ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Červenec 2013**

Informační technologie – Bezpečnostní techniky –
Řízení rizik bezpečnosti informací

ČSN
ISO/IEC 27005
36 9790

Information technology – Security techniques – Information security risk management

Technologies de l,information – Techniques de sécurité – Gestion du risque en sécurité de l,information

Tato norma je českou verzí mezinárodní normy ISO/IEC 27005:2011. 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 27005:2011. It was translated by the 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 27005 (36 9790) z července 2009.

Národní předmluva

Změny proti předchozí normě

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 27005:2009), které bylo technicky revidováno. Základní změnou je změna termínů a definic a jejich použití v normě viz Příloha G.

Informace o citovaných dokumentech

ISO/IEC 27000 zavedena v ČSN ISO/IEC 27000 (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

TNI 01 0350:2010 Management rizik – Slovník (Pokyn 73)

ČSN ISO/IEC 17799:2006 (36 9790) Informační technologie – Bezpečnostní techniky – Soubor postupů

pro management bezpečnosti informací (ISO/IEC 27002:2005)

ČSN ISO 31000:2010 (01 0351) Management rizik – Principy a směrnice

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 27005
Řízení rizik bezpečnosti informací Druhé vydání
2011-06

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 odpovědnou za identifikaci jakéhokoliv nebo všech patentových práv.

ISO/IEC 27005 vypracovala společná technická komise ISO/IEC JTC 1, *Informační technologie*, subkomise SC 27, *IT bezpečnostní techniky*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 27005:2009), které bylo revidováno.

1 Předmět normy

Tato mezinárodní norma poskytuje doporučení pro řízení rizik bezpečnosti informací.

Tato mezinárodní norma podporuje obecný koncept specifikovaný v ISO/IEC 27001 a je strukturována, aby dostatečně podporovala implementaci informační bezpečnosti založené na přístupu řízení rizik.

Znalost konceptu, modelů, procesu a terminologie popsané v ISO/IEC 27001 a ISO/IEC 27002 je důležitá pro celkové pochopení této mezinárodní normy.

Tato mezinárodní norma je aplikovatelná na všechny typy organizací (např. komerční společnosti, vládní organizace, neziskové organizace), které mají v úmyslu řídit rizika, která mohou narušit bezpečnost informací organizace.