Analýza rizik

Základní pojmy z oblasti analýzy rizik:

- **aktivum** (Asset) – vše co má pro společnost nějakou hodnotu a mělo by být odpovídajícím způsobem chráněno,
- **hrozba** (Threat) – jakákoliv událost, která může způsobit narušení důvěrnosti, integrity a dostupnosti aktiva
- **zranitelnost** (Vulnerability) – vlastnost aktiva nebo slabina na úrovni fyzické, logické nebo administrativní bezpečnosti, která může být zneužita hrozbou.
- **riziko** – pravděpodobnost, že hrozba zneužije zranitelnost a způsobí narušení důvěrnosti, integrity nebo dostupnosti.
- **opatření** (Countermeasure) – opatření na úrovni fyzické logické nebo administrativní bezpečnosti, které snižuje zranitelnost a chrání aktivum před danou hrozbou
- **ohrožení** (Exposure) – skutečnost, že existuje zranitelnost, která může být zneužita hrozbou
- **narušení** (Breach) – situace, kdy došlo k narušení důvěrnosti, integrity nebo dostupnosti v důsledku překonání bezpečnostních opatření.

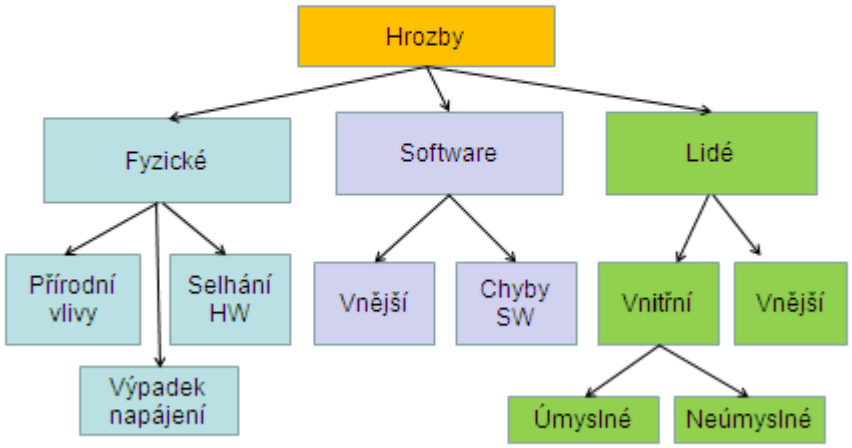
Aktivem je cokoliv, co má pro organizaci **hodnotu**:

- fyzická aktiva (např. počítačový hardware, komunikační prostředky, budovy
- informace (dokumenty, databáze,...)
- software
- schopnost vytvářet určité produkty nebo poskytovat služby – know-how
- pracovní sílu, školení pracovníků, znalosti zaměstnanců, zapracování apod.
- nehmotné hodnoty (např. abstraktní hodnota firmy, image, dobré vztahy atd..)

Postup při analýze rizik

1. Stanovení hranice
2. Identifikace aktiv
3. Stanovení hodnoty aktiv (+seskupení)
4. Identifikace hrozeb
5. Analýza hrozeb
6. Stanovení pravděpodobnosti jevu
7. Měření rizika

Analýza rizik - přehled



Analýza rizik by měla odpovědět na tyto otázky:

- Co se stane, když informace nebudou chráněny?
- Jak může být porušena bezpečnost informací?
- S jakou pravděpodobností se to stane?

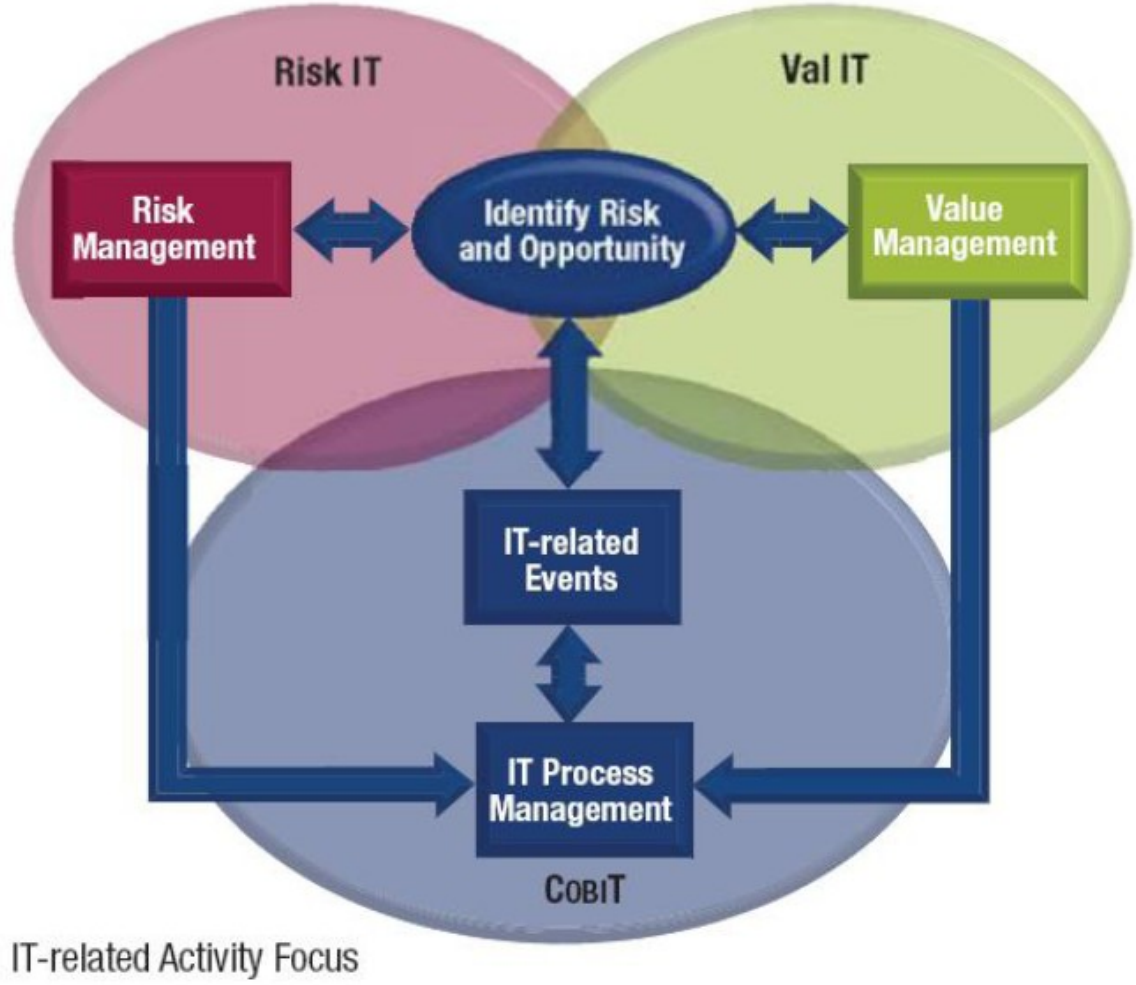
Co je cílem?

