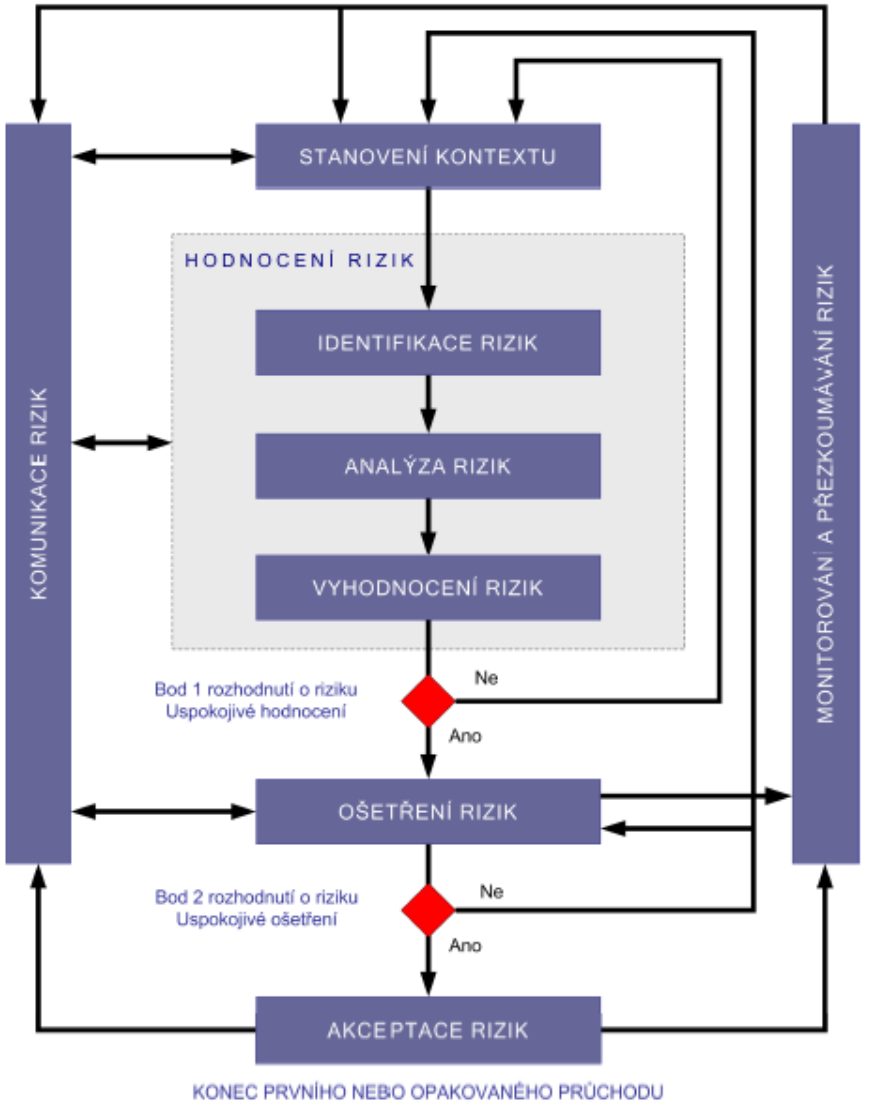
Proces riadenia rizík

RNDr. JUDr. Pavol Sokol, PhD., Msc. Terézia Mezešová

2017/2018

Riadenie rizík



Stanovenie kontextu

Vstup: Všetky informácie o organizácii

Činnosť:

- základné kritéria pre riadenie rizík
- Definícia rozsahu a hraníc
- Stanovenie príslušnej organizačnej štruktúry
- Stanovenia účelu (právna zhoda, GDPR a pod.)

