

Obsah

	Strana
Evropská předmluva	4
Předmluva	7
Úvod	9
1 Předmět normy	11
2 Citované dokumenty	11
3 Termíny a definice	12
4 Kontext organizace	12
4.1 Porozumění organizaci a jejímu kontextu	12
4.2 Porozumění potřebám a očekáváním zainteresovaných stran	12
4.3 Stanovení rozsahu systému managementu informační bezpečnosti	13
4.4 Systém managementu informační bezpečnosti	14
5 Vůdčí role	15
5.1 Vůdčí role a závazek	15
5.2 Politika	16
5.3 Role, odpovědnosti a pravomoci v rámci organizace	17
6 Plánování	19
6.1 Činnosti zaměřené na rizika a příležitosti	19
6.1.1 Obecně	19
6.1.2 Posuzování rizik informační bezpečnosti	20
6.1.3 Ošetření rizik informační bezpečnosti	21
6.2 Cíle informační bezpečnosti a plánování jejich dosažení	23
6.3 Plánování změn	24
7 Podpora	25
7.1 Zdroje	25
7.2 Kompetence	26
7.3 Povědomí	27
7.4 Komunikace	28
7.5 Dokumentované informace	30
7.5.1 Obecně	30
7.5.2 Vytváření a aktualizace	32
7.5.3 Řízení dokumentovaných informací	33
8 Provozování	35
8.1 Plánování a řízení provozu	35
8.2 Posuzování rizik informační bezpečnosti	36
8.3 Ošetření rizik informační bezpečnosti	36
9 Hodnocení výkonnosti	37
9.1 Monitorování, měření, analýza a hodnocení	37
9.2 Interní audit	38
9.2.1 Obecně	38
9.2.2 Program interního auditu	39
9.3 Přezkoumání vedením	40
9.3.1 Obecně	40

	Strana
9.3.2 Vstupy pro přezkoumání vedením.....	40
9.3.3 Výsledky z přezkoumání vedením.....	41
10 Zlepšování.....	43
10.1 Neustálé zlepšování.....	43
10.2 Neshody a nápravná opatření.....	44
Příloha A (normativní) Odkazy na opatření informační bezpečnosti.....	46
Bibliografie	52