



Informačné systémy  
Bezpečnosť  
Infraštruktúra



# Požiadavky normy ISO 31000 na manažment rizík

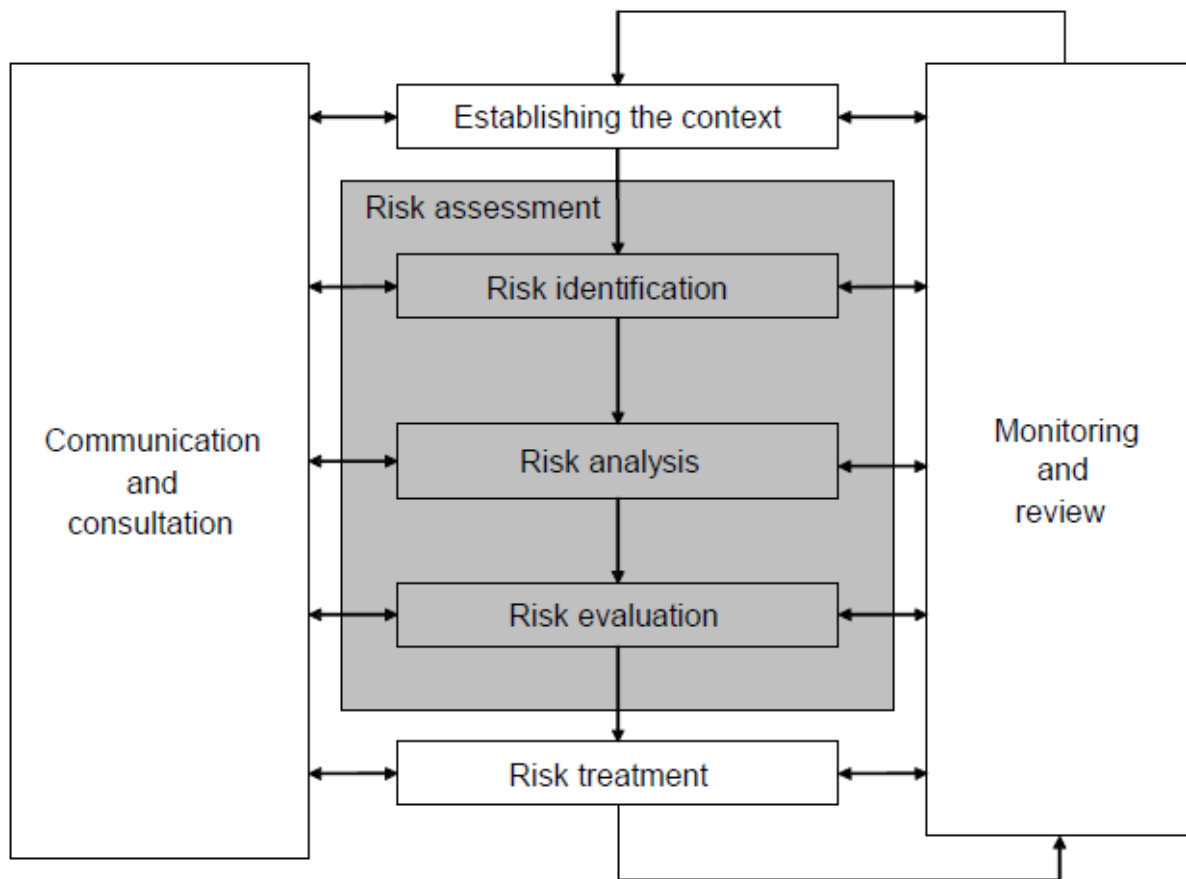
**Ing. Ladislav Martinček, CISSP, GCFA**

ISACA Open Day , 18.5.2011

## História ISO 31 000

- AS/NZS 4360:1996 – Risk Management  
(aj ako STN 01 0380)
- AS/NZS 4360:2004
- Guide 73 ( terms),
- AS/NZS ISO 31000:2009 Risk Management - Principles and Guidelines

