

Obsah:

PREDSLOV	17
ZOZNAM POUŽÍVANÝCH SKRATIEK	18
ZOZNAM OBRÁZKOV	20
ZOZNAM TABULIEK	21
1 ÚVOD	23
1.1 VYSVETLENIE VYBRANÝCH POJMOV	26
2 POŽIADAVKY NA DOKUMENTÁCIU SRIB	33
2.1 POŽIADAVKY NA DOKUMENTÁCIU SRIB PODĽA NORMY ISO/IEC 27001	33
2.1.1 Všeobecné požiadavky na dokumentáciu SRIB	33
2.1.2 Požiadavky na riadenie dokumentácie	34
2.1.3 Požiadavky na dokumentáciu SRIB vyplývajúce z obsahu normy ISO/IEC 27001	35
2.1.3.1 Prehľad požadovaných dokumentov	40
2.1.3.2 Prehľad požadovaných interných predpisov	41
2.1.3.3 Prehľad požadovaných záznamov	41
2.2 POŽIADAVKY NA DOKUMENTÁCIU SRIB VYPLÝVAJÚCE Z PRÍLOHY A NORMY ISO/IEC 27001	43
2.3 ODPORÚČANIA NA DOKUMENTÁCIU SRIB VYPLÝVAJÚCE Z NORMY ISO/IEC 27002	52
2.4 POŽIADAVKY NA DOKUMENTÁCIU SRIB PODĽA VÝNOSU MF SR Č. 312/2010 Z.z.	53
2.4.1 Základné požiadavky na architektúru riadenia	53
2.4.2 Požiadavky na dokumentáciu SRIB vyplývajúce z ďalších paragrafov Výnosu	54
2.4.3 Zhrnutie požiadaviek na dokumentáciu SRIB povinnej osoby	59
2.5 POROVNANIE POŽIADAVIEK NA DOKUMENTÁCIU SRIB PODĽA NORMY ISO/IEC 27001 A VÝNOSU MF SR Č. 312/2010 Z.z.	64
3 POLITIKA SRIB	69
4 POLITIKA INFORMAČNEJ BEZPEČNOSTI	71
4.1 DOKUMENT POLITIKY PODĽA MEDZINÁRODNÝCH NORIEM	71
4.2 DOKUMENT POLITIKY PODĽA VÝNOSU MF SR Č. 312/2010 Z.z.	72
5 ROZSAH SRIB	79
5.1 ROZSAH SRIB ORGANIZÁCIE PODĽA NORMY ISO/IEC 27001	81
5.2 ROZSAH SRIB POVINNEJ OSOBY PODĽA NORMY VÝNOSU MF SR Č. 312/2010 Z.z.	82
6 POSTUPY A OPATRENIA PODPORUJÚCE SRIB	83
6.1 POSTUPY A OPATRENIA PODĽA NORMY ISO/IEC 27001	83
6.1.1 Postupy podporujúce SRIB	83
6.1.2 Opatrenia podporujúce SRIB	84
6.2 POSTUPY A OPATRENIA PODĽA VÝNOSU MF SR Č. 312/2010 Z.z.	93
6.2.1 Postupy podporujúce SRIB	93
6.2.2 Opatrenia podporujúce SRIB	94
6.3 POROVNANIE POSTUPOV A OPATRENÍ PODPORUJÚCICH SRIB PODĽA NORMY A VÝNOSU	98
7 METODIKA PRESKÚMAVANIA RIZÍK	111
7.1 DOKUMENT METODIKY PRESKÚMANIA RIZÍK PODĽA POŽIADAVIEK NORMY ISO/IEC 27001	112
7.2 DOKUMENT METODIKY PRESKÚMANIA RIZÍK PODĽA POŽIADAVIEK VÝNOSU MF SR Č. 312/2010 Z.z.	118
8 SPRÁVA O PRESKÚMANÍ RIZÍK	121
8.1 DOKUMENT SPRÁVY O PRESKÚMANÍ RIZÍK PODĽA NORMY ISO/IEC 27001	121
8.2 DOKUMENT SPRÁVY O PRESKÚMANÍ RIZÍK PODĽA NORMY VÝNOSU MF SR Č. 312/2010 Z.z.	124
9 VYHLÁSENIE O APLIKOVATELNOSTI	127
9.1 POŽIADAVKY NA DOKUMENT VYHLÁSENIE O APLIKOVATELNOSTI PODĽA NORMY ISO/IEC 27001	127

