Risk Management in Information Systems Building

Vladimír Smejkal
court expert
Faculty of Business of Management
Brno University of Technology

Jana Fortinová
Faculty of Informatics and Statistics,
University of Economics in Prague
email: jana.fortinova@vse.cz

Abstract: *Risk management is one of the most important aspects in creating information systems. The most frequent reason for project failure is uncontrolled risk management where risks were not analyzed at all or insufficiently or counter-measure to reduce or eliminate potential risks were not adopted. The authors describe the approach that is based on the method of scenarios and the method of structured interviews but further quantifies the obtained information and, by creating a hierarchy of potential risks based on the probability of their materialization and the level of their impact, provides a clear instruction as to where to mostly focus in minimizing such risks.*

Key words: Information Systems, Information and Communication Technologies, Project Risks, Risk Analysis, Risk Management, Information Systems Security

1. Reasons for failure of implemented new IS/IT system projects

Lately the media have been discussing the problems with the new Central Vehicle Register that the Ministry of Transportation implemented. The contradictory and inconsistent information about the reasons why the register does not work would require a long analysis. However, the basic fact is that the register did not work the way it should for a long time after it was launched. Other projects were functioning and worked without any problem, but were not carried through as expected – e.g. IZIP (Internet Access to Patient Health Records). However, there are also examples where a system, whose launch was deemed by media-proficient announcers of bad news to be the biggest catastrophe after the flood of 2002, worked without any problem, and the volume of messages transmitted through the information system of data boxes keeps growing and messages delivered by login show a 97.4% success rate. We can see that there are positive and negative examples of IS building in public administration.

We should not focus only on public administration. There are also projects of private entities that were carried out without any major problem as well as those where the SAP information system was implemented so poorly that the company that planned to use IS almost went bankrupt.

Why are the results so different? How can we avoid a failure?

If we disregard sabotage, fraud and any other intentional crime, we can see that poor risk management is the most frequent reason. However, real good risk management should take into consideration even these extreme yet not impossible factors.

Many institutions and authors have analyzed the risk management of IS/IT projects, but with very different approaches. There are pre-project SWOT-type analyses, scenarios (RIPRAN method) [1], ITIL-type methodologies [2], the methods of management of IT services and information security pursuant to ISO 20000 and 27001 standards and the certification of an organization by a recognized certifying company [3]. In some cases, it is rather an assessment of project management and its success per se, while in other cases it is an informal risk assessment of the “if – then” type. The last mentioned case concerns a formal certification of the general environment (organization) but not an assessment of specific risks of a specific project in a specific situation.

The approach described below is based on the method of scenarios and the method of structured interviews but further quantifies the obtained information and, by creating a hierarchy of potential risks based on the probability of their materialization and the level of their impact, provides a clear instruction as to where to mostly focus in minimizing such risks.

2. Risk and how to manage it

We all know that there is a risk in going through a red light or being impolite to a tax officer. But this approach will not hold up in real risk management and therefore, it is necessary to know what a risk is and how we can work with it.

In older encyclopedias, risk is defined as courage or danger and “to risk” as to dare to do something. [5] Not until later was it also defined as a potential loss. [6] In technical standards, we can also see different definitions of risk: a combination of the probability of damage occurrence and the seriousness of such damage (ČSN EN ISO 12 100-1) or the effect of uncertainty to achieve goals (ČSN ISO 31000).

In general, we understand risk as **a possibility that a certain event, which differs from the expected situation or development, will occur with a certain probability**. However, risk should not be confused with, or reduced to, a mere probability since it includes both the actual probability and the quantitative scope of the given event (impact). [7]

Risk is most frequently mentioned in connection with a negative impact (although in general, the deviation can be also positive; however, nobody would probably say that there is a risk of winning a lottery). Therefore, the most adequate definition is the one according to which **risk is a situation where there is a possibility of an adverse deviation from the desired result that we hope or expect to achieve.**

In connection with IS/IT project management, we will thus be interested in the following:

1. What the potential project risks are;
2. How they can be eliminated or at least reduced.

Risk management is a process, during which the managing entity tries to prevent the effect of already existing or future factors and proposes solutions helping to eliminate adverse effects and enabling to take advantage of positive effects. Part of the risk management process is a decision-making process that is based on a risk analysis. After having considered additional factors, especially economic, technical, social, political and other factors, the managers of risk management develop, analyze and compare potential preventive and regulatory measures and select those that minimize the existing risk. [8]

In addition to a risk analysis, risk management usually includes:

1. Selection of counter-measures;
2. Cost-benefit analysis;
3. Implementation of counter-measures;
4. Testing (comprehensive verification) of counter-measures.

