ČESKÁ TECHNICKÁ NORMA

ICS 03.120.20; 35.030 **Květen 2021**

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

ČSN EN ISO/IEC 27006

36 9790

idt ISO/IEC 27006:2015 + ISO/IEC 27006:2015/Amd.1:2020

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

Informationstechnik – IT-Sicherheitsverfahren – Anforderungen an Institutionen, die Audits und Zertifizierungen
von Informationssicherheits-Managmentsystemen anbieten

Tato norma je českou verzí evropské normy EN ISO/IEC 27006:2020. Překlad byl zajištěn Českou agenturou pro stan-
dardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN ISO/IEC 27006:2020. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 27006 (36 9790) z října 2016.

Národní předmluva

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 této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článcích „Informace
o citovaných dokumentech“ a „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

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.

Upozornění na národní poznámky

Do Evropské předmluvy byla doplněna národní poznámka upozorňující na změnu
ISO/IEC 27006:2015/Amd.1:2020.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

EVROPSKÁ NORMA EN ISO/IEC 27006
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Listopad 2020

ICS 03.120.20; 35.030

Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací
(ISO/IEC 27006:2015 včetně změny ISO/IEC 27006:2015/Amd.1:2020-03)

Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
(ISO/IEC 27006:2015, including Amd 1:2020)

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
(ISO/IEC 27006:2015, y compris Amd 1:2020)

Informationstechnik – IT-Sicherheitsverfahren – Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managmentsystemen anbieten
(ISO/IEC 27006:2015, einschließlich Amd 1:2020)

Tato evropská norma byla schválena CEN dne 2020-11-16.

Členové CEN a CENELEC jsou povinni splnit vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se této evropské normě bez jakýchkoliv modifikací uděluje status národní normy. Aktualizované
seznamy a bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídicím centru CEN-CENELEC nebo u kteréhokoliv člena CEN a CENELEC.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém jiném jazyce přeložená členem CEN a CENELEC do jeho vlastního jazyka, za kterou zodpovídá a kterou notifikuje Řídicímu centru CEN-CENELEC, má stejný status jako oficiální verze.

Řídicí centrum CEN-CENELEC
Rue de la Science 23, B-1040 Brusel

Ref. č. EN ISO/IEC 27006:2020 E

Členy CEN a CENELEC jsou národní normalizační orgány a národní elektrotechnické komise Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Republiky
Severní Makedonie, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Srbska, Španělska, Švédska, Švýcarska a Turecka.

Evropská předmluva

Text ISO/IEC 27006:2015NP) vypracovala technická komise ISO/IEC JTC 1 *Informační technologie* Mezinárodní
organizace pro normalizaci (ISO) a byl převzat jako EN ISO/IEC 27006:2020 technickou komisí CEN/CLC/JTC 13 *Kybernetická bezpečnost a ochrana dat*, jejímž sekretariátem je DIN.

Této evropské normě je nutno nejpozději do května 2021 udělit status národní normy, a to buď vydáním identického textu, nebo schválením k přímému používání, a národní normy, které jsou s ní v rozporu, je nutno zrušit nejpozději do května 2021.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CEN nelze činit odpovědným za identifikaci jakéhokoliv nebo všech patentových práv.

Podle vnitřních předpisů CEN-CENELEC jsou tuto evropskou normu povinny zavést národní normalizační organizace následujících zemí: Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Republiky Severní Makedonie, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Srbska, Španělska, Švédska, Švýcarska a Turecka.

Oznámení o schválení

Text ISO/IEC 27006:2015[NP)] byl schválen CEN jako EN ISO/IEC 27006:2020 bez jakýchkoliv modifikací.

