ICS 03.120.20; 35.030 SLOVENSKÁ TECHNICKÁ NORMA December 2024

STN	**Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva informačnej bezpečnosti Časť 1: Všeobecne (ISO/IEC 27006-1: 2024)**	**STN EN ISO/IEC 27006-1** 97 4185

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 à l'audit et à la certification des systèmes 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

Táto slovenská technická norma je slovenskou verziou európskej normy EN ISO/IEC 27006-1: 2024.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN EN ISO/IEC 27006-1 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 27006-1: 2024.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN EN ISO/IEC 27006-1 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza anglickú verziu STN EN ISO/IEC 27006-1 z júla 2024, ktorá od 1. 7. 2024 nahradila STN EN ISO/IEC 27006 z júla 2021 v celom rozsahu.

139419

Národný predhovor

Obrázky a matematické výrazy v tejto STN sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2024 ISO/IEC, ref. č. ISO/IEC 27006-1: 2024 E.

Toto prvé vydanie normy ISO/IEC 27006-1 ruší a nahrádza normu ISO/IEC 27006: 2015, ktorá bola technicky revidovaná. Zahŕňa aj zmenu ISO/IEC 27006: 2015/Amd 1: 2020.

Hlavné zmeny sú tieto:

- tento dokument bol zmenený na prvú časť viacdielneho súboru;
- celý dokument bol aktualizovaný pre audity na diaľku a organizácie s malým počtom relevantných fyzických miest alebo bez nich;
- pojem osôb vykonávajúcich určité zhodné činnosti bol zavedený v bode C.3.4 a v niekoľkých boli poskytnuté aktualizácie;
- tento dokument (najmä príloha E) bol zosúladený s normami ISO/IEC 27001: 2022 a ISO/IEC 27002: 2022;
- boli odstránené nadbytočnosti s normou ISO/IEC 17021-1;
- znenie bolo spresnené a lepšie zosúladené s normou ISO/IEC 17021-1.

Zoznam všetkých častí súboru ISO/IEC 27006 nájdete na webových stránkach ISO a IEC.

Normatívne referenčné dokumenty

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN a TNI možno získať na webovom sídle www.unms.sk.

ISO/IEC 17021-1: 2015 prijatá ako STN EN ISO/IEC 17021-1: 2018 Posudzovanie zhody. Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva. Časť 1: Požiadavky (ISO/IEC 17021-1: 2015) (01 5257)

ISO/IEC 27001: 2022 prijatá ako STN EN ISO/IEC 27001: 2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Systémy manažérstva informačnej bezpečnosti. Požiadavky (ISO/IEC 27001: 2022) (97 4171)

Vypracovanie

Spracovateľ: SynCo s.r.o., Bratislava, Ing. Lenka Gondová

Technická komisia: TK 37 Informačné technológie

EURÓPSKA NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27006-1

Marec 2024

ICS 03.120.20; 35.030

Nahrádza EN ISO/IEC 27006: 2020

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva informačnej bezpečnosti Časť 1: Všeobecne (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
à l'audit et à la certification des systèmes
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)

Túto európsku normu schválil CEN 29. januára 2024.

Táto európska norma bola opravená a znovu vydaná Riadiacim strediskom CEN-CENELEC 20. marca 2024.

Členovia CEN a CENELEC sú povinní plniť vnútorné predpisy CEN-CENELEC, v ktorých sú určené podmienky, za ktorých sa tejto európskej norme bez akýchkoľvek zmien priznáva postavenie národnej normy. Aktualizované zoznamy a bibliografické odkazy týkajúce sa takýchto národných noriem možno na požiadanie dostať od Riadiaceho strediska CEN-CENELEC alebo od každého člena CEN a CENELEC.

Táto európska norma existuje v troch oficiálnych verziách (anglickej, francúzskej, nemeckej). Verzia v akomkoľvek inom jazyku, ktorú na vlastnú zodpovednosť vydal člen CEN a CENELEC v preklade do národného jazyka a ktorá bola oznámená Riadiacemu stredisku CEN-CENELEC, má rovnaké postavenie, ako majú oficiálne verzie.

Členmi CEN a CENELEC sú národné normalizačné organizácie Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédska, Talianska a Turecka.