It is necessary to realize that risk management is a never-ending process that can be illustrated e.g. as follows [9]:

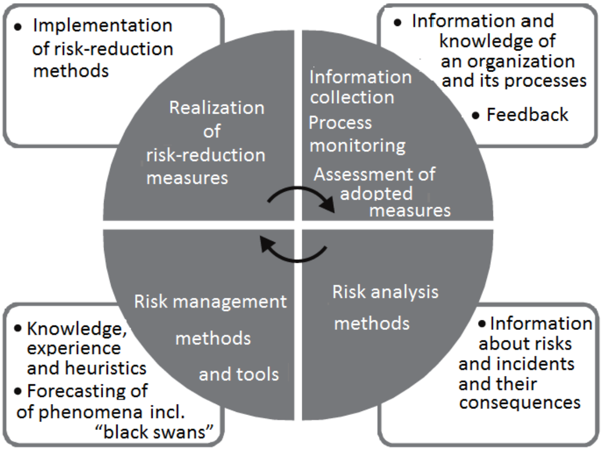

• Implementation of risk-reduction methods
Realization of risk-reduction measures
Information collection
Process monitoring
Assessment of adopted measures
• Information and knowledge of an organization and its processes
• Feedback
Risk management methods and tools
• Knowledge, experience and heuristics
• Forecasting of of phenomena incl. "black swans"
Risk analysis methods
• Information about risks and incidents and their consequences

Figure 1 Risk management as a process

3. Risk analysis methods

In analyzing IS/IT risks, the CRAMM method (CCTA Risk Analysis and Management Methodology) is probably the most famous. [10] It is mostly based on libraries that include about 3,500 security measures. Its advantage is that it complies with ISO/IEC 27002 and ISO/IEC 27001 requirements and that it is rather easy to obtain a large package of results thanks to automated processing. It is in fact an approach using gross calculating power and large databases, replacing the need of an individual approach and a deeper sophisticated analysis of solving specialists. The disadvantage of quantitative methods is, besides their high demand on results execution and processing, an often highly formalized procedure that can result in a failure to identify the specifics of an assessed entity, which can lead to its high vulnerability due to the "overload" of a recipient with a large volume of formally structured data. This can lead to a certain information overload that can be expressed by the phrase "one cannot see the forest for the trees."

On the other hand, qualitative methods are based on the description of the seriousness of a potential impact and on the probability that a given event will occur, where the impact level is usually determined by a qualified estimation and the method of structured interviews (Delphi method), which is based on a managed contact between the experts of the assessment group and the representatives of the assessed subject, is used. Qualitative methods are simpler and faster but more subjective, which can be sufficiently corrected by including experienced, highly qualified experts. The advantage of this method is that it is less source and/or time demanding and takes into consideration the specifics of an assessed system, its administrator, the environment, users, etc. The Delphi method is well suited for analyzing risks especially because it determines what can happen and under what conditions.

An interesting option is a combination of both methods where we assess risks (threats, probabilities, impacts) using a qualitative method and then using a quantitative approach, e.g. based on ČSN ISO/IEC 27005:2008. In this case, we start from the seriousness of the threat impact on the asset in the project or on the project itself and from the probability of the threat occurrence. We must take into consideration that this relationship depends on many other factors that can reflect both the actual risk of the project and the impact of system parameters.