9.2	POŽIADAVKY NA DOKUMENT VYHLÁSENIE O APLIKOVATELNOSTI PODĽA VÝNOSU MF SR Č. 312/2010 Z.z.	128
10	PLÁN OŠETRENIA RIZIKA	129
10.1	POŽIADAVKY NA PLÁN OŠETRENIA RIZÍK PODĽA NORMY ISO/IEC 27001	129
10.2	POŽIADAVKY NA PLÁN OŠETRENIA RIZÍK PODĽA VÝNOSU MF SR Č. 312/2010 Z.z.	131
11	BCM PLÁN	133
11.1	POŽIADAVKY NA BCM PLÁN PODĽA NORMY ISO/IEC 27001	135
11.2	POŽIADAVKY NA BCM PLÁN PODĽA VÝNOSU MF SR Č. 312/2010 Z.z.	137
12	PRÍRUČKA SRIB	139
13	BEZPEČNOSTNÁ PRÍRUČKA ZAMESTNANCA	145
14	ĎALŠIE DOKUMENTY	147
14.1	SPRÁVA PRE PRESKÚMANIE SRIB MANAŽMENTOM ORGANIZÁCIE	147
14.1.1	Požiadavky na správu pre preskúmanie SRIB podľa normy ISO/IEC 27001	147
14.1.2	Požiadavky na správu pre preskúmanie SRIB podľa Výnosu MF SR č. 312/2010 Z.z.	149
14.2	SPRÁVA Z INTERNÉHO AUDITU SRIB	150
14.2.1	Požiadavky na správu z interného auditu SRIB podľa normy ISO/IEC 27001	150
14.2.2	Požiadavky na správu z interného auditu SRIB podľa Výnosu MF SR č. 312/2010 Z.z.	151
15	INTERNÉ PREDPISY ORGANIZÁCIE	153
15.1	POŽIADAVKY NORMY ISO/IEC 27001 NA INTERNÉ PREDPISY	153
15.2	POŽIADAVKY VÝNOSU MF SR Č. 312/2010 Z.z. NA INTERNÉ PREDPISY	155
15.3	POROVNANIE POŽIADAVIEK NORMY A VÝNOSU NA INTERNÉ PREDPISY PRE FUNGOVANIE SRIB	158
15.4	ODPORÚČANIA PRE VYTŮVÁRANIE INTERNÝCH PREDPISOV	167
15.5	PRÍKLADY VYBRANÝCH SMERNÍC ORGANIZÁCIE SÚVISIACICH S FUNGOVANÍM SRIB	169
15.5.1	Smernica o budovaní a prevádzke SRIB	169
15.5.1.1	Aplikovanie procesného prístupu k riadeniu	170
15.5.1.2	Budovanie a prevádzka SRIB	171
15.5.1.3	Zodpovednosť za budovanie a prevádzku SRIB	171
15.5.1.4	Projekt budovania SRIB	172
15.5.1.5	Koordinácia procesu budovania SRIB	172
15.5.1.6	Aplikovanie medzinárodných noriem a právnych predpisov	173
15.5.1.7	Súčinnosť organizačných útvarov	173
15.5.1.8	Zabezpečenie prostriedkov na dobudovanie SRIB	174
15.5.1.9	Schvaľovanie vytvorených dokumentov	174
15.5.1.10	Zabezpečenie technologických opatrení	174
15.5.1.11	Určenie a zabezpečenie zdrojov pre permanentné činnosti spadajúce pod SRIB	175
15.5.1.12	Vyhodnocovanie budovania a prevádzky SRIB	175
15.5.1.13	Certifikácia SRIB	175
15.5.1.14	Prevádzka SRIB	176
15.5.1.15	Prevádzka IS a sietí	176
15.5.1.16	Analýza a riadenie rizík	176
15.5.1.17	Príprava riešení a implementácie bezpečnostných opatrení počas prevádzky SRIB	177
15.5.1.18	Monitorovanie prevádzky IS a sietí	177
15.5.1.19	Riadenie prístupových práv	178
15.5.1.20	Povinnosti manažmentu	178
15.5.1.21	Bezpečnostné testovanie	178
15.5.1.22	Vyhodnocovanie stavu plnenia požiadaviek medzinárodných noriem a právnych predpisov	178
15.5.1.23	Auditovanie SRIB	179
15.5.1.24	Preskúmanie SRIB	179
15.5.1.25	Zlepšovanie, náprava a prevencia	179
15.5.1.26	Udržiavanie dokumentácie SRIB	180
15.5.1.27	Vlastník smernice	180
15.5.1.28	Kontrola dodržiavania smernice	180
15.5.1.29	Všeobecné ustanovenia	181
15.5.1.30	Príloha - Správa schválených písomných verzií smernice	181
15.5.1.31	Príloha - Zodpovednosti a právomoci delegované normou	181
15.5.2	Smernica o auditovaní SRIB	183
15.5.2.1	Zodpovednosť	184

