

Riadenie projektových rizík podľa medzinárodných noriem a metodík

Róbert Kormaňák, R.K.C., spol. s r. o. Trnava
Bratislava, 19.4.2017

eFOCUS



Agenda

- Základné pojmy
- Projektové riziká podľa Prince2
- Projektové riziká podľa PMBoK
- Porovnanie
- Praktické príklady / odporúčania
- Závery

opportunity

An uncertain event that would have a favourable impact on objectives or benefits if it occurred.

risk

An **uncertain event** or set of events that, should it occur, will have an effect on the achievement of **objectives**. A risk is measured by a combination of the **probability** of a perceived **threat** or **opportunity** occurring and the magnitude of its **impact** on objectives.

impact

Impact is the result of a particular threat or opportunity actually occurring.

threat

An uncertain event that could have a negative impact on objectives or benefits.

probability

This is the evaluated likelihood of a particular threat or opportunity actually happening, including a consideration of the frequency with which this may arise.

business risk

Failure to achieve business **objectives/benefits**.

operational risk

Failure to achieve **business/organizational** objectives due to human error, system failures and/or inadequate procedure and controls.

programme risk

Risk concerned with transforming high-level **strategy** into new ways of working to deliver benefits to the organization.

project risk

Project risks are those concerned with the successful completion of the **project**. Typically these risks include personal, technical, cost, schedule, resource, operational support, quality and supplier issues.

Vývoj štandardov HMO



Best Practices published by OGC are distributed and maintained by Public-Private company Axelos

Riadenie rizík podľa Prince2 (a)

8.1 PURPOSE

The purpose of the Risk theme is to identify, assess and control uncertainty and, as a result, improve the ability of the project to succeed.

8.2.1 What is a risk?

A risk is an uncertain event or set of events that, should it occur, will have an effect on the achievement of objectives. It consists of a combination of the probability of a perceived threat or opportunity occurring, and the magnitude of its impact on objectives, where:

- **Threat** is used to describe an uncertain event that could have a negative impact on objectives
- **Opportunity** is used to describe an uncertain event that could have a favourable impact on objectives.

8.2.2 What is at risk?

In the context of a project, it is the project's objectives that are at risk. These will include completing the project to a number of targets, typically covering time, cost, quality, scope, benefits and risk.

8.2.3 What is risk management?

The term risk management refers to the systematic application of procedures to the tasks of identifying and assessing risks, and then planning and implementing risk responses. This provides a disciplined environment for proactive decision making.

For risk management to be effective, risks need to be:

- **Identified** This includes risks being considered that could affect the achievement of the project's objectives, and then described to ensure that there is a common understanding of these risks
- **Assessed** This includes ensuring that each risk can be ranked in terms of estimated likelihood, impact and immediacy, and understanding the overall level of risk associated with the project
- **Controlled** This includes identifying appropriate responses to risks, assigning risk owners, and then executing, monitoring and controlling these responses.

Riadenie rizík podľa Prince2 (b)

8.3.4 Risk Register

The purpose of the Risk Register is to capture and maintain information on all of the identified threats and opportunities relating to the project. Each risk on the Risk Register is allocated a unique identifier as well as details such as:

- Who raised the risk
- When it was raised
- The category of risk
- The description of the risk (cause, risk event, effect)
- Probability, impact and expected value
- Proximity
- Risk response category
- Risk response actions
- Risk status
- Risk owner
- Risk actionee.

Project Support will typically maintain the Risk Register on behalf of the Project Manager. The Risk Management Strategy will describe the procedure for registering risks and maintaining the risk register.

8.3.5 Risk management procedure

PRINCE2 recommends a risk management procedure comprising the following five steps:

- Identify (context and risks)
- Assess (i.e. Estimate and Evaluate)
- Plan
- Implement
- Communicate.

