ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Červenec 2009**

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 sécutrité – Gestion du risque en sécurité de l,information

Tato norma je českou verzí mezinárodní normy ISO/IEC 27005:2008. 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 27005:2008. 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 nahrazují ČSN ISO/IEC TR 13335-3 (36 9786) z června 2000 a ČSN ISO/IEC TR 13335-4 (36 9786) z dubna 2002.

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 27002:2005 zavedena v ČSN ISO/IEC 27002:2006 (36 9790) Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací

Souvisící ČSN

ČSN ISO/IEC 27001 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky

ČSN ISO/IEC 17799 (36 9790) Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací

ČSN ISO/IEC 27006 (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, Ing. Jan Mikulecký, CISM, Ing. Libor Široký, CISM

Technická normalizační komise: TNK 20 Informační technologie

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

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 27005
Řízení rizik bezpečnosti informací

První vydání
2008-06

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 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 a IEC nenesou odpovědnost za identifikaci všech patentových práv nebo kteréhokoliv z nich.

Mezinárodní norma ISO/IEC 27005 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie*, subkomise SC 27, *IT Bezpečnostní techniky*.

Toto první vydání ruší a nahrazuje normy ISO/IEC TR 13335-3:1998 a ISO/IEC TR 13335-4:2000, ze kterých byla v rámci technické revize tato norma sestavena.

Úvod

Tato mezinárodní norma poskytuje doporučení pro řízení rizik bezpečnosti informací v rámci organizace, zejména pak doporučení s ohledem na požadavky ISMS podle ISO/IEC 27001. Nicméně tato mezinárodní norma nenabízí konkrétní metodiku pro řízení rizik bezpečnosti informací. Záleží jen na organizaci, jaký přístup k řízení rizik zvolí, například v závislosti na rozsahu ISMS, kontextu řízení rizik, průmyslovém odvětví. V souladu se zde popsaným přístupem k řízení rizik lze pro implementaci požadavků ISMS použít některou z celé řady existujících metodik pro řízení rizik.

Tato mezinárodní norma je určená manažerům a pracovníkům, kteří jsou v rámci organizace odpovědní za řízení rizik bezpečnosti informací a tam, kde je to relevantní, také externím subjektům.

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 (například komerční společnosti, vládní organizace, neziskové organizace), které mají v úmyslu řídit rizika, která mohou narušit bezpečnost informací organizace.