15.5.2.2	Program a Plány IA	184
15.5.2.3	Fázy IA	184
15.5.2.4	Preskúvanie dokumentácie	185
15.5.2.5	Audity na mieste	185
15.5.2.6	Správa o audite	185
15.5.2.7	Súčinnosť auditovaných útvarov	185
15.5.2.8	Zistenia	186
15.5.2.9	Príprava auditorov	186
15.5.2.10	Základné zásady pre činnosť auditorov	186
15.5.2.11	Evidencia zistení z IA	186
15.5.2.12	Vlastník smernice	187
15.5.2.13	Kontrola dodržiavania smernice	187
15.5.2.14	Všeobecné ustanovenia	187
15.5.2.15	Príloha - Formulár pre vytváranie Programu IA	187
15.5.2.16	Príloha - Formulár pre plánovanie IA	187
15.5.2.17	Príloha - Formulár správy z IA	187
15.5.2.18	Príloha - Formulár požiadavky na Z_NO_PO	187
16	ZÁZNAMY SRIB	189
16.1	POŽIADAVKY NORMY ISO/IEC 27001 NA ZÁZNAMY	189
16.2	POŽIADAVKY VÝNOSU MF SR Č. 312/2010 Z.Z. NA ZÁZNAMY	193
16.3	POROVNANIE POŽIADAVIEK NORMY A VÝNOSU NA ZÁZNAMY SRIB	195
16.4	POŽIADAVKY NORMY ISO/IEC 27001 NA RIADENIE ZÁZNAMOV	204
16.5	PRÍKLADY VYBRANÝCH ZÁZNAMOV SRIB ORGANIZÁCIE	205
16.5.1	Požiadavka aplikovania procesného riadenia	205
16.5.1.1	Mapa procesov	205
16.5.1.2	Karta procesu	207
16.5.1.3	Záznam z merania procesu	213
16.5.2	Požiadavka interného auditovania SRIB	217
16.5.2.1	Program IA	217
16.5.2.2	Plán IA	217
16.5.2.3	Záznam Z_NO_PO	220
16.5.3	Požiadavka preskúvania SRIB	222
16.5.3.1	Záznam o prerokovaní správy pre preskúvanie SRIB	222
16.5.4	Požiadavka pridelenia bezpečnostnej roly	223
16.5.4.1	Poverenie na výkon bezpečnostnej roly	223
16.5.5	Požiadavka pridelenia prístupových práv	225
16.5.5.1	Protokol o pridelení prístupových práv do IS	225
16.5.5.2	Protokol o pridelení vzdialeného prístupu	227
16.5.6	Požiadavka na odobratie prístupových práv	229
16.5.6.1	Záznam o odobratí prístupových práv	229
16.5.7	Požiadavka na ošetrovanie podozrivých udalostí a bezpečnostných incidentov	231
16.5.7.1	Záznam o bezpečnostnom incidente/podozrivej udalosti	231
17	VZŤAH MEDZI DOKUMENTMI SRIB A BEZPEČNOSTNOU DOKUMENTÁCIOU IS	235
18	SYSTÉMY PRE SPRÁVU A RIADENIE DOKUMENTÁCIE A ZÁZNAMOV	237
18.1	CMS – SYSTÉM RIADENIA OBSAHU DOKUMENTOV	238
18.1.1	Základné funkcie CMS	238
18.1.2	Existujúce CMS	238
18.1.3	Hodnotenie vybraných CMS systémov	240
18.1.3.1	OpenCms	240
18.1.3.2	Alfresco	241
18.2	DMS – SYSTÉM RIADENIA DOKUMENTÁCIE	243
18.2.1	Činnosti zabezpečované DMS	243
18.2.2	Existujúce DMS	243
18.2.3	Vybrané produkty pre budovanie DMS	246
18.2.3.1	SharePoint	246
18.2.3.2	IBM FileNet	248
18.2.3.3	IBM Content Collector	248
18.2.3.4	Nintex	248
18.3	PUBLIKÁCIE A NORMY SÚVISIACE S RIADENÍM DOKUMENTOV A ICH OBSAHU	249
19	ZÁVER	251

20	LITERATÚRA	253
20.1	MONOGRAFIE A PUBLIKÁCIE	253
20.2	ČLÁNKY, WEB STRÁNKY	254
20.3	FIREMNÉ METODIKY	255
20.4	ZÁKONY A VYHLÁŠKY	255
20.5	ISO NORMY	256
20.6	ISO/IEC NORMY	256
20.7	STN NORMY	256
20.8	ČSN NORMY	257
21	SUMMARY	259