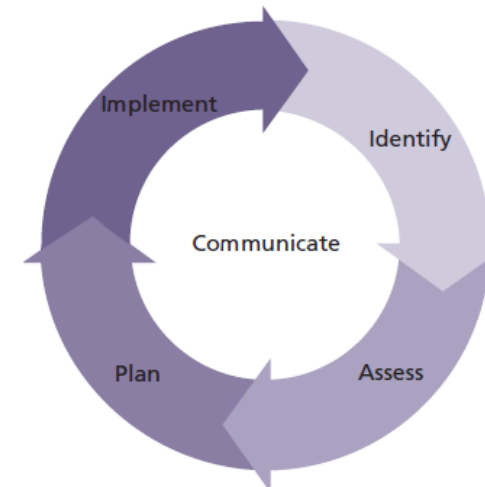


Figure 8.2 The risk management procedure

Riadenie rizík podľa Prince2 (c)

Risk Identification techniques

Risks can be identified using a number of techniques, such as:

- **Review lessons** Risks are driven by uncertainty, so one of the most effective ways to reduce uncertainty is to review similar previous projects to see what threats and opportunities affected them
- **Risk checklists** These are in-house lists of risks that have either been identified or have occurred on previous similar projects. Risk checklists are useful aids to ensure that risks identified on previous projects are not overlooked
- **Risk prompt lists** These are publicly available lists that categorize risks into types or areas and are normally relevant to a wide range of projects. Risk prompt lists are useful aids to help stimulate thinking about sources of risk in the widest context



- **Brainstorming** This enables group thinking, which can be more productive than individual thinking. However, it is important to avoid criticism during the brainstorm as this can stop people contributing. In addition to identifying risks, brainstorming can also be used to understand the stakeholders' views of the risks identified
- **Risk breakdown structure** This is a hierarchical decomposition of the project environment assembled to illustrate potential sources of risk. Each descending level represents an increasingly detailed definition of sources of risk to the project. The structure acts as a prompt and an aid to support the project management team in thinking through the potential sources of risk to the objectives. There are numerous ways to break down risk and it may be useful to do more than one list. For example, a risk breakdown structure could be broken down by PESTLE (political, economical, sociological, technological, legal/legislative, environmental), product breakdown structure, stage, benefits/objectives etc. Figure 8.3 shows a risk breakdown structure relating to financial risk. These structures will help to identify appropriate risk owners to develop responses.

Riadenie rizík podľa Prince2 (d)

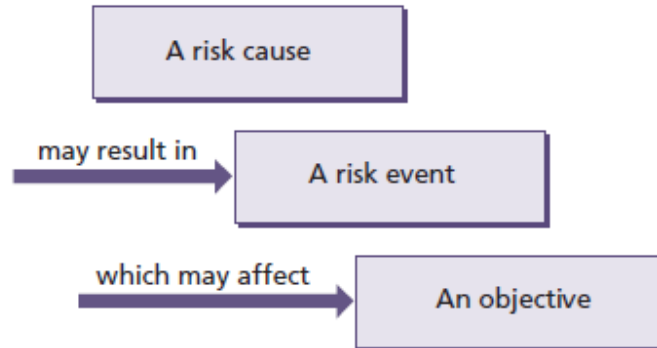


Figure 8.4 Risk cause, event and effect

- **Risk cause** This should describe the source of the risk, i.e. the event or situation that gives rise to the risk. These are often referred to as risk drivers. They are not risks in themselves, but the potential trigger points for risk. These may be either internal or external to the project
- **Risk event** This should describe the area of uncertainty in terms of the threat or the opportunity
- **Risk effect** This should describe the impact(s) that the risk would have on the project objectives should the risk materialize.

