LYNX®

Informačné systémy
Bezpečnosť
Infraštruktúra

Bezpečnosť informačných systémov

RNDr. Ján Kromel, PhD., SCSA

Program

- Úvod
- ISO vs ISO
- ISO 31000
- ISO 31010
- ISO 27k
- ISO 27005
- Závery

Úvod

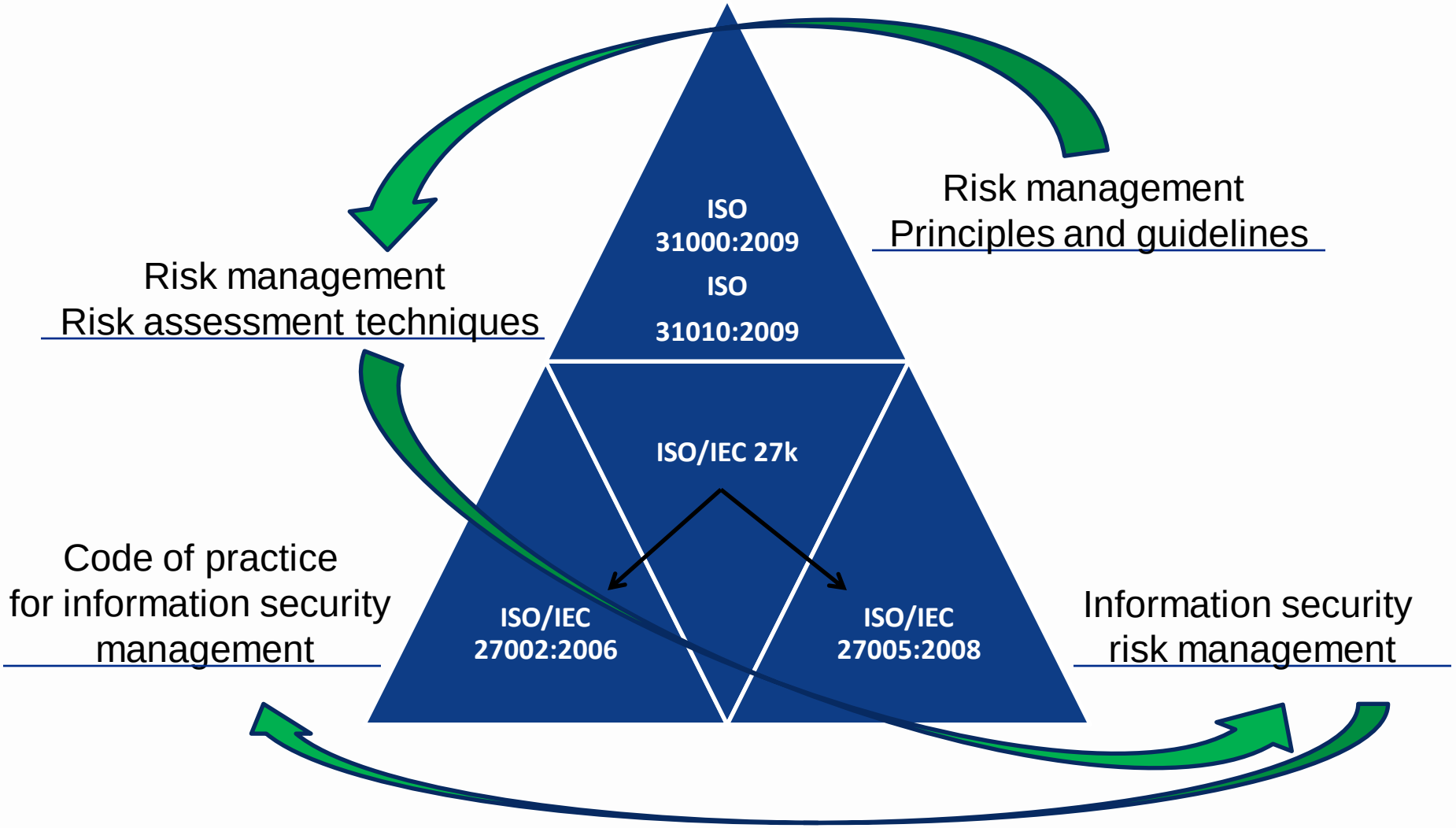
- Prečo vynakladať financie a čas na analýzu rizík ?
  - spoľahlivé a relatívne finančne nenáročné riešenie informačnej bezpečnosti
  - požiadavka zákona:
    - bezpečnostný projekt podľa zákona č. 428/2002 Z. z. o ochrane osobných údajov
    - výnos MF SR 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy – minimálne 1x ročne vykonávať analýzu rizík
  - požiadavka pre certifikáciu ISO/IEC 27001

Úvod

- Týka sa nás to vôbec? ISO 27k je aplikovateľná IBA na IT a my potrebujeme vyriešiť aj iné stránky bezpečnosti...

