ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Leden 2013**

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 a l,audit
et a la certification des systemes de management de la sécurité de l,information

Tato norma je českou verzí mezinárodní normy ISO/IEC 27006:2011. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 27006:2011. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 27006 (36 9790) z dubna 2008.

Národní předmluva

Změny proti předchozí normě

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 27006:2007), které bylo technicky revidováno. Byly provedeny opravy chyb, doplněny a zpřesněny některé články textu normy.

Informace o citovaných dokumentech

ISO/IEC 17021:2011 zavedena v ČSN ISO/IEC 17021:2011 (01 5257) Posuzování shody – Požadavky na orgány poskytující služby auditů a certifikace systémů managementu

ISO/IEC 19011 zavedena v ČSN EN ISO 19011 (01 0330) Směrnice pro auditování systémů managementu

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

Vypracování normy

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

Technická normalizační komise: TNK 20 Informační technologie

Zaměstnanec Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 27006
Požadavky na orgány provádějící audit a certifikaci Druhé vydání
systémů řízení bezpečnosti informací 2011-12

ICS 35.040

Obsah

Strana

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 ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní a nevládní mezinárodní organizace, 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 vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté společnou technickou komisí jsou rozesílány národním členům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

ISO/IEC 27006 vypracovala společná technická komise ISO/IEC JTC 1, *Information technology*, subkomise SC 27, *IT Security techniques*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 27006:2007), které bylo technicky revidováno.

Úvod

ISO/IEC 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 k vyjádření doporučení.

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.

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 určena k podpoře procesu akreditace certifikačních orgánů poskytujících certifikace ISMS.

Požadavky obsažené v této mezinárodní normě musí být demonstrované ve smyslu odborné způsobilosti a spoleh-
livosti 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.