Informační technologie - ČSN ISO/IEC 27001:2006 a další

Informace jsou majetkem, který má v dnešní době pro organizace stále větší hodnotu. S tím, jak se společnost mění v informační, je věnována bezpečnosti informací stále větší pozornost, a to zejména v oblasti elektronicky zpracovávaných informací.

Bezpečnost informací je charakterizována jako zachování:

- důvěrnosti (informace je dostupná pouze těm osobám, pro které je určena – oprávněný přístup)
- integrity (zabezpečení správnosti a kompletnosti informací a metod zpracování)
- dostupnosti (zajištění toho, aby informace byly přístupné autorizovaným uživatelům podle potřeby)

Lze jí dosáhnout zavedením soustavy opatření (stanovením a implementací příslušných pravidel, zavedením specifických organizačních struktur, odpovědností a pravomocí, definováním procesů, práv, způsobů ochrany…). Bezpečnost, která je navržena pouze jako soubor technických opatření, by mohla být nedostatečná. Z toho důvodu je vhodnější vybudovat **systém managementu bezpečnosti informací** (ISMS). Takový systém je možno implementovat a uplatňovat v souladu s požadavky **ISO/IEC 27001**. Tato norma podporuje stejně jako např. ISO 9001 nebo ISO 14001 procesní přístup při budování, zavedení, provozování a udržování ISMS.

Postup zavedení systému ISMS je zjednodušeně následující :

1) Definice rozsahu ISMS
2) Definice politiky ISMS
3) Stanovení metodiky pro hodnocení rizik a provedení hodnocení rizik
4) Řízení rizik
5) Stanovení bezpečnostních cílů a opatření včetně cílů kontrol a jednotlivých kontrol pro zvládání rizik
6) Zpracování prohlášení o aplikovatelnost

Stejně jako ostatní systémy managementu i tato norma předepisuje zavedení a provozování systému ISMS, jeho monitorování, přezkoumání, udržování a zlepšování, požadavky na dokumentaci včetně řízení dokumentů i záznamů, odpovědnost vedení, management zdrojů, odbornou způsobilost zaměstnanců, přezkoumání systému vedením, interní audity i neustálé zlepšování včetně opatření k nápravě i preventivních opatření. Norma je určená pro certifikaci, a tedy stejně jako u ostatních systémů managementu i v tomto případě je možno ověřit shodu s jejími požadavky a udělit certifikát.

Audit ISMS je dvoustupňový a kromě procesně orientovaných požadavků má některé specifické prvky:

- způsob vyhodnocení ohrožení bezpečnosti informací firmou ve vztahu k aktivům, zranitelnostem a možným dopadům (jde zejména o přiměřenost analýzy ohrožení bezpečnosti organizace, způsob řízení ohrožení – analogicky analýze a řízení rizik BOZP)
- kontrolu udržování a vyhodnocování souladu s právními předpisy organizací (analogicky s hodnocením souladu s právními požadavky EMS)
- způsob zapracování dokumentace ISMS do dokumentace dalších systémů ve firmě

Další normou nově se objevující v této oblasti je ČSN EN ISO/IEC 20000-1:2006: „**Informační technologie - Management služeb - Část 1: Specifikace“**, která představuje soubor tzv. nejlepších praktik v oboru. Tato norma je opět založená procesním přístupu, a může být použita jednak při řízení systémů managementu IT služeb organizací, které potřebují prokázat schopnost poskytovat služby splňující požadavky zákazníků; a ale rovněž jako soubor požadavků pro nezávislé ohodnocení třetí stranou.

2007-08-21, „AEC“

Accredited Europe Consultation s.r.o.,
„AEC“
kontakt: Ohradní 1159/65
CZ - 140 00
Praha 4 - Michle

Městský soud v Praze
oddíl C
č. vložky: 112028
datum zápisu: 10.března 2006
IČ: 27422968, DIČ: CZ27422968

e-mail: info@aecsro.cz
e-mail: aecsro@aecsro.cz
Tel: +420 721 438 923
Tel: +420 720 206 345
www.aecsro.cz