  - STN ISO/IEC 27002:2006:
    - „Informácie môžu existovať vo viacerých formách.“
    - „Informácie môžu byť vytlačené alebo napísané na papiery, uložené v elektronickej podobe, prenášané elektronickou cestou, ukázané vo filme alebo povedané v rozhovore.“
    - „Bez ohľadu na formu informácií alebo na formu zdieľania resp. ukladania, informácie by mali byť stále adekvátne chránené.“

ISO vs ISO


ISO
31000:2009
ISO
31010:2009
Risk management
Principles and guidelines
Risk management
Risk assessment techniques
ISO/IEC 27k
Code of practice
for information security
management
ISO/IEC
27002:2006
ISO/IEC
27005:2008
Information security
risk management

STN ISO 31000

- Risk management. Principles and guidelines (Manažérstvo rizika. Zásady a návody)

- Terminológia
- Definícia základných princípov manažmentu rizík
  - Princípy manažmentu rizík
  - Všeobecná „metodika“ (framework) manažmentu rizík
  - Proces manažmentu rizík

a) Vytvára hodnotu

b) Neoddeliteľnou súčasťou organizačných procesov

c) Časť rozhodovania

d) Explicitne adresuje neistotu

e) Systematický, štrukturovaný a včasný

f) Založený na najlepšie dostupných informáciách

g) Na mieru

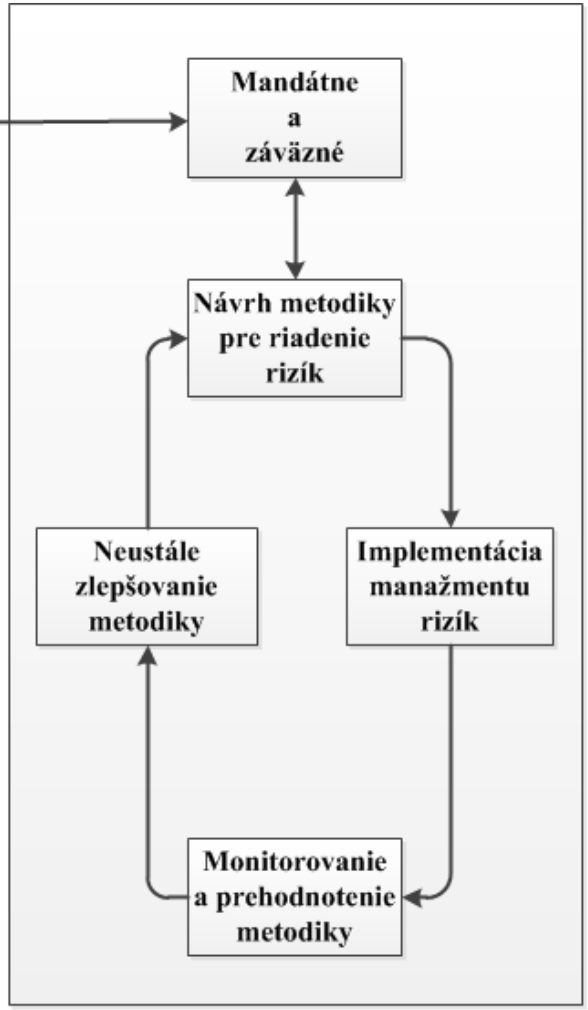
h) Berie do úvahy ľudské a kultúrne faktory