Based on the potential financial or other impact of a loss, we can divide risks into the following groups:

- Critical risk: a threat whose potential losses are such that it can lead to a company’s bankruptcy or dissolution, political destabilization (the removal of a government member, civic unrest), large damages, a person’s bodily harm or potential death, etc. (a failed project can threaten or disable basic state functions – payment of benefits, the registration of motor vehicles or real estate and, in the case of private entities, production shutdown, default on contractual obligations);
- Major risk: a threat whose potential losses do not lead to bankruptcy but to remain in operation, a company (or state) will have to e.g. borrow funds or adopt another measure that exceeds regular operation – e.g. to sell a part of assets, to remove authorized persons, to carry out a media campaign, to initiate legal steps, etc., which will result in higher expenses and/or the delay of a project;
- Regular risk: a threat that is usual in the given area of activities and the resulting potential losses can be covered with current assets without causing inadequate financial pressure, i.e. a risk whose consequences are not threatening and a project can continue without major cost and time losses.

When we know the threats affecting individual assets of a project (or an entire project), the threat levels, the vulnerability of assets with respect to such threats and the probability of threat materialization, we can determine the level of risk of a given threat with respect to the assigned asset. We can express the level of risk R, using the function of two variables where **a** is the impact of a materialized threat (in connection to the asset value) and **h** is the probability of threat materialization (in connection to the vulnerability of a project (or an entire project):

$$R = f(\mathbf{a}, \mathbf{h})$$

The higher the risk level for the threat-asset pair is, the more effective measures must be implemented in order to eliminate the risk or to reduce the risk to an acceptable level.

To assess the level of individual risks (inherent, residual and target), we use the so-called total risk matrix – see below. When analyzing risks and before adopting measures to eliminate risks, we assess inherent risks (i.e. without taking into consideration the already existing or considered measures). After having implemented the measures, we reassess the level of risks while including the level of residual risk (after the measures were implemented) or the level of target risk (requested by the analysis recipient). The target risk is based on the strategic managerial decision where the level of a given risk is determined and fully accepted, which does not mean necessarily zero risk, especially if achieving zero risk would mean inadequate expenses or the lower functioning of a system.

The risk occurrence probability in the tables is defined as follows:

Occurrence probability		
Level	% per year	Description
1	<0; 5>	Practically improbable
2	<5; 20>	Not very probable
3	<20; 50>	Occasional
4	<50; 70>	Probable to frequent
5	<70; 100>	Very frequent

The impact is rated based on the level of consequences for an entity on a 1-5 scale. The numerical data thus do not express the value or quantity of a magnitude, but its applicability to a given area. The magnitudes that fall under the defined intervals thus to some extent eliminate the different quality (different levels of assessment) of obtained information. For details, see the cited standard or literature.

4. Project risks

The risk arising from poor project management is a risk that can occur both in construction and in building information systems.

Risk project assessment and management involves four steps that must be carried out repeatedly (or nonstop in the case of major projects):

1. Risk identification;
2. Risk assessment;
3. Risk plan preparation;
4. Risk monitoring and management

The main groups of risks in IS/IT are mainly as follows [11]:

ID	Name	Description
F	Financial	Project financing and cash flows, payment guarantees, exchange rate, inflation, taxes, subsidies, interest rates
G	Guarantees and services	All terms of guarantees and services, operating costs, SLA parameter setup, update and upgrade
L	Legislative and legal	Selection of a supplier in the case of a public contract, contract, changes in legal regulations, protection of copyrights and other intellectual property rights, damage compensation, complaints
M	Managerial	Time schedule, organizations participating in a project and the division of their responsibility, project team, qualifications, relationship to an organization, project management, personnel, training
P	Procurement	Selection of suppliers in general, terms of procurement, testing and acceptance
C	Commercial	Strategies, market, final user, requests and business terms, target country
T	Technical	IS definition and parameters, hardware, software, e-communication services, data security and protection

Some risk activities, e.g. data migration, are hard to categorize and depend on a more detailed specification of the risk source. In the case of the mentioned migration, it could be an organizational problem, i.e. managerial, but the compatibility problem, i.e. technical, or even a legal problem (the right to use data under certain agreed conditions).

