

## RISK MANAGEMENT PLAN IN THE CASE OF AN INFRASTRUCTURE DEVELOPMENT PROJECT FUNDED BY THE SECTORAL OPERATIONAL PROGRAMME INCREASE OF ECONOMIC COMPETITIVENESS

Manuella Kadar<sup>1</sup>,  
Ioan Moise Achim<sup>2</sup>,  
Lucia Căbulea<sup>3</sup>

*ABSTRACT: This paper presents aspects of risk management plan achieved for the Project named „Platforma de cercetare multidisciplinara pentru coeziune interregionala si crestere a competitivitatii economice” (Multidisciplinary Research platform for interregional cohesion and increase of economic competitiveness), project that has been funded by the the Sectoral Operational Programme Increase of Economic Competitiveness in the period between 2009 - 2010. When taking about risks we have to accept that we are not dealing with reality! Therefore we enter into the field of prediction in which the approach is to estimate the level of risk on the bases of precise knowledge on “how the world is functioning”. A plan of risk management is useful and mostly required for the success of the project implementation.*

*Key words: risk management, plan, project control and monitoring.*

*JEL code:*

### **Theoretical background**

The concept of Risk Management as given by The Project Management Body of Knowledge Guide (PMBOOK) refers to the process of systemic identification, analysis and response to the risks of the project, process that is composed by sub processes such as risk identification, risk quantification, response plan to the risk, control of the response to the risk.

Bank of International Settlements (BIS) classifies the risk as follows: operational risks, legal risk, credit risk, risk of liquidity, risk of profit rate, risk on the market.

Another classification achieved by NetCom take into account the relation between the probability of the risk to happen and the impact (the severness of the risk). In this respect the tigers are with high probability and big Impact, alligators are of low Probability and Big Impact, the doggies of High Probability and Small Impact and the cats are of Low Probability and Small Impact.

Other scholars use to classify the risks as “known knowns”, “known unknowns”, “unknown unknowns”.

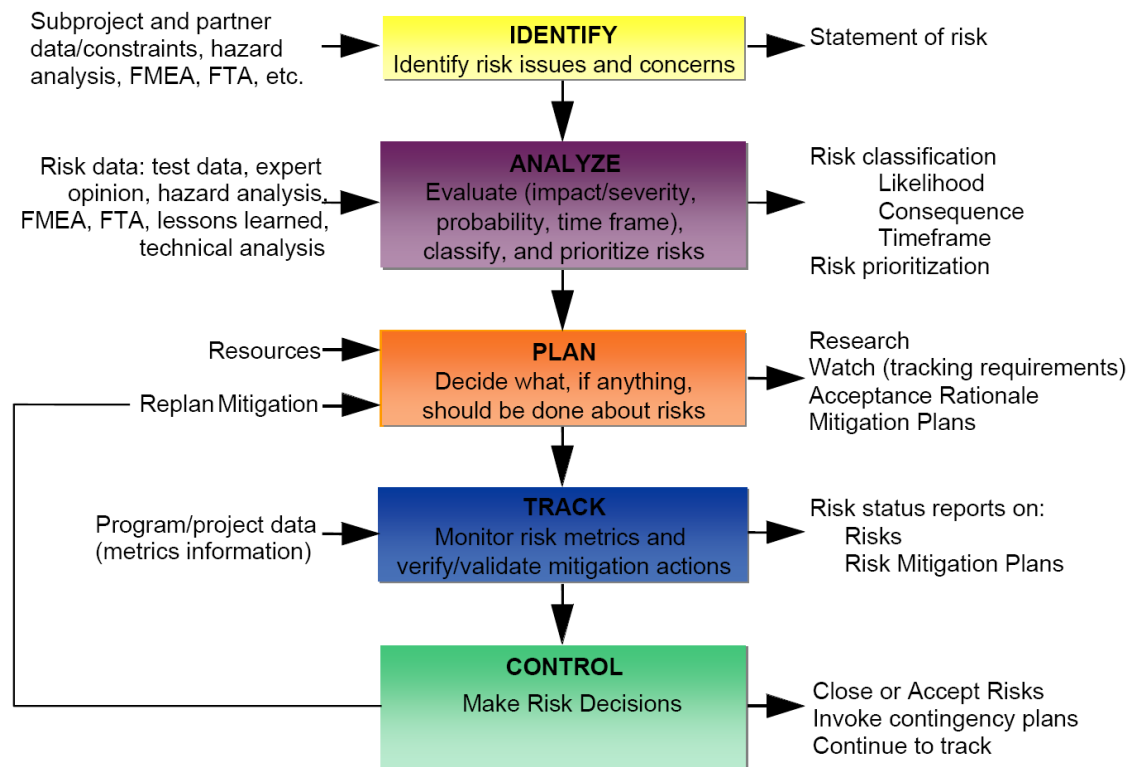
Risk differs from entity to entity therefore the plan of diminishing of the risk impact also differs. It is required in case of each project to establish some scenarios, calculate by using mathematical formulas between game miza, vulnerabilities and means of risk reduction. The establishment of the weights of scenarios and elaboration of covering means of insurance is very important in each project.