CEN

Európsky výbor pre normalizáciu
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

CENELEC

Európsky výbor pre normalizáciu v elektrotechnike
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Riadiace stredisko CEN-CENELEC: Rue de la Science 23, B-1040 Brusel

Ref. č. EN ISO/IEC 27006-1: 2024 SK

Obsah

Európsky predhovor

Tento dokument (EN ISO/IEC 27006-1: 2024) vypracovala technická komisia ISO/IEC JTC 1 Informačné technológie v spolupráci s technickou komisiou CEN-CENELEC/JTC 13 Kybernetická bezpečnosť a ochrana údajov, ktorej sekretariát je v DIN.

Tejto európskej norme sa musí priznať postavenie národnej normy buď vydaním identického textu, alebo oznámením najneskôr do septembra 2024 a národné normy, ktoré sú s ňou v rozpore, musia sa zrušiť najneskôr do septembra 2024.

Upozorňuje sa na možnosť, že niektoré časti tohto dokumentu môžu byť predmetom patentových práv. CEN-CENELEC nezodpovedajú za identifikáciu ktoréhokoľvek alebo všetkých takýchto patentových práv.

Tento dokument nahrádza EN ISO/IEC 27006: 2020.

Akákoľvek spätná väzba a otázky k tomuto dokumentu sa majú adresovať národnému normalizačnému orgánu používateľov. Kompletný zoznam týchto orgánov je na webovom sídle CEN a CENELEC.

V súlade s vnútornými predpismi CEN-CENELEC sú túto európsku normu povinné prevziať národné normalizačné organizácie týchto krajín: Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédska, Talianska a Turecka.

Oznámenie o schválení

Text medzinárodnej normy ISO/IEC 27006-1: 2024 schválil CEN-CENELEC ako EN ISO/IEC 27006-1: 2024 bez akýchkoľvek modifikácií.

Úvod

Norma ISO/IEC 17021-1 stanovuje požiadavky a usmernenia pre orgány, ktoré vykonávajú audit a certifikáciu systémov manažérstva. Ak majú takéto orgány v úmysle byť v súlade s normou ISO/IEC 17021-1 s cieľom auditovať a certifikovať systémy riadenia bezpečnosti informácií (ISMS) v súlade s normou ISO/IEC 27001, sú rozhodujúce niektoré dodatočné požiadavky a usmernenia k norme ISO/IEC 17021-1. Tieto sú uvedené v tomto dokumente.

Tento dokument špecifikuje požiadavky na orgány vykonávajúce audit a certifikáciu ISMS. Uvádza všeobecné požiadavky na takéto orgány, ktoré sa označujú ako certifikačné orgány. Dodržiavanie týchto požiadaviek má zabezpečiť, aby certifikačné orgány vykonávali certifikáciu ISMS kompetentným, konzistentným a nestranným spôsobom, a tým uľahčiť uznávanie takýchto orgánov a akceptovanie ich certifikátov na národnej a medzinárodnej úrovni.

Text v tomto dokumente sa riadi štruktúrou normy ISO/IEC 17021-1: 2015.
V tomto dokumente sa používajú tieto slovné druhy:

- „musí“ vyjadruje požiadavku;
- „má“ znamená odporúčanie;
- „smie“ znamená povolenie;
- „môže“ vyjadruje možnosť alebo schopnosť.

1 Predmet

Tento dokument špecifikuje požiadavky a poskytuje usmernenie pre orgány, ktoré vykonávajú audit a certifikáciu systému riadenia bezpečnosti informácií (ISMS), popri požiadavkách obsiahnutých v norme ISO/IEC 17021-1.

Požiadavky obsiahnuté v tomto dokumente preukazujú z hľadiska spôsobilosti a spoľahlivosti orgány poskytujúce certifikáciu ISMS. Usmernenie obsiahnuté v tomto dokumente poskytuje dodatočný výklad týchto požiadaviek pre orgány poskytujúce certifikáciu ISMS.

POZNÁMKA. – Tento dokument sa môže použiť ako dokument s kritériami pre akreditáciu, vzájomné hodnotenie alebo iný auditný proces.

2 Normatívne odkazy

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

ISO/IEC 17021-1: 2015 *Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements.* [Posudzovanie zhody. Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva. Časť 1: Požiadavky.]

ISO/IEC 27001: 2022 *Information security, cybersecurity and privacy protection – Information security management systems – Requirements.* [Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Systémy manažérstva informačnej bezpečnosti. Požiadavky.]