Stanovenie kontextu – základné kritéria

- Kritéria hodnotenia rizík
- Kritéria dopadu
- Kritéria akceptácie rizík

Posúdenie rizík

Posúdenie rizík pozostáva:

1) Identifikácia rizík
2) Analýza rizík
3) Hodnotenie rizík

Posúdenie rizík - Identifikácia rizík

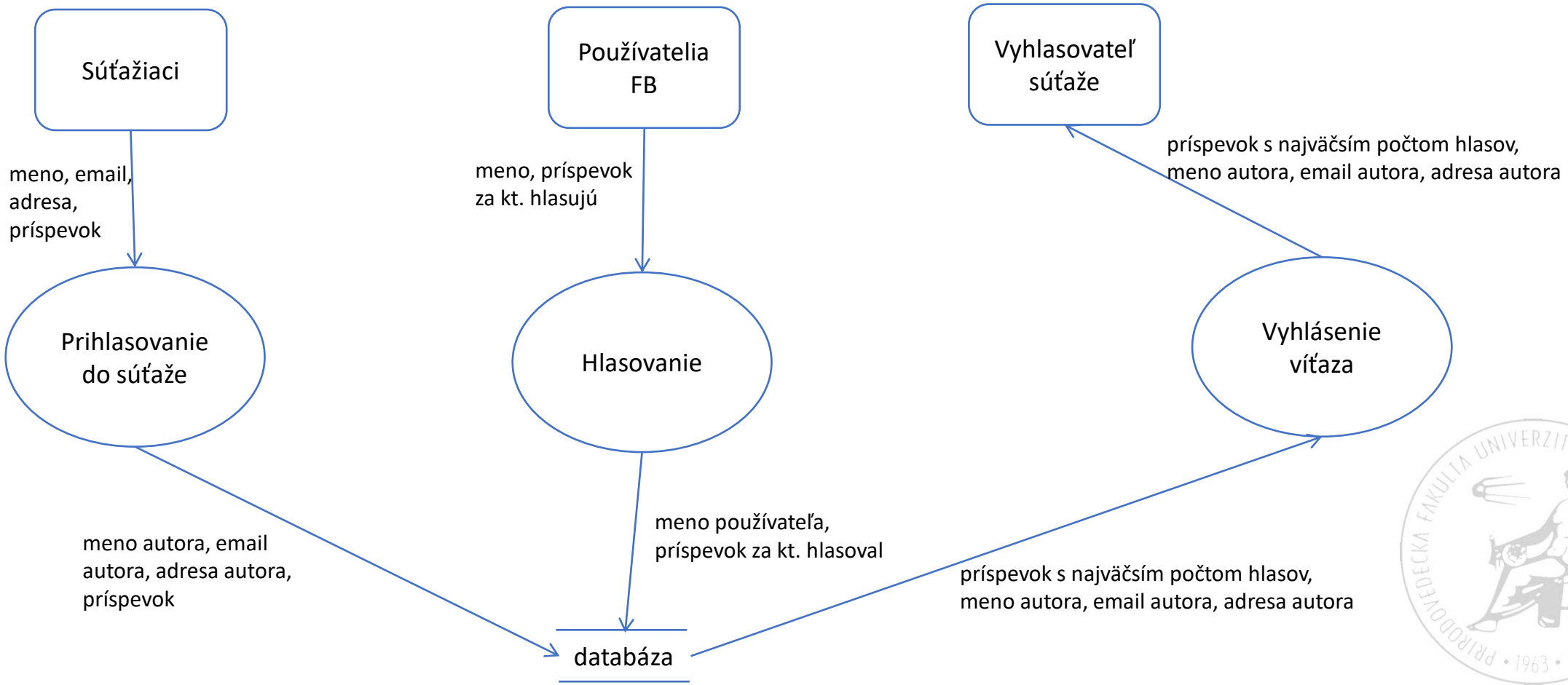
- Identifikácia aktív
- Identifikácia hrozieb
- Identifikácia existujúcich opatrení
- Identifikácia zraniteľností
- Identifikácia následkov

