

OBSAH

I. Úvod	9
1 Informační a kybernetická bezpečnost.....	12
1.1 Důvěrnost	15
1.2 Integrita.....	18
1.3 Dostupnost.....	20
1.4 Životní cyklus informace.....	24
II. Řízení rizik	27
2 Co je to riziko	31
2.1 Anatomie rizika	35
2.2 Popis rizika	38
2.3 Registr rizik	40
2.4 Rizikový profil.....	44
2.5 Risk appetite, tolerance a capacity	45
2.6 Inherentní, aktuální a reziduální riziko.....	50
2.7 Agregované a kaskádové riziko.....	52
3 Zavedení procesu řízení rizik.....	53
3.1 Role manažera řízení rizik.....	55
3.2 Organizace řízení rizik.....	58
3.3 Bezpečnost řízená riziky.....	59
3.4 Reaktivní, proaktivní a prediktivní řízení rizik.....	61
3.5 Specifické případy řízení rizik.....	63
3.6 Integrované řízení rizik.....	66
3.7 Kreativní řízení rizik.....	71

3.8	Politika řízení rizik	81
3.9	Průběžné činnosti.....	84
3.9.1	Komunikace a konzultace.....	85
3.9.2	Monitorování a přezkoumávání rizika.....	88
3.9.3	Zaznamenávání a hlášení.....	94
III.	Stanovení kontextu	97
4	Analýza vnitřního a vnějšího prostředí.....	99
4.1	Stanovení hranic analýzy.....	100
4.2	Stanovení hloubky analýzy.....	101
5	Rozhodnutí o způsobu provedení	103
5.1	Sestavení expertního týmu.....	110
5.2	Stanovení délky trvání	114
5.3	Stanovení nákladů na provedení.....	117
IV.	Posuzování rizik.....	118
6	Identifikace rizik.....	121
6.1	Přístupy a metody	121
6.2	Identifikace aktiv	131
6.2.1	Primární a podpůrná aktiva.....	136
6.2.2	Zachycení závislostí mezi aktivy.....	140
6.2.3	Identifikace primárních aktiv.....	141
6.2.4	Identifikace podpůrných aktiv	145
6.2.5	Bezpečnostní opatření jako podpůrná aktiva.....	147
6.2.6	Agregace aktiv	148
6.3	Identifikace hrozeb	149
6.3.1	Agenti hrozeb	160

6.4	Identifikace opatření	163
6.4.1	Diferenční analýza	169
6.4.2	Dokumentace bezpečnostních opatření	173
6.4.3	Stanovení vlastníka opatření	175
6.5	Identifikace zranitelností	176
6.6	Identifikace následků	177
7	Analýza rizik	178
7.1	Volba vhodné metody	178
7.1.1	Kvantitativní metody	179
7.1.2	Kvalitativní metody	180
7.1.3	Semikvantitativní metody	182
7.1.4	Srovnání jednotlivých metod	183
7.2	Analýza aktiv hrozeb a zranitelností	188
7.3	Analýza aktiv	189
7.3.1	Jak stanovit hodnotu primárního aktiva	191
7.3.2	Jak stanovit hodnotu podpůrného aktiva	192
7.4	Analýza hrozeb	193
7.4.1	Úmyslné škody	199
7.4.2	Neúmyslné škody	208
7.4.3	Technické selhání	210
7.4.4	Přírodní hrozby	212
7.5	Analýza opatření	213
7.5.1	Kvantifikace zranitelností	215
7.5.2	Ověření zranitelností	221
7.6	Analýza následků	224

7.6.1	Business Impact Analysis	225
7.6.2	Finanční ztráta	232
7.6.3	Poškození dobrého jména	235
V.	Vyhodnocení rizik	238
8	Vizualizace rizik	240
9	Návrh vhodných opatření	248
9.1	Účinnost opatření	253
9.2	Hodnocení návratnosti investice	258
10	Zpráva o posouzení rizik	263
VI.	Zvládání rizik	267
11	Metody zvládání rizik	269
11.1	Retence	273
11.2	Redukce	274
11.3	Transfer	275
11.4	Vyhnutí se riziku	275
12	Odmítnutí odpovědnosti	276
13	Plán zvládání rizik	278
	Příloha A	279
	Použitá literatura	293
	Seznam zkratk	296