ČESKÁ TECHNICKÁ NORMA

ICS 03.120.20; 35.030 **Listopad 2024**

Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Požadavky na orgány provádějící audit a certifikaci systémů managementu informační bezpečnosti – Část 1: Obecně	ČSN EN ISO/IEC 27006-1 36 9790

idt ISO/IEC 27006-1:2024

Information security, cybersecurity and privacy protection – Requirements for bodies providing audit and certification
of information security management systems –
Part 1: General

Sécurité de l,information, cybersécurité et protection de la vie privée – Exigences pour les organismes procédant a l,audit
et a la certification des systemes de management de la sécurité de l,information –
Partie 1: Généralités

Cybersicherheit und Datenschutz – Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren –
Teil 1: Allgemeines

Tato norma je českou verzí evropské normy EN ISO/IEC 27006-1:2024. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN ISO/IEC 27006-1:2024. 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 EN ISO/IEC 27006-1 (36 9790) ze září 2024.

Národní předmluva

Změny proti předchozí normě

Proti předchozí normě dochází ke změně způsobu převzetí EN ISO/IEC 27006-1:2024 do soustavy norem ČSN. Zatímco ČSN EN ISO/IEC 27006-1 ze září 2024 převzala EN ISO/IEC 27006-1:2024 schválením k přímému používání jako ČSN oznámením ve Věstníku ÚNMZ, 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 27001:2022 zavedena v ČSN EN ISO/IEC 27001:2023 (36 9797) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky

Souvisící ČSN

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

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

ČSN EN ISO/IEC 27002 (36 9798) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti

ČSN EN ISO/IEC 27007 (36 9790) Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Směrnice pro audit systémů řízení bezpečnosti informací

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

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 článku „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).

Pro účely této normy je anglický termín „guidance“ přeložen jako „pokyn“ vzhledem k jeho používání v oboru IT a v návaznosti na vydané normy z oboru IT, zejména normy řady ISO/IEC 27XXX. Český ekvivalent „návod“ je vzhledem ke kontextu nevhodný a v praxi se v souvislosti s řadou norem ISO/IEC 27XXX nepoužívá.

Upozornění na národní poznámku

K terminologickému heslu 3.10 byla doplněna národní poznámka upozorňující na zrušený dokument.

Vypracování normy

Zpracovatel odborného překladu: Ing. Vladimír Pračke, IČO 40654419

Technická normalizační komise: TNK 20 Informační technologie

Vydala: Česká agentura pro standardizaci, státní příspěvková organizace

Citované dokumenty a souvisící ČSN lze získat na e-shopu.

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
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27006-1

Březen 2024

ICS 03.120.20; 35.030

Nahrazuje
EN ISO/IEC 27006:2020

Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Požadavky na orgány provádějící audit a certifikaci systémů managementu informační bezpečnosti – Část 1: Obecně (ISO/IEC 27006-1:2024)

Information security, cybersecurity and privacy protection – Requirements for bodies providing audit and certification of information security management systems – Part 1: General (ISO/IEC 27006-1:2024)

Sécurité de l,information, cybersécurité et protection de la vie privée – Exigences pour les organismes procédant a l,audit et a la certification des systemes de management de la sécurité de l,information – Partie 1: Généralités (ISO/IEC 27006-1:2024)

Cybersicherheit und Datenschutz – Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren – Teil 1: Allgemeines (ISO/IEC 27006-1:2024)

Tato evropská norma byla schválena CEN dne 2024-01-29.

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 27006-1:2024 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

Tento dokument (EN ISO/IEC 27006-1:2024) vypracovala technická komise ISO/IEC JTC 1 *Informační technologie* ve spolupráci s technickou komisí CEN-CENELEC/JTC 13 *Kybernetická bezpečnost a ochrana dat*, jejímž sekretariátem je DIN.

Této evropské normě je nutno nejpozději do září 2024 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 září 2024.

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

Tento dokument nahrazuje EN ISO/IEC 27006:2020.

Jakákoli zpětná vazba a otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na webových stránkách CEN a CENELEC.

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 27006-1:2024 byl schválen CEN-CENELEC jako EN ISO/IEC 27006-1:2024 bez jakýchkoliv modifikací.

Obsah

Strana

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 nebo www.iec.ch/members_experts/refdocs).

