the relevant information, data and resources. Analysis may be qualitative, semi-quantitative or quantitative or a combination of these. In any case, the type of analysis performed should, as stated above, be consistent with the criteria developed as part of the definition of the Risk Management context.

A short description of the above-mentioned types of analysis types is as follows in qualitative analysis, the magnitude and likelihood of potential consequences are presented and described in detail. The scales used can be formed or adjusted to suit the circumstances, and different descriptions may be used for different risks.

Qualitative analysis may be used:

- as an initial assessment to identify risks which will be the subject of further, detailed analysis;
- where non-tangible aspects of risk are to be considered (e.g. reputation, culture, image etc.);
- where there is a lack of adequate information and numerical data or resources necessary for a statistically acceptable quantitative approach.

In semi-quantitative analysis the objective is to try to assign some values to the scales used in the qualitative assessment. These values are usually indicative and not real, which is the prerequisite of the quantitative approach.

Therefore, as the value allocated to each scale is not an accurate representation of the actual magnitude of impact or likelihood, the numbers used must only be combined using a formula that recognizes the limitations or assumptions made in the description of the scales used.

It should be also mentioned that the use of semi-quantitative analysis may lead to various inconsistencies due to the fact that the numbers chosen may not properly reflect analogies between risks, particularly when either consequences or likelihood are extreme.

In quantitative analysis numerical values are assigned to both impact and likelihood. These values are derived from a variety of sources. The quality of the entire analysis depends on the accuracy of the assigned values and the validity of the statistical models used.

Impact can be determined by evaluating and processing the various results of an event or by extrapolation from experimental studies or past data. Consequences may be expressed in various terms of:

- monetary impact criteria;
- technical impact criteria;
- operational impact criteria;
- human impact criteria.

As it is made clear from the above analysis, the specification of the risk level is not unique. Impact and likelihood may be expressed or combined differently, according to the type of risk and the scope and objective of the Risk Management process.

During the risk evaluation phase decisions have to be made concerning which risks need treatment and which do not, as well as concerning on the treatment priorities. Analysts need to compare the level of risk determined during the analysis process with risk criteria established in the Risk Management context (i.e. in the risk criteria identification stage). It is important to note that in some cases the risk evaluation may lead to a decision to undertake further analysis.

The criteria used by the Risk Management team have to also take into account the organization objectives, the stakeholder views and of course the scope and objective of the Risk Management process itself.

The decisions made are usually based on the level of risk but may also be related to thresholds specified in terms of:

- consequences (e.g. impacts);
- the likelihood of events;
- the cumulative impact of a series of events that could occur simultaneously.