- Zajištění důvěrnosti dat
- Zajištění integrity dat
- Zajištění dostupnosti

Metodiky pro analýzu rizik

- **CRAMM** (CCTA Risk Analysis and Management Method)
  - BS7799, ISO/IEC 27001:2005
  - Vyžadováno např. u IS pro NATO
- **OCTAVE-S** (Operationally Critical Threat, Asset and Vulnerability Evaluation) – pro menší firmy
- **RISK IT –** kompatibilní s metodikou CoBit

RISK IT



Zdroj: FISCHER, U. Risk IT [prezentace]. Rolling Meadows, USA : ISACA, 2009. Dostupné z WWW: <http://www.isaca.org/Knowledge-Center/Standards/Documents/Risk-IT-Overview.ppt>.

OCTAVE-S

Fáze	Proces	Aktivita
Fáze 1: Návrh profilů hrozeb pro aktiva	Proces S1: Určení informací o organizaci	S1.1 Stanovení kritérií pro posuzování dopadů
		S1.2 Určení aktiv organizace
		S1.3 Zhodnocení bezpečnostních postupů organizace
	Proces S2: Vytvoření profilů hrozeb	S2.1 Zvolení kritických aktiv
		S2.2 Určení bezpečnostních požadavků na kritická aktiva
		S2.3 Určení hrozeb pro kritická aktiva
Fáze 2: Určení zranitelností infrastruktury	Proces S3: Šetření počítačové infrastruktury ve vztahu ke kritickým aktivům	S3.1 Zjištění přístupových cest
		S3.2 Analyzování procesů spojených s technologiemi

OCTAVE-S

Fáze 3: Vytvoření bezpečnostní strategie a plánů	Proces S4: Identifikování a analýza rizik	S4.1 Ohodnocení dopadů hrozeb
		S4.2 Stanovení pravděpodobností pro hodnotící kritéria
		S4.3 Stanovení pravděpodobností výskytu hrozeb
	Proces S5: Vytvoření strategie ochrany a plánů pro zmírnění dopadů	S5.1 Zhodnocení současné bezpečnostní strategie
		S5.2 Zvolení přístupů pro snížení dopadů hrozeb
		S5.3 Vytvoření plánů pro snížení rizika dopadů hrozeb
		S5.4 Určení změn v bezpečnostní strategii
		S5.5 Definování dalších kroků

Bezpečnostní studie

- Odhad hrozeb
- Škoda způsobená incidentem – dočasná nebo trvalá?
- Analýza zranitelnosti
- Odhad dopadů incidentu:
  - Stanovením finančních nákladů
  - Stupnice 1-10
  - Ohodnocení – nízký, střední, vysoký
- Analýza rizik: riziko je potenciální možnost, že daná hrozba využije zranitelnosti

Bezpečnostní politika

Bezpečnostní politika je soubor pravidel, který má za úkol zajistit bezpečnost IS s přihlédnutím k nákladové efektivitě a musí odpovídat na tyto otázky:

- Kdo nese zodpovědnost?
- Kdy to bude efektivní?
- Jak to bude vynuceno?
- Kdy a jak to bude uvedeno do praxe?

Standardní kroky pro zajištění bezpečnosti:

- studie informační bezpečnosti – aktuální stav,
- riziková analýza,
- tvorba bezpečnostní politiky - vytýčení cílů,
- bezpečnostní standardy – pro naplnění cílů bezpečnostní politiky,
- bezpečnostní projekt – technická opatření,
- implementace bezpečnosti – nasazení výše uvedeného,
- monitoring a audit – prověřování, zda vytvořené bezpečnostní mechanismy odpovídají dané situaci.

Bezpečnost je *kompromis* mezi **úrovní zabezpečení** a **náklady**.

Business Continuity Management

je manažerská disciplína, která se zaměřuje na identifikaci potencionálních dopadů, jež organizaci hrozí po havárii. Vytváří rámec pro zajištění určité míry odolnosti a schopnosti reagovat na neočekávané události

Havarijní plán

- Postup a reakce v případě havárie, poruchy nebo nefunkčnosti IS
- Součást „Bezpečnostní politiky“
- Uživatel IS by měl vědět KOHO a JAK informovat v případě poruchy