Very high				1 3	
High	2				4
Medium		8		6	
Low		10		7	
Very low	9		2		5
Prob. Impact	Very low	Low	Medium	High	Very high

----- Risk tolerance line

Figure 8.6 Summary risk profile

Riadenie rizík podľa Prince2 (e)



Probability	0.9	Very high 71–90%	0.045	0.09	0.18	0.36	0.72
	0.7	High 51–70%	0.035	0.07	0.14	0.28	0.56
	0.5	Medium 31–50%	0.025	0.05	0.10	0.20	0.40
	0.3	Low 11–30%	0.015	0.03	0.06	0.12	0.24
	0.1	Very low up to 10%	0.005	0.01	0.02	0.04	0.08
			Very low	Low	Medium	High	Very high
			0.05	0.1	0.2	0.4	0.8
			Impact				

Figure 8.5 Probability Impact grid

Riadenie rizík podľa Prince2 (f)



Threat responses	Opportunity responses
Avoid	Exploit
Reduce (probability and/or impact) Fallback (reduces impact only) Transfer (reduces impact only, and often only the financial impact)	Enhance
Share	
Accept	Reject

Figure 8.7 Threat and opportunity responses

Riadenie rizík podľa Prince2 (f)



Threat responses	Opportunity responses
Avoid	Exploit
Reduce (probability and/or impact) Fallback (reduces impact only) Transfer (reduces impact only, and often only the financial impact)	Enhance
Share	
Accept	Reject

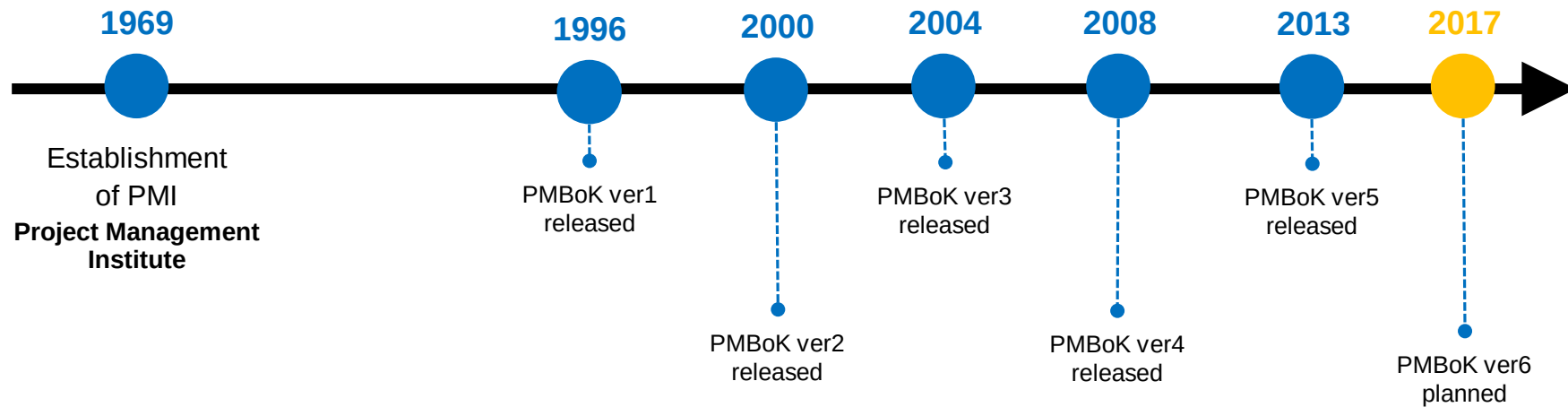
Figure 8.7 Threat and opportunity responses

Riadenie rizík podľa Prince2 (g)