Aktíva

Asset owner - osoba zodpovedná za aktívum

Asset	Information class	Security criterion	Asset owner	Asset value	Asset description
Príspevky do súťaže	Informacie	integrita dostupnosť			
Priebežný stav hlasovania	Informacie	integrita dostupnosť			
Konečný stav hlasovania	Informacie	integrita dostupnosť			
Ceny pre víťazov					
Zmluvy so sponzormi	Informacie	dôvernosť integrita			
Doklady k cenám	Informacie	integrita dostupnosť			
Potvrdenia o prevzatí ceny	Informacie	integrita dostupnosť			
Hardvér	Hardvér				
Softvér na správu príspevkov	Softvér	integrita dostupnost			
Sejf	Hardvér			2	
Server	Hardvér	dostupnost		3	
Zamestnanci				1	
Sietove prvky	Hardvér				
Pocitace					
Sutaziaci					
Stranka				3	
Softver					
Dokumentacia (zmluvy,...)				3	
Serverovna					
OS					
DBS					
Softver na prihlasenie					
Softver na hlasovania					

Data flow diagram príklad



Hrozby

Threat id	Threat	Threat type	Threat source
T01	Zavazna nehoda (Fyzicke poskodenie)		
T02			
T03	Poškodenie dát		
T04	Vyzradenie		
T05	Nesprávna údržba		
T06	Výpadok elektriny		
T07	Nesprávne používanie		
T08	Chybne fungovanie aplikacneho programoveho vybavenia		

Zraniteľnosti

Vulnerability id	Source of vulnerability (asset)	Description of vulnerability
V01	Sejf	Ľahko uhádnuteľný kód
V02	Sejf	Jednoduchý fyzický prístup bez kódu
V03	Softvér na správu hlasovania	Dovolí jednej osobe hlasovať viackrát
V04	Softvér na správu hlasovania	Dovolí hlasovať po uzatvorení
V05	Softvér na správu príspevkov	Nezaradí príspevok do súťaže
V06	Softvér na správu príspevkov	Odstráni príspevok počas hlasovania
V07	Softvér na správu príspevkov	Priradí príspevok nesprávnemu súťažiacemu

Posúdenie rizík - Analýza rizík

2 základné prístupy:

- Kvantitatívny – stupnica s číselnými hodnotami
- Kvalitatívny – škála kvalifikačných atribútov

Riziko = pravdepodobnosť * dopad hrozby

Riziká - identifikácia

		Sejf Ľahko uhádnuteľný kód	Sejf Jednoduchý fyzický prístup bez kódu	Softvér na správu hlasovania Dovolí jednej osobe hlasovať viackrát	Softvér na správu hlasovania Dovolí hlasovať po uzatvorení	Softvér na správu príspevkov Nezaradí príspevok do súťaže	Softvér na správu príspevkov Odstráni príspevok počas hlasovania	Softvér na správu príspevkov Priradí príspevok nesprávnemu súťažiacemu
		V01	V02	V03	V04	V05	V06	V07
Zavazna nehoda (Fyzicke poskodenie)	T01		R				R	
0	T02							
Poškodenie dát	T03			R	R	R	R	R
Vyzradenie	T04							
Nesprávna údržba	T05	R	R					
Výpadok elektriny	T06		R					
Nesprávne používanie	T07					R		
Chybne fungovanie aplikacneho programoveho vybavenia	T08			R	R	R	R	R

Analýza rizík II. - dopad

Kvalitatívne úrovne dopadu:

- **Nízky** – strata CIA – má **obmedzený** negatívny vplyv na činnosť organizácie, jej aktíva
- **Stredný** - strata CIA – má **závažný** negatívny vplyv na činnosť organizácie, jej aktíva
- **Vysoký** - strata CIA – má **veľmi závažný až katastrofický** negatívny vplyv na činnosť organizácie, jej aktíva

Analýza rizík III. - pravdepodobnosť

Označenie	Pomenovanie	Poznámka
0	**Nulová**	Udalosť nenastane
1	**Nízka**	Udalosť nenastala, alebo sa vyskytne raz za niekoľko rokov
2	**Stredná**	Raz za rok
3	**Vysoká**	Niekoľkokrát mesačne / týždenne

