



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



RISK ANALYSIS CONSULTANTS

# BS ISO/IEC 27002:2005

## Information Security Management

Information Technology - Security techniques - Code of practice for information security management

Překlad a interpretace pro české prostředí



**RAC**<sup>®</sup>

RISK ANALYSIS CONSULTANTS



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

Licence k užití pro: Risk Analysis Consultants, s.r.o.  
Datum verze 6.9.2007, výtisk #2  
© 2007 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 vytváření 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 mikrofilmů, 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 27002:2005 Information Technology – Security techniques – Code of practice for information security management* 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 27002:2005 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 27002:2005 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	viii
0 Úvod	ix
0.1 Co je bezpečnost informací?	ix
0.2 Proč je nezbytná bezpečnost informací	ix
0.3 Jak stanovit bezpečnostní požadavky	ix
0.4 Hodnocení bezpečnostních rizik	x
0.5 Výběr opatření	x
0.6 Východiska bezpečnosti informací	x
0.7 Kritické faktory úspěchu	xi
0.8 Vytváření vlastních směrnic	xi
1 Předmět normy	1
2 Termíny a definice	1
2.1 aktivum ( <i>asset</i> )	1
2.2 opatření ( <i>control</i> )	1
2.3 metodický postup, doporučení, postup ( <i>guideline</i> )	1
2.4 prostředky pro zpracování informací ( <i>information processing facilities</i> )	1
2.5 bezpečnost informací ( <i>information security</i> )	1
2.6 bezpečnostní událost ( <i>information security event</i> )	1
2.7 bezpečnostní incident ( <i>information security incident</i> )	2
2.8 politika ( <i>policy</i> )	2
2.9 riziko ( <i>risk</i> )	2
2.10 analýza rizik ( <i>risk analysis</i> )	2
2.11 hodnocení rizik ( <i>risk assessment</i> )	2
2.12 vyhodnocení rizik ( <i>risk evaluation</i> )	2
2.13 řízení rizik ( <i>risk management</i> )	2
2.14 zvládání rizik ( <i>risk treatment</i> )	2
2.15 třetí strana ( <i>third party</i> )	2
2.16 hrozba ( <i>threat</i> )	3
2.17 zranitelnost ( <i>vulnerability</i> )	3
3 Struktura normy	4
3.1 Oblasti bezpečnosti	4
3.2 Hlavní kategorie bezpečnosti	4
4 Hodnocení a zvládání rizik	5
4.1 Hodnocení bezpečnostních rizik	5
4.2 Zvládání bezpečnostních rizik	5
5 Bezpečnostní politika	7

5.1	Politika bezpečnosti informací	7
6	Organizace bezpečnosti informací	9
6.1	Interní organizace	9
6.2	Externí subjekty	13
7	Řízení aktiv	19
7.1	Odpovědnost za aktiva	19
7.2	Klasifikace informací	20
8	Bezpečnost lidských zdrojů	23
8.1	Před vznikem pracovního vztahu	23
8.2	Během pracovního vztahu	25
8.3	Ukončení nebo změna pracovního vztahu	26
9	Fyzická bezpečnost a bezpečnost prostředí	29
9.1	Zabezpečené oblasti	29
9.2	Bezpečnost zařízení	32
10	Řízení komunikací a řízení provozu	36
10.1	Provozní postupy a odpovědnosti	36
10.2	Řízení dodávek služeb třetích stran	38
10.3	Plánování a přejímání systémů	40
10.4	Ochrana proti škodlivým programům a mobilním kódům	41
10.5	Zálohování	43
10.6	Správa bezpečnosti sítě	44
10.7	Bezpečnost při zacházení s médii	45
10.8	Výměna informací	47
10.9	Služby elektronického obchodu	51
10.10	Monitorování	53
11	Řízení přístupu	57
11.1	Požadavky na řízení přístupu	57
11.2	Řízení přístupu uživatelů	58
11.3	Odpovědnosti uživatelů	60
11.4	Řízení přístupu k síti	62
11.5	Řízení přístupu k operačnímu systému	66
11.6	Řízení přístupu k aplikacím a informacím	69
11.7	Mobilní výpočetní zařízení a práce na dálku	70
12	Akvizice, vývoj a údržba informačních systémů	73
12.1	Bezpečnostní požadavky informačních systémů	73
12.2	Správné zpracování v aplikacích	73
12.3	Kryptografická opatření	76
12.4	Bezpečnost systémových souborů	78
12.5	Bezpečnost procesů vývoje a podpory	80
12.6	Řízení technických zranitelností	83