---

<sup>1</sup> “1 Decembrie 1918” University of Alba Iulia.

<sup>2</sup> “1 Decembrie 1918” University of Alba Iulia.

<sup>3</sup> “1 Decembrie 1918” University of Alba Iulia.



FMEA – Failure Modes and Effects Analysis  
FTA – Fault Tree Analysis

**Fig. no. 1. Continuous risk management process flow [8]**

### Methodology and examples

The risk management plan contains an analysis of likely risks with both high and low impact, as well as mitigation strategies to help the project avoid being derailed should common problems arise. Risk management plans should be periodically reviewed by the project team in order to avoid having the analysis become stale and not reflective of actual potential project risks.

Risk management plans include also risk strategy. Broadly, there are four potential strategies, with numerous variations. Projects may choose to:

- Accept the risk; simply take the chance that the negative impact will be incurred
- Avoid risk; changing plans in order to prevent the problem from arising
- Mitigate risk; lessening its impact through intermediate steps
- Transfer risk; outsource risk to a capable third party that can manage the outcome

**Identification.** Risk identification involves determining which risks might affect the project and documenting their characteristics. A risk is any event that could prevent the project from progressing as planned, or from successful completion. Risks can be identified from a number of different sources. Some may be quite obvious and will be identified prior to project kickoff. Others will be identified during the project lifecycle, and a risk can be identified by anyone associated with the project. Some risk will be inherent to the project itself, while others will be the result of external influences that are completely outside the control of the project team.

Table no. 1.

| <b>Risk identification</b> |             |                                      |                              |  |  |  |
|----------------------------|-------------|--------------------------------------|------------------------------|--|--|--|
| <b>Identification</b>      |             |                                      |                              |  |  |  |
| <b>Status</b>              | <b>ID #</b> | <b>Date Identified Project Phase</b> | <b>Functional Assignment</b> | <b>Threat/Opportunity Event</b>                                  | <b>SMART Column</b>  | <b>Risk Trigger</b>  |
| (2)                        | (3)         | (4)                                  | (5)                          | (6)  | (7)  | (8)  |
| Dormant                    | 1           | 16/07/09<br>PID                      | Infrastructure               | Dysfunction in the functioning of the university network         | Hardware and/or software problems at the application sever level (direct connection to users ) | Impossibility of access to the Web page  |
| Dormant                    | 2           | 16/07/09<br>PID                      | Infrastructure               | Dysfunction in the functioning of the university database server | Problems with the DBMS used by the application   | "Connection Error to the database"<br>The application is working, do not return valid data |
| Retired                    | 3           | 31/07/09<br>PA&ED                    | Infrastructure               | Lack of Internet connection                                      | Ping to external addresses return time-out   | Risk occurs when the service provider do not provide best quality services                 |
| Dormant                    | 4           | 19/09/10                             | Staff                        | Changes during the project implementation                        | 2 members of the team has quitted  | Risk due to the quitting of team members   |

