Konzultace

Informační bezpečnost

Nástroje pro podporu řízení

Certifikace a vzdělávání

Potřeba jednotného řízení a konsolidace rizik

13. ročník konference ISSS

Hradec Králové

Josef Šustr

12. dubna 2010

ITEG

Riziko

- Riziko je **potenciální možnost**, že se něco stane, co ovlivní dosažení našich cílů.
- Riziko má 2 parametry
  - pravděpodobnost, že se něco stane,
  - následky, když se to stane.
- Riziko NENÍ nedostatek !!

Praxe: Riziko má obvykle negativní následky (škoda).
Obecně mohou být i pozitivní výsledky (příležitosti).

- Každý z nás „nějak“ řídíme rizika.
- Převážná většina rizik je řízena **neformálně** a často **intuitivně**.

ITEG

Oblasti rizik

V orgánech veřejné správy i komerčních podnicích lze nalézt například následující rizika:

- strategického směrování
- organizační
- personální a kompetenční
- shody s legislativou a dobrými mravy
- financí, účetnictví a výkaznictví
- hlavních a podpůrných procesů
- projektů
- změn
- obchodní, marketingová a smluvní
- investiční
- jakosti produkce
- právních sporů
- pojišťovací strategie
- bezpečnosti
  - aktiv (security)
  - osob (safety)
- podvodů a jiné trestné činnosti
- korupční rizika
- ….. a mnohá další

ITEG

„Klasické“ oblasti řízení rizik

- Rizika bezpečnosti informací
  - v posledních 10 – 15 letech v souvislosti se strmým nárůstem závislosti organizací na informačních systémech
  - ČSN ISO/IEC 27005:2009 (ISO 13335, CRAMM atd.)
- Rizika provozní a finanční
  - prevence před falšováním účetních výkazů (Sarbanes-Oxley Act v USA)
  - zákon č. 320/2001 Sb., o finanční kontrole (COSO ERM, CHJ-6 atd.)
- Rizika projektů
  - všechny projekty spolufinancované ze strukturálních fondů EU
- Rizika klíčových rozhodnutí
  - následky připravovaných změn a realizace (nerealizace) navrhovaných opatření

ITEG

Potřeba konsolidace rizik

- Různé světy, různé metriky, různí adresáti:
  - radnice připravuje programové prohlášení,
  - zastaralá technika zvyšuje pravděpodobnost výpadků počítačové sítě,
  - je třeba splnit legislativní požadavky
  - atd.

- Nutno umět **porovnat** rizika z různých oblastí z hlediska možných škod / příležitostí …
- … a vybrat taková opatření, která povedou k **efektivnímu pokrytí největších rizik**

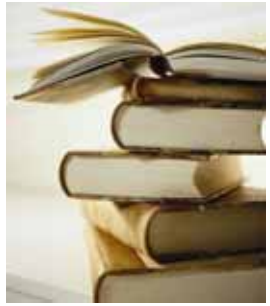
ITEG

ISO 31000

- Potřeba standardizace dlouhodobě nazrávala
  - Turnbull framework (1999)
  - Casualty Actuarial Society Enterprise Risk Management (CAS ERM, 2003)
  - Committee of Sponsoring Organizations Risk Management Integrated Framework (COSO ERM, 2006)
  - ONR 49002-1:2004 Risk management for organizations and systems (Rakousko)
  - AS/NZS 6340:2004 Enterprise Risk management (Austrálie)
- Mezinárodní organizace pro stadardizaci (ISO)
  - ISO 31000:2009
    Risk management – Principles and guidelines
  - ISO/IEC 31010:2009
    Risk management – Risk assessment techniques
  - ISO Guide 73:2009
    Risk management - Vocabulary

ITEG

Klíčové vlastnosti ISO 31000



- ISO 31000 nijak nevynucuje uniformitu řízení rizik v organizaci a mezi organizacemi
  - různé metody, metodiky i nástroje
- Smyslem ISO 31000 je **harmonizovat procesy managementu rizik** v organizaci v rozsahu:
  - zacelení mezer v systému odpovědnosti za řízení rizik,
  - „zarovnání“ cílů řízení rizik v jednotlivých oblastech,
  - nastavení komunikačních mechanizmů pro sdílení informací o řízení rizik (jazyk, struktura),
  - vytvoření jednotných kritérií a metrik pro hodnocení rizik (umožnění srovnání rizik z různých oblastí vztahujících se ke stejným cílům),

ITEG

Centrum řízení rizik

- Systém umožňující
  - rizika identifikovat, hodnotit, porovnávat, klasifikovat a ošetřovat,
  - provazbu na související úkoly, projekty, opatření a odpovědnost za jejich realizaci,
  - poskytovat aktuální informace zainteresovaným osobám a umožnit rychle zjistit stav a vývoj zejména největších rizik.
- Realizace
  - vhodný nástroj – „Katalog rizik“ (od sešitu po systémy typu GRCM),
  - sada procesů,
  - odpovědná osoba.

ITEG

Aktuálnost pro orgány veřejné správy

- Zákon č. 320/2001 Sb. o finanční kontrole ve VS, §25:
  - vedoucí orgánu VS je povinen zavést a udržovat vnitřní kontrolní systém způsobilý včas zjišťovat, vyhodnocovat a minimalizovat provozní, finanční, právní a jiná rizika,
  - všichni vedoucí zaměstnanci … jsou povinni podávat vedoucímu orgánu VS včasné a spolehlivé informace … o vzniku významných rizik…
- ISMS (Systém řízení rizik bezpečnosti informací)
  - analýzy rizik jsou předepsány (ČSN ISO/IEC 27001, ČSN ISO/IEC 27005)
- Vztahy s dodavateli
- Velké projekty

ITEG

Jsou ovšem i problémy…

- Mechanické svalení odpovědnosti za řízení rizik na útvary interního auditu
  - ale názory se vyvíjejí
  - „Koordinátor řízení rizik“ mimo interní audit
- Katalog rizik je často jen seznamem náhodně sebraných rizik, nedostatků a nápadů

Řešení:

- *systematická práce s riziky*
- *využití dlouhodobě sesbíraných zkušeností a osvědčených praktik ERM*

ITEG

Závěr

Děkuji za pozornost.

Prosím Vaše názory, dotazy…

Ing. Josef Šustr
+ 420 603 234 517
josef.sustr@iteg.cz

ITEG a.s.
City Tower, Hvězdova 1716/2b, 140 78 Praha 4
www.iteg.cz

ITEG