Kvalitatívne vyjadrenie úrovne pravdepodobnosti udalosti

Analýza rizík IV. - riziko

Dopad → Pravdepodobnosť ↓	nízky	stredný	Vysoký
Nulová	Nulové	Nulové	Nulové
Nízka	Nízke	Nízke	Stredné
Stredná	Nízke	Stredné	Vysoké
Vysoká	Stredné	Vysoké	Vysoké

Kvalitatívne vyjadrenie rizika

Posúdenie rizík - Hodnotenie rizík

Vstup:

- Zoznam rizík s priradenými hodnotami
- kritéria pre hodnotenie rizík

Napr:

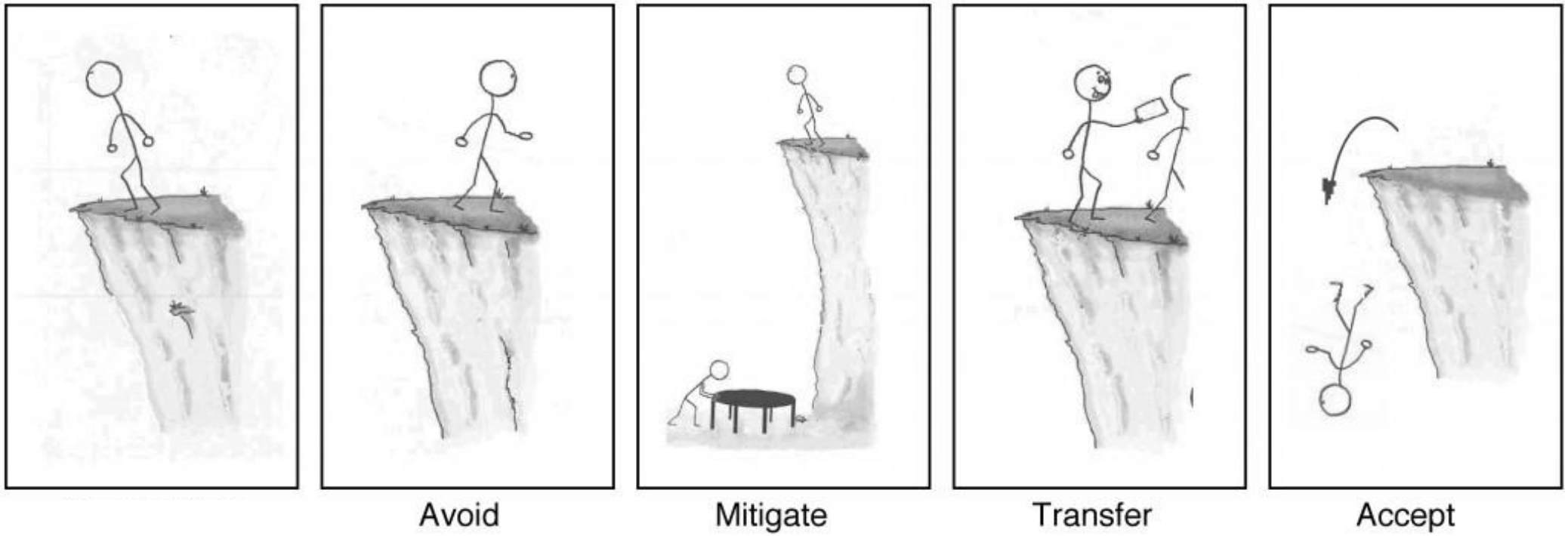
- 1 - 3 : akceptovateľné riziko
- 4 – 5 : významné riziko
- 6 – 7 : neakceptovateľné riziko

Riziká - ohodnotenie

Risk id	Threat id	Vulnerability id	Identified risk/Risk statement	Likelihood	Impact	Risk level	Risk Indicator
R01	T01	V02	V prípade fyzického poškodenia sa sejf otvorí bez kódu	1	Major	M	otvorený sejf
R02	T03	V03	Poškodením dát dovolí softvér jednej osobe hlasovať viackrát	3	Major	H	novinova sprava

