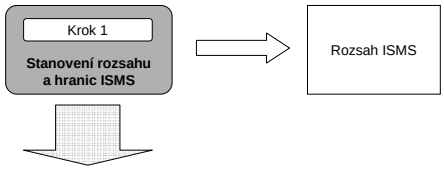
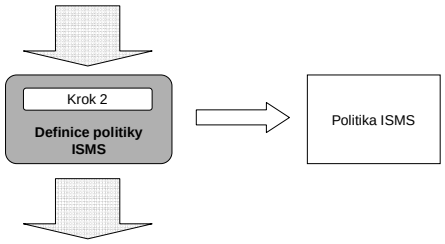
Implementace systému ISMS

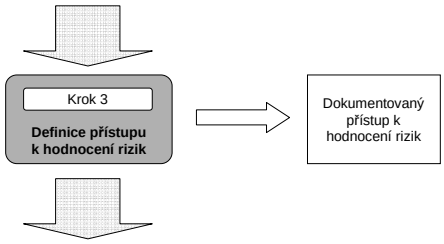
Ustavení ISMS



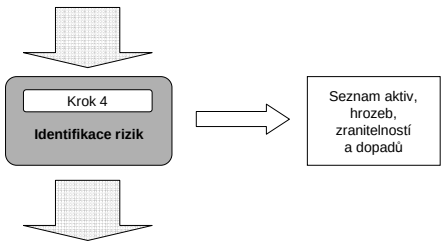
Ustavení ISMS



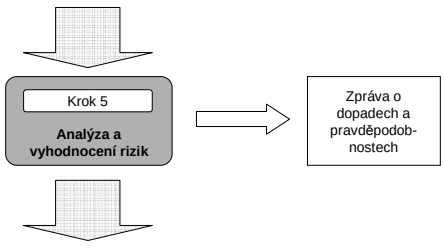
Ustavení ISMS



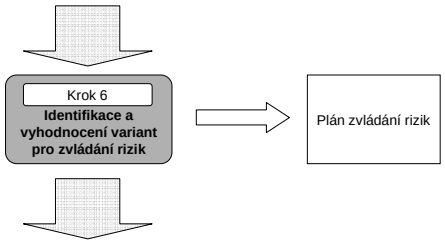
Ustavení ISMS



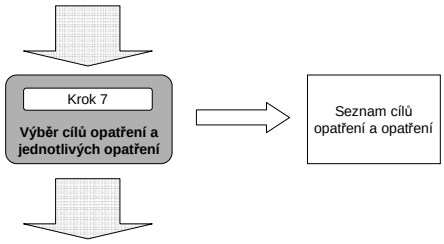
Ustavení ISMS



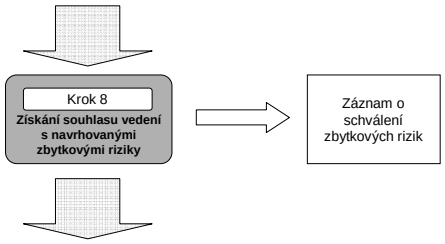
Ustavení ISMS



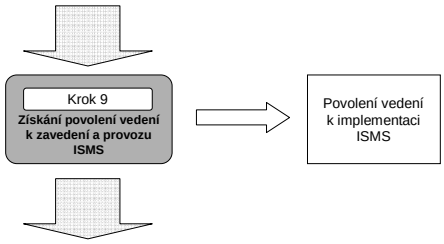
Ustavení ISMS



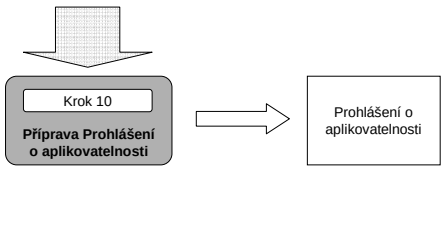
Ustavení ISMS



Ustavení ISMS



Ustavení ISMS



Zvládání rizik

Reálné pořadí hrozeb podle následků a výše škod

- Poruchy hardwaru (výpadek sítě, havárie disku)
- Výpadek elektrického napájení
- Porucha softwaru (systému nebo aplikace)
- Viry
- Chyba uživatele (vysoká přístupová práva)
- Krádeže zařízení
- Neoprávněná manipulace (útoky) zevnitř organizace
- Neoprávněná manipulace zvenčí.

