

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 sécurité – 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

Úvod 3

1 Předmět normy 3

2 Citované normativní dokumenty 3

3 Termíny a definice 3

4 Struktura této mezinárodní normy 3

5 Podklady 3

6 Přehled procesu řízení rizik bezpečnosti informací 3

7 Stanovení kontextu 3

7.1 Obecná hlediska 3

7.2 Základní kritéria 3

7.3 Rozsah a hranice 3

7.4 Organizační struktura pro řízení rizik bezpečnosti informací 3

8 Hodnocení rizik bezpečnosti informací 3

8.1 Všeobecný popis hodnocení rizik bezpečnosti informací 3

8.2 Analýza rizik 3

8.2.1 Identifikace rizik 3

8.2.2 Odhad rizik 3

8.3 Vyhodnocení rizik 3

9 Zvládání rizik bezpečnosti informací 3

9.1 Všeobecný popis zvládání rizik 3

9.2 Redukce rizik 3

9.3 Podstoupení rizik 3

9.4 Vyhnutí se riziku 3

9.5 Přenos rizik 3

10 Akceptace rizik bezpečnosti informací 3

11 Komunikace rizik bezpečnosti informací 3

12 Monitorování a přezkoumávání rizik bezpečnosti informací 3

12.1 Monitorování a přezkoumávání rizikových faktorů 3

12.2 Monitorování, přezkoumávání a zlepšování řízení rizik 3

Příloha A (informativní) Definování rozsahu a hranic procesu řízení rizik bezpečnosti informací 3

A.1 Studie organizace 3

A.2 Seznam omezení ovlivňující organizaci 3

A.3 Seznam legislativních a regulačních doporučení použitelných v organizaci 3

A.4 Seznam omezení ovlivňujících rozsah 3

Strana

Příloha B (informativní) Identifikace a ohodnocení aktiv a zjišťování dopadu 3

B.1 Příklady identifikace aktiv 3

B.1.1 Identifikace primárních aktiv 3

B. 1.2 Seznam a popis podpůrných aktiv 3

B.2 Ohodnocení aktiv 3

B.3 Hodnocení dopadu 3

Příloha C (informativní) Příklady typických hrozeb 3

Příloha D (informativní) Zranitelnosti a metody pro hodnocení zranitelností 3

D.1 Příklady zranitelností 3

D.2 Metody hodnocení technických zranitelností 3

Příloha E (informativní) Přístupy k hodnocení rizik bezpečnosti informací 3

E.1 Přehledové hodnocení rizik bezpečnosti informací 3

E.2 Detailní hodnocení rizik bezpečnosti informací 3

E.2.1 Příklad 1 Matice s předem definovanými hodnotami 3

E.2.2 Příklad 2 Třídění hrozeb pomocí míry rizika 3

E.2.3 Příklad 3 Stanovení hodnoty pravděpodobnosti a možných následků rizik 3

Příloha F (informativní) Omezení pro redukci rizik 3

Bibliografie 3

Odmítnutí odpovědnosti za manipulaci s PDF souborem

Tento soubor PDF může obsahovat vložené typy písma. V souladu s licenční politikou Adobe lze tento soubor tisknout nebo prohlížet, ale nesmí být editován, pokud nejsou typy písma, které jsou vloženy, používány na základě licence a instalovány v počítači, na němž se editace provádí. Při stažení tohoto souboru přejímají jeho uživatelé odpovědnost za to, že nebude porušena licenční politika Adobe. Ústřední sekretariát ISO nepřijímá za její porušení žádnou odpovědnost.

Adobe je obchodní značka „Adobe Systems Incorporated“.

Podrobnosti o softwarových produktech použitých k vytvoření tohoto souboru PDF lze najít ve Všeobecných informacích, které se vztahují k souboru; parametry, pomocí kterých byl PDF soubor vytvořen, byly optimalizovány pro tisk. Soubor byl zpracován s maximální péčí tak, aby ho členské organizace ISO mohly používat.

V málo pravděpodobném případě, tj. když vznikne problém, který se týká souboru, informujte o tom Ústřední sekretariát ISO na níže uvedené adrese.



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO 2007

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně fotokopíí a mikrofilmů, bez písemného svolení buď od organizace ISO na níže uvedené adrese, nebo od členské organizace ISO v zemi žadatele.

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 Směrnice

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 popsáním přístupem k řízení rizik lze pro implementaci požadavků ISMS použít některou z celé řady existujících metodik pro řízení rizik.

Tato mezinárodní norma je určena 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.

Konec náhledu - text dále pokračuje v placené verzi ČSN.