Journal of Defense Management
ISSN: 2167-0374
Georgiev, J Def Manag 2012, 3:1
DOI: 10.4172/2167-0374.1000e119
Editorial
Open Access

Risk Management Language and Concepts

Venelin Georgiev*
Information Technologies for Security Department, Institute on Information and Communication Technologies, Bulgarian Academy of Sciences, Bulgaria

Successful implementation of the risk management concept in the defense begins, passes and develops through utilization of specific language and conceptual models. This statement is as simple as it is fundamental and its misunderstanding ensures failure in trials to implement the risk management practices in organizations.

In the literature there are different definitions of what constitutes risk. According to some authors, the risk is a measure of the potential inability to achieve the organizational goals within the planned expenditure of resources, limitations and time horizons[1]. According to other authors, the risk is potentially an event or situation, the realization of which can lead to negative consequences for the implementation of the plan, program or project[2]. In both cases, however, the risk content includes two components: the probability of occurrence and size of the possible consequences of implementation.

Risk can be defined in different ways depending on the situational context. For example in engineering, engineering quantitative definition of risk could be expressed by the following formula:

$$\text{Risk}=(\text{probability of accident}) \times (\text{losses from incident}) \quad (1)$$

Financial risk is often defined as the unexpected modification of the expected return and therefore includes two options: worse than expected and better than expected return on investment.

In statistics, the risk is associated with the probability of an event that is defined as unwanted. Typically, the probability of such an event and evaluating the likely effects of its implementation is considered in the developed scenario. The theory of statistical decisions, risk is seen as a function of the assessor $\delta(x)$ for the parameter θ, calculated on a variable xi and is defined as the expected value of the loss function L:

$$L=[\theta, \delta(x)]=\int L[\theta, \delta(x)].F(x/\theta)\,dx \quad (2)$$

In information security risk is a function of three variables: the probability of the existence of a threat, the probability of the existence of a vulnerability and potential impact. In cases where any of the three variables is zero, then the general risk assessment also should be considered zero.

In the field of insurance, the insurance is considered as an investment in risk reduction or sharing whereby the insured pays a small fixed amount to be protected against potential future losses.

The risk for human health can be reduced by primary prevention actions that reduce the likelihood of disease or secondary prevention actions after detection of clinical signs or symptoms identified as risk factors.

Risk assessment is complex and consists of an evaluation of its two components: the likelihood and extend of the expected consequences. There are some extreme cases of risk assessment such as: if the probability of occurrence of a risk is assessed as very high, but at the same time it does not lead to serious consequences for the implementation of organizational activities, the overall risk can not be assessed as significant. On the other hand risk with low probability of occurrence but with significant consequences should be identified as significant. A typical example of the second type of risks is those related to defense and security, which are generally regarded as significant despite the low probability of their realization. Risk accompanies the realization of any activity, but its existence in itself does not lead to a change in the status of the organization.

Included in the definition of risk is the concept that says the risk is a future event, a potential problem that creates uncertainty in achieving the organization's objectives. Important risk feature is the time period from the moment of risk identification till its implementation, because the time is a critical element in choosing a solution to counter the risk.

The problem is most often defined as the risk that has materialized. After realizing the risk and related consequences the state of the organization is modified. The problem can also be defined as an event that is sure to come true and it will have a negative impact on the achievement of targets.

Risk events are events representing those sides of the content of the activities that could develop unfavorably in achievement of the defined goals and which must be evaluated to determine the level of risk. After studying the characteristics of the particular organizational activities sets of potential risk events (risk areas) could be defined, which are analyzed and evaluated during the risk management process.

Symptoms are the risk events or scenarios, which enable transformation of the risk in problem. Some authors called risk symptoms with the term "risk triggers"[3].

The impact of risk is represented by the inability to achieve part of the pre-set organizational programs and projects goals. It affects areas related to the cost, time horizons for implementation and other aspects such as safety, quality, effectiveness, efficiency of operations, etc. The impact of risk is reflected by the consequences for the implementation of organizational programs and projects. Consequences of risk can be assessed qualitatively as negligible, medium, major and catastrophic or quantitatively using different scales.

The probability of occurrence of risk is expressed by the probability of transforming the risk in a problem. Quantification is expressed as an absolute value in the range from 0 to 1 and relative terms as a percentage from 0% to 100%. For example, depending on its size, the

***Corresponding author:** Venelin Georgiev, Information Technologies for Security Department, Institute on Information and Communication Technologies, Bulgarian Academy of Sciences, Bulgaria, E-mail: georgiev@defencemanagement.org

Received November 08, 2012; **Accepted** November 12, 2012; **Published** November 19, 2012

Citation: Georgiev V (2012) Risk Management Language and Concepts. J Def Manag 3:e119. doi:10.4172/2167-0374.1000e119

probability of occurrence of risk can be assessed as very low - from 0% to 20% lower - from 21% to 40% average - from 41% to 60% higher - from 61% to 80%, much higher - from 81% to 100%.

