

OBSAH

Autorský kolektiv	9
Předmluva	11
Úvod.....	13
1 Integrovaný systém řízení	19
1.1 Model PDCA	20
1.2 Řízení jakosti - QMS	23
1.2.1 Nástroje systému řízení jakosti	23
1.2.2 Proč zavádět systém řízení jakosti?	25
1.2.3 Normy ISO pro QMS	26
1.3 Systém řízení vztahu k okolí - EMS	27
1.3.1 Proč zavádět a zavést EMS?	31
1.3.2 Návaznost na systém řízení jakosti	32
1.4 Řízení bezpečnosti a ochrany zdraví při práci - OHSASMS	33
2 Řízení informatiky a bezpečnosti informací v organizaci	37
2.1 Vývoj řízení informatiky v organizacích.....	37
2.2 Koncepce řízení informatiky.....	40
2.2.1 IT Governance - ITG	40
2.2.2 IT Service Management - ITSM	42
2.3 Information Security Governance - ISG	44
2.4 Metodiky	48
2.4.1 COBIT.....	48
2.4.2 ITIL.....	53
2.4.3 Porovnání metodik ITIL a COBIT	57
3 Východiska řízení bezpečnosti informací	59
3.1 Vymezení bezpečnosti informací	59
3.2 Historický vývoj.....	64
3.2.1 Trusted Computer Security Evaluation Criteria -TCSEC	65
3.2.2 Information Technology Security Evaluation Criteria - ITSEC ..	67
3.2.3 Canadian Trusted Computer Product Evaluation Criteria - CTCPEC.....	69
3.2.4 Federal Criteria - FC	70
3.3 Porovnání kritérií hodnocení bezpečnosti	71

3.4	Common Criteria - CC	73
3.4.1	Obecný model hodnocení	74
3.4.2	Požadavky na bezpečnostní funkce	78
3.4.3	Požadavky na záruky	81
3.5	Normalizace řízení bezpečnosti informací	86
3.5.1	Historie normalizace řízení bezpečnosti informací	86
3.5.2	Řada ISO/IEC 27000 – Řízení bezpečnosti informací.....	89
4	Systém řízení bezpečnosti informací	95
4.1	Ustanovení ISMS.....	96
4.1.1	Definice rozsahu a hranic ISMS.....	97
4.1.2	Prohlášení o politice ISMS	98
4.1.3	Pravidla a postupy řízení rizik.....	98
4.1.4	Souhlas vedení se zavedením ISMS a se zbytkovými riziky....	107
4.1.5	Prohlášení o aplikovatelnosti	108
4.1.6	Shrnutí etapy ustanovení ISMS.....	110
4.2	Zavádění a provoz ISMS	111
4.2.1	Plán zvládnání rizik	112
4.2.2	Příručka bezpečnosti informací	113
4.2.3	Prohlubování bezpečnostního povědomí.....	113
4.2.4	Měření účinnosti ISMS	114
4.2.5	Řízení provozu, zdrojů, dokumentace a záznamů ISMS.....	122
4.3	Monitorování a přezkoumání ISMS	123
4.3.1	Provádění kontrol ISMS	123
4.3.2	Interní audity ISMS	124
4.3.3	Přezkoumání ISMS vedením organizace.....	124
4.4	Udržba a zlepšování ISMS	125
4.4.1	Soustavné zlepšování ISMS.....	126
4.4.2	Odstraňování nedostatků ISMS.....	126
4.5	Shrnutí celého cyklu ISMS.....	127
4.6	Praktické zkušenosti	128
5	Realizace bezpečnostních opatření.....	131
5.1	Bezpečnostní politika	133
5.2	Organizace bezpečnosti informací.....	134
5.2.1	Organizační struktury.....	135
5.3	Řízení aktiv	138
5.4	Bezpečnost z hlediska lidských zdrojů.....	139

5.5	Fyzická bezpečnosti a bezpečnost prostředí	140
5.6	Řízení komunikací a řízení provozu	142
5.7	Řízení přístupu	144
5.7.1	Principy řízení přístupu	145
5.8	Akvizice, vývoj a údržba informačních systémů	146
5.9	Zvládání bezpečnostních incidentů.....	147
5.9.1	Principy zvládání bezpečnostních incidentů.....	147
5.9.2	Životní cyklus SIMS	149
5.9.3	Organizační struktury a odpovědnosti spojené s řešením bezpečnostních incidentů.....	154
5.9.4	Podpora mezinárodními normami	155
5.10	Řízení kontinuity činností organizace.....	157
5.10.1	Principy řízení kontinuity činností organizace.....	157
5.11	Soulad s požadavky	158
6	Úřady, instituce a organizace zabývající se bezpečností informací... 161	
6.1	Právní rámec bezpečnosti informací v České republice.....	161
6.2	Tuzemské instituce	174
6.2.1	Úřad pro ochranu osobních údajů - ÚOOÚ	175
6.2.2	Národní bezpečnostní úřad - NBÚ	176
6.2.3	Ministerstvo vnitra – MV ČR, Odbor koncepce a koordinace ISVS.....	179
6.2.4	Český normalizační institut - ČNI	182
6.2.5	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví - ÚNMZ.....	185
6.2.6	Český institut pro akreditaci – ČIA	186
6.2.7	Český telekomunikační úřad – ČTÚ.....	187
6.3	Zahraniční a mezinárodní normalizační organizace	188
6.3.1	Americký národní normalizační institut - ANSI	188
6.3.2	Asociace pro audit a řízení informačních systémů - ISACA	188
6.3.3	British Standards Institute - BSI.....	189
6.3.4	Bundesamt für Sicherheit in der Informationstechnik – německý BSI.....	189
6.3.5	Evropský institut telekomunikačních norem - ETSI.....	190
6.3.6	Evropská komise pro normalizaci CEN	190
6.3.7	Institute of Electrical and Electronics Engineers - IEEE.....	191
6.3.8	International Electrotechnical Commission – IEC	191
6.3.9	Internet Engineering Task Force - IETF	191

6.3.10	Mezinárodní organizace pro normalizaci – ISO.....	191
6.3.11	Národní institut pro normy a technologie - NIST.....	195
6.3.12	National Security Agency – NSA.....	196
6.3.13	RSA Laboratories – standardy PKCS	196
6.3.14	Vládní úřad pro obchod - OGC	197
7	Audit a testování bezpečnosti informací.....	199
7.1	Základy auditu bezpečnosti	200
7.1.1	Principy auditu	200
7.1.2	Postup auditu.....	201
7.1.3	Základní typy auditů	203
7.2	Certifikace systému řízení bezpečnosti informací.....	204
7.2.1	Certifikace versus akreditace	204
7.2.2	Průběh certifikace ISMS	206
7.2.3	Údržba a obnova certifikátu.....	207
7.3	Techniky pro provádění testů bezpečnosti informací	207
8	Trendy a vývoj bezpečnosti informací.....	209
8.1	Stav bezpečnosti informací v České republice.....	209
8.1.1	Hlavní zjištění	210
8.1.2	Dílní zjištění.....	211
8.1.3	Celkové zhodnocení.....	218
8.2	Trendy v bezpečnosti informací a v bezpečnosti IS/ICT	218
8.2.1	Trendy v České republice	218
8.2.2	Světové a evropské trendy	219
	Závěr.....	221
	Použitá literatura a další zdroje.....	223
	Seznam obrázků a tabulek.....	235
	Rejstřík.....	237