



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



RISK ANALYSIS CONSULTANTS

# BS ISO/IEC 27001:2005

## Information Security Management Systems

Information technology - Security techniques - Information security management systems - Requirements

Překlad a interpretace pro české prostředí



RAC<sup>®</sup>

RISK ANALYSIS CONSULTANTS



© 2005, British Standards Institution  
© 2005, Risk Analysis Consultants

Licence k použití pro: Risk Analysis Consultants, s.r.o.

Datum verze 15.2.2006, výtisk #2

© 2006 Risk Analysis Consultants

Překlad, kopírování a sdílení zakázáno

### Upozornění k manipulaci s PDF souborem

Tento soubor PDF může obsahovat vložené typy písma. V souladu s licenční politikou Adobe lze tento soubor tisknout nebo prohlížet, ale nesmí být editován, ledaže by typy písma, které jsou vloženy, byly používány na základě licence a instalovány v počítači, na němž se editace provádí. Při stažení tohoto souboru přejímají jeho uživatelé odpovědnost za to, že nebude porušena licenční politika Adobe. Ústřední sekretariát ISO nepřijímá za její porušení žádnou odpovědnost.

Adobe je obchodní značka „Adobe Systems Incorporated“.

Podrobnosti o softwarových produktech použitých k vytvoření tohoto souboru PDF, lze najít ve Všeobecných informacích, které jsou k souboru připojeny; parametry, pomocí kterých byl PDF soubor vytvořen, byly optimalizovány pro tisk. Soubor byl zpracován s maximální péčí tak, aby ho členské organizace ISO mohly používat. V málo pravděpodobném případě, tj. když vznikne problém, který se týká souboru, informujte o tom na níže uvedené adrese Ústřední sekretariát ISO.



© ISO/IEC 2005

Všechna práva vyhrazena. Není-li uvedeno jinak, nesmí být žádná část této publikace reprodukována nebo zpracována jakoukoliv jinou formou, jako jsou například elektronické nebo mechanické prostředky, včetně fotokopíí a mikrofilmu, bez písemného povolení ISO; povolení lze vyžádat na níže uvedené adrese nebo u členské národní organizace v zemi žadatele.

ISO copyright office  
Case postale 56, CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

## Preambule

Dokument je překladem a interpretací britské normy *BS ISO/IEC 27001:2005 Information Technology – Security techniques – Information security management systems – Requirements* pro využití v podmínkách České republiky. Dokument využívá terminologii a pojmy blízké normám, standardům a praktikám platným nebo užívaným v českém prostředí ve spojení s problematikou bezpečnosti informačních technologií a systémů.

Dokument je určen pro vedoucí a řídicí pracovníky, specialisty a odborníky pracující v oblasti bezpečnosti informačních systémů v České republice jako odborná publikace obsahující český překlad a interpretaci jedné ze světově uznávaných norem v této oblasti pro účely její implementace v rámci informačních systémů v České republice.

Dokument oproti originálu neobsahuje některé úvodní a závěrečné informace, které nejsou pro podmínky České republiky přímo relevantní. Pro seznámení se s těmito informacemi je nutno využít anglický originál.

### Statut dokumentu

This document is a translation of BS ISO/IEC 27001:2005 into the Czech language by Risk Analysis Consultants with the approval of the British Standards Institution. BSI takes no responsibility for the accuracy of this translation. In any cases of dispute the English original shall be taken as authoritative.

Překlad: Tento dokument je překlad BS ISO/IEC 27001:2005 do češtiny, provedený společností Risk Analysis Consultants se souhlasem British Standards Institution. BSI neodpovídá za správnost překladu. Ve sporných případech je směrodatným anglický originál.

### Autorská práva

Autorská práva anglického originálu vlastní British Standards Institution a autorská práva překladu vlastní Risk Analysis Consultants, s.r.o. Jakékoliv použití tohoto dokumentu nebo jeho části pro účely další distribuce, prodeje, kopírování, rozmnožování nebo jiného způsobu šíření není bez souhlasu vlastníků autorských práv možné. Dokument může být použit jenom v souladu s požadavky na ochranu autorských práv a „tak jak je“ jako překlad a interpretace pro české prostředí bez nároku na úhradu možných škod způsobených jeho vlastní aplikací na konkrétní podmínky organizace.

### Informace

Společnost Risk Analysis Consultants, s.r.o., si vyhrazuje právo na změny v dokumentu bez oznámení subjektům, které dokument užívají v souladu s licenčními podmínkami. Připomínky a návrhy na změnu obsahu dokumentu, požadavky na informace o aktuální verzi dokumentu je možno zasílat na níže uvedenou adresu.

Risk Analysis Consultants, s. r. o.

