

**2006**

Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky	ČSN ISO/IEC 27001  36 9790
--	-------------------------------------

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

Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences

Tato norma je českou verzí mezinárodní normy ISO/IEC 27001:2005. Překlad byl zajištěn Českým normalizačním institutem. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 27001:2005. It was translated by Czech Standards Institute. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN BS 7799-2 (36 9790) z prosince 2004.



© Český normalizační institut, 2006

**76533**

Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu.

## Změny proti předchozím normám

Oproti předchozímu vydání normy ČSN BS 7799 bylo z Přílohy A odstraněno devět bezpečnostních opatření a sedmnáct nových jich přibylo.

## Informace o citovaných normativních dokumentech

ISO 9001:2000 zavedena v ČSN EN ISO 9001:2001 (01 0321) Systémy managementu jakosti - Požadavky

ISO 14001 zavedena v ČSN EN ISO 14001:2005 (010901) Systémy environmentálního managementu - Požadavky s návodem pro použití

ISO/IEC 13335-1:2004 dosud nezavedena

ISO/IEC TR 13335-3:1998 zavedena v ČSN ISO/IEC TR 13335-3:2000 (36 9786) Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti IT

ISO/IEC 17799:2005 zavedena v ČSN ISO/IEC 17799:2006 (36 9790) Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací

EN ISO 19011:2002 zavedena v ČSN EN ISO 19011:2003 (01 0330) Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu

## Související ČSN

ČSN ISO/IEC 17799 (36 9790) Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací

## Vysvětlivky k textu převzaté normy

Nesoulad v překladu jednotlivých kapitol v Příloze C je způsoben různými překlady předchozích vydání norem ČSN EN ISO 9001 a ČSN EN ISO 14001.

## Vypracování normy

Zpracovatel: Risk Analysis Consultants, s.r.o., IČ 63672774, Ing. Libor ©iroký

Technická normalizační komise: TNK 20 Informační technologie

Zaměstnanec Českého normalizačního institutu: Ing. Petr Wallenfels

#### Odmítavé stanovisko 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 jakoukoli 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.ch](mailto:copyright@iso.ch)

Web [www.iso.ch](http://www.iso.ch)

Strana 4

---

Obsah

Strana

## **0**

Úvod

..... 6

## **0.1**

Všeobecně

..... 6

## **0.2** Procesní

přístup

.....

<b>0.3</b>	Kompatibilita s jinými systémy managementu.....	7
<b>1</b>	Předmět normy ..... ..	8
<b>1.1</b>	Všeobecně ..... .....	8
<b>1.2</b>	Použití ..... .....	8
<b>2</b>	Normativní odkazy .....	8
<b>3</b>	Termíny a definice .....	8
<b>4</b>	Systém managementu bezpečnosti informací.....	10
<b>4.1</b>	Všeobecné požadavky .....	10
<b>4.2</b>	Ustavení a řízení ISMS..... 10	
<b>4.2.1</b>	Ustavení ISMS ..... ..	10
<b>4.2.2</b>	Zavádění a provozování ISMS.....	12
<b>4.2.3</b>	Monitorování a přezkoumání ISMS.....	12
<b>4.2.4</b>	Udržování a zlepšování ISMS.....	13

<b>4.3</b>	Požadavky na dokumentaci.....	13
<b>4.3.1</b>	Všeobecně.....	13
<b>4.3.2</b>	Řízení dokumentů.....	14
<b>4.3.3</b>	Řízení záznamů.....	14
<b>5</b>	Odpovědnost vedení.....	14
<b>5.1</b>	Závazek vedení.....	14
<b>5.2</b>	Řízení zdrojů.....	15
<b>5.2.1</b>	Zajištění zdrojů.....	15
<b>5.2.2</b>	Čkolení, informovanost a odborná způsobilost.....	15
<b>6</b>	Interní audity ISMS.....	15
<b>7</b>	Přezkoumání ISMS vedením organizace.....	15
<b>7.1</b>	Všeobecně.....	15
<b>7.2</b>	Vstup pro	

přezkoumání	16
7.3 Výstup z přezkoumání	16
8 Zlepšování ISMS	16
8.1 Neustálé zlepšování	16
8.2 Opatření k nápravě	16
8.3 Preventivní opatření	17
<b>Příloha A</b> (normativní) Cíle opatření a jednotlivá bezpečnostní opatření	18
<b>Příloha B</b> (informativní) Principy směrnice OECD a norma ISO/IEC 27001	32
<b>Příloha C</b> (informativní) Vztah mezi ISO 9001:2000, ISO 14001:2004 a touto normou	33
Bibliografie	35

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

Strana 6

---

## 0 Úvod

### 0.1 Všeobecně

Tato mezinárodní norma byla připravena proto, aby poskytla podporu pro ustavení, zavádění, provozování, monitorování, udržování a zlepšování systému managementu 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 činnosti (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 management 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 management 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 popsány ve směrnici OECD (2002)<sup>1</sup> pro řízení bezpečnosti informačních systémů a sítí. Norma ISO/IEC 27001 poskytuje celistvý model pro zavedení principů popsanych v této směrnici, které upravují hodnocení rizik, návrh a zavedení bezpečnosti, management bezpečnosti a opětovné hodnocení bezpečnosti.

