ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Říjen 2016**

Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

ČSN
ISO/IEC 27006
36 9790

Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

Technologies de l,information – Techniques de sécurité – Exigences pour les organismes procédant a l,audit
et a la certification des systemes de management de la sécurité de l,information

Tato norma je českou verzí mezinárodní normy ISO/IEC 27006:2015. 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 27006:2015. 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 27006 (36 9790) z června 2016.

Národní předmluva

Změny proti předchozí normě

Proti předchozí normě dochází ke změně způsobu převzetí ISO/IEC 27006:2015 do soustavy norem ČSN.
Zatímco ČSN ISO/IEC 27006 z června 2016 převzala ISO/IEC 27006:2015 převzetím anglického originálu, tato norma ji přejímá překladem.

Informace o citovaných dokumentech

ISO/IEC 17021-1:2015 zavedena v ČSN EN ISO/IEC 17021-1:2016 (01 5257) Posuzování shody – Požadavky na orgány poskytující služby auditů a certifikace systémů managementu – Část 1: Požadavky

ISO/IEC 27000 zavedena v ČSN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ISO/IEC 27001:2013 zavedena v ČSN ISO/IEC 27001:2014 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

Souvisící ČSN

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

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

ČSN EN ISO 9001 (01 0321) Systémy managementu kvality – Požadavky

Vysvětlivky k textu převzaté normy

Pro účely této normy je anglický termín „teleworking“ použit v původním tvaru, vzhledem k rozšíření tohoto
termínu v odborné komunitě a absenci českého ekvivalentu.

Pro účely této normy je použit překlad anglického termínu „management“ jako „řízení“, s ohledem na jeho používání v oblasti IT, a v souladu s vydanými normami řady ČSN ISO/IEC 27XXX.
V některých případech je anglický termín „management“ ponechán v původním tvaru, s ohledem na kontext, v jakém je v textu normy použit.

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 – Požadavky ISO/IEC 27006
na orgány provádějící audit a certifikaci systémů řízení bezpečnosti Třetí vydání
informací 2015-10-01

