

Konzultace

Informační bezpečnost

Nástroje pro podporu řízení

Certifikace a vzdělávání



# System řízení rizik ve státní správě

ISSS 2011  
Hradec Králové

RNDr. Ilona Štěpánková





# Obsah

- Téma je mimořádně aktuální
- Umíme rizika opravdu řídit?
- Práce s riziky – Registr rizik
- Na co nikdy nezapomínat





# Aktuální téma...

- Zákon č. 320/2001 Sb., o finanční kontrole
- Práce s riziky má hluboký smysl
- Nové podmínky, nové výzvy 😊
- Rizika projektů  
(spolufinancovaných ze strukturálních fondů)
- Možnost čerpání dotací na řízení rizik



???



Rizika ČEHO ???

JAKÁ analýza rizik a PROČ ???

- **ISO/IEC 31010:2009**
  - systemizace a popis 30 nejrozšířenějších druhů analýz rizik

## Zásady pro volbu a provádění AR:

- **Vycházet z daného oboru**  
(AR bezpečnosti informací není totéž co AR ICT)
- **Vycházet z cíle** (míra detailu)
- **Paretovo pravidlo „80/20“**

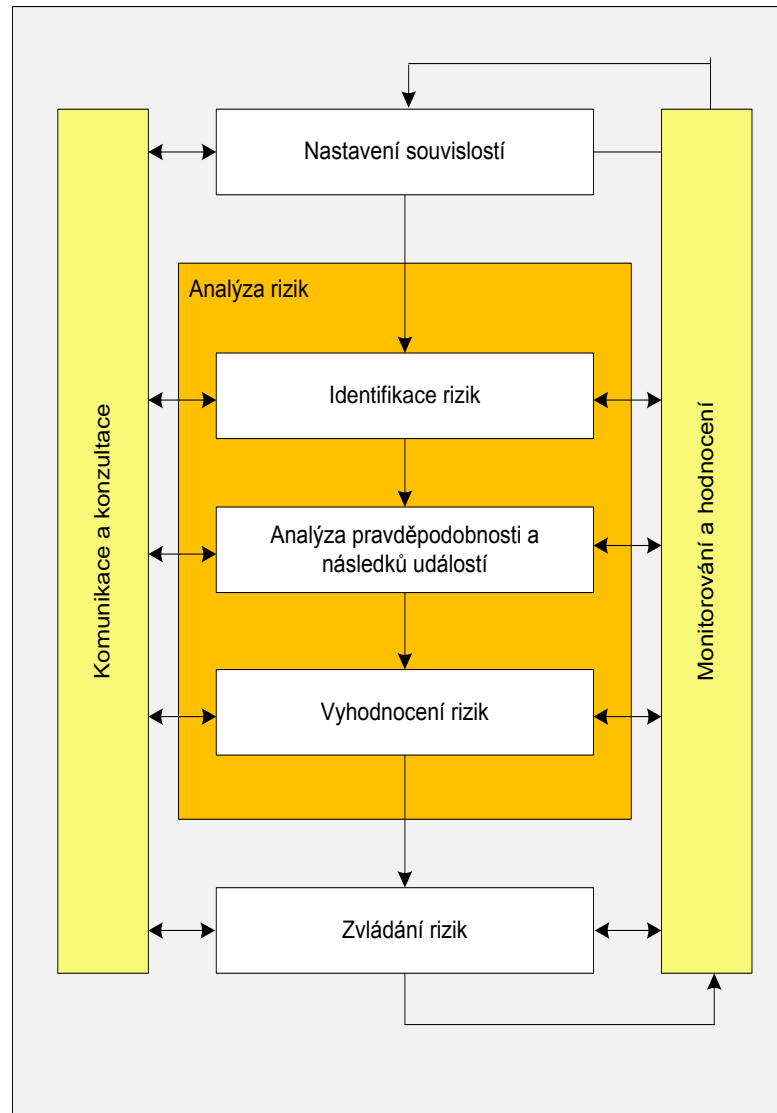


# Zvládání rizik

- Analýzou rizik práce s riziky nekončí
- Volba způsobu zvládání rizika
  - Modifikace (snížení)
  - Sdílení
  - Vyhnutí se
  - Akceptace
- Je třeba činit mnohá rozhodnutí  
(zvládání rizik je o kompromisech)



# Řízení rizik



Zdroj: ISO 31000:2009

- Je třeba mít systém evidence rizik:
  - trvalý přehled o rizicích, jejich velikosti (významnosti) a možných následcích
  - rozhodnutí o způsobech zvládnání rizik
  - přijatá opatření
  - odpovědnost (vlastnictví rizik)
  - možnost reakce na probíhající změny
  - zachycení rozhodnutí učiněných v rámci řízení rizik
  - participace více různých zainteresovaných osob (řízení přístupu)





# Registr rizik

Hledat [ Upřesnit ]

**Katalog Rizik - Seznam**

Katalog Rizik [ --Akce-- ]

Filtr [ --Vybrat-- ] [ Rozbalit filtr ]