Španělská 2, 120 00 Praha 2, CZ

Tel. +420-2 21 62 84 00, fax +420 2 21 62 84 01

rac@rac.cz, www.rac.cz

Copyright © 2005 British Standards Institution

Translation © 2005 Risk Analysis Consultants

## Obsah

Preambule	iv
Předmluva	vii
0 Úvod	viii
0.1 Všeobecně	viii
0.2 Procesní přístup	viii
0.3 Kompatibilita s jinými systémy řízení	ix
1 Předmět normy	1
1.1 Všeobecně	1
1.2 Použití	1
2 Normativní odkazy	2
3 Termíny a definice	2
3.1 aktivum (asset)	2
3.2 dostupnost (availability)	2
3.3 důvěrnost (confidentiality)	2
3.4 bezpečnost informací (information security)	2
3.5 bezpečnostní událost (information security event)	2
3.6 bezpečnostní incident (information security incident)	2
3.7 systém řízení bezpečnosti informací ISMS (information security management system)	3
3.8 integrita (integrity)	3
3.9 zbytkové riziko (residual risk)	3
3.10 akceptace rizik (risk acceptance)	3
3.11 analýza rizik (risk analysis)	3
3.12 hodnocení rizik (risk assessment)	3
3.13 vyhodnocení rizik (risk evaluation)	3
3.14 řízení rizik (risk management)	3
3.15 zvládání rizik (risk treatment)	4
3.16 prohlášení o aplikovatelnosti (statement of applicability)	4
4 Systém řízení bezpečnosti informací	4
4.1 Všeobecné požadavky	4
4.2 Ustavení a řízení ISMS	4
4.3 Požadavky na dokumentaci	7
5 Odpovědnost vedení	9
5.1 Závazek vedení	9
5.2 Řízení zdrojů	9
6 Interní audity ISMS	10
7 Přezkoumání ISMS vedením organizace	10
7.1 Všeobecně	10

7.2	Vstup pro přezkoumání	10
7.3	Výstup z přezkoumání	11
8	Zlepšování ISMS	11
8.1	Neustálé zlepšování	11
8.2	Opatření k nápravě	11
8.3	Preventivní opatření	11
	Příloha A	13
	(normativní)	13
	Cíle opatření a jednotlivá bezpečnostní opatření	13
	Příloha B	28
	(informativní)	28
	Principy směrnice OECD a norma ISO/IEC 27001	28
	Příloha C	29
	(informativní)	29
	Vztah mezi ISO 9001:2000, ISO 14001:2004 a touto normou	29
	Bibliografie	31

## Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím technických komisí zřízených příslušnou organizací k tomu, aby se zabývaly určitou oblastí technické činnosti. V oblastech společného zájmu technické komise ISO a IEC spolupracují. Práce se zúčastňují i jiné mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informačních technologií zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou zpracovány v souladu s pravidly uvedenými v části 2 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je připravovat mezinárodní normy. Návrhy mezinárodních norem přijaté společnou technickou komisí se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Pozornost je třeba věnovat možnosti, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nenesou odpovědnost za identifikaci všech patentových práv nebo kteréhokoliv z nich.

Mezinárodní norma ISO/IEC 27001 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Information technology*, subkomise SC 27, *IT Security techniques*.

## 0 Úvod

### 0.1 Všeobecně

Tato mezinárodní norma byla připravena proto, aby poskytla podporu pro ustavení, zavádění, provozování, monitorování, udržování a zlepšování systému řízení bezpečnosti informací (Information Security Management System nebo ISMS). Přijetí ISMS by mělo být strategickým rozhodnutím organizace. Návrh a zavedení ISMS v organizaci je podmíněno potřebami a cíli činností (business) požadavky na bezpečnost, dále pak používanými procesy a velikostí a strukturou organizace. Všechny tyto a jejich podpůrné systémy podléhají změnám v čase. Předpokládá se, že jednoduché situace vyžadují jednoduchá řešení ISMS.

Tato norma je určena k posuzování souladu ze strany zainteresovaných interních i externích stran.

### 0.2 Procesní přístup

Tato mezinárodní norma prosazuje přijetí procesního přístupu pro ustavení, zavádění, provozování, monitorování, udržování a zlepšování ISMS v organizaci.

Aby organizace fungovala efektivně, musí identifikovat a řídit mnoho vzájemně propojených činností. Činnost, která využívá zdroje a je řízena za účelem přeměny vstupů na výstupy, může být považována za proces. Výstup z jednoho procesu často přímo tvoří vstup pro následující proces.

Aplikace systému procesů v organizaci, spolu s identifikací těchto procesů, jejich vzájemným působením a řízením může být označováno jako "procesní přístup".

Při použití procesního přístupu pro řízení bezpečnosti informací tak, jak je prezentován v této normě, je kladen důraz na:

- a) pochopení požadavků na bezpečnost informací organizace a potřebu stanovení politiky a cílů bezpečnosti informací;
- b) zavedení a provozování opatření pro řízení bezpečnosti informací v kontextu s řízením celkových rizik činností organizace;
- c) monitorování a přezkoumání výkonnosti a účinnosti ISMS;
- d) neustálé zlepšování založené na objektivním měření.

Model známý jako "Plánuj-Dělej-Kontroluj-Jednej" (Plan-Do-Check-Act nebo PDCA) může být aplikován na všechny procesy ISMS tak, jak jsou zavedeny touto normou. Obrázek 1 znázorňuje, jak ISMS přijímá požadavky bezpečnosti informací a očekávání zainteresovaných stran jako vstup, a jak pomocí nezbytných činností a procesů vytváří výstupy bezpečnosti informací, které splňují tyto požadavky a očekávání. Obrázek 1 také znázorňuje propojení procesů uvedených v kapitolách 4, 5, 6, 7 a 8.

Zavedení modelu PDCA bude také odrážet principy, které jsou definovány ve směrnici OECD (2002)<sup>1</sup> pro řízení bezpečnosti informačních systémů a sítí. Norma ISO/IEC 27001 poskytuje celistvý model pro zavedení principů definovaných v této směrnici, které upravují hodnocení rizik, návrh a zavedení bezpečnosti, řízení bezpečnosti a opětovné hodnocení bezpečnosti.

#### PŘÍKLAD 1

Může být například požadováno, aby v případě narušení bezpečnosti nebyly způsobeny organizaci vážné finanční škody ani jiné těžkosti (např. ztráta image).

<sup>1</sup> OECD. OECD Guidelines for the Security of Information systems and Network – Towards a Culture of Security. Paris: OECD, July 2002. [www.oecd.org](http://www.oecd.org).

(Směrnice pro bezpečnost informačních systémů a sítí - Směrem ke kultuře bezpečnosti.)