ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Červenec 2013**

Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací

ČSN ISO/IEC 27007
36 9790

Information technology – Security techniques –
Guidelines for information security management systems auditing

Technologies de l,information – Techniques de sécurité –
Lignes directrices pour l,audit des systemes de management de la sécurité de l,information

Tato norma je českou verzí mezinárodní normy ISO/IEC 27007:2011. 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 27007:2011. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO 19011:2011 zavedena v ČSN EN ISO 19011:2012 (01 0330) Směrnice pro auditování systémů managementu

ISO/IEC 27000:2009 zavedena v ČSN ISO/IEC 27000:2010 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

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

Souvisící ČSN

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

ČSN ISO/IEC 27002:2006 (36 9790) Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací

ČSN ISO/IEC 27003:2011 (36 9790) Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací

ČSN ISO/IEC 27004:2011 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření

ČSN ISO/IEC 27005:2013 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

ČSN ISO/IEC 27006:2013 (36 9790) Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

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 27007
Směrnice pro audit systémů řízení První vydání
bezpečnosti informací 2011-11

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 27007 vypracovala společná technická komise ISO/IEC JTC 1, *Informační technologie*, subkomise SC 27, *IT bezpečnostní techniky*.

Úvod

Tato mezinárodní norma poskytuje doporučení pro řízení programu auditů systému řízení bezpečnosti informací (ISMS) a provádění interních nebo externích auditů v souladu s ISO/IEC 27001:2005, jakož i doporučení pro odbornou způsobilost a hodnocení auditorů ISMS, která by se měla používat v souvislosti s doporučením obsaženým v ISO 19011. Tato mezinárodní norma neuvádí požadavky.

Toto doporučení je určeno pro všechny uživatele, včetně malých a středních organizací.

ISO 19011, *Směrnice pro auditování systémů managementu* poskytuje doporučení pro řízení programů auditů, provádění interních i externích auditů systémů řízení, jakož i pro odbornou způsobilost a hodnocení auditorů systému řízení.

Text v této mezinárodní normě vychází ze struktury ISO 19011 a dodatečné doporučení, jež se konkrétně týká ISMS pro použití ISO 19011 pro audity ISMS, je identifikováno písmeny „IS“.

1 Předmět normy

Kromě doporučení obsažených v ISO 19011 poskytuje tato mezinárodní norma doporučení pro řízení programu auditů systému řízení bezpečnosti informací (ISMS), pro provádění auditů a pro odbornou způsobilost auditorů ISMS.

Tuto mezinárodní normu mohou používat ti, kdo potřebují pochopit nebo provádět interní a externí audity ISMS nebo řídit program auditů ISMS.