**Qualitative analysis**

Qualitative analysis is the process of assessing the impact and the likelihood of identified risks. This process prioritizes risks according to their potential effect on project objectives. Risk assessment is the act of determining the probability that a risk will occur and the impact that event would have, should it occur. This is basically a “cause and effect” analysis. The “cause” is the event that might occur, while the “effect” is the potential impact to a project, should the event occur. Assessment of a risk involves two factors. First is the probability which is the measure of certainty that an event, or risk, will occur. This can be measured in a number of ways, but for the most projects will be assigned a probability percentage for 1% to 100%. A risk with no probability of occurring will obviously pose no threat, while a risk of 100% means the risk event has occurred.

Table no. 2.

| Quantitative analysis   |          |             |           |             |
|---|----------|-------------|-----------|-------------|
| Threat/Opportunity Event  | Type     | Probability | Impact    | Risk Matrix |
| (6)   | (9)      | (10)        | (11)      | (12)        |
| Dysfunctions in the functioning of the university network         | Scope    | Low         | High      |             |
|   |          |             |           |             |
| Dysfunctions in the functioning of the university database server | Scope    | Very Low    | High      |             |
|   |          |             |           |             |
| Lack of Internet connection                                       | Schedule | Very Low    | Very High |             |
|   |          |             |           |             |
| Changes during the project implementation                         | Schedule | Low         | Moderate  |             |
|   |          |             |           |             |

**Quantitative analysis**

The objective of quantitative risk analysis is to analyze numerically the probability of each risk and its consequence on the project objectives as well as the extent of the overall project risk.

The second factor is estimate of the impact on the project. This can be a subjective assessment, but should be quantified whenever possible. The estimated cost, the duration of the potential delay, the changes in scope and the reduction in quality are in most cases factors that can be estimated and documented in the risk statement and then measured using the standard project management tools (i.e. project plan, budget, statements of work).

Table no. 3.

| <b>Threat/Opportunity Event</b>                                   | <b>Probability (%)</b> | <b>Impact (\$ or days)</b> | <b>Effect (\$ or days)</b> |
|---|------------------------|----------------------------|----------------------------|
| Dysfunctions in the functioning of the university network         | 30%                    | 5.000                      | 1.500                      |
| Dysfunctions in the functioning of the university database server | 10%                    | 80.000                     | 8.000                      |
| Lack of Internet connection                                       | 10%                    | 50.000                     | 5.000                      |
| Changes during the project implementation                         | 50%                    | 4.000                      | 2.000                      |

**Response strategy**

Risk response planning is the process of developing options and determining actions to enhance opportunities and reduce threats to the project’s objectives.

The possible response options are:

- Avoidance – Change the project to avoid the risk. Change scope, objectives, etc.
- Transference – Shift the impact of a risk to a third party (like a subcontractor). It does not eliminate it, it simply shifts responsibility.
- Mitigation – Take steps to reduce the probability and/or impact of a risk. Taking early action, close monitoring, more testing, etc.
- Acceptance – Simply accept that this is a risk. When choosing acceptance as a response this is stating that given the probability of occurring and the associated impact to the project that results, they are not going to take any actions and will accept the cost, schedule, scope, and quality impacts if the risk event occurs.
- Deferred – A determination of how to address this risk will be addressed at a later time.

The results of the risk assessment process are documented in each Risk Statement and summarized in the Risk Register which will be reported on a monthly basis.