13	Zvládání bezpečnostních incidentů	85
13.1	Hlášení bezpečnostních událostí a slabin	85
13.2	Zvládání bezpečnostních incidentů a kroky k nápravě	86
14	Řízení kontinuity činností organizace	89
14.1	Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	89
15	Soulad s požadavky	93
15.1	Soulad s právními normami	93
15.2	Soulad s bezpečnostními politikami, normami a technická shoda	96
15.3	Hlediska auditu informačních systémů	97
	Bibliografie	99
	Rejstřík	101



## 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 informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou zpracovány v souladu s pravidly uvedenými v části 2 Směrnice 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 27002 byla připravena společnou technickou komisí ISO/IEC JTC 1 *Information technology*, subkomise SC 27, *IT Security techniques*.

Toto druhé vydání nahrazuje ISO/IEC 17799:2000, které tímto pozbývá platnosti.

Technická komise ISO/IEC JTC 1/SC 27 připravuje soubor mezinárodních norem věnovaných systému řízení bezpečnosti informací (ISMS). Soubor norem zahrnuje požadavky na systém řízení bezpečnosti informací, řízení rizik, metriky a měření výkonu a doporučení k implementaci. Soubor těchto norem bude vydán v sérii 27000.

**Dne 31. Června 2007 došlo k přečíslování ISO/IEC 17799:2005 na ISO/IEC 27002:2005, text normy zůstal beze změny.**

## 0 Úvod

### 0.1 Co je bezpečnost informací?

Informace jsou aktiva, která mají pro organizaci hodnotu. Je tedy nutné je vhodným způsobem chránit. Obzvláště se vzrůstající propojeností prostředí jednotlivých organizací je tato potřeba stále více aktuální. S rostoucí propojeností jsou informace vystaveny zvyšujícímu se počtu různých hrozeb a zranitelností (viz také Směrnice OECD pro bezpečnost informačních systémů a sítí: směrem ke kultuře bezpečnosti <sup>1</sup>).

Informace mohou existovat v různých podobách. Mohou být vytištěny nebo napsány na papíře, uloženy v elektronické podobě, posílány poštou nebo elektronickou cestou, zachyceny na film nebo vyřčeny při konverzaci.

Bezpečnost informací je zaměřena na širokou škálu hrozeb a zajišťuje tak kontinuitu činností organizace, minimalizuje obchodní ztráty a maximalizuje návratnost investic a podnikatelských příležitostí.

Bezpečnosti informací lze dosáhnout implementací soustavy opatření, která mohou existovat ve formě pravidel, postupů, procedur, organizační struktury, programových a hardwarových funkcí. Tato opatření musí být ustavena, zavedena, provozována, monitorována, přezkoumávána a zlepšována proto, aby bylo dosaženo specifických bezpečnostních cílů organizace. Toto všechno by mělo být prováděno v souladu s ostatními řídicími procesy organizace.

### 0.2 Proč je nezbytná bezpečnost informací

Informace a podpůrné procesy, systémy a sítě jsou důležitými aktivy organizace. Vymezení, zavádění, podpora a zlepšování bezpečnosti informací může být zásadní pro udržení konkurenceschopnosti, peněžních toků (cash-flow), ziskovosti, právní shody a dobrého jména organizace.

