ICS 03.120.20; 35.030 SLOVENSKÁ TECHNICKÁ NORMA Júl 2021

STN	**Informačné technológie Bezpečnostné metódy Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva informačnej bezpečnosti (ISO/IEC 27006: 2015, vrátane Amd 1: 2020)**	**STN EN ISO/IEC 27006** 36 9795

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 à l'audit et à la certification des systèmes de management de la sécurité de l'information

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

Táto norma je slovenskou verziou európskej normy EN ISO/IEC 27006: 2020.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
Táto norma má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 27006: 2020.
It was translated by Slovak Office of Standards, Metrology and Testing.
It has the same status as the official versions.

Nahradenie predchádzajúcich noriem

Táto norma nahrádza anglickú verziu STN EN ISO/IEC 27006 z júna 2021, ktorá od 1. 6. 2021 nahradila STN ISO/IEC 27006 zo septembra 2020 v celom rozsahu.

132990

Národný predhovor

Obrázky v tejto norme sú prevzaté z elektronických podkladov dodaných z CEN, © CEN 2020, ref. č. EN ISO/IEC 27006: 2020.

Normatívne referenčné dokumenty

Nasledujúce dokumenty, celé alebo ich časti, sú v tomto dokumente normatívnymi odkazmi a sú nevyhnutné pri jeho používaní. Pri datovaných odkazoch sa použije len citované vydanie. Pri nedatovaných odkazoch sa použije najnovšie vydanie citovaného dokumentu (vrátane všetkých 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 možno získať na webovej stránke www.unms.sk.

ISO/IEC 17021-1: 2015 zavedená v 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 27000 zavedená v STN EN ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000) (36 9789)

ISO/IEC 27001: 2013 zavedená v STN EN ISO/IEC 27001: 2019 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky (ISO/IEC 27001: 2013 vrátane Cor. 1: 2014 a Cor. 2: 2015) (36 9789)

Vypracovanie normy

Spracovateľ: Pro Excellence, s. r. o.

Technická komisia: TK 37 Informačné technológie

EURÓPSKA NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27006

November 2020

ICS 03.120.20; 35.030

Informačné technológie
Bezpečnostné metódy
Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva informačnej bezpečnosti (ISO/IEC 27006: 2015, vrátane Amd 1: 2020)

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
à l'audit et à la certification des systèmes
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)

Túto európsku normu schválil CEN 16. novembra 2020.

Táto európska norma bola opravená a opätovne publikovaná Riadiacim strediskom CEN-CENELEC 24. februára 2021.

Členovia CEN 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.

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

Členmi CEN 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: 2020 SK

Obsah

strana

Európsky predhovor

Tento dokument (ISO/IEC 27006: 2015, vrátane Amd 1: 2020) vypracovala technická komisia ISO/IEC JTC 1 „Informačné technológie“ medzinárodnej organizácie pre normalizáciu (ISO) a bol prevzatý ako EN ISO/IEC 27006: 2020 technickou komisiou CEN/CLC/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 najneskoršie do mája 2021 a národné normy, ktoré sú s ňou v rozpore, musia sa zrušiť najneskoršie do mája 2021.

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

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 ISO/IEC 27006: 2015, vrátane Amd 1: 2020 chválil CEN ako EN ISO/IEC 27006: 2020 bez akýchkoľvek modifikácií.

Úvod

Norma ISO/IEC 17021-1 stanovuje kritériá pre orgány vykonávajúce audit a certifikáciu systémov manažérstva. Ak sú tieto orgány akreditované podľa normy ISO/IEC 17021-1 s cieľom auditovania a certifikovania systémov manažérstva informačnej bezpečnosti (ISMS) v súlade s normou ISO/IEC 27001: 2013, sú potrebné ďalšie dodatočné požiadavky a návod k norme ISO/IEC 17021-1. Tie poskytuje táto medzinárodná norma.

Text v tejto medzinárodnej norme kopíruje štruktúru normy ISO/IEC 17021-1 a dodatočné špecifické požiadavky ISMS a návod na aplikáciu normy ISO/IEC 17021-1 na certifikáciu ISMS sú identifikované písmenami „IS“.

Termín „musieť“ (v angličtine shall) v príslušnom tvare sa v tejto medzinárodnej norme používa všade na označenie ustanovení odrážajúcich požiadavky noriem ISO/IEC 17021-1 a ISO/IEC 27001, ktoré sú záväzné. Termín „môcť“ (v angličtine should) v príslušnom tvare sa používa na označenie odporúčania.

Prvotným účelom tejto medzinárodnej normy je umožniť akreditačným orgánom efektívnejšie harmonizovať ich aplikáciu noriem oproti tým, ktoré sú viazané na posudzovanie certifikačných orgánov.

V celej tejto medzinárodnej norme sa termíny „systém manažérstva“ a „systém“ používajú zameniteľne. Definíciu systému manažérstva možno nájsť v norme ISO 9000: 2005. Systém manažérstva, ako sa používa v tejto medzinárodnej norme, nemožno zamieňať s inými typmi systémov, ako IT systémy.

1 Predmet normy

Táto medzinárodná norma špecifikuje požiadavky a poskytuje návod pre orgány vykonávajúce audit a certifikáciu systému manažérstva informačnej bezpečnosti (ISMS) vo väzbe na požiadavky nachádzajúce sa v normách ISO/IEC 17021-1 a ISO/IEC 27001. To je primárne určené na podporu akreditácie certifikačných orgánov vykonávajúcich certifikáciu ISMS.

Požiadavky, ktoré obsahuje táto medzinárodná norma, je potrebné preukázať, pokiaľ ide o kompetentnosť a spoľahlivosť, certifikácie ISMS vykonanej akýmkoľvek orgánom a návod obsiahnutý v tejto medzinárodnej norme poskytuje dodatočnú interpretáciu týchto požiadaviek pre akýkoľvek orgán vykonávajúci certifikáciu ISMS.

POZNÁMKA. – Túto medzinárodnú normu možno využiť ako dokument s kritériami na akreditáciu, vzájomné posudzovanie alebo iné procesy auditu.

2 Normatívne odkazy

Nasledujúce dokumenty, celé alebo ich časti, sú v tomto dokumente normatívnymi odkazmi a sú nevyhnutné pri jeho používaní. Pri datovaných odkazoch sa použije len citované vydanie. Pri nedatovaných odkazoch sa použije najnovšie vydanie citovaného dokumentu (vrátane všetkých 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 27000 *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. [Informačné technológie. Bezpečnostné metódy. Systémy manažérstva informačnej bezpečnosti. Prehľad a slovník.]

ISO/IEC 27001: 2013 *Information technology – Security techniques – Information security management systems – Requirements*. [Informačné technológie. Bezpečnostné metódy. Systémy manažérstva informačnej bezpečnosti. Požiadavky.]