ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Duben 2008**

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.

Národní předmluva

Informace o citovaných normativních dokumentech

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

Souvisíjící 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

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

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
Web www.iso.org

Published in Switzerland

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 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*.

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 auditovaní 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.

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 demonstrované 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 kriteriální dokument pro akreditaci, pro interní hodnocení nebo při jiných auditních procesech.

-- Vynechaný text --