Stále rostoucí měrou jsou organizace a jejich informační systémy vystavovány bezpečnostním hrozbám z různých zdrojů, včetně počítačových podvodů, špionáže, sabotáže, vandalizmu, požárů a povodní. Zdroje škod, jako jsou počítačové viry, útoky hackerů a útoky typu odepření služby (denial of service), jsou stále častější, roste jejich nebezpečnost a sofistikovanost.

Bezpečnost informací je důležitá z hlediska ochrany kritické infrastruktury a to jak v soukromém, tak ve státním sektoru. V obou sektorech je bezpečnost informací důležitá pro existenci některých služeb, například e-governmentu nebo e-komerce a zároveň kvůli vyhnutí se nebo snížení relevantních rizik. Propojení veřejných a privátních sítí i sdílení informačních zdrojů zvyšuje obtížnost řízení přístupu. Trend směřující k distribuovanému zpracování oslabil efektivnost centrální kontroly prováděné specialisty.

Mnoho informačních systémů nebylo navrženo tak, aby byly bezpečné. Bezpečnost, která může být dosažena technickými prostředky, je nedostačující a měla by být doplněna odpovídajícím řízením a postupy. Pro určení opatření, která je třeba přijmout, je nutné pečlivé plánování a rozbor každého detailu. Řízení bezpečnosti informací proto vyžaduje alespoň nějakou spoluúčasť všech zaměstnanců organizace. Může rovněž zahrnovat spolupráci majitelů organizace (akcionářů), dodavatelů, třetích stran, zákazníků a dalších externích subjektů. V neposlední řadě může být potřebná i rada od specialistů z jiných organizací.

### 0.3 Jak stanovit bezpečnostní požadavky

Je nezbytné, aby organizace určila své bezpečnostní požadavky. K tomu existují tři hlavní zdroje.

1. Prvním zdrojem je hodnocení rizik, která organizaci hrozí, beroucí v potaz celkovou strategii a cíle organizace. V rámci hodnocení rizik se identifikují hrozby působící vůči aktivům, zranitelnosti, které mohou být hrozbami využity i pravděpodobnost jejich výskytu, a provádí se odhad jejich potenciálního dopadu.

<sup>1</sup> OECD Guidelines for the Security of Information systems and Network – Towards a Culture of Security.

2. Druhým zdrojem jsou požadavky zákonů a podzákoných norem, smluvní ujednání a místní zvyklosti, které organizace, její obchodní, smluvní partneři a poskytovatelé služeb musí splňovat.
3. Třetím zdrojem jsou konkrétní principy, cíle a požadavky na zpracování informací, které si organizace vytvořila pro podporu své činnosti.

#### 0.4 Hodnocení bezpečnostních rizik

Požadavky na bezpečnost jsou stanoveny za pomoci metodického hodnocení bezpečnostních rizik. Výdaje na bezpečnostní opatření by měly odpovídat ztrátám způsobeným narušením bezpečnosti.

Výsledky hodnocení rizik pomohou určit vedení organizace odpovídající kroky i priority pro řízení bezpečnostních rizik u informací a pro realizaci opatření určených k zamezení jejich výskytu.

Hodnocení rizik by mělo být prováděno periodicky, aby bylo možné včas reagovat na jakékoliv změny v bezpečnostních požadavcích.

Více informací o hodnocení rizik je uvedeno v kapitole 4.1 „Hodnocení bezpečnostních rizik“.

#### 0.5 Výběr opatření

Jakmile jsou identifikovány bezpečnostní požadavky a rizika, a bylo rozhodnuto jakým způsobem bude se zjištěnými riziky naloženo, měla by být vybrána a implementována opatření zajišťující snížení rizik na přijatelnou úroveň. Taková opatření mohou být vybrána z tohoto dokumentu nebo i z jiných souborů opatření. Pro pokrytí specifických potřeb mohou být vytvořena zcela nová opatření. Výběr konkrétních opatření je na rozhodnutí každé organizace. Rozhodnutí je založeno na kritériích určujících akceptaci nebo zvládnutí rizika a celkovém přístupu organizace k řízení rizik. Při výběru opatření by měla být zohledněna příslušná národní a mezinárodní legislativa a regulace.