Plán zvládání rizik

- Je koordinační dokument definující činnosti ke snížení neakceptovatelných rizik a implementaci požadovaných opatření k ochraně informací.

Možnosti zvládání rizik

- Akceptování zbytkového rizika
- Vyhnutí se riziku
- Přenos rizika – např. pojištění
- Snížení rizika na akceptovatelnou úroveň

Úroveň zbytkového rizika

- Není možné dosáhnout totální bezpečnosti
- Vždy bude nějaké zbytkové riziko
- Jaká míra zbytkového rizika je pro firmu akceptovatelná?

Zvládání rizik

- Umístění
- Existující zabezpečení
- Počet útočníků
- Zařízení, která jsou k dispozici
- Kumulované příležitosti
- Výše publicity
- Plánování kontinuity činností

Zvládání rizik

- Opatření musí odrážet firemní strategii řízení rizik
- Musí být zvažován dopad bezpečnostních rizik na podnikání

Zvládání rizik

- Definování akceptovatelné úrovně zbytkového rizika
- Neustálé přezkoumání hrozeb a zranitelností
- Přezkoumání existujících bezpečnostních opatření
- Aplikace dalších bezpečnostních opatření – ISO/IEC 27001
- Předložení politiky a postupů

Ochranná opatření

- Technická
  - bezpečnostní vlastnosti počítačů, OS, databází, aplikací
  - bezpečnostní vlastnosti komunikačních technologií
  - speciální bezpečnostní HW, SW a komunikační technologie

Ochranná opatření

- Organizační
  - bezpečnostní postupy (procedury)
  - organizace a řízení, odpovědnostní struktura
  - personální opatření, připravenost a motivace lidí

Ochranná opatření

- Fyzická
  - výběr a vybavení budov a místností
  - regulace vstupů, zábrany, signalizace
  - náhradní umístění, prostředky a zdroje

Výběr opatření

- Riziko
- Požadovaná míra zabezpečení
- Náklady
- Snadnost implementace
- Údržba
- Zákonné požadavky
- Zákaznické a smluvní požadavky

Náklady

- Rozpočtová omezení
- Jsou náklady spojené s aplikovaným opatřením odpovídající k hodnotě aktiva?
- Může se vybrat „nejlepší rozsah" opatření?

Snadnost implementace

- Podporuje prostředí dané opatření?
- Jak dlouho bude trvat implementace opatření?
- Je opatření běžně dostupné?

Údržba

- Jsou k dispozici znalosti nutné pro řízení opatření?
- Jsou běžně dostupné aktualizace?
- Je zařízení podporováno zdejšími techniky/dodavateli?

Opatření – best practice

- Dokument politiky bezpečnosti informací
- Přidělení odpovědnosti za bezpečnost informací
- Vzdělávání a výcvik
- Hlášení bezpečnostních incidentů
- Řízení kontinuity činností

Zákaznické a smluvní požadavky

- Prověřování pracovníků
- Omezený přístup
- Fyzické perimetry
- Uložení dat
- Kryptování
- Elektronické podpisy

Prohlášení o aplikovatelnosti

- Dokumentované prohlášení popisující cíle opatření a jednotlivá opatření, která jsou relevantní a aplikovatelná v rámci ISMS organizace.

Prohlášení o aplikovatelnosti

- Zdůvodnění relevantních opatření
- Záznam všech nerelevantních opatření
- Hodnocení rizik určí, která opatření by měla být implementována
- Nedílná součást přehledu dokumentace
- Pomáhá při sestavování plánu auditu

Jestliže nebyly požadavky implementovány, tak proč?

- Riziko – nezdůvodněné vystavení riziku
- Rozpočet – finanční omezení
- Prostředí – vliv na zabezpečení (klima, prostor atd.)
- Technologie – některá opatření nejsou technicky proveditelná
- Kultura – sociologické omezení
- Čas – některá opatření nemohou být implementována ihned
- N/A – neaplikovatelná
- Další