Zkušenosti se zaváděním ISMS z pohledu auditora

Luděk Novák, ANECT a.s.,
vedoucí auditor pro ISO/IEC 27001, ISO/IEC 20000

7. bezpečnostní seminář

22. září 2011, Praha

Obsah

- **Obsah**
- **Principy auditu**
- **Postup auditu ISMS**
- **Kritická místa implementace ISMS (pohled auditora)**
- **Závěr**

ANECT

Základní principy auditu

- **Etické chování**
  - důvěryhodnost, jednotnost, důvěrnost a diskrétnost vztahu auditora a auditované činnosti a při manipulaci s informacemi a daty
- **Spravedlivé prezentování**
  - zjištění, závěry a zprávy z auditu musí být vždy pravdivé a musí přesně popisovat veškeré činnosti provedené v průběhu auditu
- **Povinnost profesionálního přístupu**
  - auditor musí mít vysokou odbornou a profesní způsobilost a musí využívat své odborné zkušenosti dané nejlepší vžitou praxí v oblasti IT
- **Nezávislost**
  - auditor musí být naprosto nezávislý na auditované činnosti a prováděný audit je důsledně veden s cílem nalézt objektivní stanovisko
- **Průkaznost**
  - veškeré závěry a informace z provedeného auditu musí být zpětně ověřitelné

Postup auditu ISMS

- **ČSN EN ISO 19011:2003 – Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu**

- **Prověřované oblasti**
  - Soulad dokumentace ISMS s požadavky normy ISO/IEC 27001:2005
  - Soulad skutečného fungování ISMS s dokumentací ISMS
  - Účinnost a výkonnost ISMS

Kritická místa implementace ISMS (pohled auditora) 1

- **Kompetence odpovědných osob**
  - **Případ 1: Manažer bezpečnosti navštívil po roce zavádění ISMS odborné školení**
  - Požadavky normy obsahují některá specifika, která nejsou z textu normy srozumitelná
  - Dobré školení dovolí pracovníkům pochopit souvislosti
  - Školení je potřeba na počátku – získané znalosti by se měly projevit již při zavádění ISMS
- **Rozsah ISMS**
  - Málo s pracuje s rozšiřováním rozsahu ISMS – je výhodné si zavedení nekomplikovat a omezit se na podstatné
  - Další rozvoj realizovat s ohledem na získané zkušenosti

ANECT

Kritická místa implementace ISMS (pohled auditora) 2

- **Řízení rizik ISMS**
  - **Případ 2: Hodnocení rizik obsahuje hodně čísel a málo informací**
  - Řízení rizik neslouží ke stanovení priorit ISMS
  - Řízení rizik je příliš podrobné
  - Chybí vazby mezi riziky a opatřeními – nezbytné pro účinné řízení ISMS
  - Prohlášení o aplikovatelosti není základním dokument ISMS
- **Dokumentace a povědomí ISMS**
  - **Případ 3: Bezpečnostní výbor nebyl schopen dodržet pravidla administrativní bezpečnosti**
  - Podrobná dokumentace není podmínkou certifikace
  - Důležité je systematické prosazování zvyklostí – dokumentace není cíl, ale nástroj
  - Ne vždy se při tvorbě dokumentace myslí na následky
  - Podpora vedení je i o příkladu pro ostatní

ANECT

Kritická místa implementace ISMS (pohled auditora) 3

- **Záznamy ISMS**
  - **Případ 4: V provozním deníku neexistovaly všechny záznamy o vyhodnocení provozních záznamů**
  - Důležité téma pro auditory ISMS
  - Nestačí pořídit záznamy – důležité je též provést vyhodnocení záznamu za dané období
  - Nemusí se nutně jednat o papírovou válku
- **Audity a přezkoumání ISMS**
  - **Případ 5: Na odborné konferenci renovovaný odborník prohlásit, že ..., a proto jsme ...**
  - Cílem auditu je nalezení shody s normou – ne všichni jsou na tuto skutečnost připraveny
  - Program interního auditu souvisí s výsledky řízení rizik
  - Interní auditoři ISMS potřebují kvalitní zaškolení
  - Přezkoumání ISMS – chvilka času pro přemýšlení o budoucnosti

ANECT

Certifikace ISMS

Proč certifikace?

- **Ochrana zájmů organizace**
  - Realizace opatření jako výsledek řízení rizik
- **Dobré praktiky pro řízení rizik organizace**
- **Prokázání schopnosti řídit bezpečnost informací**
  - Vnější – klienti, obchodní partneři, státní orgány, regulační úřady, …
  - Vnitřní – majitelé, akcionáři, vedení
- **Konkurenční výhody**
- **Soulad s regulacemi**

Průběh certifikace

- **Před-audit**
  - Není povinné
  - Je vhodné a lze jen doporučit
- **Certifikační audit**
  - Fáze I – Prověrka dokumentace
  - Fáze II – Audit implementace ISMS
- **Pravidelný dohled**
  - Perioda 6 až 12 měsíců
- **Re-certifikace**
  - Každé 3 roky

ANECT

Závěr

- **Kvalitní audit ISMS je užitečný (pravda někdy bolí)**
  - Kvalitní zpětná vazba je základem účinného rozvoje
- **Auditor (externí) musí rychle proniknout k podstatě**
  - Odpovědné osoby se mohou opřít o zkušenosti a intuici
- **Certifikace brání ve stagnaci ISMS**
  - Alespoň jednou za rok se pod tlakem auditu zvýší priorita
- **Certifikace vřele doporučuji**
  - Asi by se dalo hovořit z mé strany o konfliktu zájmů
- **Výsledek často auditor uvidí rychle**
  - Časově náročné je získání důkazů

ANECT

Děkuji za pozornost!

ludek.novak@anect.com