<input type="checkbox"/>	Název	ID	Míra (významnost) rizika	Statut	Oblast rizika	Stav realizace opatření	Vlastník rizika
<input type="checkbox"/>	Únik informací z PERS	RIMS000003	⚠	Otevřeno	Bezpečnosti informací	🚩 30%	
<input type="checkbox"/>	Krádež notebooku	RIMS000004	⚠	Čeká na přehodnocení	Bezpečnosti majetku	🚩 Dosud nezahájeno	
<input type="checkbox"/>	Vyzrazení informací z notebooku	RIMS000005	⚠	Otevřeno	Bezpečnosti informací	🚩 Dosud nezahájeno	
<input type="checkbox"/>	Nevymahatelná ustanovení smluv	RIMS000006	⚠	Otevřeno	Provozní	🟢 80%	
<input type="checkbox"/>	Požár objektu Z113	RIMS000007	⚠	Otevřeno	Bezpečnosti majetku	✅ 100%	
<input type="checkbox"/>	Účast v tendru GALILEO	RIMS000008	⚠	Uzavřeno	Obchodní a marketingová	✅ 100%	
<input type="checkbox"/>	Účast v projektu GALILEO - příležitost	RIMS000009	⚠	Otevřeno	Obchodní a marketingová	🚩 30%	

Celkové výsledky: 7

Nové  Odstranit

Zvýrazněné řádky = Míra (významnost) rizika

# Registr rizik

**Katalog Rizik Vlastnosti** (Katalog Rizik: Únik informací z PERS) [Katalog Rizik - Správa karet]

Vlastnosti Procesy

Uložit Odeslat Storno [Zobrazit vše] [Kopírovat z] [Exportovat do souboru XML]

**Obecné**

Název Únik informací z PERS Vytvořil-a Šustr, Josef

ID RIMS000003 Vlastník rizika [ ] [ ]

Datum vytvoření 13.5.2010 Statut Otevřeno

Ukončeno [ ] [ ]

Popis rizika Únik informací (osobních údajů) z personálního informačního systému PERS.  
Popis zdroje rizika:  
Existuje velké množství uživatelů se silnými přístupovými právy.

**Detail**

Míra (významnost) rizika (Střední)

Oblast rizika Bezpečnosti informací

Zdroj rizika Provoz

Souvislost s jinými riziky [ ] [ ]

Popis cíle (chráněných aktiv) Ochrana osobních údajů zaměstnanců

Popis zdroje rizika Technologie výroby a provozu

**Role**

Řešitel [ ] [ ]

Schvalující osoba [ ] [ ]

**Struktury organizačního uspořádání**

Organizace RIMS /IT/Systemy/Windows [ ] [ ]

Uložit Odeslat Storno [Zobrazit vše] [Kopírovat z] [Exportovat do souboru XML]

■ = Požadováno ■ = Jedinečné

# Registr rizik

## Katalog Rizik Vlastnosti

( Katalog Rizik: Únik informací z PERS )

[Katalog Rizik - Správa karet

Vlastnosti

Procesy

Obecné

### Analýza a hodnocení rizika

Zvládnání rizika

Změna - Seznam

Přístup k tomuto objektu

▸ Úplné zobrazení

▸ Zdroj

▸ Skupina

▸ Jednotka OBS

Uložit Odeslat Storno

### Míra rizika

Míra (významnost) rizika ⚠ (Střední)

### Analýza

Pravděpodobnost události Střední ⚠

Komentář k pravděpodobnosti K vyzrazení OU již u nás došlo, odhaduji, že 1x ročně by se to mohlo stát.

( Specifikujte důvody hodnocení pravděpodobnosti )

Následek události Vysoký ⚠

Scénář Poškození dobrého jména

Komentář následku události Vyzrazení OU by mohlo mít soudní dohru, což by bylo velmi nepříjemné z hlediska dobrého jména firmy.

Uložit Odeslat Storno

# Registr rizik

**Katalog Rizik Vlastnosti** (Katalog Rizik: Únik informací z PERS) [Katalog Rizik - Správa karet]

Vlastnosti | Procesy

Obecné

Analýza a hodnocení rizika

**Zvládání rizika**

Změna - Seznam

Přístup k tomuto objektu

- Úplně zobrazení
- Zdroj
- Skupina
- Jednotka OBS

Uložit | Odeslat | Storno

**Obecné**

Způsob zvládání rizika Změna velikosti rizika

Komentář ke zvládání rizika

Popis opatření Snížit počet zaměstnanců divize ICT se silnými právy na nezbytné minimum.

Stav realizace opatření 30%

Popis realizace opatření Úkol byl uložen vedoucímu divize ICT na poradě vedení dne 20.5.2010.

Termín splnění 31.5.2010

Uložit | Odeslat | Storno

- **Jeden systém řízení rizik**
  - Na úrovni organizace (úřadu, orgánu VS) by měl být jednotný systém řízení rizik.
- **Nástroj (SW) nestačí**
  - Žádný nástroj, ani ten nejpropracovanější, nenaplní očekávání jeho protagonistů, pokud není součástí příslušného procesu řízení rizik.
- **Je to jednoduché**
  - Řízení rizik není nic složitého, vyžaduje to jen zájem, alespoň základní znalosti (zkušenosti) a samozřejmě práci...



# Děkujeme za pozornost

Prosím Vaše názory, dotazy...