Risk level legend		
	1 - 2	Low
	3 - 4	Medium
	6 - 9	High

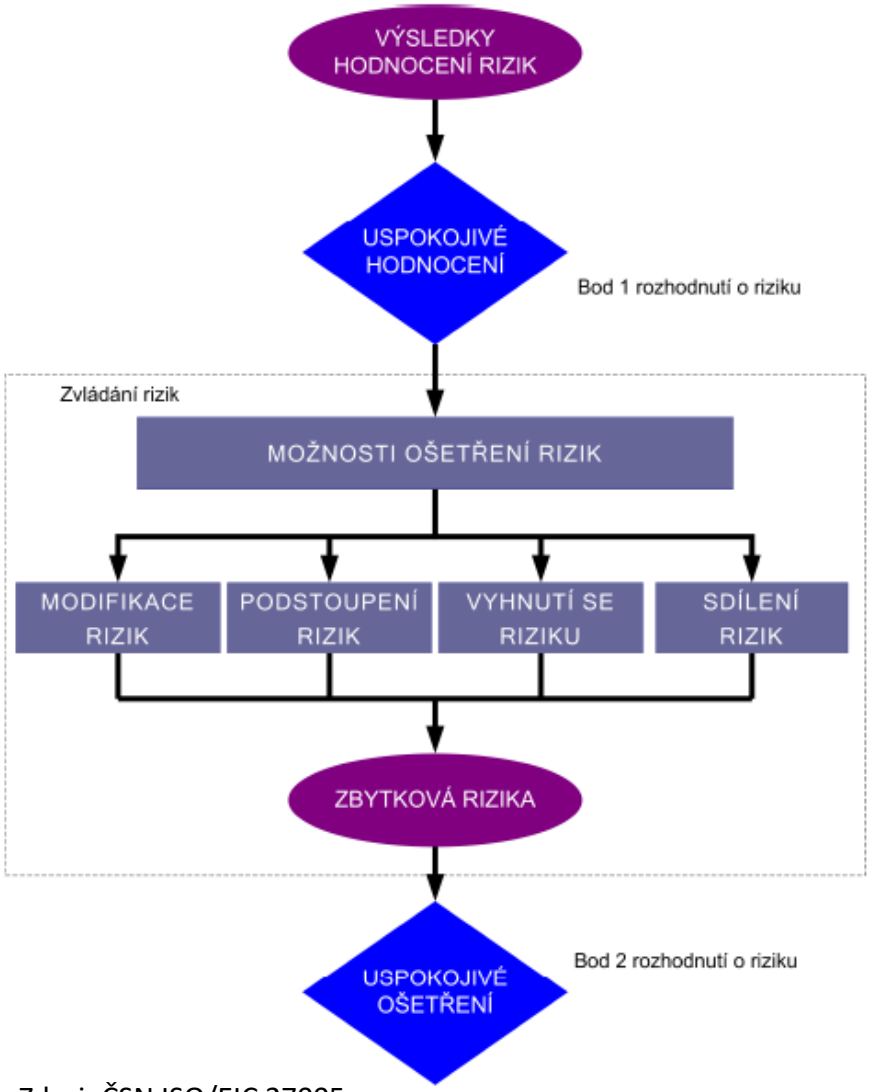
Ošetrenie rizika



Zdroj: http://cnx.org/content/col11120/1.4/

Ošetrenie rizika I.

- Akceptovanie rizika (acceptance)
- Vyhnutie sa riziku (avoidance)
- Limitácia rizika (limitation)
- Prenesenie rizika (transference)



Zdroj: ČSN ISO/EIC 27005

Riziká - ošetrenie

Risk id	Identified risk/Risk Statement	Risk level	Risk Treatment	Rationale	Risk owner	Risk response	Planned Due Date	Risk response owner	Risk Status
R01	0								
R02	0								
R03	0								
R04	0								
R05	0								
R06	0								
R07	0								

Acceptance
Avoidance
Limitation
Transference

Risk owner - osoba zodpovedná za riziko

Risk response owner – osoba zodpovedná za vykonanie stanovených opatrení

Ďakujem za pozornosť!

pavol.sokol@upjs.sk

terezia.mezesova@student.upjs.sk