In implementing IS/I in an organization, the authors defined the following threats:

Wrong strategy of the organization management

Ill-defined goals
Poorly formulated request
Limited finances
Selection proceedings with legal and factual defects
Poorly selected supplier
Bad contract – time-limits, sanctions, performance verification, testing and complaints, SLA setup, source text availability and usability
Poor communication, non-functioning information transmission
Disinterest of top management

Performance (project realization)

Poor division of competences and responsibilities
Non-functioning project management (steering committee etc.)
Poorly set up change management (uncontrolled quantity of changes as we go, budget increase, extended time-limits)
Poor estimation of system overload (necessary output and transmission capacities to identify response time)

Poor communication, non-functioning information transmission
Disinterest of top management, which is usually accompanied by delegating project management to a very low level of corporate hierarchy
Unwillingness of employees
Insufficient capacity of solving specialists
Changes in goals and system requirements
Incompliance of a proposal with a client's requests
Insufficient testing
Unrealistic time-limits
Interface that does not work in the environment
Changes in legislation
No data security and protection
Non-existing or bad documentation – user, administrator and other documentation
Unavailability of source texts and no opportunity to use them in an unlimited manner

Putting the system into operation

Unwillingness of employees
Poor assessment of key users' comments (inability to listen, disinterest in feedback)
Uncontrolled data migration
Poor communication, non-functioning information transmission
Non-existing or bad documentation – user, administrator and other documentation
Unavailability of source texts and no opportunity to use them in an unlimited manner
Poor training of users
Poor training of administrators
No data security and protection
Insufficient testing and poor-quality acceptance

Routine operation

Unwillingness of employees
Poorly set up change management (uncontrolled quantity of changes as we go)
Changes in legislation
Poor communication, non-functioning information transmission
Personnel security risks (accumulation of positions, neglecting the four-eye principle, absence of control mechanisms)
Non-existing or bad documentation – user, administrator and other documentation
Unavailability of source texts and no opportunity to use them in an unlimited manner
No data security and protection
No update (e.g. with respect to changes in legislation) and no upgrade (modernization, further product development)
Insufficient services

5. Reasons for threats

It is obvious that the mentioned and other threats of IS/IT building can have different reasons. They are very poignantly discussed in the paper [12] and they do not have to be necessarily at the level of the IT Department, but at any other level of a person responsible for project management and realization.

1) The project lacks human capital with required know-how and skills;
2) The project lacks experienced project managers;
3) The IT Department is overloaded with many processes;
4) IT does not monitor the impact of partial changes on an entire project;
5) IT does not know the current state of a project;
6) IT ignores problems;
7) IT failed to define the framework scope of an entire project;
8) IT does not take into consideration the interdependency of projects;
9) IT does not take into consideration Murphy’s law (does not expect the occurrence of unexpected events, the so-called black swans; [13])
10) IT does not pay attention to project change management;
11) IT ignores absurdly set up dates for finishing partial project activities;
12) Poor communication between IT, parties interested in the project and investors.

According to the authors, the reasons for threats in compliance with Voříšek [14] are key reasons and, after generalization, apply to public administration as well:

1. Ill-defined ideas regarding project reasons, meaning and goals due to a non-existing, ill-defined or wrong strategy of the organization management (governmental department);
2. Disinterest of top management, which is usually accompanied by delegating project management to a very low level of corporate hierarchy;
3. A project focuses on IT delivery and not on achieving the goal based on the strategy of the management of an organization, governmental department or state;
4. Insufficient specification of IS requirements, expansion of IS requirements and changes in creating a system;
5. Poor estimation of time and financial demands of a project;
6. Limited financing during project solving (e.g. due to a world economic crisis);
7. Bad contract; [15]
8. Insufficient or unsuitable process of testing and data migration;
9. Insufficient preparation of, and communication with, users or the public. Failure to involve them already during the proposal of a system. Ignoring socio-psychological aspects of the switch to (new) IS.

6. Consequences of threats

The materialization of threats usually has financial consequences (extra expenses, lost profit, legal expenses, damage compensation, etc.). But it can also have social-political consequences (the inability of a state or local government to ensure a certain activity stipulated by the law or arising from a competent authority's own decision) as well as legal consequences (violation of a law – e.g. the protection of personal data).

Some of them can be quantified (in particular financial consequences) but others cannot. In such a case, the aforesaid qualified estimation on a 1-5 scale comes in handy.

