# Řízení informačních rizik

AEC

Služby v oblasti řízení informačních rizik zahrnují posouzení aktuálního stavu bezpečnosti IS, tvoří důležitý podklad pro zajištění informační a kybernetické bezpečnosti a slouží jako podklady pro rozhodování o investicích do bezpečnosti.

Důležitou součástí je také zajištění shody s požadavky akcionářů, regulátorů a klientů.

## V této oblasti Vám můžeme nabídnout:

- Analýzu současného stavu – rychlá identifikace slabých míst a nedostatků v zabezpečení, návrh doporučení pro jejich odstranění.
- Analýzu rizik IS – komplexní identifikace aktiv, hrozeb a slabých míst, kvantifikace rizik, kterým je systém vystaven, podpora při rozhodování o řízení rizik.
- Návrh plánu zvládání rizik – návrh bezpečnostních opatření/doporučení.
- Specializované audity/analýzy zaměřené na určitou oblast.

**Společnost AEC provádí analýzy a audity IS na základě bohatých zkušeností získaných během svého dlouhodobého působení na trhu v oblasti bezpečnosti ICT a podle uznávaných standardů:**

- ISO 31000 Management rizik,
- Normy řady ISO/IEC 27000 zaměřené na řízení bezpečnosti.
- Naši metodiku lze přizpůsobit požadavkům klienta, případně legislativy (např. Zákon o kybernetické bezpečnosti).

**www.aec.cz**

# Řízení informačních rizik

## Kdy provést analýzu rizik?

**Analýza rizik informačního systému se typicky provádí v následujících situacích:**

- Vznikl požadavek na zjištění aktuálního stavu bezpečnosti IS.
- Existuje potřeba kvantifikace rizik, kterým je Váš informační systém vystaven.
- Padlo rozhodnutí o potřebě řídit informační bezpečnost podle jasně definovaných pravidel.
- Chcete zavést systém řízení informační bezpečnosti (ISMS).
- Jde o požadavek auditorských firem, akcionářů apod.
- Potřebujete podklad pro rozhodování o implementaci nákladných bezpečnostních opatření.
- Jedná se o požadavek legislativy (například Zákon o kybernetické bezpečnosti).
- V případě vážných pochyb o bezpečnosti informací (nedůvěra v třetí stranu, která spravuje Váš IS, Vaše společnost se stala terčem útoku apod.).

## Mezi hlavní přínosy realizace služeb z oblasti řízení informačních rizik patří:

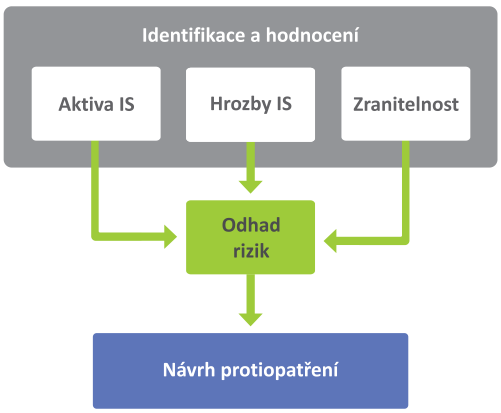
- Určení priorit pro další investice a projekty v oblasti bezpečnosti;
- Stanovení optimálního poměru mezi investicemi a dosaženou úrovní zabezpečení;
- Získání informací o dosažené úrovni bezpečnosti IS nezávislou stranou;
- Identifikace rizik a slabých míst, které bezprostředně ohrožují klíčové funkce a aktiva organizace;
- Vytvoření podkladů pro tvorbu bezpečnostní dokumentace ICT v organizaci;
- Identifikace hrozeb typu úniku dat, zneužití privilegií, lidské chyby atd. včetně možných scénářů zneužití;
- Významné zvýšení bezpečnosti IS implementací navržených opatření;
- Získání argumentů pro rozhodnutí managementu o přidělení investic do bezpečnosti IS.

## Naše přednosti

Společnost AEC využívá svých dlouholetých zkušeností při budování systémů řízení informační bezpečnosti a provádění úloh s tím spojených.

**Naše řešení charakterizuje:**

- silný tým analytiků a technických konzultantů;
- úzká vazba na technickou bezpečnost – do analýzy rizik jsme schopni zahrnout také technické testy;
- využití kvalitativního i kvantitativního přístupu k hodnocení rizik;
- podpora procesu analýzy použitím vlastního SW nástroje;
- vysoká flexibilita a otevřenost k požadavkům zákazníka – jsme schopni přizpůsobit metodiku požadavků klienta či využít jeho interní postupy.




Zjednodušený model Analýzy rizik IS.

AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283