Některá opatření v tomto dokumentu mohou být chápána jako základní doporučení pro řízení bezpečnosti informací a mohou být využita ve většině organizací. Detailněji jsou vysvětlena v části „Východiska bezpečnosti informací“.

Další informace o výběru opatření a způsobech zvládnutí rizik jsou uvedeny v kapitole 4.2 „Zvládnutí bezpečnostních rizik“.

#### 0.6 Východiska bezpečnosti informací

Řada opatření může být považována za základní principy představující dobrá východiska pro implementaci bezpečnosti informací. Mohou vycházet ze základních legislativních požadavků nebo jsou obecně považována za nejlepších způsob řešení bezpečnosti informací.

Opatření, která by měla být pro organizaci podstatná z pohledu legislativy, jsou:

- a) ochrana osobních údajů (viz 15.1.4);
- b) ochrana důležité dokumentace organizace, jako například účetních záznamů (viz 15.1.3);
- c) ochrana duševního vlastnictví (viz 15.1.2).

Opatření, považovaná za základ nejlepších praktik (best practices) pro zajištění bezpečnosti informací, jsou:

- a) dokument bezpečnostní politiky informací (viz 5.1.1);
- b) přidělení odpovědností v oblasti bezpečnosti informací (viz 6.1.3);
- c) vzdělávání, školení a zvyšování povědomí v oblasti bezpečnosti informací (viz 8.2.2);
- d) bezchybné zpracování v aplikačních systémech (viz 12.2);
- e) řízení technických zranitelností (viz 12.6);
- f) řízení kontinuity činností organizace (viz 14);
- g) zvládnutí bezpečnostních incidentů a kroky k nápravě (viz 13.2).

Tato opatření fungují ve většině organizací a prostředí.

Ačkoliv všechna opatření uvedená v tomto dokumentu jsou důležitá, je nutné si uvědomit, že o výběru a aplikaci konkrétních opatření by mělo být rozhodnuto až ve světle specifických rizik, kterým organizace čelí. I když výše uvedené doporučení může být považováno za dobré východisko, nenahrazuje výběr opatření vycházející z hodnocení rizik.

## 0.7 Kritické faktory úspěchu

Jak ukazuje zkušenost, pro úspěšnou implementaci bezpečnosti informací v organizaci jsou často kritické následující faktory:

- a) bezpečnostní politika, bezpečnostní cíle a činnosti, které respektují cíle činností organizace;
- b) přístup k zavádění, udržování, monitorování a zlepšování bezpečnosti informací v souladu s kulturou organizace;
- c) zřetelná podpora a angažovanost ze strany vedení organizace;
- d) dobré pochopení bezpečnostních požadavků, hodnocení a řízení rizik;
- e) účinný marketing bezpečnosti vůči vedení organizace, zaměstnancům a jiným stranám;
- f) rozšíření směrnic a norem bezpečnostní politiky informací mezi všechny zaměstnance, vedení organizace a třetí strany;
- g) zdroje na financování činností souvisejících s řízením bezpečnosti informací;
- h) realizace odpovídajících školení, vzdělávání a programů zvyšování povědomí;
- i) zavedení procesu zvládání bezpečnostních incidentů;
- j) komplexní a vyvážený systém pro ohodnocení míry účinnosti řízení bezpečnosti informací a získávání návrhů ke zlepšení na základě zpětné vazby.

## 0.8 Vytváření vlastních směrnic

Tento soubor postupů může být chápán jako východisko pro vytváření specifických směrnic organizace. Ne všechna doporučení a opatření tohoto souboru postupů mohou být použitelná. Kromě toho mohou být nezbytná i další opatření, která nejsou v tomto dokumentu uvedena. V takovém případě je užitečné zanechat v nich odkaz na tuto normu a usnadnit tak ověření shody prováděné auditory a obchodními partnery.