ISO a IEC upozorňují na možnost, že implementace tohoto dokumentu smí vyžadovat využití patentu (patentů). V souvislosti s tím ISO a IEC nezaujímají žádné stanovisko týkající se důkazů, platnosti nebo použitelnosti všech uplatňovaných patentových práv. Ke dni zveřejnění tohoto dokumentu ISO a IEC neobdržely oznámení o patentu (patentech), který smí být vyžadován pro implementaci tohoto dokumentu. ISO a IEC však upozorňují implementující organizace, že se nemusí jednat o nejnovější informace, které lze získat z databáze patentů dostupné na www.iso.org/patents a https://patents.iec.ch. ISO a IEC nelze činit odpovědné za identifikaci jakéhokoliv nebo všech takových patentových práv.

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), viz www.iso.org/iso/foreword.html. V IEC viz www.iec.ch/understanding-standards.

Tento dokument vypracovala společná technická komise ISO/IEC JTC1 *Informační technologie*, subkomise SC 27 *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí* ve spolupráci s technickou komisí Evropského výboru pro normalizaci (CEN) CEN/CLC/JTC 13 *Kybernetická bezpečnost a ochrana dat* na základě Dohody o technické spolupráci mezi ISO a CEN (Vídeňská dohoda).

Toto první vydání ISO/IEC 27006-1 zrušuje a nahrazuje ISO/IEC 27006:2015, které bylo technicky zrevidováno. Zahrnuje také změnu ISO/IEC 27006:2015/Amd.1:2020.

Hlavní změny jsou:

- tento dokument byl převeden na první část souboru;
- celý dokument byl aktualizován pro vzdálené audity a organizace s malým počtem relevantních fyzických míst nebo bez nich;
- v C.3.4 byl zaveden pojem osob vykonávajících určité shodné činnosti a bylo provedeno několik aktualizací;

- tento dokument (zejména příloha E) byl uveden do souladu s ISO/IEC 27001:2022 a ISO/IEC 27002:2022;
- byly odstraněny redundance s ISO/IEC 17021-1;
- znění bylo upřesněno a více sladěno s textem ISO/IEC 17021-1.

Seznam všech částí souboru ISO/IEC 27006 lze nalézt na webových stránkách ISO a IEC.

Jakákoliv zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na www.iso.org/members.html a_www.iec.ch/national-committees.

Úvod

ISO/IEC 17021-1 stanovuje požadavky a pokyny pro orgány provádějící audit a certifikaci systémů managementu. Pokud tyto orgány hodlají být v souladu s ISO/IEC 17021-1 s cílem provádění auditů a certifikace systémů mana-
gementu informační bezpečnosti (ISMS) v souladu s ISO/IEC 27001, jsou zásadní některé další požadavky a pokyny k ISO/IEC 17021-1. Ty poskytuje tento dokument.

Tento dokument specifikuje požadavky na orgány provádějící audit a certifikaci ISMS. Uvádí obecné požadavky na tyto orgány, které jsou označovány jako certifikační orgány. Dodržování těchto požadavků má zajistit, aby certifikační orgány prováděly certifikaci ISMS kompetentně, konzistentně a nestranným způsobem, čímž se usnadní uznávání těchto orgánů a akceptace jejich certifikací na národní a mezinárodní úrovni.

Text v tomto dokumentu se řídí strukturou ISO/IEC 17021-1:2015.

V tomto dokumentu jsou použity tyto slovesné formy:

- „musí“ vyjadřuje požadavek;
- „má“ vyjadřuje doporučení;
- „smí“ vyjadřuje dovolení;
- „může“ vyjadřuje možnost nebo schopnost.

1 Předmět normy

Tento dokument specifikuje požadavky a poskytuje pokyny pro orgány provádějící audit a certifikaci systému
managementu informační bezpečnosti (ISMS), které doplňují požadavky obsažené
v ISO/IEC 17021-1.

Požadavky obsažené v tomto dokumentu prokazují z hlediska kompetence a spolehlivosti orgány poskytující certifikaci ISMS. Pokyny obsažené v tomto dokumentu poskytují další výklad těchto požadavků pro orgány poskytující certifikaci ISMS.

POZNÁMKA Tento dokument může být použit jako dokument s kritérii pro akreditaci, vzájemné hodnocení nebo jiné auditní procesy.