Table no. 4.

| <b>Response Strategy</b> |  |                                 |
|--------------------------|--|---------------------------------|
| <b>Strategy</b>          | <b>Response Actions including advantages and disadvantages</b> | <b>Affected WBS Tasks</b>       |
| (16)                     | (17)   | (18)                            |
| Mitigation               | Construction of a logical architecture with                    | 2.1 Achievement of the hardware |

|            |   |  |
|------------|---|--|
|            | application servers, functioning in cluster<br>Advantage: increase of the system availability<br>Disadvantages: costs increase  | infrastructure                         |
| Mitigation | Construction of a logical architecture with 2 database servers, functioning in cluster<br>Advantage: increase of the system availability<br>Disadvantages: costs increase | 2.2 Order & software acquisition       |
| Avoidance  | Routing of the server to another provider, with 2 Internet connections<br>Advantage: increase of the system availability<br>Disadvantage: costs increase                  | 1.2 Communication Center redevelopment |
| Acceptance | Risk has been accepted by the provider  | 3.2. Test of the application           |

### Monitoring and control

Risk monitoring and control is the process of keeping track of the identified risks, monitoring residual risks, ensuring the execution of risk plans and evaluating their effectiveness in reducing risks. As project activities are conducted and completed, risk factors and events will be monitored to determine if in fact trigger events have occurred that would indicate the risk is now a reality [9].

Table no. 5.

### Monitoring and control

| Monitoring and Control        |                                    |                                  |
|-------------------------------|------------------------------------|----------------------------------|
| Responsibility (Task Manager) | Status Interval or Milestone Check | Date, Status and Review Comments |

| (19)                   | (20)  | (21)   |
|------------------------|---|--|
| Infrastructure Manager | Equipment install   | The problem has been solved by adoption of a HA with 2 application servers |
| Infrastructure Manager | Software install  | The problem has been solved by adoption of a HA with 2 database servers    |
| Infrastructure Manager | Equipment install   | The problem has been solved by adoption of a HA with 2 providers           |
| Infrastructure Manager | Monitoring activities in the test phase and acceptance of the application<br>Monthly analysis of the number of extra paid hours | Assumed risk, taking into account the team members of the project          |

### Conclusions

Risk management is an ongoing process that continues through the life of a project. It includes processes for risk management planning, identification, analysis, monitoring and control. Many of these processes are updated throughout the project lifecycle as new risks can be identified at any time. It's the objective of risk management to decrease the probability and impact of events adverse to the project. On the other hand, any event that could have a positive impact should be exploited.

### References

1. Bourne L., 2007. Avoiding the successful failure, PMI Global Congress, [www.mosaicprojects.com.au](http://www.mosaicprojects.com.au)
2. Măzăreanu V.P., 2006. Reflecții pe marginea conceptului de risc, Revista de Audit Financiar, anul IV, nr.6/2006.
3. Mocanu M., Schuster C., 2001. Managementul proiectelor, Calea spre creșterea competitivității, Editura ALL BECK, București.
4. Project Management Institute, PMBOK Guide, 3rd edition, cap. XI, Project Risk Management la <http://www.pmi.org>

5. Somerville I, 2006. Management of software projects, Software Engineering, 7th edition, Ed. Pearson, la <http://www.cs.st-andrews.ac.uk/~ifs/Books/SE7/Presentations/index.html>
6. Weaver P., 2008. The Meaning of Risk in an Uncertain World, PMI Global Congress – EMEA, la [www.mosaicprojects.com.au/Resources/Papers.html/Risk#](http://www.mosaicprojects.com.au/Resources/Papers.html/Risk#)
7. <http://www.scribd.com/doc/18992727/Reflectii-Pe-Marginea-Conceptului-de-Risc>
8. [http://www.nasa.gov/pdf/413721main\\_ESMD-RMP-04.06\\_Rev\\_2\\_FINAL.pdf](http://www.nasa.gov/pdf/413721main_ESMD-RMP-04.06_Rev_2_FINAL.pdf) - 2010
9. [http://interop.mt.gov/content/docs/IM\\_Risk\\_Management\\_Plan\\_v4\\_0.pdf](http://interop.mt.gov/content/docs/IM_Risk_Management_Plan_v4_0.pdf) -2010