Table 8.2 Risk responses

Response	Definition	Example
<u>Avoid</u> (threat)	Typically involves changing some aspect of the project, i.e. the scope, procurement route, supplier or sequence of activities, so that the threat either can no longer have an impact or can no longer happen.	A critical meeting could be threatened by air travel disruption so the project chooses to hold the meeting by conference call instead.
<u>Reduce</u> (threat)	Proactive actions taken to: ■ Reduce the probability of the event occurring, by performing some form of control ■ Reduce the impact of the event should it occur.	To reduce the likelihood of users not using a product, the number of training events is increased. To reduce the timescale impact should a prototype be damaged in transit, two prototypes are built.
<u>Fallback</u> (threat)	Putting in place a fallback plan for the actions that will be taken to reduce the impact of the threat should the risk occur. This is a reactive form of the 'reduce' response which has no impact on likelihood.	The company's test facility is only available for two weeks in August. To reduce the impact should the product not be available in time, there is a fallback plan to hire an alternate test facility (at a greater expense).
<u>Transfer</u> (threat)	A third party takes on responsibility for some of the financial impact of the threat. (For example, through insurance or by means of appropriate clauses in a contract.) This is a form of the 'reduce' response which only reduces the financial impact of the threat.	To reduce the financial impact should a prototype be damaged in transit, it is insured. To reduce the financial impact if a product is not available to launch in time for a trade show, the contract with the supplier includes liquidated damage clauses for any delays.
<u>Accept</u> (threat)	A conscious and deliberate decision is taken to retain the threat, having discerned that it is more economical to do so than to attempt a threat response action. The threat should continue to be monitored to ensure that it remains tolerable.	There is a threat that a competitor may launch a rival product first, thus affecting the expected market share for the product. The choice is to accelerate the project by increasing the resources, to reduce the product's scope so that it can be finished earlier, or to do nothing.

Riadenie rizík podľa PMBoK



Riadenie rizík podľa PMBoK (a)

11

PROJECT RISK MANAGEMENT



Project Risk Management includes the processes of conducting risk management planning, identification, analysis, response planning, and controlling risk on a project. The objectives of project risk management are to increase the likelihood and impact of positive events, and decrease the likelihood and impact of negative events in the project.

- *Risk appetite*, which is the degree of uncertainty an entity is willing to take on in anticipation of a reward.
- *Risk tolerance*, which is the degree, amount, or volume of risk that an organization or individual will withstand.
- *Risk threshold*, which refers to measures along the level of uncertainty or the level of impact at which a stakeholder may have a specific interest. Below that risk threshold, the organization will accept the risk. Above that risk threshold, the organization will not tolerate the risk.

Riadenie rizík podľa PMBoK (b)

Table 11-1. Definition of Impact Scales for Four Project Objectives

Defined Conditions for Impact Scales of a Risk on Major Project Objectives (Examples are shown for negative impacts only)					
Project Objective	Relative or numerical scales are shown				
	Very low /0.05	Low /0.10	Moderate /0.20	High /0.40	Very high /0.80
Cost	Insignificant cost increase	< 10% cost increase	10 – 20% cost increase	20 – 40% cost increase	> 40% cost increase
Time	Insignificant time increase	< 5% time increase	5 – 10% time increase	10 – 20% time increase	> 20% time increase
Scope	Scope decrease barely noticeable	Minor areas of scope affected	Major areas of scope affected	Scope reduction unacceptable to sponsor	Project end item is effectively useless
Quality	Quality degradation barely noticeable	Only very demanding applications are affected	Quality reduction requires sponsor approval	Quality reduction unacceptable to sponsor	Project end item is effectively useless
This table presents examples of risk impact definitions for four different project objectives. They should be tailored in the Risk Management Planning process to the individual project and to the organization's risk thresholds. Impact definitions can be developed for opportunities in a similar way.					

Riadenie rizík podľa PMBoK (c)