i) Transparentný a širokozáberový

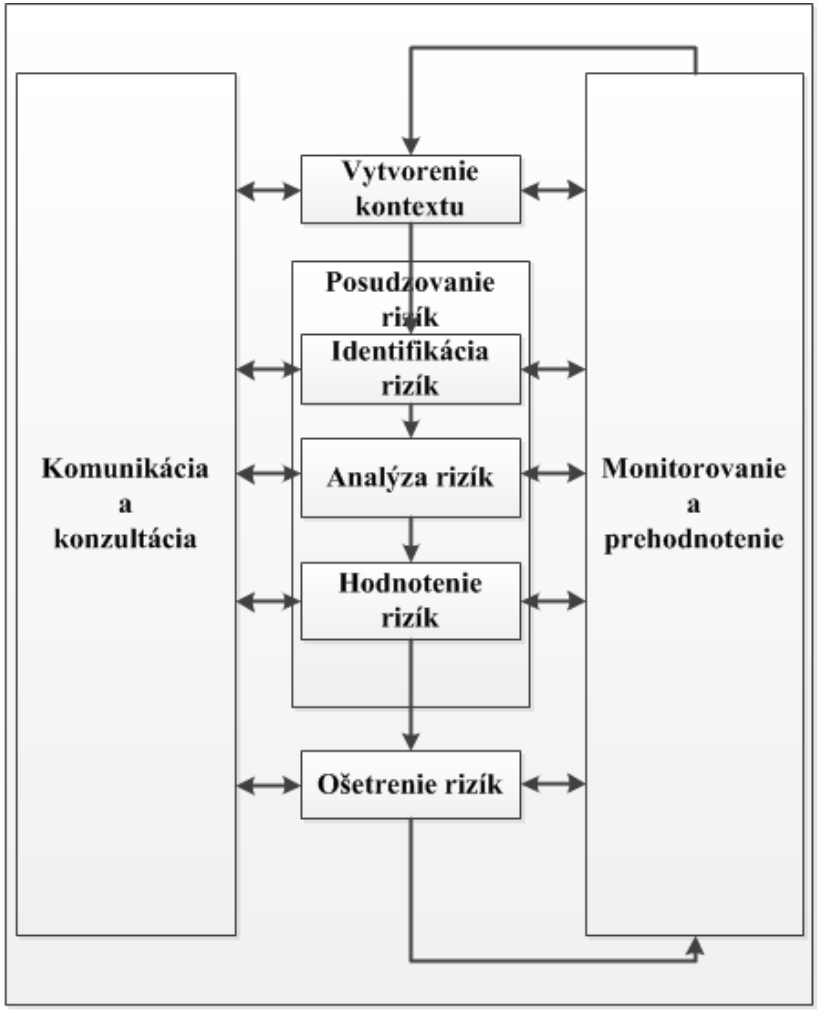
j) Dynamický, vyvíjajúci sa a reagujúci na zmeny

k) Uľahčuje kontinuálne zlepšenia organizácie

Princípy pre manažment rizík



Metodika pre manažment rizík



Proces manažmentu rizík

STN ISO 31010

- Risk management. Risk assessment techniques (Manažérstvo rizika. Techniky posúdenia rizika)

- 31 metód pre potreby ohodonetia rizík
  - široký záber, nielen pre IT
- Metódy rozdelené a opísané podľa parametrov:

  - Identifikácia rizík
  - Analýza rizík – analýza dopadov
  - Analýza rizík – kvalitatívny, kvantitatívny alebo semi-kvantitatívny odhad pravdepodobnosti
  - Analýza rizík - posudzovanie účinnosti akýchkoľvek existujúcich opatrení
  - Analýza rizík - odhad úrovne (miery) rizika
  - Ohodnotenie rizík

STN ISO 31010

- Parametre pre výber metódy:
  - Zložitosť analyzovaného problému
  - Zložitosť vybranej metódy
  - Povaha a miera neistoty z ohodnotenia rizík
  - Časová náročnosť analýzy
  - Odborná náročnosť na výkon analýzy
  - Finančná náročnosť

STN ISO 31010

- Príklady metód:
  - Vyhľadávacie metódy:
    - Kontrolné zoznamy (check-lists)
    - Prvotná analýza hrozieb (Preliminary hazard analysis)
  - Podporné metódy:
    - Brainstorming
    - Analýza ľudskej spoľahlivosti (Human reliability analysis)
  - Scenárová analýza:
    - Analýza pomocou scenára (Scenario analysis)
    - Analýza stromu udalostí (Event tree analysis)
  - Funkčná analýza:
    - Analýza spôsobu a dôsledku porúch (Failure mode effect analysis)
    - Analýza parazitného obvodu (Sneak circuit analysis)

STN ISO 31010

- Ohodnotenie kontrolných mechanizmov:
  - Analýza ochrannej vrstvy (Layer of protection analysis)
  - Analýza typu motýlik (Bow tie analysis)
- Štatistické metódy:
  - Markovova analýza (Markov analysis)
  - Bayesova štatistika a Bayesove siete (Bayesian statistics and Bayes Nets)
- Iné metódy:
  - FN krivky (FN curves)
  - **Matica dopad/pravdepodobnosť (Consequence/probability matrix)**

ISO 27k

ISO 27k

- Celá sústava noriem ISO: 27000, 27001, 27002, 27003, 27004, 27005, 27006, 27011, 27031, 27033-1, 27799 a ďalšie v príprave

- Analýza rizík:

  - ISO 27000 – Prehľad a slovník
  - ISO 27002 – Súbor postupov pre riadenie informačnej bezpečnosti
  - **ISO 27005 – Riadenie rizík bezpečnosti informácií**
  - ISO 27799 – Management bezpečnosti informácií v zdravotníctve podľa normy ISO / IEC 27002

ISO 27005

- Postup analýzy rizík:

  - Zoznámenie sa s analyzovaným prostredím
  - Stanovenie hraníc prostredia

  - Identifikácia aktív
  - Klasifikácia aktív

  - Identifikácia hrozieb
  - Ohodnotenie hrozieb

  - Identifikácia zraniteľností – **ISO 27002**
  - Ohodnotenie zraniteľností

  - Ohodnotenie rizík
  - Návrh opatrení
  - Určenie zvyškových rizík

ISO 27005

- Aktívum
  - Všetko čo má pre subjekt hodnotu
  - Stanovenie je v niektorých prípadoch komplikované
  - Určenie vlastníkov resp. správcov aktív
  - Ohodnotenie je zvyčajne „bolestivý“ proces – napr. MS Office

ISO 27005

- Hrozba
  - Možná príčina neželaného incidentu, ktorý môže vyústiť do poškodenia systému alebo subjektu
  - Rôzneho charakteru – napr. prírodné, spoločenské, technické...
  - Ohodnotenie si vyžaduje dokonalé znalosti prostredia a požiadaviek použitej metódy

ISO 27005

- Zraniteľnosť
  - Slabina aktíva alebo skupiny aktív, ktorá môže byť zneužitá hrozbami
  - ISO 27002 – pre potreby vysokoúrovňovej analýzy
  - Nízkoúrovňová analýza – špecifické check-listy, odporúčania a best practices pre jednotlivé časti systému
  - Vysokoúrovňová analýza – dostačujúca pre „legislatívne“ potreby

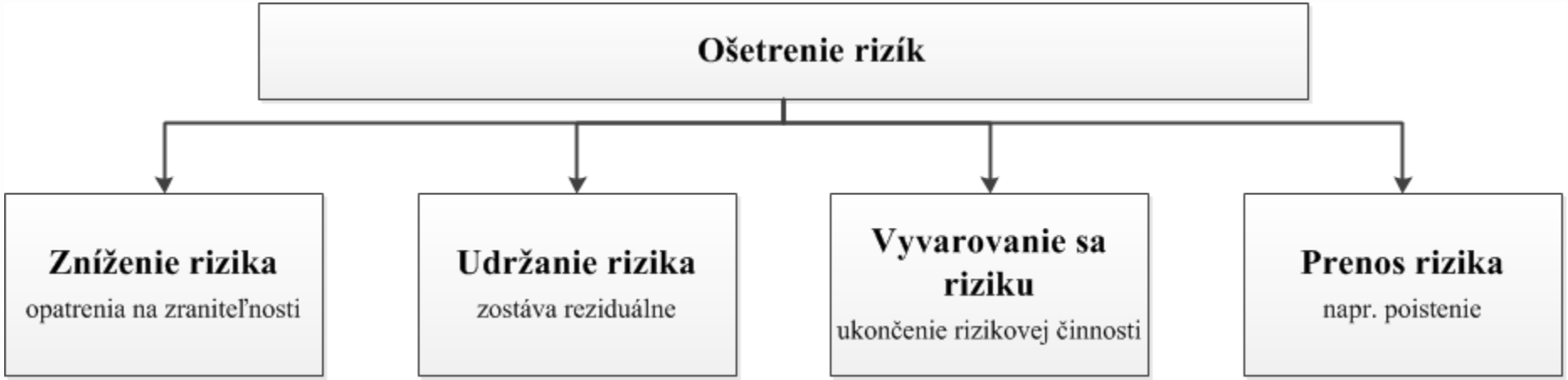
ISO 27005

- Riziko
  - Kombinácia pravdepodobnosti nastania udalosti a jej možného následku
  - Priame spojenie s **ISO 31010**

Matica dopad/pravdepodobnosť (Consequence/probability matrix)

	Pravdepodobnosť vzniku hrozby	Veľmi nízka	Nízka	Stredná	Vysoká	Veľmi vysoká
Dopad hrozby	Veľmi nízky	0	1	2	3	4
	Nízky	1	2	3	4	5
	Stredný	2	3	4	5	6
	Vysoký	3	4	5	6	7
	Veľmi vysoký	4	5	6	7	8

ISO 27005


Ošetrenie rizík
Zníženie rizika
opatrenia na zraniteľnosti
Udržanie rizika
zostáva reziduálne
Vyvarovanie sa riziku
ukončenie rizikovej činnosti
Prenos rizika
napr. poistenie

ISO 27005

- Opatrenie
  - Prostriedok manažmentu rizika, vrátane politík, procedúr, smerníc, praktík alebo organizačných štruktúr, ktoré môžu mať administratívny, technický, riadiaci alebo právny charakter
  - V prípade vysokoúrovňovej analýzy ICT/IS – ISO 27002
  - Nízkoúrovňová analýza – best practices, system designs, odporúčania výrobcov...

ISO 27005

- Zvyškové riziko
  - Zostatkové riziko v analyzovanom systéme po aplikácii opatrení

ISO 27005

- Zvyškové riziko
  - Prijateľné vs Neprijateľné
  - Neprijateľné – aplikácia alternatívnych opatrení, napr.

BUSINESS CONTINUITY MANAGEMENT

Ďakujem za pozornosť

jan.kromel@lynx.sk