The authors consider the following to be key consequences:

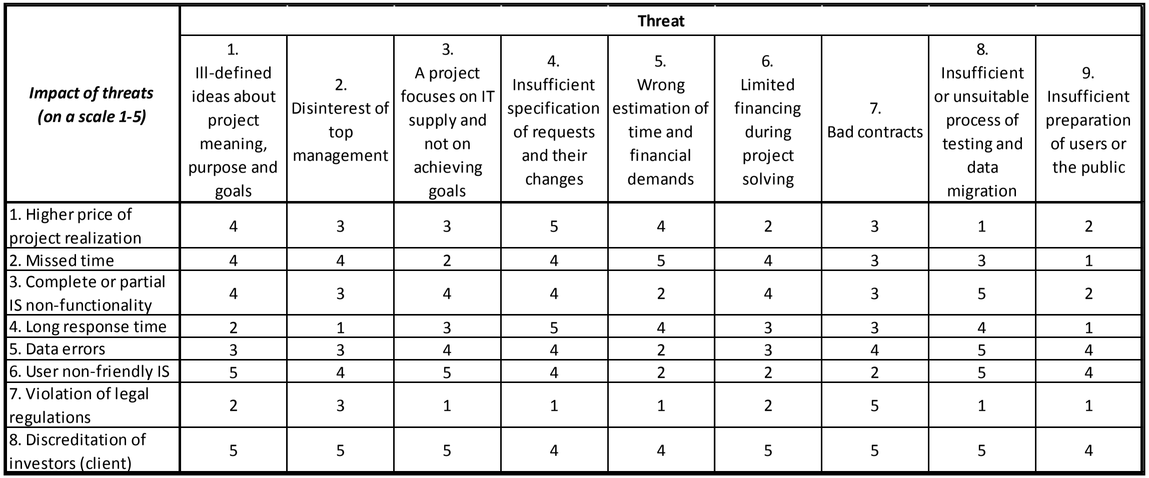
1. Higher price of project realization;
2. Missed time schedule;
3. Complete or partial IS non-functionality;
4. Long response time;
5. Data errors;
6. User non-friendly IS;
7. Violation of legal regulations;
8. Discreditation of investors (client).

7. Example of a risk analysis for the zeppelin register

In order to avoid any connotation of existing problems, the authors prepared an example of a risk analysis for a fictitious zeppelin register that was originally operated in an obsolete application on personal computers in the Foxbase database and communicated with users with command prompt. Data were batch loaded in the central computer every night. This system was operated by the Ministry of Land Transportation. It was a political request to create a new register that would be modern, beautiful, colorful and graphical as well as highly secured, fast and interconnected to similar registers in other EU states and would be operated by the Ministry of Air Transportation.

The analysis was performed for the major threats, as shown under Items 1 through 7 above, with the results shown below. It is an assessment of the inherent risk, i.e. the risk in the given environment before adapting risk-reduction measures.

It is a model example, but in reality we could and should differentiate individual risks in more detail. For instance, bad contracts could have the following subcategories: performance specification, time schedule, a provider's obligations, a client's obligations, the protection of intellectual property rights, the rights to source texts, guarantees, damage compensation, sanctions, a major breach of contract, acceptance, contract termination, etc.



Impact of threats (on a scale 1-5)	**Threat**								
	1. Ill-defined ideas about project meaning, purpose and goals	2. Disinterest of top management	3. A project focuses on IT supply and not on achieving goals	4. Insufficient specification of requests and their changes	5. Wrong estimation of time and financial demands	6. Limited financing during project solving	7. Bad contracts	8. Insufficient or unsuitable process of testing and data migration	9. Insufficient preparation of users or the public
1. Higher price of project realization	4	3	3	5	4	2	3	1	2
2. Missed time	4	4	2	4	5	4	3	3	1
3. Complete or partial IS non-functionality	4	3	4	4	2	4	3	5	2
4. Long response time	2	1	3	5	4	3	3	4	1
5. Data errors	3	3	4	4	2	3	4	5	4
6. User non-friendly IS	5	4	5	4	2	2	2	5	4
7. Violation of legal regulations	2	3	1	1	1	2	5	1	1
8. Discreditation of investors (client)	5	5	5	4	4	5	5	5	4

