ČESKÁ TECHNICKÁ NORMA

ICS 01.040.35; 35.040 **Květen 2010**

Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ČSN ISO/IEC 27000
36 9790

Information technology – Security techniques – Information security management systems – Overview and vocabulary

Technologies de l,information – Techniques de sécurité – Systemes de question de la sécurité des informations –
Vue d,ensemble et vocabulaire

Tato norma je českou verzí mezinárodní normy ISO/IEC 27000:2009. 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 27000:2009. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

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 řízení bezpečnosti informací – Požadavky

ISO/IEC 27002:2005 zavedena v ČSN ISO/IEC 17799:2006 (36 9790) Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací

ISO/IEC 27003 dosud nezavedena

ISO/IEC 27004 dosud nezavedena

ISO/IEC 27005:2008 zavedena v ČSN ISO/IEC 27005:2009 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

ISO/IEC 27006:2007 zavedena v ČSN ISO/IEC 27006:2008 (36 9790) Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

ISO/IEC 27007 dosud nezavedena

ISO/IEC 27011 dosud nezavedena

ISO 27799:2008 zavedena v ČSN EN ISO 27799:2010 (98 2021) Zdravotnická informatika – Řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002

Souvisící ČSN

ČSN ISO/IEC 17021:2007 (01 5257) Posuzování shody – Požadavky na orgány provádějící audit a certifikaci systémů managementu

ČSN EN ISO 9000:2006 (01 0300) Systémy managementu kvality – Základní principy a slovník

ČSN EN ISO 19011:2003 (01 0330) Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu

Vysvětlivky k textu převzaté normy

Pro účely této normy byl použit

- překlad anglického výrazu *control* kromě v definici uvedeného řízení nebo kontrola také jako opatření nebo kontrolní opatření, a to z důvodu návaznosti na některé vydané normy řady 27XXX
- překlad anglického výrazu *guideline* jako směrnice s ohledem na běžné použití tohoto překladu v základních normách počítačové bezpečnosti
- alternativní překlad anglického termínu *Do* jako Prováděj
- v případech, kdy u definice převzaté z Guide 73 jsou uvedeny dva termíny, první z nich je termín používaný v IT

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 20 Informační technologie

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

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

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 27000
Systémy řízení bezpečnosti informací – První vydání
Přehled a slovník 2009-05

Obsah

Strana

Příloha B (informativní) Kategorizované termíny 22

Bibliografie 24

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených příslušnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk. ISO a IEC ustavily v oblasti informačních technologií společnou technickou komisi, ISO/IEC JTC 1.

Mezinárodní normy jsou navrhovány v souladu s pravidly uvedenými v části 2 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Pozornost je věnována možnosti, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nepřebírají zodpovědnost za identifikaci jakýchkoliv nebo všech takových patentových práv.

Mezinárodní norma ISO/IEC 27000 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie*, subkomisí SC 27, *Bezpečnostní techniky IT*.

0 Úvod

0.1 Přehled

Mezinárodní normy pro systémy řízení poskytují model určený k využití při vytváření a provozování systému řízení. Tento model obsahuje rysy, u kterých experti v daném oboru dosáhli shody, pokud jde o poslední stav mezinárodního vývoje. ISO/IEC JTC 1 SC 27 udržuje komisi expertů, která se věnuje vývoji mezinárodních norem systémů řízení bezpečnosti informací, nazývaných také rodina norem ISMS (Systém řízení bezpečnosti informací – Information Security Management System).

Organizace mohou použitím rodiny norem ISMS vyvinout a implementovat rámec pro řízení bezpečnosti svých informačních aktiv a připravit nezávislé ohodnocení svých ISMS týkající se ochrany informací, např. finančních informací, duševního vlastnictví a podrobností o zaměstnancích, nebo informací, které jim byly svěřeny zákazníky nebo třetími stranami.

0.2 Rodina norem ISMS

Rodina norem ISMSmá pomoci organizacím všech typů a velikostí zavést a provozovat ISMS. Rodina norem ISMS sestává z dále uvedených mezinárodních norem se souhrnným názvem *Informační technologie – Bezpečnostní techniky*:

- ISO/IEC 27000:2009, *Systémy řízení bezpečnosti informací – Přehled a slovník*
- ISO/IEC 27001:2005, *Systémy řízení bezpečnosti informací – Požadavky*
- ISO/IEC 27002:2005, *Soubor postupů pro management bezpečnosti informací*
- ISO/IEC 27003, *Směrnice pro implementaci systému řízení bezpečnosti informací*
- ISO/IEC 27004, *Řízení bezpečnosti informací – Měření*
- ISO/IEC 27005:2008, *Řízení rizik bezpečnosti informací*

- ISO/IEC 27006:2007, *Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací*
- ISO/IEC 27007, *Směrnice pro auditování systémů řízení bezpečnosti informací*
- ISO/IEC 27011, *Směrnice pro řízení bezpečnosti informací telekomunikačních organizací založené na ISO/IEC 27002*

POZNÁMKA Souhrnný název „*Informační technologie – Bezpečnostní techniky*“ označuje, že tyto normy byly připraveny společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomisí SC27*, Bezpečnostní techniky IT*.

Mezinárodní normy, které nejsou uvedeny pod tímto souhrnným názvem, ale jsou také součástí rodiny norem ISMS, jsou následující:

- ISO 27799:2008, *Zdravotnická informatika – Řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002*

0.3 Účel této mezinárodní normy

Tato mezinárodní norma poskytuje přehled systémů řízení bezpečnosti informací, které tvoří předmět rodiny norem ISMS, a definuje související termíny.

POZNÁMKA V příloze A je objasněno, jak jsou použity slovesné tvary k vyjádření požadavků a/nebo pokynů v rodině
norem ISMS.

Rodina norem ISMS zahrnuje normy, které:

a. definují požadavky na ISMS a na ty, kteří certifikují takové systémy;
b. poskytují přímou podporu, podrobné pokyny a/nebo interpretaci pro všechny procesy Plánuj-Prováděj(Dělej) -Kontroluj-Jednej (Plan-Do-Check-Act (PDCA)) a požadavky;
c. se zabývají směrnicemi pro ISMS specifickými pro jednotlivá odvětví;
d. se zabývají posuzováním shody ve vztahu k ISMS.

Termíny a definice uvedené v této mezinárodní normě:

- týkají se termínů a definic obecně použitých v rodině norem ISMS;
- netýkají se všech termínů a definic použitých v rodině norem ISMS; a
- neomezují rodinu norem ISMS v definování termínů pro vlastní použití.

Normy zabývající se pouze implementací kontrolních opatření z ISO/IEC 27002, na rozdíl od soustředění se na všechna kontrolní opatření, jsou vyloučeny z rodiny norem ISMS.

Tato mezinárodní norma bude opakovaně aktualizována častěji, než je to běžné u jiných norem ISO/IEC, aby vyjadřovala měnící se status rodiny norem ISMS.

1 Předmět normy

Tato mezinárodní norma poskytuje:

a. přehled rodiny norem ISMS;
b. úvod k systémům řízení bezpečnosti informací (ISMS);
c. krátký popis procesu Plánuj-Prováděj(Dělej)-Kontroluj-Jednej (Plan-Do-Check-Act (PDCA)); a
d. termíny a definice určené k použití v rodině norem ISMS.

Tato mezinárodní norma je použitelná pro všechny druhy organizací (např. pro obchodní podniky, vládní úřady, neziskové organizace).