

Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací	ČSN ISO/IEC 27006  36 9790
---	-------------------------------------

Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

Technologies de l'information - Techniques de sécurité - Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

Tato norma je českou verzí mezinárodní normy ISO/IEC 27006:2007. Překlad byl zajištěn Českým normalizačním institutem. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 27006:2007. It was translated by Czech Standards Institute. It has the same status as the official version.



ISO/IEC 27001:2005 zavedena v ČSN ISO/IEC 27001:2006 (36 9790) Informační technologie -  
Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky

ISO/IEC 17021:2006 zavedena v ČSN ISO/IEC 17021:2007 (01 5257) Posuzování shody - Požadavky na  
orgány provádějící audit a certifikaci systémů managementu

ISO 19011 zavedena v ČSN EN ISO 19011 (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

Vypracování normy

Zpracovatel: Risk Analysis Consultants, s.r.o., IČ 63672774

Technická normalizační komise: TNK 20 Informační technologie

Zaměstnanec Českého normalizačního institutu: Ing. Petr Wallenfels

Strana 3

---

MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky  
Požadavky na orgány provádějící audit a certifikaci  
systémů řízení bezpečnosti informací

ISO/IEC 27006  
První vydání  
2007-03

ICS 35.040

Obsah

Strana

Úvod

.....  
..... 7

**1** Předmět  
normy

.....  
.. 8

**2** Citované normativní  
dokumenty..... 8

**3** Termíny a  
definice..... 8

<b>4</b>	Principy	9
<b>5</b>	Obecné požadavky	9
<b>5.1</b>	Právní a smluvní záležitosti	9
<b>5.2</b>	Řízení nestrannosti	9
<b>5.3</b>	Záruky a financování	9
<b>6</b>	Požadavky na strukturu	9
<b>6.1</b>	Organizační struktura a vrcholové vedení	9
<b>6.2</b>	Komise pro zabezpečování nestrannosti	9
<b>7</b>	Požadavky na zdroje	9
<b>7.1</b>	Odborná způsobilost managementu a pracovníků	9
<b>7.2</b>	Pracovníci podílející se na certifikačních činnostech	10
<b>7.3</b>	Použití externích auditorů a technických expertů	11
<b>7.4</b>	Záznamy o pracovnících	12
<b>7.5</b>	Outsourcing	12
<b>8</b>	Požadavky na	

informace.....	12
<b>8.1</b> Veřejně dostupné informace.....	12
<b>8.2</b> Certifikační dokumenty.....	12
<b>8.3</b> Seznam certifikovaných zákazníků.....	12
<b>8.4</b> Odkazování se na certifikaci a používání značek.....	12
<b>8.5</b> Důvěrnost.....	13
<b>8.6</b> Výměna informací mezi certifikačním orgánem a jeho zákazníky.....	13
<b>9</b> Požadavky na procesy.....	13
<b>9.1</b> Obecné požadavky.....	13
<b>9.2</b> Úvodní audit a certifikace.....	16
<b>9.3</b> Dohledové činnosti.....	19
<b>9.4</b> Recertifikace.....	20
<b>9.5</b> Speciální audity.....	20
<b>9.6</b> Pozastavení, odnětí nebo omezení rozsahu certifikace.....	20

## 9.7

Odvolání

..... 20

## 9.8

Stížnosti

..... 20

Strana 4

---

Strana

**9.9** Záznamy o žadatelích a  
zákaznících..... 20

**10** Požadavky na systém řízení certifikačního  
orgánu..... 21

### 10.1

Možnosti

..... 21

**10.2** Možnost první - Požadavky na systém řízení podle ISO  
9001..... 21

**10.3** Možnost druhá - Obecné požadavky na systém  
řízení..... 21

**Příloha A** (informativní) Analýza komplexnosti organizace a oborově - specifických  
aspektů..... 22

**Příloha B** (informativní) Příklady požadované odborné způsobilosti znalostí  
auditora..... 25

**Příloha C** (informativní) Trvání  
auditu..... 27

**Příloha D** (informativní) Doporučení pro přezkoumání opatření zavedených  
normou ISO/IEC 27001:2005,  
Příloha  
A

..... 31

Strana 5

---

#### Odmítnutí odpovědnosti za 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, pokud nejsou typy písma, které jsou vloženy, 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 se vztahují k souboru; 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 Ústřední sekretariát ISO na níže uvedené adrese.



