



Information Security Management
Information Risk Management
Business Continuity Management
Information Forensic Analysis



RISK ANALYSIS CONSULTANTS

BS 7799-3:2006

Information Security Management Systems

Guidelines for information security risk management

Překlad a interpretace pro české prostředí



RAC[®]

RISK ANALYSIS CONSULTANTS



© 2006, British Standards Institution
© 2006, Risk Analysis Consultants

Obsah

Statut dokumentu / Document status	i
Autorská práva / Copyright	i
Informace / Information	i
Ediční historie / Publication history	ii
Poznámka k českému vydání	ii
Předmluva	vii
0 Úvod	1
0.1 Všeobecně	1
0.2 Procesní přístup	1
1 Působnost	3
2 Normativní odkazy	3
3 Termíny a definice	3
3.1 bezpečnostní událost (<i>information security event</i>)	3
3.2 bezpečnostní incident (<i>information security incident</i>)	3
3.3 zbytkové riziko (<i>residual risk</i>)	3
3.4 riziko (<i>risk</i>)	3
3.5 akceptace rizika (<i>risk acceptance</i>)	4
3.6 analýza rizik (<i>risk analysis</i>)	4
3.7 hodnocení rizik (<i>risk assessment</i>)	4
3.8 vyvarování se rizik (<i>risk avoidance</i>)	4
3.9 seznámení s rizikem (<i>risk communication</i>)	4
3.10 regulace rizik (<i>risk control</i>)	4
3.11 měřítko rizik (<i>risk criteria</i>)	4
3.12 vyhodnocení rizik (<i>risk evaluation</i>)	5
3.13 řízení rizik (<i>risk management</i>)	5
3.14 systém řízení rizik (<i>risk management system</i>)	5
3.15 redukce rizika (<i>risk reduction</i>)	5
3.16 přenos rizika (<i>risk transfer</i>)	5
3.17 zvládání rizik (<i>risk treatment</i>)	5
3.18 hrozba (<i>threat</i>)	6
3.19 zranitelnost (<i>vulnerability</i>)	6
4 Rizika bezpečnosti informací v rámci organizace	7
4.1 Rozsah a politika systému řízení bezpečnosti informací	7
4.2 Přístup k rizikům	7
5 Hodnocení rizik	9
5.1 Proces hodnocení rizik	9
5.2 Identifikace aktiv	9

5.3	Identifikace právních požadavků a požadavků organizace	10
5.4	Hodnocení aktiv	10
5.5	Identifikace a hodnocení hrozeb a zranitelností	11
5.6	Hodnocení hrozeb a zranitelností	11
5.7	Vypočtení a vyhodnocení rizika	12
5.8	Poradce pro rizika	13
6	Zvládání rizik	14
6.1	Všeobecně	14
6.2	Rozhodování o způsobu zvládání rizik	14
6.3	Snížení rizik	14
6.4	Vědomá a objektivní akceptace rizik	15
6.5	Sdílení rizik	15
6.6	Vyvarování se rizik	16
6.7	Zbytkové riziko	16
6.8	Plán zvládání rizik	16
7	Trvalé řízení rizik	18
7.1	Trvalé řízení bezpečnostních rizik	18
7.2	Údržba a monitorování	18
7.3	Přezkoumání ISMS	18
7.4	Přehodnocení rizik	19
7.5	Audity	19
7.6	Dokumentace	19
7.7	Nápravné a preventivní činnosti	19
7.8	Hlášení rizik a komunikace	20
7.9	Manažer bezpečnostních rizik	20
	Příloha A	22
	(informativní)	22
	Příklady souladu s právními a regulatorními požadavky	22
A.1	Všeobecně	22
A.2	Právní rámec	22
A.3	Národní bezpečnost	22
A.3.1	Všeobecně	22
A.3.2	Evropa	23
A.3.2	Severní Amerika	23
A.4	Řízení a správa společnosti	23
A.4.1	Všeobecně	23
A.4.2	Evropa	23
A.4.3	Severní Amerika	23
A.5	Elektronický obchod, právní rámec	24
A.5.1	Všeobecně	24

