

Obsah

1	Bezpečnost informací a řízení bezpečnosti informací	6
2	Historie / vývoj normy ISO 27001 / ISO 17799	10
3	Vymezení, prostředí, jiné standardy a normy k tématu bezpečnosti informací	11
3.1	Kritéria srovnávání	12
3.2	Příručka základní ochrany IT	14
3.3	ISO/ IEC 17799 a ISO 27001	16
3.4	ISO TR 13335	19
3.5	ITSEC/ Common Criteria (ISO 15408)	21
3.6	CobIT	24
3.7	Kombinace	27
3.7.1	ISO 17799 + Příručka základní ochrany IT	27
3.7.2	ISO 17799 + ISO 9000	27
4	ISO 27001 / ISO 17799, obsahy normy a realizace v praxi	28
4.1	Struktura normy ISO 27001 a ISO17799	28
4.2	ISO 17799	29
4.2.1	Vymezení pojmů	29
4.3	11 stěžejních témat normy	35
4.3.1	Bezpečnostní politika	35
4.3.2	Organizace bezpečnosti informací	37
4.3.3	Řízení aktiv	43
4.3.4	Personální bezpečnost	44
4.3.5	Fyzická bezpečnost a bezpečnost prostředí	48
4.3.6	Řízení systému (správa počítačů a sítě)	52
4.3.7	Řízení přístupu k systému	63
4.3.8	Nákup, vývoj a údržba systému	71
4.3.9	Řízení bezpečnostních incidentů	77
4.3.10	Řízení kontinuity činnosti organizace (BCM)	78
4.3.11	Splnění zákonných a smluvních závazků	81
4.4	ISO 27001	84
4.4.1	Zavedení ISMS (PLAN)	86
4.4.2	Implementace a provoz ISMS (DO)	88
4.4.3	Monitorování a kontrola ISMS (CHECK)	88
4.4.4	Údržba a zlepšování ISMS (ACT)	89
4.4.5	Součásti dokumentace ISMS	89
4.4.6	Požadavky na dokumentaci	90
4.4.7	Odpovědnost managementu	91
4.4.8	Řízení zdrojů	91
4.4.9	Interní audity ISMS	92
4.4.10	Hodnocení ISMS managementem organizace	92
4.4.11	Zlepšování ISMS	93
4.5	Interní a externí audity	94