ČESKÁ TECHNICKÁ NORMA

ICS 01.040.35; 35.040 **Říjen 2014**

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 management de la sécurité de l,informations –
Vue d,ensemble et vocabulaire

Tato norma je českou verzí mezinárodní normy ISO/IEC 27000:2014. 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 27000:2014. 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 27000 (36 9790) z května 2010.

Národní předmluva

Změny proti předchozí normě

Toto třetí vydání rozšiřuje terminologický slovník, nově zařazuje přílohu B a popis nově vydaných norem této řady.

Souvisící ČSN

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

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

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

ČSN ISO/IEC 27001 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

ČSN ISO/IEC 27002 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

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

ČSN ISO/IEC 27004:2011 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti infor-
mací – 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

ČSN ISO/IEC 27007:2013 (36 9790) Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací

ČSN EN ISO 27799:2010 (98 2021) Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002

TNI 01 0350:2009 (01 0350) Management rizik – Slovník (Pokyn 73)

ČSN ISO/IEC 15939:2011 (36 9040) Systémové a softwarové inženýrství – Proces měření

Vysvětlivky k textu převzaté normy

Pro účely této normy byl použit

- překlad anglického termínu „management“ jako „řízení“ s ohledem na jeho preferované používání v oblasti IT a návaznosti na vydané normy z oblasti IT, zejména normy řady 27XXX;
- překlad anglického termínu „control“ jako „opatření, řízení nebo kontrola“;
- v případech, kdy jsou u definice převzaté z odkazovaných norem uvedeny dva termíny (nebo více termínů), je první z nich termín preferovaně používaný v IT.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Škop

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 27000
Systémy řízení bezpečnosti informací – Třetí vydání
Přehled a slovník 2014-01-15

ICS 01.040.35; 35.040

Obsah

Strana

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 příprava mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům 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 27000 vypracovala společná technická komise ISO/IEC JTC1 *Informační technologie,* subkomise SC 27 *IT Bezpečnostní techniky*.

Toto třetí vydání zrušuje a nahrazuje druhé vydání (ISO/IEC 27000:2012), které bylo technicky revidováno.

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 řada norem Systém řízení bezpečnosti informací – Information Security Management System (ISMS).

Organizace mohou použitím řady norem ISMS vyvinout a implementovat rámec pro řízení bezpečnosti svých informačních aktiv zahrnujících finanční informace, duševní vlastnictví a podrobnosti o zaměstnancích, nebo informace, které jim byly svěřeny zákazníky nebo třetími stranami. Tyto normy mohou být také použity pro přípravu na nezávislé posouzení jejich ISMS, týkající se ochrany informací.

0.2 Řada norem ISMS

Řada norem ISMS (viz kapitola 4) má pomoci organizacím všech typů a velikostí zavést a provozovat

ISMS. Sestává z následujících mezinárodních norem se společným názvem *Informační technologie – Bezpečnostní techniky* (uvedených dále v číselném pořadí):

- ISO/IEC 27000 *Systémy řízení bezpečnosti informací – Přehled a slovník*
- ISO/IEC 27001 *Systémy řízení bezpečnosti informací – Požadavky*
- ISO/IEC 27002 *Soubor postupů pro opatření bezpečnosti informací*
- ISO/IEC 27003 *Směrnice pro implementaci systému řízení bezpečnosti informací*
- ISO/IEC 27004 *Řízení bezpečnosti informací – Měření*
- ISO/IEC 27005 *Řízení rizik bezpečnosti informací*
- ISO/IEC 27006 *Požadavky na orgány poskytující audit a certifikaci systémů řízení bezpečnosti informací*
- ISO/IEC 27007 *Směrnice pro audit systémů řízení bezpečnosti informací*
- ISO/IEC TR 27008 *Směrnice pro audit opatření ISMS*
- ISO/IEC 27010 *Směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi*
- ISO/IEC 27011 *Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002*
- ISO/IEC 27013 *Návod pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1*
- ISO/IEC 27014 *Správa bezpečnosti informací*
- ISO/IEC TR 27015 *Směrnice pro řízení bezpečnosti informací pro finanční služby*
- ISO/IEC TR 27016 *Řízení bezpečnosti informací – Organizační ekonomika*

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

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

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 a definuje související termíny.

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

Řada norem ISMS zahrnuje normy, které:

a. stanovují požadavky na ISMS a na pracovníky, kteří takové systémy certifikují;
b. poskytují přímou podporu, podrobný návod a/nebo interpretaci pro celkový proces ustavení, implementování, udržování a zlepšování ISMS;
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:

- zahrnují běžně používané termíny a definice v řadě norem ISMS;
- nezahrnují všechny termíny a definice použité v rámci řady norem ISMS;
- neomezují řadu norem ISMS v definování nových termínů.

1 Předmět normy

Tato mezinárodní norma podává přehled systémů řízení bezpečnosti informací a termíny a definice, běžně používané v řadě norem ISMS. Tato mezinárodní norma je použitelná pro všechny typy a velikosti organizací (například pro obchodní podniky, vládní úřady, neziskové organizace).