#### PŘÍKLAD 1

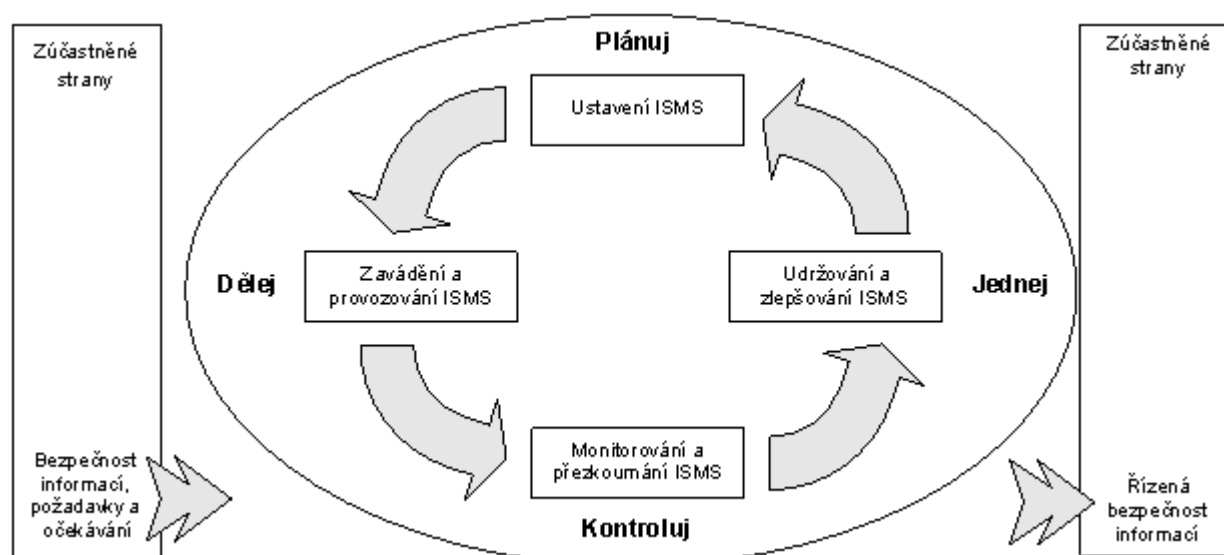
Může být například požadováno, aby v případě narušení bezpečnosti nebyly způsobeny organizaci vážné finanční škody ani jiné těžkosti (např. ztráta image).

#### PŘÍKLAD 2

Vyskytne-li se závažný incident, například napadení (hacking) eBusiness systému organizace (web site) očekává se, že pro minimalizaci dopadů incidentu budou k dispozici dostatečně vyškolení zaměstnanci.

<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).

Strana 7



Obrázek 1 - PDCA model aplikovaný na procesy ISMS



<b>Plánuj (ustavení ISMS)</b>	Ustavení politiky ISMS, cílů, procesů a postupů souvisejících s managementem rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace.
<b>Dělej (zavedení a provozování ISMS)</b>	Zavedení a využívání politiky ISMS, opatření, procesů a postupů.
<b>Kontroluj (monitorování a přezkoumání ISMS)</b>	Posouzení, kde je to možné i měření výkonu procesu vůči politice ISMS, cílům a praktickým zkušenostem a hlášení výsledků vedení organizace k přezkoumání.
<b>Jednej (udržování a zlepšování ISMS)</b>	Přijetí opatření k nápravě a preventivních opatření, založených na výsledcích interního auditu ISMS a přezkoumání systému řízení ze strany vedení organizace tak, aby bylo dosaženo neustálého zlepšování ISMS.

### 0.3 Kompatibilita s jinými systémy managementu

Tato mezinárodní norma je propojena s normami ISO 9001:2000 a ISO 14001:2004 tak, aby bylo podpořeno jejich konzistentní a jednotné zavedení a provoz. Jeden vhodně navržený systém managementu tak může naplnit požadavky všech těchto norem. Tabulka C.1 znázorňuje vztah mezi kapitolami této normy, ISO 9001:2000 a ISO 14001:2004.

Tato norma je navržena tak, aby organizaci umožnila propojit nebo integrovat ISMS s odpovídajícími požadavky systému managementu.

Strana 8

Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky

**Důležité upozornění - Tato publikace nemůže obsáhnout všechna opatření z oblasti jejího určení. Uživatelé jsou odpovědní za její správné použití. Shoda s normou sama o sobě nezbavuje organizaci odpovědnosti za splnění závazků vyplývajících ze zákona.**

#### 1 Předmět normy

##### 1.1 Všeobecně

Tato mezinárodní norma je použitelná pro všechny typy organizací (např. komerční organizace, vládní agentury a úřady, neziskové organizace). Norma specifikuje požadavky na ustavení, zavedení, provoz, monitorování, přezkoumání, udržování a zlepšování dokumentovaného ISMS v kontextu celkových rizik činností organizace. Specifikuje požadavky na zavedení bezpečnostních opatření, upravených podle potřeb jednotlivých organizací nebo jejich částí.

ISMS je navržen tak, aby zajistil odpovídající a přiměřená bezpečnostní opatření chránící informační aktiva a poskytující odpovídající jistotu zainteresovaným stranám.

**POZNÁMKA 1** Slovo „business“ je v textu normy překládáno jako „činnost organizace“, v kontextu celé normy jsou činnostmi organizace myšleny veškeré aktivity, které jsou důležité pro existenci organizace a naplňování jejích cílů.

POZNÁMKA 2 ISO/IEC 17799 poskytuje doporučení, která mohou být použita při návrhu a realizaci jednotlivých opatření.

---

**-- Vynechaný text --**