ICS 03.120.20; 35.030 SLOVENSKÁ TECHNICKÁ NORMA Jún 2022

STN	**Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Návod na auditovanie systémov riadenia informačnej bezpečnosti (ISO/IEC 27007: 2020)**	**STN EN ISO/IEC 27007** 36 9796

Information security, cybersecurity and privacy protection
Guidelines for information security management systems auditing

Sécurité de l'information, cybersécurité et protection des données privées
Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

Informationstechnik
Sicherheitsverfahren
Leitfäden für das Auditieren von Informationssicherheitsmanagementsystemen

Táto slovenská technická norma je slovenskou verziou európskej normy EN ISO/IEC 27007: 2022.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej repuliky.
STN EN ISO/IEC 27007 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 27007: 2022.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN EN ISO/IEC 27007 has the same status as the official versions.

Nahradenie predchádzajúcich slovenských technických noriem

Táto slovenská technická norma nahrádza STN ISO/IEC 27007 z októbra 2021 v celom rozsahu.

134901

Národný predhovor

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 19011: 2018 prijatá ako v STN EN ISO 19011: 2019 Návod na auditovanie systémov manažérstva (ISO 19011: 2018) (01 0330)

ISO/IEC 27000: 2018 prijatá ako v STN EN ISO/IEC 27000: 2020 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000: 2018) (36 9789)

Vypracovanie slovenskej technickej normy

Spracovateľ: Pro Excellence, s. r. o., Bratislava, Ing. Lenka Gondová

Technická komisia: TK 37 Informačné technológie

EURÓPSKA NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27007

Január 2022

ICS 03.120.20; 35.030

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Návod na auditovanie systémov riadenia informačnej bezpečnosti (ISO/IEC 27007: 2020)

Information security, cybersecurity and privacy protection
Guidelines for information security management systems auditing
(ISO/IEC 27007: 2020)

Sécurité de l'information, cybersécurité
et protection des données privées
Lignes directrices pour l'audit des systèmes
de management de la sécurité de l'information
(ISO/IEC 27007: 2020)

Informationstechnik
Sicherheitsverfahren
Leitfäden für das Auditieren von
Informationssicherheitsmanagementsystemen
(ISO/IEC 27007: 2020)

Túto európsku normu schválil CEN 26. decembra 2021.

Táto európska norma bola opravená a znovu vydaná riadiacim strediskom CEN-CENELEC 26. januára 2022.

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/CENELEC.

Táto európska norma existuje v troch oficiálnych verziách (anglickej, francúzskej, nemeckej). Verzia v akomkoľvek inom jazyku, ktorú na vlastnú zodpovednosť vydal člen CEN/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 Electrotéchnique
Europäisches Komitee für Elektrotechnische Normung

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

Ref. č. EN ISO/IEC 27007: 2022 SK

Obsah

Európsky predhovor

Tento dokument ISO/IEC 27007: 2020 vypracovala technická komisia ISO/IEC JTC 1 „Informačné technológe“, medzinárodnej organizácia pre normalizáciu (ISO) a bol prevzatý ako EN ISO/IEC 27007: 2022 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 najneskoršie do júla 2022 a národné normy, ktoré sú s ňou v rozpore, musia sa zrušiť najneskoršie do júla 2022.

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.

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 ISO/IEC 27007: 2020 schválil CEN-CENELEC ako EN ISO/IEC 27007: 2022 bez akýchkoľvek modifikácií.

Úvod

Kritériami vykonania auditu systému manažérstva informačnej bezpečnosti (ISMS), a to samostatne alebo v kombinácii, môžu byť:

- požiadavky definované v norme ISO/IEC 27001: 2013;
- politiky a požiadavky stanovené príslušnými zainteresovanými stranami;
- zákonné a regulačné požiadavky;
- procesy a opatrenia ISMS definované organizáciou alebo inými stranami;
- plány systému riadenia týkajúce sa poskytovania konkrétnych výstupov ISMS (napr. plány na zvládanie rizík a príležitostí pri zavádzaní ISMS, plány na dosiahnutie cieľov informačnej bezpečnosti, plány ošetrenia rizík, plány projektu).

Tento dokument poskytuje návod pre všetky veľkosti a typy organizácií a audity ISMS rôzneho predmetu a rozsahu vrátane auditov vykonávaných veľkými audítorskými tímami, zvyčajne väčších organizácií, a auditov jednotlivých audítorov, či už vo veľkých alebo malých organizáciách. Tento návod by sa mal primerane prispôsobiť rozsahu, zložitosti a rozsahu programu auditu ISMS.

Tento dokument sa zameriava na interné audity ISMS (audit prvou stranou) a audity ISMS vykonávané organizáciami u ich externých poskytovateľov a iných externých zainteresovaných strán (audit druhou stranou). Tento dokument môže byť užitočný aj pre externé audity ISMS vykonávané na iné účely, ako je certifikácia systému manažérstva informačnej bezpečnosti. Norma ISO/IEC 27006 poskytuje požiadavky na auditovanie ISMS pre certifikáciu treťou stranou; tento dokument môže poskytnúť ďalšie užitočné návody.

Tento dokument sa má používať v spojení s pokynmi obsiahnutými v norme ISO 19011: 2018.

Tento dokument dodržiava štruktúru normy ISO 19011: 2018.

Norma ISO 19011: 2018 poskytuje návod na riadenie programov auditu, na vykonávanie interných alebo externých auditov systémov manažérstva, ako aj na odbornú spôsobilosť a hodnotenie audítorov systému manažérstva.

Príloha A poskytuje návod na audítorské postupy ISMS spolu s požiadavkami kapitol 4 až 10 normy ISO/IEC 27001: 2013.

1 Predmet

Tento dokument okrem pokynov uvedených v norme ISO 19011 poskytuje aj návod na riadenie programu auditu systému riadenia informačnej bezpečnosti (ISMS), na vykonávanie auditov a na kvalifikáciu audítorov ISMS.

Tento dokument je použiteľný pre tých, ktorí potrebujú porozumieť interným alebo externým auditom ISMS alebo ich vykonávať alebo riadiť program auditu ISMS.

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 používa len citované vydanie. Pri nedatovaných odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane všetkých zmien).

ISO 19011: 2018 *Guidelines for auditing management systems*. [Pokyny na auditovanie systémov riadenia.]

ISO/IEC 27000: 2018 *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. [Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník.]