Obsah

Strana

Předmluva..... 7

Úvod..... 8

1..... Předmět normy..... 9

2..... Citované dokumenty..... 9

3..... Termíny a definice..... 9

4..... Principy..... 9

5..... Obecné požadavky..... 9

5.1..... Právní a smluvní záležitosti..... 9

5.2..... Management nestrannosti..... 9

5.2.1... IS 5.2 Střet zájmů..... 10

5.3..... Záruky a financování..... 10

6..... Požadavky na strukturu..... 10

7..... Požadavky na zdroje..... 10

7.1..... Kompetence zaměstnanců..... 10

7.1.1... IS 7.1.1 Obecné záležitosti..... 10

7.1.2... IS 7.1.2 Stanovení kompetenčních kritérií..... 10

7.2..... Zaměstnanci zapojeni do certifikačních činností..... 13

7.2.1... IS 7.2 Prokazování znalostí a zkušeností auditora..... 13

7.3..... Využití externích auditorů a externích technických expertů..... 14

7.3.1... IS 7.3 Využití externích auditorů nebo externích technických expertů jako členů auditního týmu..... 14

7.4..... Záznamy zaměstnanců..... 14

7.5..... Outsourcing..... 14

8..... Požadavky na informace..... 14

8.1..... Veřejné informace..... 14

8.2..... Certifikační dokumenty..... 14

8.2.1... IS 8.2 Certifikační dokumenty ISMS..... 14

8.3..... Odkazy na certifikaci a užití značek..... 15

8.4..... Důvěrnost..... 15

8.4.1... IS 8.4 Přístup k záznamům organizace..... 15

8.5..... Výměna informací mezi certifikačním orgánem a jeho klienty..... 15

9..... Požadavky na proces..... 15

9.1..... Činnosti před certifikací..... 15

9.1.1... Žádost..... 15

9.1.2... Přezkoumání žádosti..... 15

9.1.3... Program auditů..... 15

9.1.4... Stanovení doby trvání auditu..... 16

9.1.5... Vzorkování na více místech..... 16

9.1.6... Kombinované systémy řízení..... 17

9.2..... Plánování auditů..... 17

9.2.1... Stanovení cílů, rozsahu a kritérií auditu..... 17

9.2.2... Výběr auditního týmu a přidělování úkolů..... 17

9.2.3... Auditní plán..... 18

9.3..... Prvotní certifikace..... 18

9.3.1... IS 9.3.1 Prvotní certifikační audit..... 18

9.4..... Provádění auditů..... 19

9.4.1... IS 9.4 Obecně..... 19

9.4.2... IS 9.4 Specifické prvky auditu ISMS..... 19

9.4.3... IS 9.4 Auditní zpráva..... 20

9.5..... Rozhodnutí o certifikaci..... 20

9.5.1... IS 9.5 Rozhodnutí o certifikaci..... 20

9.6..... Udržování platnosti certifikace..... 20

9.6.1... Obecně..... 20

9.6.2... Dohledové činnosti..... 20

9.6.3... Recertifikace..... 21

9.6.4... Speciální audity..... 21

9.6.5... Pozastavení, odnětí nebo omezení rozsahu

certifikace..... 22

9.7.....
Odvolání.....
..... 22

9.8.....
Stížnosti.....
..... 22

9.8.1... IS 9.8
Stížnosti.....
..... 22

9.9..... Záznamy
o klientech.....
..... 22

10..... Požadavky systému řízení na certifikační
orgány..... 22

10.1....
Možnosti.....
..... 22

10.1.1 IS 10.1 Implementace
ISMS.....
22

10.2.... Možnost A: Obecné požadavky na systém
řízení..... 22

10.3.... Možnost B: Požadavky na systém řízení v souladu
s ISO 9001..... 22

Příloha A (informativní) Znalosti a dovednosti pro audit a certifikaci
ISMS..... 23

Příloha B (normativní) Doba trvání
auditu..... 25

Příloha C (informativní) Metody výpočtu doby trvání
auditu..... 29

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

Bibliografie.....
..... 40

ISO copyright office
CP 401 · Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail: copyright@iso.org
Website: www.iso.org
Publikováno ve Švýcarsku

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 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 i nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk.

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. 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) nebo v seznamu patentových prohlášení obdržených IEC (viz http://patents.iec.ch).

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

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), jsou uvedeny na www.iso.org/iso/foreword.html.

Tento dokument vypracovala společná technická komise ISO/IEC JTC1 *Informační technologie,* subkomise SC 27 *Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí.*

Jakákoliv zpětná vazba nebo otázky týkající se tohoto dokumentu by měly být směrovány na národní normalizační orgán uživatele. Úplný seznam těchto orgánů lze nalézt na www.iso.org/members.html.

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.

NP) NÁRODNÍ POZNÁMKA V přejímané normě chybí informace o zahrnuté změně ISO/IEC 27006:2015/Amd.1:2020.