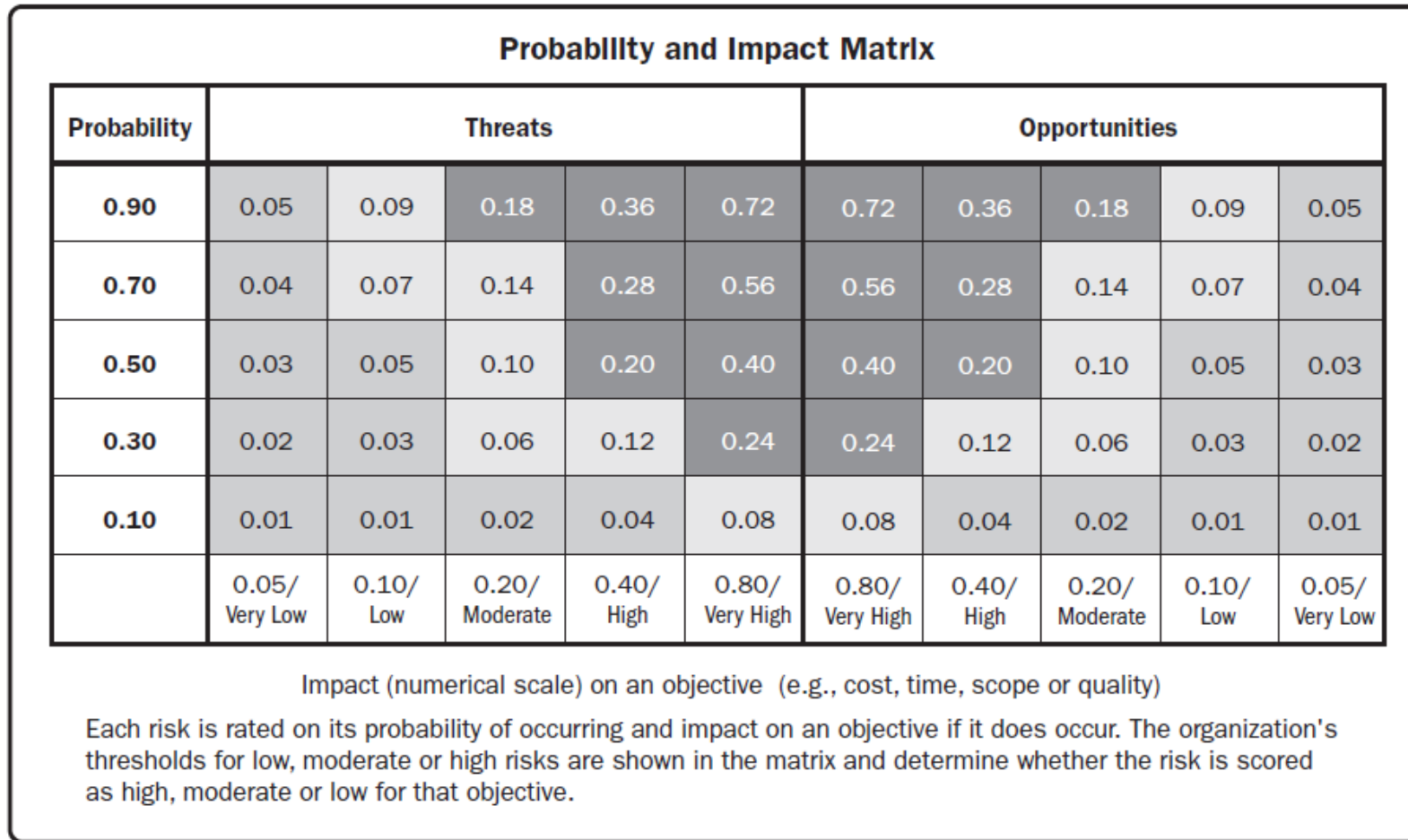


Figure 11-10. Probability and Impact Matrix

Riadenie rizík podľa PMBoK (d)

