ICS 35.030; 03.120.20 SLOVENSKÁ TECHNICKÁ NORMA Október 2021

STN	**Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Návod na auditovanie systémov riadenia informačnej bezpečnosti**	**STN 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
Leitfaden für das Audit von Informationssicherheitsmanagementsystemen

Táto norma obsahuje slovenskú verziu normy ISO/IEC 27007: 2020.

This standard includes the Slovak version of ISO/IEC 27007: 2020.

Nahradenie predchádzajúcich noriem

Táto norma nahrádza anglickú verziu STN ISO/IEC 27007 zo septembra 2020 v celom rozsahu.

133566

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

ISO/IEC 27000: 2018 zavedená 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 normy

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

Technická komisia: TK 37 Informačné technológie

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia
Návod na auditovanie systémov riadenia informačnej bezpečnosti

ISO/IEC 27007
Tretie vydanie
2020-01

ICS 35.030; 03.120.20

Obsah

strana

Predhovor

ISO (Medzinárodná organizácia pre normalizáciu) a IEC (Medzinárodná elektrotechnická komisia) vytvárajú špecializovaný systém celosvetovej normalizácie. Národné orgány, ktoré sú členmi ISO alebo IEC, sa zúčastňujú na tvorbe medzinárodných noriem prostredníctvom technických komisií ustanovených týmito organizáciami pre jednotlivé oblasti technickej činnosti. Technické komisie ISO a IEC spolupracujú v oblasti spoločného záujmu. S ISO a IEC spolupracujú aj iné medzinárodné vládne a mimovládne organizácie.

Postupy využité na vytvorenie tohto dokumentu a určené na jeho ďalšie udržiavanie sú opísané v smerniciach ISO/IEC, v časti 1. Treba najmä poznamenať, že pre rôzne typy dokumentov sú potrebné rozličné kritériá na schvaľovanie. Tento dokument bol vypracovaný v súlade s redakčnými pravidlami smerníc ISO/IEC, časť 2 (pozri www.iso.org/directives).

Upozorňuje sa na možnosť, že niektoré časti tohto dokumentu môžu byť predmetom patentových práv. ISO a IEC nezodpovedajú za identifikáciu ktoréhokoľvek ani všetkých takýchto patentových práv. Podrobnosti akýchkoľvek patentových práv identifikované počas vývoja dokumentu budú uvedené v úvode alebo na zozname vymenovaných patentov ISO (pozri www.iso.org/patents) alebo na zozname vymenovaných patentov IEC (pozri http://patents.iec.ch).

Nijaké obchodné meno použité v tomto dokumente nie je informáciou, ktorá by zvýhodňovala používateľa a nepredstavuje jeho podporovanie.

Vysvetlenie dôležitosti špecifických termínov ISO a výrazov týkajúcich sa posudzovania zhody, ako aj informácií o zachovávaní princípov dobrovoľnosti ISO a WTO v Technických bariérach obchodovania (TBT) pozri na adrese www.iso.org/iso/foreword.html.

Tento dokument pripravila spoločná subkomisia SC 27 *Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia* technickej komisie ISO/IEC JTC 1 *Informačné technológie.*

Toto tretie vydanie ruší a nahrádza druhé vydanie (ISO/IEC 27007: 2017), ktoré sa technicky revidovalo.

Hlavné zmeny v porovnaní s predchádzajúcim vydaním sú tieto:

- dokument bol zosúladený s normou ISO 19011: 2018;
- úvod bol preformulovaný a rozšírený;
- v čl. 5.1 bol odstránený celý text;
- v čl. 5.2.2 bola odstránená predchádzajúca položka d);
- v čl. 5.3 bol odstránený celý text;
- v čl. 5.5.2.2 bola odstránená predchádzajúca položka b) a ďalší odsek;
- v čl. 6.5.2.2 bol prvý odsek odstránený a POZNÁMKA bola preformulovaná.

Akákoľvek spätná väzba alebo otázky týkajúce sa tohto dokumentu by mali byť smerované na národný normalizačný orgán používateľa. Kompletný zoznam týchto orgánov možno nájsť na stránke:

www.iso.org/members.html.

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 normy

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 techniky. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník