Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

# Bezpečnostný projekt IS

Ivan Kopáčik

Máj 2013

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

# Agenda

Motivácia

Legislatívne východiská

Obsah a rozsah bezpečnostného projektu

Analýza a riadenie rizík

Bezpečnostné smernice

Analýza rizík – ukážka (ak ostane čas a chuť ...) / Diskusia

Záver

KPMG
cutting through complexity™

# Motivácia

Každá zlozitejšia a komplexnejšia aktivita musí byť vopred „naprojektovaná“ (stavba RD, implementácia IS, výrobný postup ...).

Projekt: konkrétne vypracovaný návrh uskutočnenia určitého zámeru.

Projekt musí mať:

- Vopred identifikované definované požiadavky (prečo? ako? kto?)
- Stanovené ciele, rozsah a výstupy
- Harmonogram vypracovania a realizácie
- Pridelené  zdroje potrebné na jeho vypracovanie a realizáciu

# Bezpečnostný projekt - východiská

Pre podmienky verejnej správy

- Zákon o ochrane osobných údajov
- Výnos Ministerstva financií Slovenskej republiky č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy (ďalej len Výnos)
- Zákon č. 45/2011 o kritickej infraštruktúre
- „Zdravý rozum“
- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností

# Zákon o ochrane osobných údajov I.

- Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ. Prevádzkovateľ je povinný chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania. Na tento účel príjme primerané technické, organizačné a personálne opatrenia (ďalej len „bezpečnostné opatrenia“) zodpovedajúce spôsobu spracúvania osobných údajov, pričom berie do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému.
- Bezpečnostné opatrenia prevádzkovateľ zdokumentuje v bezpečnostnom projekte informačného systému.

# Zákon o ochrane osobných údajov II.

- Bezpečnostný projekt vymedzuje rozsah a spôsob bezpečnostných opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

- Bezpečnostný projekt obsahuje najmä
  - názov informačného systému, na ktorý sa vzťahuje,
  - bezpečnostný zámer,
  - analýzu bezpečnosti informačného systému,
  - bezpečnostnú smernicu.

# Zákon o ochrane osobných údajov III.

Bezpečnostný zámer vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu informačného systému pred ohrozením jeho bezpečnosti.

Bezpečnostný zámer obsahuje najmä:

- formuláciu základných bezpečnostných cieľov a minimálne požadovaných bezpečnostných opatrení,
- špecifikáciu technických, organizačných a personálnych opatrení na zabezpečenie ochrany osobných údajov v infomačnom systéme a spôsob ich využitia,
- vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti,
- vymedzenie hraníc určujúcich množinu zvyškových rizík.

# Zákon o ochrane osobných údajov IV.

Analýza bezpečnosti informačného systému je podrobný rozbor stavu bezpečnosti informačného systému s vymedzením rozsahu jeho odolnosti a zraniteľnosti. Analýza bezpečnosti obsahuje najmä:

- kvalitatívnu analýzu rizík, v rámci ktorej sa identifikujú hrozby pôsobiace na jednotlivé aktíva infomačného systému spôsobilé narušiť jeho bezpečnosť alebo funkčnosť; výsledkom kvalitatívnej analýzy rizík je zoznam hrozieb pre dôvernosť, integritu a dostupnosť spracúvaných osobných údajov, s uvedením rozsahu možného rizika, návrhov opatrení na elimináciu alebo minimalizáciu vplyvu rizík a s vymedzením súpisu nepokrytých rizík,
- použitie bezpečnostných štandardov (Napríklad STN ISO/IEC 27001, STN ISO/IEC 27002, Výnos Ministerstva financií Slovenskej republiky č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov) a určenie iných metód a prostriedkov ochrany osobných údajov; súčasťou analýzy bezpečnosti informačného systému je posúdenie zhody navrhnutých bezpečnostných opatrení s použitými bezpečnostnými štandardami, metódami a prostriedkami.

# Zákon o ochrane osobných údajov V.

Bezpečnostná smernica obsahuje najmä:

- popis technických, organizačných a personálnych opatrení a spôsob ich uplatňovania v konkrétnych podmienkach,
- rozsah oprávnení, popis povolených činností a spôsob identifikácie a autentizácie jednotlivých oprávnených osôb,
- rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov,
- spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému,
- postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie rizika vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou, poruchou alebo inou mimoriadnou situáciou.

# Výnos

Analyzovanie rizík vyplývajúcich z hrozieb pre informačné systémy verejnej správy, od ktorých závisia kritické procesy.

Analýza rizík v súvislosti s informačnými systémami verejnej správy, vyplývajúcich z činnosti tretích strán v týchto informačných systémoch, najmä dodávateľov, externých spolupracovníkov, orgánov verejnej správy, fyzických osôb, a zabezpečenie takých technických, organizačných a právnych podmienokna činnosť tretích strán v informačných systémoch verejnej správy, aby nebola narušená bezpečnosť informačného systému verejnej správy a bezpečnostná politika povinnej osoby.

# Zákon č. 45/2011 o kritickej infraštruktúre

Bezpečnostný plán

- obsahuje popis možných spôsobov hrozby narušenia alebo zničenia prvku, zraniteľné miesta prvku a bezpečnostné opatrenia na jeho ochranu.

Bezpečnostné opatrenia sú najmä

- mechanické zábranné prostriedky, technické zabezpečovacie prostriedky, bezpečnostné prvky informačných systémov, fyzická ochrana, organizačné opatrenia, kontrolné opatrenia a ich vzájomná kombinácia.

Rozsah bezpečnostných opatrení na ochranu prvku sa určuje na základe posúdenia hrozby narušenia alebo zničenia prvku.

# Zákon č. 45/2011 o kritickej infraštruktúre

Pri vypracúvaní bezpečnostného plánu sa postupuje nasledovne:

- Určujú sa dôležité zariadenia prvku.
- Vyhodnocuje sa riziko hrozby narušenia alebo zničenia jednotlivých zariadení prvku, ich zraniteľné miesta, predpokladané
- dôsledky ich narušenia alebo zničenia na funkčnosť, integritu a kontinuitu činnosti prvku.
- Uskutočňuje sa výber hlavných bezpečnostných opatrení na ochranu prvku, ktoré sa členia na
  - trvalé bezpečnostné opatrenia, ktorými sú investície a postupy na zabezpečenie ochrany prvku, a to
    - mechanické zábranné prostriedky,
    - technické zabezpečovacie prostriedky,
    - bezpečnostné prvky informačných systémov,
    - organizačné opatrenia s dôrazom na postup pri vyrozumení a varovaní, ako aj na krízové riadenie,
    - odborná príprava osôb, ktoré zabezpečujú ochranu prvku,
    - kontrolné opatrenia na dodržiavanie trvalých bezpečnostných opatrení,
  - mimoriadne bezpečnostné opatrenia, ktoré sa uplatňujú v závislosti od intenzity hrozby narušenia alebo zničenia prvku.
- Určujú sa hlavné bezpečnostné opatrenia na ochranu prvku.
- Bezpečnostný plán sa počas jeho tvorby konzultuje s orgánmi, ktorých súčinnosť sa predpokladá pri ochrane prvku.

# Zdravý rozum

Pri implementácii nových alebo aktualizácii existujúcich IS sa odporúča v primeranej miere aplikovať nasledovné princípy:

- súčasťou každého projektu IS musí byť analýza rizík súvisiaca s vývojom a prevádzkovým prostredím nových prvkov IS,
- pre každý projekt IS musia byť identifikované a špecifikované bezpečnostné požiadavky,
- súčasťou každého projektu IS musí byť návrh bezpečnostných testov a návrh formy overenia dostatočnosti bezpečnosti nových prvkov IS pred ich zavedením do rutinnej prevádzky,
- súčasťou každého projektu IS musí byť vypracovanie príslušnej projektovej dokumentácie (používateľskej, administrátorskej a prevádzkovej dokumentácia k IS),
- v každom projekte IS musí byť zriadená a obsadená rola, ktorá zodpovedá za integráciu bezpečnostných opatrení do predmetu projektu IS,
- na zaistenie primeranej úrovne bezpečnosti musí byť v každom projekte IS vývojové a testovacie prostredie oddelené od produkčného prostredia,
- v každom projekte IS sa musia určiť role, ktoré budú vykonávať údržbu predmetu projektu IS po jeho zavedení do rutinnej prevádzky.

# Obsah a rozsah bezpečnostného projektu I.

- „Prečo,  ako a čoho bezpečnosť vlastne ideme riešiť?“
- „Akú metodiku / štandard použijeme?“
- „Aké sú právne požiadavky na riešenie bezpečnosti?“
- „Ako „vysokú„ bezpečnosť potrebujeme dosiahnuť?“
- „Aké okruhy rizík ideme minimalizovať?“
- „Aké riziká sú pre nás akceptovateľné?“
- „Aké opatrenia sme schopní prijať?“

1. časť bezpečnostného projektu: **<u>bezpečnostný zámer</u>**

# Obsah a rozsah bezpečnostného projektu II.

- „Čo sú naše hodnoty (aktíva), čo chceme chrániť?“
- „Pred akými hrozbami chceme naše aktíva chrániť?“
- „Aké negatívne dôsledky nám hrozby môžu spôsobiť?“
- „Aká je šanca (pravdepodobnosť), že riziko sa naplní?“
- „Ako veľké sú riziká, ktoré nám hrozia?“
- „Aké opatrenia treba prijať, aby sa riziká minimalizovali na prijateľnú úroveň“?

2. časť bezpečnostného projektu: **<u>analýza bezpečnosti.</u>**

# Obsah a rozsah bezpečnostného projektu III.

- „Ako zavedieme do praxe jednotlivé opatrenia?“
- „Ako budeme používať a dodržiavať jednotlivé opatrenia?“
- „Čo budeme robiť, ked niektoré riziko skutočne nastane?“
- „Ako budeme hodnotiť dostatočnosť a účinnosť opatrení?“
- „Ako odhalíme nové riziká?“
- „Kto a za čo je z hľadiska bezpečnosti zodpovedný?“
- „Aké sú práva a povinnosti zúčastnených strán?“

3. časť bezpečnostného projektu: **bezpečnostné smernice.**

# Bezpečnostný zámer

Obsah podľa  OOÚ

Zohľadnenie požiadaviek ďalších právnych predpisov

Zohľadnenie stavu IS (existujúci vs. plánovaný)

Špecifické bezpečnostné ciele nad rámec OOÚ

Väzby na existujúcu bezpečnostnú dokumentáciu

# Analýza bezpečnosti

Popis použitej metodiky

Použité katalógy (hrozieb, aktív, dopadov)
Identifikácia a klasifikácia rizík

Návrh a prioritizácia opatrení na elimináciu alebo minimalizáciu vplyvu rizík a s vymedzením súpisu nepokrytých rizík.

# Bezpečnostné smernice

Rozsah podľa OOÚ

Špecifická smernica pre ochranu osobných údajov (ak sú spracúvané)

Bezpečnosť na úrovni zariadení, operačných systémov a databáz

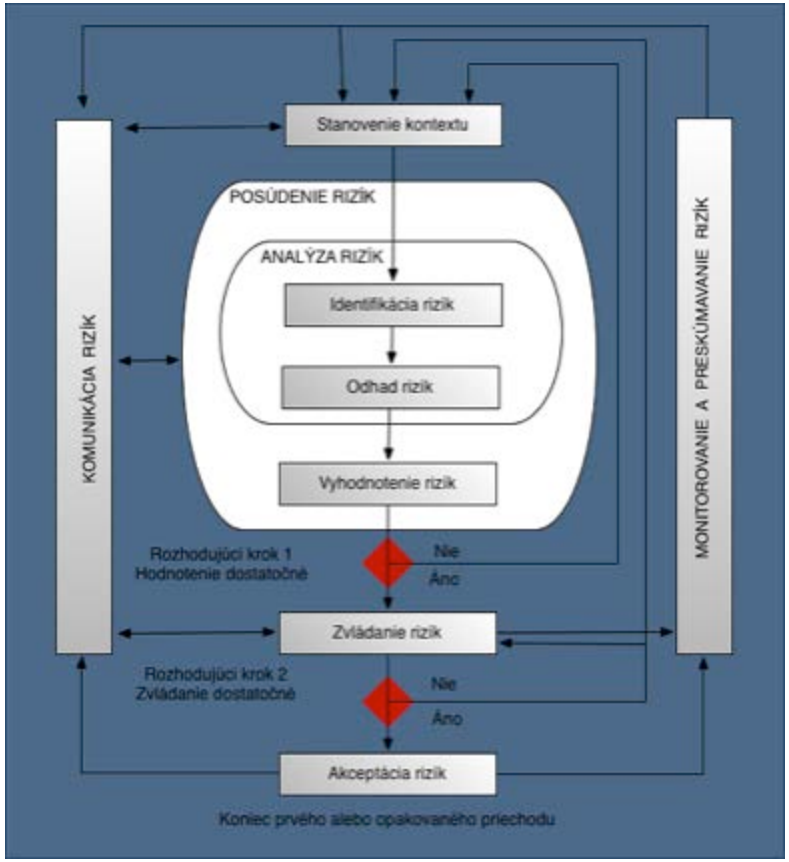
Monitorovanie a dohľad

- Monitorovanie na úrovni infraštruktúry
- Auditovanie údajov a operácií
- Vyhodnocovanie zaznamenaných udalostí

Vývoj, nasadzovanie a riadenie zmien

.....

# Riadenie rizík – komplexný pohľad ISO27005



# Analýza rizík – pojmy I.

- ***Aktívum*** je dôležitá informácia a dokumentácia, zmluva, programové vybavenie, technické zariadenie, poskytovaná služba, kvalifikovaní ľudia, dobré meno a ďalšie skutočnosti, ktoré považuje organizácia za hodnotné a vyžadujúce si ochranu. ***Informačné aktívum*** chápeme ako dokument, údaj, súbor alebo ich logické zoskupenie s definovaným významom, vlastníkom a určením.
- ***Analýza rizík*** je činnosť, ktorej náplňou je identifikácia a ohodnocovanie bezpečnostných rizík.
- ***Analýza bezpečnosti*** je zisťovanie rizík informačného systému s cieľom navrhnúť spôsob jeho maximálneho zabezpečenia (pojem „ analýza rizík“ je synonymum).

# Analýza rizík – pojmy II.

- ***Hrozba*** je objektívna skutočnosť, ktorá môže využitím zraniteľnosti aktíva negatívne ovplyvniť činnosť, stav alebo existenciu daného aktíva
- ***Zraniteľnosť*** je technické riešenie, okolnosť, spôsob použitia, slabé miesto, nedostatok alebo nejaká vlastnosť aktíva, ktorá umožňuje, aby došlo k naplneniu hrozby voči aktívu vyznačujúcemu sa danou zraniteľnosťou
- ***Dopad hrozby*** predstavuje negatívne dôsledky naplnenia hrozby voči aktívu (zníženie až strata funkčnosti, poškodenie, zníženie hodnoty až zničenie) na aktívum a inštitúciu, ktorá je vlastníkom aktíva
- ***Bezpečnostné opatrenie*** je technické, organizačné, právne alebo iné riešenie, ktoré úplne alebo čiastočne odstraňuje zraniteľnosť aktíva, a/alebo znižuje pravdepodobnosť naplnenia hrozby a/alebo v prípade jej naplnenia znižuje jej dopad na aktívum a organizáciu, ktorá ho

# Analýza rizík – pojmy III.

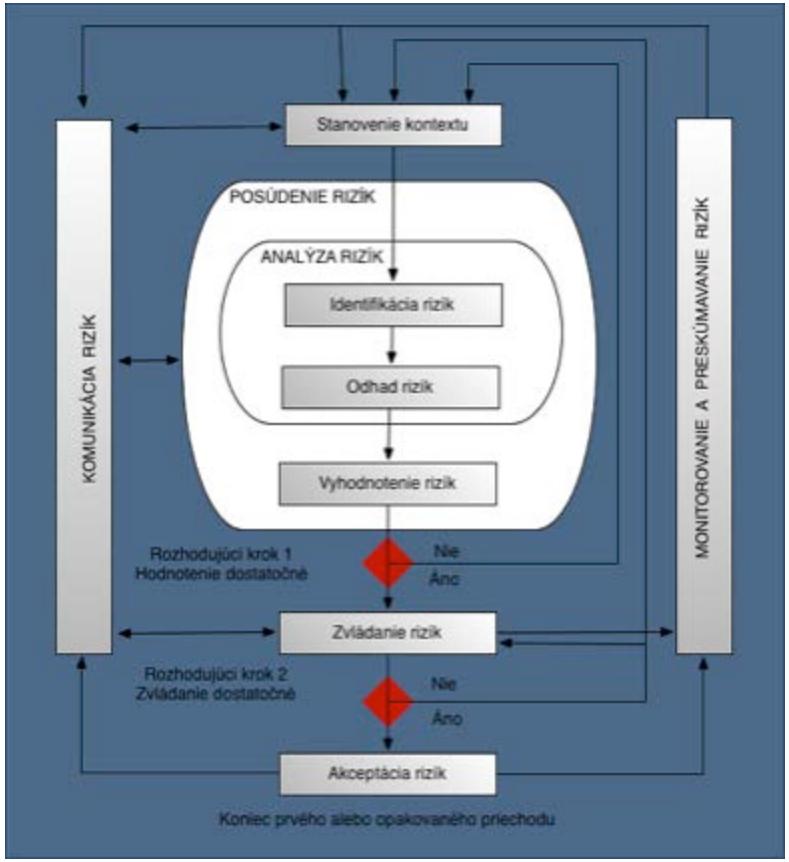
- ***Riziko*** predstavuje pravdepodobnosť, že zraniteľnosť v IS ovplyvní overenie alebo dostupnosť, pravosť, integritu alebo dôvernosť spracúvaných alebo prenesených údajov, ako aj vážnosť dopadu úmyselného alebo neúmyselného využitia takejto zraniteľnosti.
- ***Zvyškové riziko*** je riziko, ktoré ostane po prijatí bezpečnostných opatrení zameraných na jeho minimalizáciu.
- ***Riadenie rizika*** je vedomý proces pochopenia rizika, dohodnutia sa na príslušných opatreniach a realizácii týchto opatrení na zníženie rizika na definovanú úroveň, ktorá je akceptovateľnou úrovňou rizika pri akceptovateľných nákladoch; tento prístup je charakterizovaný identifikovaním, meraním a riadením rizík na úroveň odpovedajúcu stanovenej úrovni.

# Analýza rizík – východiská

- Množstvo metodík, nástrojov a techník (kvalitatívny versus kvantitatívny prístup, kontrolné zoznamy/Checklists, analýzy pomocou scenára, FRAP, brainstorming, BIA, matice hodnoty aktív/zraniteľností/dopadov, ISO/IEC-27005 *Riadenie rizík informačnej bezpečnosti*, ISO 31000 *Manažérstvo rizika. Zásady a návod,* generické katalógy aktív/hrozieb/dopadov, automatizované nástroje CRAMM, ALE /Annual Loss Expectancy ...).

- Neexistuje univerzálna metodika vhodná „pre všetko“- výber a použitie vhodnej metodiky závisí na cieľoch, rozsahu a hĺbke analýzy, veľkosti a charaktere organizácie, zložitosti IKT infraštruktúry, stave IKT – prevádzkový IS versus implementovaný IS, ...).

# Riadenie rizík – komplexný pohľad ISO27005



# Riadenie rizík – stanovenie kontextu I.

- Určenie kontextu – vstupom na určenie sú všetky informácie o organizácii významné na určenie kontextu riadenia rizík informačnej bezpečnosti.
- Mal by sa určiť vonkajší a vnútorný kontext pre riadenie rizík informačnej bezpečnosti, čo zahŕňa určenie základných kritérií potrebných na riadenie rizík informačnej bezpečnosti , definovanie rozsahu a hraníc a vytvorenie vhodnej organizačnej štruktúry na zabezpečenie riadenia rizík informačnej bezpečnosti.
- Potrebné je určiť účel riadenia rizík informačnej bezpečnosti (napr. dodržiavanie právnych predpisov a dôkazy o odbornej starostlivosti; príprava plánu kontinuity činnosti;príprava plánu reakcií na incidenty; opis požiadaviek na informačnú bezpečnosti, produktu, služby alebo mechanizmu.)

# Riadenie rizík – stanovenie kontextu II.

Základné prístupy a kritéria

- Prístup podľa riadenia rizík
- Kritérium vyhodnotenia rizík
- Kritérium vplyvu
- Kritérium akceptácie rizík
- Rozsah a hranice
- Organizácia riadenia rizík informačnej bezpečnosti

# Riadenie rizík – prístupy

Zohľadnenie základných kritérií (kritérium vyhodnotenia rizík, kritérium vplyvu rizík, kritérium prijatia rizík).

Organizácia mala posúdiť, či má k dispozícii potrebné prostriedky na:

- vykonanie posúdenia rizík a vytvorenie plánu na ošetrenie rizík,
- definovanie a implementovanie politík a postupov vrátane implementácie zvolených opatrení,
- monitorovanie opatrení,
- monitorovanie procesu riadenia rizík informačnej bezpečnosti.

# Riadenie rizík – kritérium vyhodnotenia rizík

Kritériá na vyhodnotenie rizík by mali zohľadňovať:

- strategickú hodnotu procesu obchodných informácií,
- kritickosť zahrnutých informačných aktív,
- právne a regulačné požiadavky a zmluvné záväzky,
- prevádzkový a obchodný význam dostupnosti, dôvernosti a integrity,
- očakávania a predstavy zainteresovaných účastníkov a negatívne následky na reputáciu dobré meno.

Kritériá na vyhodnotenie rizík sa dajú využiť na nastavenie priorít pre ošetrenie rizík.

# Riadenie rizík – kritérium vplyvu

Vytvorené a nastavené z hľadiska úrovne škody alebo nákladov organizácie spôsobených udalosťou informačnej bezpečnosti, zohľadňujúce:

- stupeň klasifikácie ovplyvnených informačných aktív,
- narušenie informačnej bezpečnosti (napr. straty dôvernosti, integrity a dostupnosti),
- zhoršenie operácií (vnútorných alebo tretích strán),
- porušovanie plánov a termínov,
- poškodenie reputácie,
- porušovanie právnych, regulačných a zmluvných požiadaviek.

# Riadenie rizík – kritérium akceptácie rizík

Organizácia by mala definovať svoju vlastnú stupnicu pre úrovne akceptácie rizík. Ďalej:

- kritérium pre akceptáciu rizík môže obsahovať niekoľko prahov s požadovanou cieľovou úrovňou rizík, ako aj prijatie rizík vrcholovými manažérmi nad túto úroveň iba za definovaných okolností,
- rôzne kritériá na prijatie rizík možno použiť na rôzne triedy rizík, napr. riziká, ktoré by mohli viesť k nesúladu s právnymi a regulačnými predpismi, sa neakceptujú, zatiaľ čo akceptácia iných vysokých rizík môže byť povolená (ak je to uvedené ako zmluvná požiadavka),
- kritériá na prijatie rizík môžu obsahovať požiadavky na budúce dodatočné ošetrenie rizika (napr. riziko sa smie akceptovať, ak je súčasťou akceptácie záväzok na jeho zníženie na prijateľnú úroveň v určenom časovom období).

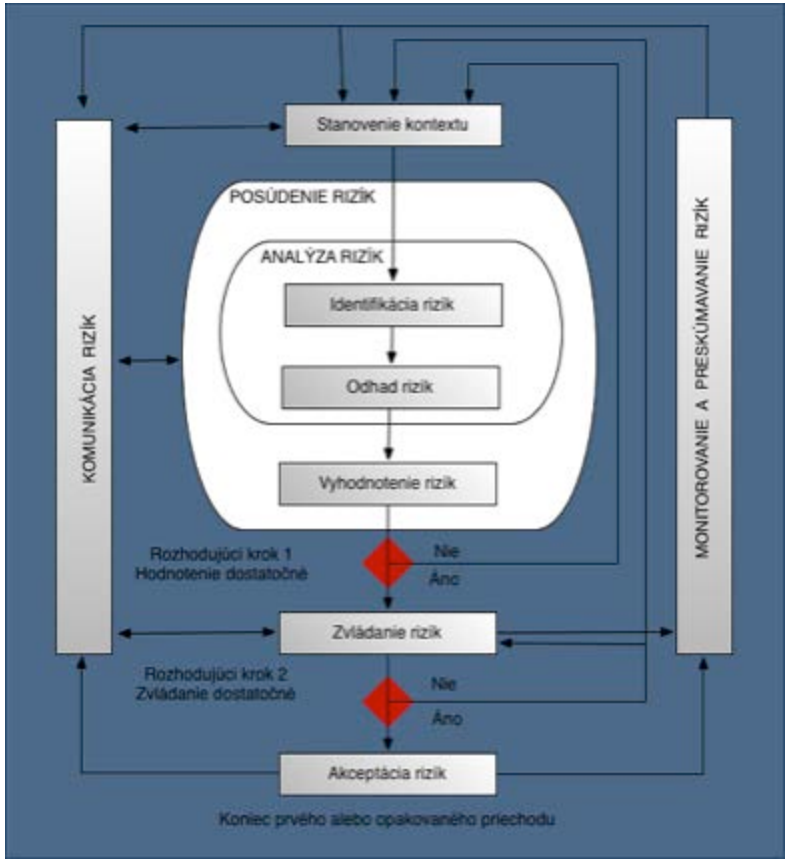
# Riadenie rizík – rozsah a hranice

Pri určovaní rozsahu a hraníc zvažujeme:

- strategické obchodné ciele organizácie,
- stratégie a politiky,
- funkciu a štruktúru organizácie,
- právne, regulačné a zmluvné požiadavky vzťahujúce sa na organizáciu,
- politiku informačnej bezpečnosti organizácie,
- informačné aktíva,
- umiestnenie organizácie a jej geografické charakteristiky,
- obmedzenia ovplyvňujúce organizáciu,
- rozhrania (t. j. výmena informácií s prostredím).

Okrem toho by organizácia mala poskytnúť zdôvodnenie pre akékoľvek vyňatie zo stanoveného rozsahu.

# Riadenie rizík – posúdenie rizík

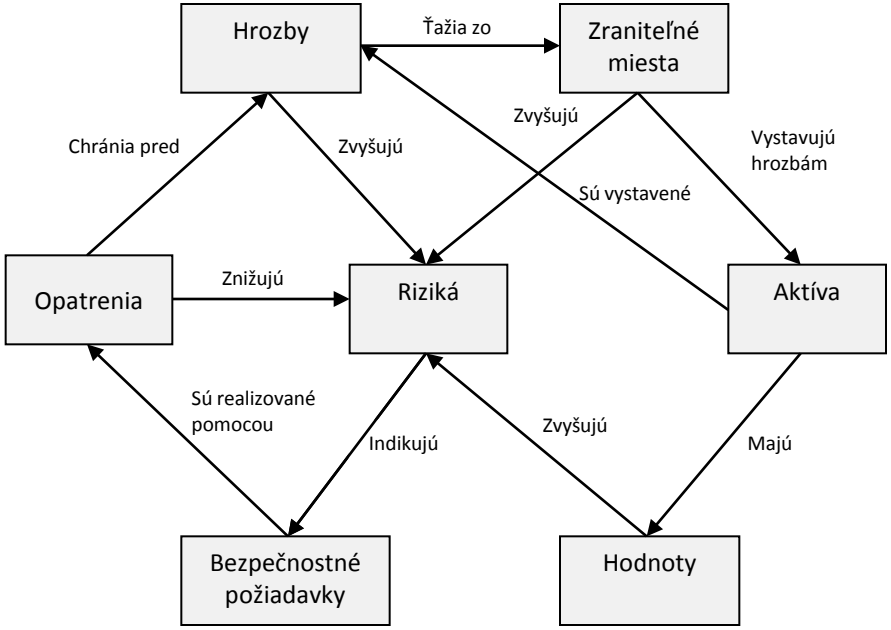


# Posúdenie rizík

Riziká by sa mali identifikovať, kvantifikovať alebo kvalitatívne opísať a prioritizovať vzhľadom na kritériá vyhodnotenia rizík a cieľov organizácie.

Pre posúdenie rizík je kľúčová analýza rizík zahŕňajúca pre každé riziko jeho identifikáciu a analýzu / ohodnotenie súvisiacich aktív, hrozieb, zraniteľností, dopadov.

# Anatómia rizika



# Analýza rizík

Bez ohľadu na zvolenú metodiku zahŕňa:

- Identifikáciu rizík
- Preskúmanie a ohodnotenie rizík

Posúdenie rizík sa často vykonáva vo viacerých iteráciách:

- vysokoúrovňové (identifikácia potenciálne vysokých rizík, ktoré si vyžadujú ďalšie posúdenie),
- dôkladnejšie (hĺbkové) preskúmanie potenciálne vysokých rizík zistených počas úvodnej iterácie.

# Analýza rizík – identifikácia rízik

„Čo zlé sa môže stať, aby to spôsobilo potenciálnu stratu ?"

Identifikácia rizík

- Identifikácia aktív
- Identifikácia hrozieb
- Identifikácia existujúcich opatrení
- Identifikácia zraniteľnosti
- Identifikácia dopadov

# Analýza rizík I. – identifikácia aktív

## Identifikácia hodnôt vyžadujúcich si ochranu

- Máme rozsah a hranice na posúdenie rizík
- V rámci stanoveného rozsahu je potrebné určiť aktíva (primárne, sekundárne/podporné)
- Úroveň detailnosti popisu identifikovaných aktív má byť taká, aby aktíva boli konkrétne a jednoznačne rozlíšiteľné
- Pre každé aktívum (alebo skupinu súvisiacich aktív) sa stanoví vlastník (ak ešte nie je)
- V závislosti od zvolenej metodiky sa aktíva ohodnotia

| Druh aktíva | ID | Aktívum |
|---|---|---|
| Primárne | 1. | hlavné servery systému (aplikačný, databázový) |
| | 2. | pracovná stanica |
| | 3. | zálohovacie zariadenie |
| | 4. | aktívne sieťové prvky |
| | 5. | operačné systémy klientskych staníc |
| | 6. | operačné systémy serverov |
| | 7. | aplikačné programové vybavenie serverov |
| | 8. | služby poskytované webovou aplikáciou |
| Sekundárne | 9. | UPS |
| | 10. | antivírová aplikácia |
| | 11. | firewall |
| | 12. | priestory umiestnenia serverov |
| | 13. | priestory umiestnenia klientskych staníc |

# Analýza rizík II. – identifikácia hrozieb

Stanovenie a klasifikácia hrozieb

- Brainstorming, výber relevantných hrozieb z katalógu, určenie zdrojov hrozieb ...
- Znútra/zvonka organizácie, ľudská/technická, náhodná/úmyselná, ...

Pri popisovaní hrozieb je potrebné si uvedomiť, že každá hrozba zahŕňa:

- zdroj hrozby (kto alebo čo spôsobuje hrozbu),
- cieľ hrozby (okruh aktív, ktorých sa daná hrozba dotýka),
- príčiny hrozby (faktory spôsobujúce vznik hrozby).

# Analýza rizík III. – identifikácia opatrení

## Identifikácia existujúcich opatrení

- Zavedené aj plánovené opatrenia treba mať „zachytené“
- Informácie od vlastníkov aktív, používateľov a správcov IKT, bezpečnostných špecialistov, ...
- Overenie dostatočnosti , účinnosti a vhodnosti opatrení
- Nefunkčné opatrenie môže spôsobiť zraniteľnosť

# Analýza rizík IV. – identifikácia zraniteľností

## Identifikácia zraniteľností

- Existencia zraniteľnosti nespôsobuje sama osebe škodu
- Zraniteľnosť sa môže využiť hrozbami na spôsobenie škody na aktívach
- Nesprávne realizované alebo zle použité opatrenie môže vytvoriť novú zraniteľnosť
- Zraniteľnosť môže byť spojená s vlastníctvom aktív, ak sa tieto použijú nevhodným spôsobom alebo s iným cieľom, ako bolo stanovené

# Analýza rizík V. – identifikácia dopadov

Praktickým dopadom realizovaného rizika je škoda (strata)
Škody môžeme konkretizovať napríklad nasledovnými kategóriami:

- finančná strata,
  - priama finančná strata,
  - priame finančné náklady na riešenie následkov a obnovenie funkčnosti aktíva,
  - spoluzodpovednosť za škody,
- dôsledky na ľudské zdroje,
  - ohrozenie zdravia a života,
  - zdroje potrebné na riešenie následkov realizácie rizika,
  - zdroje potrebné na obnovenie pôvodnej prevádzky a funkčnosti aktíva,
- dôsledky na prevádzkové prostredie,
  - neposkytovanie zákonom stanovených služieb,
  - nesplnenie plánu úloh,
  - porušenie právnych predpisov a stanovených požiadaviek súvisiacich s výkonom činností organizácie,
- dôsledky na vonkajšie a vnútorné vzťahy,
  - narušenie dobrého mena organizácie,
  - narušenie morálky a produktivity práce zamestnancov.

# Analýza rizík – metodiky na vykonanie

- Analýzy rizík sa môžu vykonávať na rôznych úrovniach podrobnosti v závislosti od kritickosti aktív, rozsahu známych zraniteľnosti a relevantných hrozieb týkajúcich sa organizácie.
- Kvalitatívna, kvantitatívna metodika alebo ich kombinácia, FRAP (Facilitated risk analysis process), ...
- Forma analýzy by mala byť konzistentná s kritériami vyhodnotenia rizík vypracovaných v rámci stanovenia kontextu.

# Kvalitatívna analýza rizík

Postavená na opisoch a expertných zhodnoteniach, využívajúcich dostupné zdroje informácií.

Používa stupnicu na kvalitatívny opis rozsahu možných následkov (napr. nízky, stredný, vysoký).

Kvalitatívny odhad sa môže použiť

- ako začiatočná mapovacia činnosť,
- na identifikáciu rizík, ktoré vyžadujú podrobnejšiu analýzu,
- tam, kde je potrebný pre rýchlu efektívnu podporu prijatia rozhodnutí,
- tam, kde číselné dáta (napr. finančné, časové) sú neadekvátne pre kvantitatívny prístup.

# Kvantitatívna analýza rizík

Využíva stupnicu s číselnými hodnotami v stanovených metrických jednotkách (finančných, časových a pod.).

Vyžaduje si historické dáta na určenie reálnej pravdepodobnosti realizácie rizika.

Použiteľná v organizáciach, kde sa dajú presne kvantifikovať dopady rizík (finačné inštitúcie, výrobne podniky).

# Hodnotenie dopadov

- Berieme do úvahy identifikované aktíva a ich hodnoty.
- „Čo by stálo opätovné vytvorenie aktíva?“
- „Aké dôsledky bude mať, keď aktívum nebude možné použiť minútu/hodinu/deň...?“
- Rôzne hrozby a zraniteľnosti majú rôzne vplyvy na aktíva (strata dôvernosti, integrity alebo dostupnosti).
- Dopady môžu byť vyjadrené v peňažných, technických alebo personálnych metrikách alebo v iných jednotkách.

# Pravdepodobnosti scenárov rizík

Máme: zoznam identifikovaných relevantných scenárov rizík zahŕňajúci identifikáciu hrozieb, dotknuté aktíva, využité zraniteľnosti a dopady; zoznamy všetkých existujúcich a plánovaných opatrení vrátane vyhodnotenia ich efektívnosti a stavu využívania.

Posúdime pravdepodobnosť scenárov prihliadajúc na skúsenosti a použiteľné štatistiky pre pravdepodobnosť hrozby; úmyselné zdroje hrozby (motiváciu, schopnosti a dostupné zdroje pre možných útočníkov), náhodné zdroje hrozby (geografické faktory napr. blízkosť chemických závodov, možnosť extrémneho počasia, záplavová zóna); faktory, ktoré môžu ovplyvniť ľudské chyby a zlyhania zariadení; existujúce opatrenia a ich efektívnosť znižovania zraniteľnosti.

# Stanovenie úrovne rizík - príklad

| | Pravdepodobnosť výskytu hrozby | Nízka | | | Stredná | | | Vysoká | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Jednoduchosť zneužitia | N | S | V | N | S | V | N | S | V |
| Hodnota aktíva | 0 | 0 | 1 | 2 | 1 | 2 | 3 | 2 | 3 | 4 |
| | 1 | 1 | 2 | 3 | 2 | 3 | 4 | 3 | 4 | 5 |
| | 2 | 2 | 3 | 4 | 3 | 4 | 5 | 4 | 5 | 6 |
| | 3 | 3 | 4 | 5 | 4 | 5 | 6 | 5 | 6 | 7 |
| | 4 | 4 | 5 | 6 | 5 | 6 | 7 | 6 | 7 | 8 |

zdroj STN ISO/IEC 27005

Hodnoty aktíva, úrovne hrozby a zraniteľnosť relevantné pre každý typ dopadu sú zoradené v matici, ako je napr. Matica na identifikáciu relevantnej miery rizika na stupnici od 0 do 8.

# Stanovenie úrovne rizík – iný príklad

| | | | | |
|---|---|---|---|---|
| **Pravdepodobnosť realizácie rizika** | vysoká | **2** | **3** | **4** |
| | stredná | **2** | **3** | **3** |
| | malá | **1** | **2** | **2** |
| | | malá | preukázateľná | vážna |
| | | **Rozsah škôd** | | |

Výsledná miera (stupeň) rizika priamo určuje spôsob zaobchádzania s rizikom. Interpretácia číselného ohodnotenia je nasledovná:

4 – čo najskôr musia byť prijaté opatrenia na zníženie rizika,
3 – opatrenia na zníženie rizika by mali byť prijaté (v dlhšom časovom horizonte),
2 – opatrenia nemusia byť prijaté, ale riziko je treba priebežne sledovať,
1 – akceptovateľné riziko, nevyžaduje prijatie bezpečnostných opatrení.

# FRAP (Facilitated Risk Analysis Proces)

Metodika analýzy rizík, ktorá:

- má formalizovaný kvalitatívny charakter,
- zohľadní bezpečnostné požiadavky procesov vo väzbe na IS,
- má vecné a rozsahom prakticky použiteľné výstupy,
- umožňuje aktívne zapojenie  vlastníkov informačných aktív.

Dôležitým prvkom FRAPu sú worskhopy.

Cieľom workshopu je identifikovať potenciálne riziká, ohodnotiť ich z hľadiska možného dopadu na bezpečnosť (narušenie utajenia, integrity, dostupnosti).

# Zvládanie a riadenie rizík

Návrh opatrení na zníženie rizík

- obídenie rizika: rozhodnutie zmeniť prostredie, v ktorom sa riziko vyskytuje tak, aby toto riziko neprichádzalo do úvahy,
- prenesenie rizika: rozhodnutie preniesť následky realizácie rizika mimo organizáciu,
- redukcia rizika: rozhodnutie pomocou vhodných opatrení dosiahnuť zníženie následkov realizácie rizika alebo zníženie pravdepodobnosti jeho realizácie,
- akceptácia rizika.

Počas výberu opatrenia je dôležité zvážiť náklady na obstaranie, implementáciu, správu, prevádzku, monitorovanie a údržbu opatrení oproti hodnote chránených aktív.

# Výber opatrení

## Opatrenia podľa  času ich realizácie

- preventívne opatrenia: vykonávajú sa pred vznikom rizika,
- reakčné opatrenia: vykonávajú sa po vzniku rizika (ich cieľom je redukcia škôd, ktoré riziko spôsobí, zníženie nákladov na zvládnutie dôsledkov rizika alebo zefektívnenie procesu zvládnutia situácie).

## Vyberáme najvýhodnejšiu možnosť z hľadiska nasledovných kritérií

- minimalizácia nákladov na realizáciu opatrení (napríklad finančné, časové, organizačné náklady),
- minimalizácia negatívnych dopadov opatrení na používateľov IS, nimi vykonávaných činnosti a iných neželaných efektov,
- dostupnosť zdrojov potrebných na realizáciu a prevádzku opatrení (napríklad technika, ľudské zdroje),
- zohľadnenie štandardne používaných postupov v organizácii pre danú oblasť rizík.

# Riadenie a monitorovanie rizík

Cieľom riadenia rizík je zníženie a udržiavanie závažnosti rizík na prijateľnej úrovni.

Riadenie rizík v praxi znamená predovšetkým:

- evidovanie rizík,
- sledovanie rizík,
- priebežné vyhodnocovanie rizík.

Vedenie organizácie prostredníctvom riadenia rizík získava:

- informácie o najdôležitejších rizikách, s ktorými sa organizácia stretáva,
- zabezpečenie primeranej úrovne uvedomovania si rizík v celej organizácii,
- ubezpečenie sa o účinnom zvládaní rizík.

# Monitorovanie rizík

Monitorovanie riadenia rizík je kontinuálne vykonávaný proces, ktorý permanentne overuje a ubezpečuje vedenie organizácie o tom, že riadenie rizík je funkčné a plní svoje úlohy.

Monitorovanie má poskytovať informácie o:

- priebehu riadenia rizík pre potreby vedenia organizácie,
- realizácii kontrolných aktivít v oblasti riadenia rizík,
- prijímaní opatrení na skvalitnenie procesu riadenia rizík,
- vyhodnotení účinnosti prijatých opatrení.

# Výsledky monitorovania rizík a ich riadenia

Monitorovanie riadenia rizík môže viesť k úprave alebo pridaniu prístupu, metodiky alebo nástrojov používaných v závislosti od

- identifikovaných zmien,
- iterácie posúdenia rizík,
- cieľa procesu riadenia rizík informačnej bezpečnosti,
- predmetu procesu riadenia rizík informačnej bezpečnosti (napr. celá organizácia, organizačná jednotka, informačný proces, jeho technická implementácia, aplikácia, pripojenie k internetu).

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

# Otázky a diskusia

Ďakujem za pozornosť

KPMG
cutting through complexity™