- **Avoid.** Risk avoidance is a risk response strategy whereby the project team **acts to eliminate the threat** or protect the project from its impact. It usually involves changing the project management plan to eliminate the threat entirely. The project manager may also isolate the project objectives from the risk's impact or change the objective that is in jeopardy. Examples of this include extending the schedule, changing the strategy, or reducing scope. The most radical avoidance strategy is to shut down the project entirely. Some risks that arise early in the project can be avoided by clarifying requirements, obtaining information, improving communication, or acquiring expertise.
- **Transfer.** Risk transference is a risk response strategy whereby the project team **shifts the impact of** a threat **to a third party**, together with ownership of the response. Transferring the risk simply gives another party responsibility for its management—it does not eliminate it. Transferring does not mean disowning the risk by transferring it to a later project or another person without his or her knowledge or agreement. Risk transference nearly always involves payment of a risk premium to the party taking on the risk. Transferring liability for risk is most effective in dealing with financial risk exposure. Transference tools can be quite diverse and include, but are not limited to, the use of insurance, performance bonds, warranties, guarantees, etc. Contracts or agreements may be used to transfer liability for specified risks to another party. For example, when a buyer has capabilities that the seller does not possess, it may be prudent to transfer some work and its concurrent risk contractually back to the buyer. In many cases, use of a cost-plus contract may transfer the cost risk to the buyer, while a fixed-price contract may transfer risk to the seller.

11.5.2.1 Strategies for Negative Risks or Threats

Riadenie rizík podľa PMBoK (e)

- **Mitigate.** Risk mitigation is a risk response strategy whereby the project team **acts to reduce the probability of occurrence or impact of a risk.** It implies a reduction in the probability and/or impact of an adverse risk to be within acceptable threshold limits. Taking early action to reduce the probability and/or impact of a risk occurring on the project is often more effective than trying to repair the damage after the risk has occurred. Adopting less complex processes, conducting more tests, or choosing a more stable supplier are examples of mitigation actions. Mitigation may require prototype development to reduce the risk of scaling up from a bench-scale model of a process or product. Where it is not possible to reduce probability, a mitigation response might address the risk impact by targeting linkages that determine the severity. For example, designing redundancy into a system may reduce the impact from a failure of the original component.
- **Accept.** Risk acceptance is a risk response strategy whereby the project team decides to acknowledge the risk and **not take any action unless the risk occurs.** This strategy is adopted where it is not possible or cost-effective to address a specific risk in any other way. This strategy indicates that the project team has decided not to change the project management plan to deal with a risk, or is unable to identify any other suitable response strategy. This strategy can be either passive or active. Passive acceptance requires no action except to document the strategy, leaving the project team to deal with the risks as they occur, and to periodically review the threat to ensure that it does not change significantly. The most common active acceptance strategy is to establish a contingency reserve, including amounts of time, money, or resources to handle the risks.

11.5.2.1 Strategies for Negative Risks or Threats

Porovnanie protirizikových stratégií

Prince2	PMBok
Avoid	Avoid
Reduce (prob. & impact) Fallback (impact only)	Mitigate
Transfer	Transfer
Share	n.a.
Accept	Accept

Praktické príklady

- Najreálnejšie riziká spoznáme na základe „lessons learned“ (skúsenosti z minulosti, analógie)
- Väčšinu projektových rizík nájdeme v hierarchickej štruktúre prác projektu - WBS (príklad „úradný poplatok 10 Euro“)
- Kľúčovým rizikom každého projektu sú jeho stakeholderi-zúčastnené strany (príklad „cyklo-klub“)

Róbert Kormaňák



- Vzdelanie
 - MFF UK Bratislava – Mgr. 1991
 - PrF TU Trnava – Mgr. 2008
 - Prince2 Practitioner, MSP Practitioner, P3O Foundation,
 - Auditor ISO 9000, ISO 20000, ISO 27000
 - ITIL Foundation, SCRUM, Six Sigma, EOQ Manažér kvality
- Členstvo v odborných asociáciách
 - PMI Slovensko
 - Slovenská spoločnosť pre kvalitu
- Členstvo v technických komisiách STN
 - TK22 – kvalita, riadenie rizík, riadenie projektov
 - TK37 – softvérové inžinierstvo, riadenie IT služieb
- Delegát v medzinárodných technických komisiách ISO
 - TC258 – Project, Program and Portfolio Management
 - JTC1/SC7 – Software and systems engineering
 - JTC1/SC40 – IT Service Management and IT Governance

Ďakujeme za pozornosť