ICS 35.040

Obsah

Strana

Předmluva 4

Úvod 7

1 Předmět normy 8

2 Citované dokumenty 8

3 Termíny a definice 8

4 Principy 8

5 Obecné požadavky 8

5.1 Právní a smluvní záležitosti 8

5.2 Management nestrannosti 8

5.2.1 IS 5.2 Střet zájmů 8

5.3 Záruky a financování 9

6 Požadavky na strukturu 9

7 Požadavky na zdroje 9

7.1 Kompetence zaměstnanců 9

7.1.1 IS 7.1.1 Obecné záležitosti 9

7.1.2 IS 7.1.2 Stanovení kompetenčních kritérií 9

7.2 Zaměstnanci zapojeni do certifikačních činností 12

7.2.1 IS 7.2 Prokazování znalostí a zkušeností auditora 12

7.3 Využití externích auditorů a externích technických expertů 13

7.3.1 IS 7.3 Využití externích auditorů nebo externích technických expertů jako členů auditního týmu 13

7.4 Záznamy zaměstnanců 13

7.5 Outsourcing 13

8 Požadavky na informace 13

8.1 Veřejné informace 13

8.2 Certifikační dokumenty 13

8.2.1 IS 8.2 Certifikační dokumenty ISMS 13

8.3 Odkazy na certifikaci a užití značek 13

8.4 Důvěrnost 13

8.4.1 IS 8.4 Přístup k záznamům organizace 13

8.5 Výměna informací mezi certifikačním orgánem a jeho klienty 14

9 Požadavky na proces 14

9.1 Činnosti před certifikací 14

9.1.1 Žádost 14

9.1.2 Přezkoumání žádosti 14

9.1.3 Program auditů 14

9.1.4 Stanovení doby trvání auditu 15

9.1.5 Vzorkování na více místech 15

9.1.6 Kombinované systémy řízení 16

9.2 Plánování auditů 16

9.2.1 Stanovení cílů, rozsahu a kritérií auditu 16

9.2.2 Výběr auditního týmu a přidělování úkolů 16

9.2.3 Auditní plán 17

9.3 Prvotní certifikace 17

9.3.1 IS 9.3.1 Prvotní certifikační audit 17

9.4 Provádění auditů 18

9.4.1 IS 9.4 Obecně 18

9.4.2 IS 9.4 Specifické prvky auditu ISMS 18

9.4.3 IS 9.4 Auditní zpráva 18

9.5 Rozhodnutí o certifikaci 19

9.5.1 IS 9.5 Rozhodnutí o certifikaci 19

9.6 Udržování platnosti certifikace 19

9.6.1 Obecně 19

9.6.2 Dohledové činnosti 19

9.6.3 Recertifikace 20

9.6.4 Speciální audity 20

9.6.5 Pozastavení, odnětí nebo omezení rozsahu certifikace 20

9.7 Odvolání 20

9.8 Stížnosti 20

9.8.1 IS 9.8 Stížnosti 21

9.9 Záznamy o klientech 21

10 Požadavky systému řízení na certifikační orgány 21

10.1 Možnosti 21

10.1.1 IS 10.1 Implementace ISMS 21

10.2 Možnost A: Obecné požadavky na systém řízení 21

10.3 Možnost B: Požadavky na systém řízení v souladu s ISO 9001 21

Příloha A (informativní) Znalosti a dovednosti pro audit a certifikaci ISMS 22

Příloha B (normativní) Doba trvání auditu 24

Příloha C (informativní) Metody výpočtu doby trvání auditu 28

Příloha D (informativní) Návod pro přezkoumání implementovaných opatření z ISO/IEC 27001:2013, Příloha A 32

Bibliografie 42

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

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 mezi-
národních norem prostřednictvím svých 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.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnicích ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím

kritériím potřebným pro různé druhy dokumentů ISO. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnicích ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti
o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržených ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená schválení.

Vysvětlení významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy WTO týkající se technických překážek obchodu (TBT), jsou uvedeny na tomto odkazu URL: Foreword – Supplementary information

Za tento dokument je odpovědná komise ISO/IEC JTC 1 *Informační technologie*, SC 27 *IT Bezpečnostní techniky*.

ISO/IEC 27006 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 27006:2011), které bylo technicky zrevidováno.

Úvod

ISO/IEC 17021-1 nastavuje kritéria pro organizace zabývající se auditem a certifikací systémů řízení. Pokud chtějí být tyto organizace akreditované pro shodu s ISO/IEC 17021-1 za účelem auditování a certifikace systémů řízení bezpečnosti informací (Information Security Management System nebo ISMS) v souladu s ISO/IEC 27001:2013, je nutné ISO/IEC 17021-1 doplnit o dodatečné požadavky a doporučení. Takovéto dodatečné požadavky a doporučení poskytuje tato mezinárodní norma.

Text této mezinárodní normy dodržuje strukturu ISO/IEC 17021-1, dodatečné specifické požadavky a doporučení na použití ISO/IEC 17021-1 pro certifikaci ISMS jsou v textu označeny písmeny „IS“.

Termín „shall (muset)“ je v textu této mezinárodní normy použit ke zdůraznění těch opatření, která vyjadřují
požadavky ISO/IEC 17021-1 a ISO/IEC 27001, a jsou povinná. Termín „should (měl by)“ je použit k vyjádření doporučení.

Hlavním cílem této mezinárodní normy je umožnit akreditačním orgánům její efektivní použití a harmonizaci s ostatními normami, podle kterých se provádí hodnocení certifikačních orgánů usilujících o akreditaci.

V této mezinárodní normě jsou termíny „systém řízení“ a „systém“ zaměnitelné. Definice systému řízení je uvedena v ISO 9000:2005. Systém řízení použitý v této mezinárodní normě by neměl být zaměňován s jinými typy systémů, jako jsou například systémy IT.

1 Předmět normy

Tato mezinárodní norma specifikuje požadavky a poskytuje doporučení pro orgány provádějící audit a certifikaci systému řízení bezpečnosti informací (Information Security Management System nebo ISMS) a doplňuje tak požadavky obsažené v ISO/IEC 17021-1 a ISO/IEC 27001. Norma je primárně určena k podpoře procesu akreditace certifikačních orgánů poskytujících certifikace ISMS.

Požadavky obsažené v této mezinárodní normě musí být prokázané ve smyslu odborné způsobilosti a spolehlivosti kteréhokoliv orgánu poskytujícího certifikaci ISMS, a návody obsažené v této mezinárodní normě poskytují dodatečnou interpretaci jednotlivých požadavků pro kterýkoliv orgán poskytující certifikaci ISMS.

POZNÁMKA Tato mezinárodní norma může být použita jako kriteriální dokument pro akreditaci, pro interní hodnocení nebo při jiných auditních procesech.