Figure 2 Threat assessment

Probability of threats (on a scale 1-5)	**Threat**								
	1. Ill-defined ideas about project meaning, purpose and goals	2. Disinterest of top management	3. A project focuses on IT supply and not on achieving goals	4. Insufficient specification of requests and their changes	5. Wrong estimation of time and financial demands	6. Limited financing during project solving	7. Bad contracts	8. Insufficient or unsuitable process of testing and data migration	9. Insufficient preparation of users or the public
1. Higher price of project realization	4	4	4	4	3	2	2	3	2
2. Missed time	2	4	3	5	4	4	2	4	3
3. Complete or partial IS non-functionality	3	1	4	4	2	4	1	5	3
4. Long response time	1	1	3	2	2	3	1	4	2
5. Data errors	1	1	4	3	2	3	3	4	4
6. User non-friendly IS	2	2	5	3	3	2	1	4	3
7. Violation of legal regulations	1	3	1	1	1	1	3	1	1
8. Discreditation of investors (client)	4	3	4	2	3	3	3	4	3

Figure 3 Estimated probability of threat materialization

Risk = impact + probability	Threat								
Impact of threats	1. Ill-defined ideas about project meaning, purpose and goals	2. Disinterest of top management	3. A project focuses on IT supply and not on achieving goals	4. Insufficient specification of requests and their changes	5. Wrong estimation of time and financial demands	6. Limited financing during project solving	7. Bad contracts	8. Insufficient or unsuitable process of testing and data migration	9. Insufficient preparation of users or the public
1. Higher price of project realization	8	7	7	9	7	4	5	4	4
2. Missed time schedule	6	8	5	9	9	8	5	7	4
3. Complete or partial IS non-functionality	7	4	8	8	4	8	4	10	5
4. Long response time	3	2	6	7	6	6	4	8	3
5. Data errors	4	4	8	7	4	6	7	9	8
6. User non-friendly IS	7	6	10	7	5	4	3	9	7
7. Violation of legal regulations	3	6	2	2	2	3	8	2	2
8. Discreditation of investors (client)	9	8	9	6	7	8	8	9	7

Figure 4 Final risk assessment

The darkest color risks fall under the category “must be resolved immediately” while the gray color risks mean “must be resolved.” As soon as the risk-reduction measures are adopted (in the selected category “bad contract” e.g. an external legal audit before a contract is signed, the opinion of the Office for the Protection of Competition, an expert opinion, etc.), we will make a reassessment and examine whether or not the threat probability is lower. If so, the table of risks will change and the inherent risk will become the residual risk. We must then assess whether or not it is the target risk or it is necessary to adopt another measure.

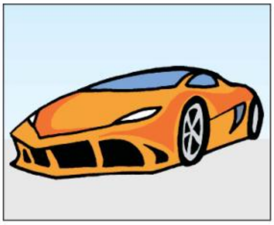
8. Conclusion

Objectively speaking, risk management is a never-ending, continuous process that takes place within us and around us in our everyday professional and personal life. We can see examples of uncontrolled risks every day – accidents, injuries, disasters, damages, divorce or crime.

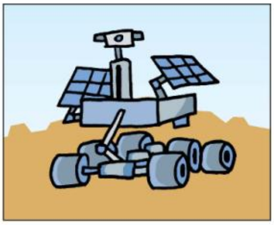
Unfortunately, underestimating risks (we will see what will happen), disregarding risks (could this really happen?), relying on good luck (nothing ever happened), lack of knowledge (a risk can be somehow managed?) or greediness (we will definitely not increase our costs) usually lead to tragedies, such as insolvency proceedings, media scandals, removal from office or even the fall of a government.

The ability to recognize on time and to effectively manage risks becomes an integral part of strategic management and nowadays not only in the case of business companies. Risk reduction is even more important for public administration authorities – from state governments to local governments. Risk management should be a matter-of-fact of all projects that the state realizes: from purely legislative projects (amendments of laws or implementing regulations and passing new bills) to IS/IT projects that are the subject-matter of this paper.

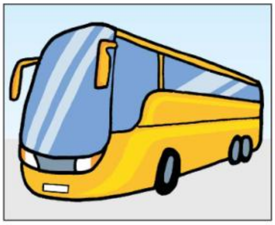
The entities that fail to recognize on time the scope and force of the impact of related risks and to create an effective mechanism for risk management gamble with their own stability, wind down the interest and trust of their investors (sponsors, the public) and thus increase their cost of financing (deplete the state or private budget).