A.5.2 Evropa	24
A.5.3 Severní Amerika	24
A.6 Krádež identity, ochrana dat	24
A.6.1 Všeobecně	24
A.6.2 Evropa	24
A.6.3 Severní Amerika	24
A.7 Ochrana duševního vlastnictví	25
A.8 Oborově závislé	25
Příloha B	26
(informativní)	26
Rizika bezpečnosti informací a rizika v organizaci	26
B.1 Procesy a vzájemné vztahy v organizaci	26
B.1.1 Všeobecně	26
B.1.2 Vnější procesy organizace	26
B.1.3 Vnitřní procesy organizace	26
B.2 Rizika v organizaci	27
B.3 Řízení a správa společnosti	27
Příloha C	29
(informativní)	29
Příklady aktiv, hrozeb, zranitelností a metod hodnocení rizik	29
C.1 Identifikace aktiv	29
C.2 Příklady hrozeb	29
C.3 Příklady hrozeb a BS ISO/IEC 17799:2005	32
C.3.1 Všeobecně	32
C.3.2 Fyzická bezpečnost a bezpečnost prostředí	32
C.3.2.1 Zabezpečené oblasti	32
C.3.2.2 Bezpečnost zařízení	33
C.3.3 Řízení komunikací a řízení provozu	34
C.3.3.1 Provozní postupy a odpovědnosti	34
C.3.4 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	34
C.3.5 Soulad s požadavky	35
C.3.5.1 Soulad s právními normami	35
C.3.5.2 Soulad s bezpečnostními politikami, normami a technická shoda	35
C.3.5.3 Hlediska auditu informačních systémů	36
C.4 Příklady zranitelností a BS ISO/IEC 17799:2005	36
C.4.1 Všeobecně	36
C.4.2 Bezpečnost lidských zdrojů (BS ISO/IEC 17799:2005, kapitola 8)	37
C.4.3 Fyzická bezpečnost a bezpečnost prostředí (BS ISO/IEC 17799:2005, kapitola 9)	37
C.4.4 Řízení komunikací a řízení provozu (BS ISO/IEC 17799:2005, kapitola 10)	37
C.4.5 Řízení přístupu (BS ISO/IEC 17799:2005, kapitola 11)	38

C.4.6 Nákup, vývoj a údržba informačního systému	39
C.5 Příklady metod hodnocení rizik	39
C.5.1 Stupnice oceňování aktiv	39
C.5.2 Hodnotící stupnice hrozeb a zranitelností	39
C.5.3 Matice hodnoty aktiv a závažnosti hrozeb a zranitelností	40
C.5.4 Klasifikace incidentů podle měřítek rizik	41
Příloha D	42
(informativní)	42
Nástroje řízení rizik	42
D.1 Všeobecně	42
D.2 Volba nástroje řízení rizik	42
Příloha E	43
(informativní)	43
Vztah mezi BS ISO/IEC 27001:2005 a BS 7799-3:2005	43
Bibliografie	45
Související normy	45
Další publikace	45
Rejstřík	47

Předmluva

Publikační informace

Tato britská norma byla publikována BSI a vešla v platnost dne 17. března 2006. Byla připravena technickou komisí BDD/2, *Information security management*.

Vztah k dalším publikacím

Tato britská norma obsahuje a nahrazuje doporučení k BS 7799 uvedená v publikacích BSI PD 3002 a PD 3005.

Norma je v souladu s ostatními dokumenty ISO/IEC, zejména s BS ISO/IEC 17799:2005 a BS ISO/IEC 27001:2005 (revidovaná verze dokumentu BS 7799-2:2002), kvůli zajištění shody terminologie a metod.