# Hlavný proces



# Communication and consultation

Komunikácia a konzultácie

Prechádza všetkými procesmi

Konzultácie

- Interné (interní experti, zainteresované osoby)
- Externé (spoločnosti zaoberajúce sa bezpečnosťou)

## Establishing the context

Obsahová náplň manažmentu rizík

Určiť základné požiadavky manažmentu

- určiť náplň riadenia rizík určením jeho hraníc, organizačnej štruktúry, aktivít tímu a zdrojov.
- určiť základné role a zodpovednosti v rámci riadenia rizík a kompetenčné vzťahy s ostatnými organizačnými jednotkami, určenie podmienok na vykonávanie činností a kritériá hodnotenia

# Establishing the context

Obsahová náplň manažmentu rizík

Určiť vonkajšie prostredie

- fyzické okolie, ktoré na aktívum pôsobí ( pre fyzickú bezpečnosť napríklad - prírodné podmienky, ako sú záplava, zosuv pôdy, vietor, mráz, prašnosť ... )
- vplyvy ľudskej činnosti (pre fyzickú bezpečnosť napríklad - sociálne podmienky ľudí v okolí, vzdialenosti obydlií, cesty alebo komunikácie)

# Risk assessment

Hodnotenie rizík pozostáva z :

- Identifikácia rizík
- Analýza rizík
- Ohodnotenie rizík

Na hodnotenie rizík – využitie podľa ISO 31 010 (31 modelov)

## Risk assessment

ISO/IEC 31010:2009 poskytuje ďalšiu príručku na výber a aplikáciu niektorej zo systematických techník hodnotenia rizík. Vykonaná analýza rizík zvažuje možnosti spôsobovania, zdrojov, pravdepodobnosti a súvislostí hodnotených rizík.

Opatrenia manažmentu by mal identifikovať a zhodnotiť efektívnosť hodnotenia rizík a určiť úroveň zostatkových rizík. Po analýze rizík a určení úrovne rizika je potrebné rozhodnúť o ďalšom riadení rizík.

# Risk treatment

## Ošetrenie rizík

- Udržanie rizika (zostáva reziduálne)
- Zníženie rizika (opatrenia na zraniteľnosti)
- Vyvarovanie sa riziku (ukončenie rizikovej činnosti)
- Prenos rizika (napr. poistenie)
  