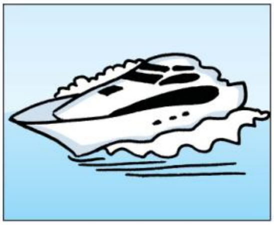
Client´s request



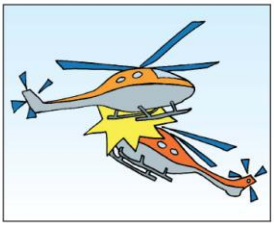
Specification under the contract



Project manager interpretation



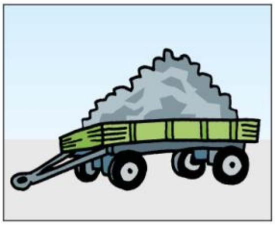
Consultant´s definition



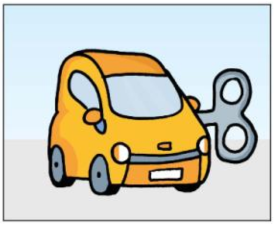
Risk based on an analysis

Draft of an analyst

Programmer´s output

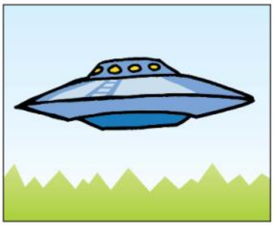


Performance in accordance with documentation

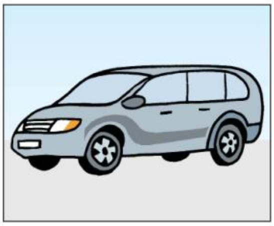


What was installed

What was invoiced



What the project´s report contained



What the client really needed

***Acknowledgement**: This paper is prepared as one of the outputs of the research project No. P403-10-0092 Advanced Principles and Models for Enterprise ICT Management by the Grant Agency of Czech Republic.*

9. Literature

[1] Doležal, J., Máchal, P., Lacko, B. et al. *Projektový management podle IPMA (Project Management According to IPMA)*, updated and extended edition. Prague: GRADA, 2012, p. 83 et sequentur

[2] www.itil.cz

[3] E.g. Det Norske Veritas, see www.dnv.com

[4] Smejkal, V., Rais, K. *Řízení rizik ve firmách a jiných organizacích (Risk Management in Companies and Other Organizations)*. 3rd edition. Prague: GRADA, 2009, p. 90 – 91

[5] *Ottův obchodní slovník (Otto Commercial Dictionary)*, Prague 1924

]6] *Masarykův slovník naučný (Masaryk Encyclopedia)*, Prague 1932

[7] Pearce, D. W.: *Macmillanův slovník moderní ekonomie (Macmillan Dictionary of Modern Economics)*. Victoria Publishing, Prague 1995, p. 361

[8] Smejkal, V., Rais, K. *Řízení rizik ve firmách a jiných organizacích (Risk Management in Companies and Other Organizations)*. 3rd edition. Prague: GRADA, 2009, p. 112.

[9] Ibid, p. 118

[10] www.cramm.com

[11] Korecký, M. Trkovský, V. *Management rizik projektů – se zaměřením na projekty v průmyslových podnicích (Project Risk Management Focusing on Projects in Industrial Enterprises)*. Prague: Grada, 2011, p. 180.

[12] Levinson, M. and Krupičková, I. *13 nejčastějších chyb v IT projektech (The 13 Most Frequent Mistakes in IT Projects)*. CIO Business World, 20. 8. 2010. http://businessworld.cz/business-rizeni-podniku/13-nejcastejsich-chyb-v-it-projektech-6742.

[13] Taleb, N. N. *The Black Swan. The Impact of the Highly Improbable.* Penguin Books Ltd., 2008.

[14] Voříšek, J. *Kritické faktory úspěchu a rizika informačních system (Critical Factors of Success and Information System Risks).* 1996. Available at http://nb.vse.cz/~vorisek/FILES/Clanky/1996_Csf_a_rizika_IS.htm.

[15] Smejkal, V., Rais, K. *Řízení rizik ve firmách a jiných organizacích (Risk Management in Companies and Other Organizations)*. 3rd edition. Prague: GRADA, 2009, p. 299 et sequentur.

JEL Classification C83, M15