Informace o tomto dokumentu

Tato britská norma poskytuje doporučení a podporu pro implementaci normy BS ISO/IEC 27001:2005 a je dostatečně obecná k použití v malých, středních i velkých organizacích. Doporučení a rady podané v této britské normě nejsou vyčerpávající a organizace může mít potřebu doplnit je dalšími doporučeními dříve, než se mohou stát základem systému řízení rizik podle BS ISO/IEC 27001:2005 (revidovaná verze BS 7799-2:2002).

Tato norma je průvodcem, proto má podobu doporučení. Neměla by se doslovně citovat, jako kdyby byla specifikací, a zejména je vhodné se ujistit, že tvrzení o shodě s normou nejsou zavádějící.

Smluvní a právní otázky

Tato publikace nemůže obsáhnout všechna opatření z oblasti jejího určení. Uživatelé jsou sami odpovědní za její správné použití.

Shoda s normou sama o sobě neposkytuje imunitu před plněním zákonných závazků.

0 Úvod

0.1 Všeobecně

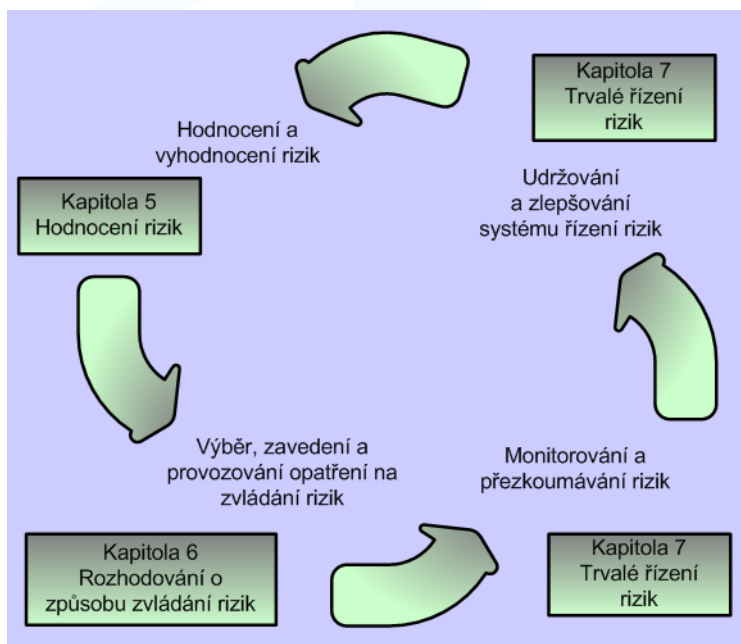
Tato norma byla připravena pro ty manažery a zaměstnance organizace, kteří se v rámci systému řízení bezpečnosti informací (Information Security Management System, ISMS) zabývají řízením rizik. Norma především poskytuje doporučení a rady k implementaci těchto požadavků stanovených v BS ISO/IEC 27001:2005, které se týkají procesů řízení rizik a souvisejících aktivit. Tabulka E.1 ukazuje vztah mezi oběma dokumenty.

0.2 Procesní přístup

Tato britská norma prosazuje přijetí procesního přístupu pro hodnocení a zvládání rizik, jejich následné monitorování, přezkoumávání a přehodnocování. Procesní přístup napomáhá uživatelům zdůraznit význam:

- počpení požadavků organizace na bezpečnost informací a potřeby stanovení politiky a cílů bezpečnosti informací;
- výběru, zavedení a provozování opatření v souvislosti s celkovým řízením rizik činností organizace;
- monitorování a přezkoumávání funkčnosti a výkonnosti systému řízení bezpečnosti informací (ISMS) při řízení rizik;
- neustálého zlepšování založeného na objektivním měření rizik.

Viz. obrázek 1.



Obrázek 0-A Proces řízení rizik

Proces řízení rizik dovoluje organizaci porozumět rizikům a umožňuje efektivní rozhodování o správě rizik. Proces řízení rizik je trvalá aktivita, jejímž cílem je soustavné zlepšování její účinnosti a výkonnosti.