#### **DOKUMENT CHRÁNĚNÝ COPYRIGHTEM**

© ISO/IEC 2007

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně fotokopíí a mikrofilmů, bez písemného svolení buď od organizace ISO na níže uvedené adrese nebo od členské organizace ISO 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)

Published in Switzerland

Strana 6

#### 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 nenese odpovědnost za identifikaci všech patentových práv nebo kteréhokoliv z nich.

Mezinárodní norma ISO/IEC 27006 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie, subkomise SC 27, IT Bezpečnostní techniky*.

Strana 7

---

## Úvod

ISO/IEC 17021 je mezinárodní norma, která nastavuje kritéria pro organizace zabývající se auditem a certifikací systémů řízení organizace. Pokud chtějí být tyto organizace akreditované pro shodu s ISO/IEC 17021 za účelem auditování a certifikace systému řízení bezpečnosti informací (Information Security Management System nebo ISMS) v souladu s ISO/IEC 27001:2005, je nutné ISO/IEC 17021 doplnit o dodatečné požadavky a doporučení. Takovéto dodatečné požadavky a doporučení poskytuje tato mezinárodní norma.

Text této mezinárodní normy kopíruje strukturu ISO/IEC 17021, dodatečné specifické požadavky a doporučení na aplikaci ISO/IEC 17021 pro certifikaci ISMS jsou v textu označeny písmeny „IS“.

Sloveso „muset“, je v textu normy použito ke zdůraznění těch opatření, která vyjadřují požadavky ISO/IEC 17021 a ISO/IEC 27001, a jsou povinná. Podmiňovací „měl by“ je použito ke zvýraznění těch opatření, která jsou vedena jako doporučená, ale přesto se očekává, že je certifikační orgán aplikuje.

Jedním z cílů této mezinárodní normy je umožnit akreditačním orgánům její efektivní aplikaci a harmonizaci s ostatními normami, podle kterých se provádí hodnocení certifikačních orgánů usilujících o akreditaci. V tomto kontextu, je jakákoliv odchylka certifikačního orgánu od doporučení této normy chápána jako výjimka. Takové odchylky budou ze strany akreditačního orgánu posuzovány případ od případu a povoleny pouze poté, co certifikační orgán doloží, že splňuje relevantní požadavek ISO/IEC 17021, ISO/IEC 27001 a této normy jiným ekvivalentním způsobem.

POZNÁMKA V celé normě jsou termíny „systém řízení“ a „systém“ zaměnitelné. Definici systému řízení je možné nalézt v ISO 9000:2005. Systém řízení ve smyslu používaném v této mezinárodní normě nesmí být zaměňován s dalšími typy systémů, jako jsou například systémy IT.

Strana 8

---

### 1 Předmět normy

Tato mezinárodní norma specifikuje požadavky a poskytuje doporučení pro orgány provádějící audit a certifikaci systému řízení bezpečnosti informací (Information Security Management System nebo

ISMS) a doplňuje tak požadavky obsažené v ISO/IEC 17021 a ISO/IEC 27001. Norma je primárně určená k podpoře procesu akreditace certifikačních orgánů poskytujících certifikace ISMS.

Požadavky obsažené v této mezinárodní normě musí být demonstrovány ve smyslu odborné způsobilosti a spolehlivosti orgánů poskytujících certifikace ISMS , doporučení obsažená v této mezinárodní normě poskytují dodatečnou interpretaci jednotlivých požadavků.

POZNÁMKA Tato mezinárodní norma může být použita jako kritériální dokument pro akreditaci, pro interní hodnocení nebo při jiných auditních procesech.

---

**-- Vynechaný text --**