The risk index is a personal identification risk metric that serves as the ranking in the priority list of risks identified to a specific program or project. In the simplest case, the risk index is defined as the product of the estimated likelihood for realizing and the extend of anticipated consequences.

Property of chaining or risks connectivity for the organizational programs and projects has meant that a particular risk can lead to the emergence of a second, and he, in turn, to the emergence of the third, and so on, until it comes to failure to achieve objectives, costs and time limits for the implementation of programs and projects. As an example: the withdrawal of an important member of the project team (risk 1) can lead to a reduction in team capacity (risk 2), and hence the delay in the implementation of the project (risk 3) which is not acceptable for achieving the ultimate goals (impact risk). Some risks impact does not occur until the onset of the associated risks. Chaining risk affects the opportunities for aggregation. An effective strategy to mitigate the effects of risks aims to break chaining of the identified risks.

Conceptual apparatus in the field of risk management is extremely rich and diverse. In the literature other definitions of the above concepts could be found in the order to expand knowledge and language of risk. The next step in risk understanding is related to the risk management concept.

Risk management is a set of practices and procedures which allow for the identification, analysis, mitigation and control of risk before and during its transformation into a problem. It can be defined as a process of identifying and assessing risk, deciding to counteract it and monitoring the current condition and the emergence of new risks[4]. Planning as a part of risk management is seen as a process of developing and documenting systematic and comprehensive strategies, approaches and techniques for identifying risks, developing plans to counter the risk, performing continuous risk assessment to determine alterations, and resource planning for risk management.

Risk assessment is a process of risk identifying and analyzing. When identifying the risk areas and sources of risk to the organizational programs and projects are explored and identified and during the risk analysis the identified risks are examined to determine the probability of occurrence and the size of the expected consequences.

Risk counteracting is a process for identification, assessment, selection and implementation of appropriate strategies (techniques) to counteract the identified and evaluated risks in order to reduce the impact to acceptable levels set in advance in defining the assumptions and limitations of programs and projects. Risk monitoring is a process of systematic monitoring and evaluation of the strategies to counter the risk and developing improved or new ones. Counteraction is implemented using strategies, examples of which are:

- Avoidance of risk, where risk is countering by removing its causes;

- Transfer (sharing) risk by transferring the responsibility for the consequences of the implementation of risk (e.g., insurance);

- Containment of risk regarded as a technique to counter the risk, expressed in risk control through the establishment of adequate reserves, which cover the cost of mitigation.

- Counteract the risk by identifying alternative strategies to avoid the transformation of the risk into problem;

- Ignoring the risk, seen as the only alternative to counteract risk that does not apply the process of risk management. In these cases, the realization of organizational programs and projects do not take into account the existence of associated risk.

Risk management is an essential and important management concept that affects all organizational programs and projects and assisting managers in making informed and responsible decisions. At the same time the risk management process is organized and systematic evaluation and control of the associated in the organizational activities, programs and projects risk. This process involves the identification and analysis of risks, and development and implementation of effective measures against it.

Risk management is a vital tool to the success of any organization. It requires managerial support from the highest levels of the organizational management, understanding that the risk should be identified, analyzed and managed each day, and a commitment to quality performance of risk management activities. An effective process for risk management requires a high degree of commitment from all levels and departments of the organizational structure. The trend or standard is making risk management a priority policy and management activities for modern organization. Stressed the importance of risk management stems from the desire to reduce costs in the implementation of plans, programs and projects and increase the effectiveness of management in general.

Risk management could be seen as a challenge because it requires thinking that at first glance seems to be harmful and detrimental to the realization of the organizational programs and projects. Better identification of associated risks requires "negative" thinking and looking for potential problems. Amid constructive thinking, typical for the successful implementation of programs and projects, such "negative" thinking sounds weird. At the same time, the demand of difficulties and their management in a way that avoids surprises lead to the successful achievement of organizational goals.

Risk management should be considered as an integral part of the overall management of organizational activities. Well designed and precisely executed the risk management plan is a useful tool for balancing the goals of cost and time deadlines of the programs and projects. It is good to understand that risk management is not a separate function but integrated part of organizational management. Effective management of risk is related to the cost of resources. Studies show that rational conducted risk management can provide a return on investment made in it in relation to 1:20[5].

Organizational programs and projects and associated risks for which a comprehensive database exists could be evaluated and analyzed statistically, but from a practical point of view, there are no two completely identical objects, which excludes this possibility. Sometimes the implementation of programs and projects from the organizational portfolio is difficult for reasons with unique character that makes using the systematic approach in assessing and managing risk better than the intuitive approach. It is necessary to know and better understand

that the perception of risk assessment and risk management as a management practice or style may require modification of the decision making model.

To know or to understand the language of risk and risk concepts seems as a little step in the way of development but it is enormous achievement in the field of success.

Footnotes

1. Risk Management. AFMC Pamphlet 63-101. 1997.

2. American Systems Corporation. Risk Management Process and Implementation. 2003.
3. American Systems Corporation. Risk Management Process and Implementation. 2003.
4. Department of Commerce. Project Risk Management Guideline. 2004
5. Department of Commerce. Project Risk Management Guideline. 2004