Proces řízení rizik by měl být aplikován na celý ISMS (specifikovaný v BS ISO/IEC 27001:2005) a je vhodné nové informační systémy integrovat do ISMS už v etapě plánování a návrhu kvůli zabezpečení vhodného ošetření všech rizik vztahujících se k bezpečnosti informací. Tento dokument popisuje součásti a důležitá hlediska procesu řízení těchto rizik.

Rizika bezpečnosti informací je třeba posuzovat v souvislostech organizace a je nutné určit jejich vztah k ostatním funkcím organizace, jakými jsou lidské zdroje, výzkum a vývoj, produkce a provoz, administrativa, IT, finance a zákazníci, pro získání úplného a celkového náhledu na

tato rizika. Posouzení zahrnuje uvážení rizik organizace a použití představ a myšlenek řízení a správy společnosti. To vše, spolu se zájmy organizace, účinností a právním a regulačním prostředím podněcuje a motivuje k úspěšnému procesu řízení rizik. Tyto úvahy jsou podrobněji popsány v kapitole 4.

Důležitou částí procesu řízení rizik je hodnocení rizik týkajících se k bezpečnosti informací, které je nezbytné k pochopení požadavků organizace na bezpečnost informací, a rizik pro obchodní aktiva organizace. Jak popisuje také BS ISO/IEC 27001:2005 hodnocení rizik zahrnuje následující činnosti a aktivity, které jsou podrobněji popsány v kapitole 5.

- Identifikace aktiv.
- Identifikace právních požadavků a požadavků organizace vztahujících se k daným aktivům.
- Ohodnocení daných aktiv, posouzení určených právních požadavků a požadavků organizace a následků ztráty důvěrnosti, integrity a dostupnosti.
- Identifikace podstatných hrozeb a zranitelnosti daných aktiv.
- Odhad pravděpodobnosti hrozeb a zranitelností.
- Výpočet rizika.
- Posouzení závažnosti rizika podle předem zavedené stupnice.

Dalším krokem procesu řízení rizik je stanovení vhodného postupu při zvládnání každého identifikovaného rizika. Rizika je možné ošetřit pomocí preventivních a detekčních opatření, vyhnout se riziku, pojištění a/nebo prostého podstoupení rizika. Poté, co bylo riziko ohodnoceno, musí být učiněno rozhodnutí o tom, jaké kroky podniknout. Ve všech případech by rozhodnutí mělo vycházet z obchodního případu, který rozhodnutí odůvodňuje a který může být akceptován nebo napaden zainteresovanými stranami. Kapitola 6 popisuje různé možnosti zvládnání rizik a faktory ovlivňující toto rozhodnutí.

Poté, co byla zavedena vybraná opatření vyplývající z rozhodnutí o způsobu zvládnání rizik, měly by započít následné činnosti řízení rizik. Mezi tyto činnosti patří proces monitorování rizik a výkonu ISMS kvůli ubezpečení, že zavedená opatření plní požadovaný účel. Další činností je přezkoumání a přehodnocení rizik, nezbytné k přizpůsobení hodnocení rizik změnám, které se mohly přihodit během času v prostředí jednotlivých organizací. Hlášení a komunikování rizik jsou nezbytné k zajištění, že rozhodnutí jsou prováděna v kontextu přístupu celé organizace k rizikům. Koordinace různých procesů týkajících se rizik by měla zaručit, že provoz organizace bude výkonný a účinný. Soustavné zlepšování je podstatným prvkem probíhajících aktivit řízení rizik, vedoucí ke zvýšení účinnosti zavedených opatření a k dosažení cílů stanovených pro ISMS. Průběh aktivit řízení rizik popisuje kapitola 7.

Úspěšné zavedení procesu řízení rizik vyžaduje jasné rozdělení a plnění rolí a odpovědností v organizaci. Kde je to relevantní, dokument popisuje role a odpovědnosti vztahující se k procesu řízení rizik.