- Plán realizácie opatrení

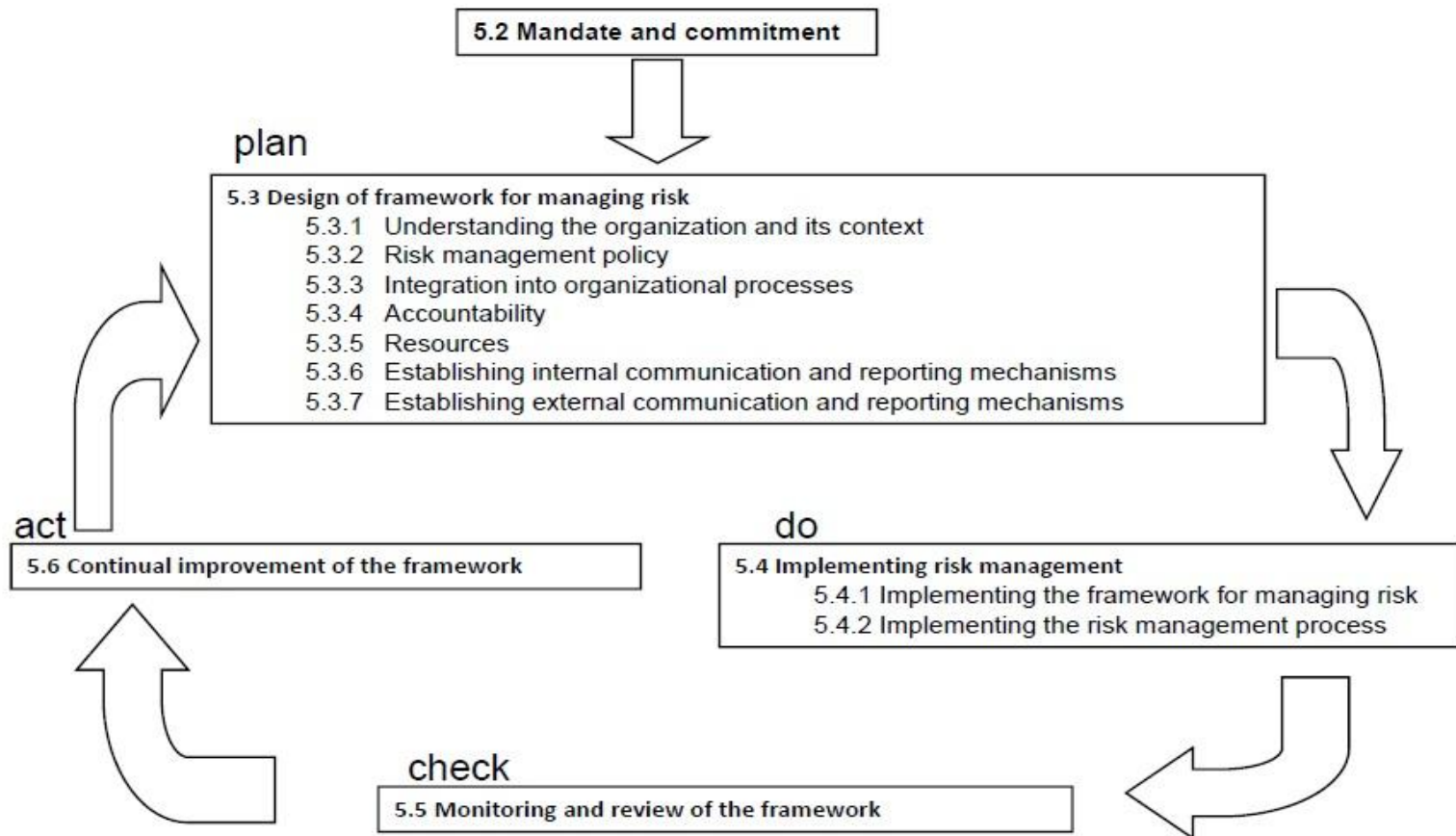
# Monitoring and Review

Monitorovanie a prehodnotenie

Uplatňuje sa vo všetkých častiach procesu

Je aktivačným prvkom modelu PDCA (plánovanie, zavedenie, kontrola, využitie)

# Analógia PDCA



## Mandate and commitment

Udelenie mandátu a prevzatie záväzkov

- Riadenie rizík nie je iba jedným z projektov; je to trvalá aktivita požadujúca trvalé záväzky.
- Musí byť pridelená vrcholným manažmentom na implementáciu do úrovne stredného manažmentu a podporovaná musí byť manažmentom na každej úrovni aby sa stala trvalou aktivitou.

## Design of framework for managing risk

### Návrh rámca pre riadenie rizík

- Ako všetky dobré projekty, procesy a stratégie aj proces riadenia rizík musí byť vhodne navrhnutý aby mohol byť vôbec implementovaný.
- Definovaním rámca riadenia rizík, formulovaním politiky riadenia rizík, zvedením procesu do praxe, určením zdrojov a zodpovedností sú dané kľúčové elementy návrhu na účinný rámec riadenia rizík.
- Vhodne navrhnuté periodické reportovanie zúčastneným stranám a efektívny mechanizmus komunikácie účinne podporí implementáciu.

# Implementing risk management

## Implementácia riadenia rizík

- Ak je už raz rámec riadenia rizík navrhnutý, implementácia je iba o prenesení teórie do života.
- Je to o uistení sa, že proces riadenia rizík je pochopený vlastníkmi rizík, aktivity riadenia rizík sú skutočne zaradené a pochopenie rizík je faktorom rozhodovania a riadenia obchodných procesov.

# Monitoring and review

## Monitorovanie a prehodnotenie

- Je zaradenie uistenia sa, že rôzne elementy a aktivity riadenia rizík skutočne efektívne fungujú v súlade s očakávaniami. Každý rozdiel musí byť dokumentovaný a napravený.

# Continual improvement of the framework

Neustále zlepšovanie rámca

- Toto je o vylepšovaní a zdokonaľovaní kľúčových elementov riadenia rizík buď na zlepšenie aktuálnych procesov alebo postupu dopredu k dokonalejšiemu rámcu riadenia rizík.

# Princípy riadenia rizík

Hlavné zdokonalenie ISO 31000 je pridanie jedenástich princípov ako návodu na uplatnenie riadenia rizík.

## 1. Vytváranie hodnôt

- Prispieva k dosiahnutiu cieľov.
- Chráni hodnoty – minimalizuje riziká, ochraňuje ľudí, systémy a procesy.

# Princípy riadenia rizík

## 2. Je integrálnou súčasťou procesov organizácie

- Riadenie rizík nie je oddelenou samostatnou aktivitou systému manažovania organizácie.
- Riadenie rizík je súčasťou procesu a nie iba pridanou úlohou na súlad so štandardami.

## 3. Je súčasťou rozhodovania

- Riadenie rizík pomáha pri výbere rozhodnutí, priorít a rozlišovať medzi alternatívami.
- Pomáha alokovať drahé zdroje.

## Princípy riadenia rizík

### 4. Otvorené riešenie pochybností

- Riadenie rizík sa otvorene zaoberá pochybnosťami, ich podstatou a ako môžu byť riešené.
- Riadenie rizík rieši pochybnosti, nezaoberá sa ale úrovňou pochybností.

### 5. Systematickosť, štruktúrovanosť a časovosť

- Systematický, časový a štruktúrovaný prístup na riadenie rizík prispieva k efektivite a konzistentným, porovnateľným a spoľahlivým výsledkom.
- Čím angažovanejší, tým efektnejší a efektívnejší.

# Princípy riadenia rizík

## 6. Založený na najprístupnejších informáciách

- Vstupy do procesu riadenia rizík sú založené na informačných zdrojoch ako sú historické údaje, skúsenosti, spätné ohlasy zainteresovaných, pozorovania, predpovede a posudky expertov.
- Informácie stoja peniaze. Správne informácie nie sú vždy prístupné.
- Požaduj viac informácií, tak ako stúpa úroveň rizika.

# Princípy riadenia rizík

## 7. Šité na mieru

- Riadenie rizík je závislé na internom a externom kontexte organizácie a profile rizika.
- Rôznorodosť v pôsobení rizík a rôznorodosť opatrení.

## 8. Brať do úvahy ľudské a kultúrne faktory

- Riadenie rizík rozpoznáva možnosti, pohľady a zámery ľudí, ktoré môžu byť v každej organizácii odlišné.

# Princípy riadenia rizík

## 9. Transparentnosť a prístupnosť

- Vhodné a časovo aktuálne zapojenie všetkých zúčastnených na všetkých úrovniach organizácie na uistenie sa, že výstupy riadenia rizík sú relevantné a aktuálne.
- Riadenie rizík musí byť definované v náplni práce/ zmluvách o vykonaní prác a každoročne posudzované

## 10. Dynamickosť, opakovateľnosť a prístupnosť zmenám

- Externé a interné udalosti sa stávajú, obsah a znalosti sa menia, uplatňuje sa monitoring a revízia, nové riziká sa vynoria, niektoré sa zmenia a iné sa stratia.
- Je potrebné udržať relevantné a adresné riadenie rizík tak ako podporovať rozhodnutia a stratégie.
- Pravidelná revízia katalógu rizík a jeho rámca.
- Interný auditor má byť informovaný o katalógu rizík organizácie.

# Princípy riadenia rizík

## 11. Uľahčenie neustáleho zlepšovania a posilňovania organizácie

- Organizácia by mala vyvíjať a implementovať stratégie na zdokonalenie riadenia rizík v súlade so zlepšovaním všetkých aspektov ich manažmentu.
- Zdokonaľovanie a zlepšovanie stratégie by byť súčasťou plánu riadenia rizík.



**Ďakujem za pozornosť**

**ladislav.martincek@lynx.sk**