ČESKÁ TECHNICKÁ NORMA

ICS 35.030; 03.120.20 **Říjen 2020**

Informační technologie, kybernetická bezpečnost a ochrana soukromí – Směrnice pro audit systémů řízení bezpečnosti informací	ČSN ISO/IEC 27007 36 9790

Information Technology, 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 systemes
de management de la sécurité de l,information

Tato norma je českou verzí mezinárodní normy ISO/IEC 27007:2020. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 27007:2020. It was translated by the Czech Agency for Standardization. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 27007 (36 9790) z července 2018.

Národní předmluva

Změny proti předchozí normě

Hlavní část této normy byla upravena tak, aby byla v souladu s normou ISO 19011:2018. Byl přeformulován a rozšířen úvod, v některých kapitolách a článcích byly vypuštěny části textu.

Informace o citovaných dokumentech

ISO 19011:2018 zavedena v ČSN EN ISO 19011:2019 (01 0330) Směrnice pro auditování systémů managementu

ISO/IEC 27000:2018 zavedena v ČSN EN ISO/IEC 27000:2020 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

Souvisící ČSN

ČSN EN ISO/IEC 17021-1:2016 (01 5257) Posuzování shody – Požadavky na orgány poskytující služby auditů a certifikace systémů managementu – Část 1: Požadavky

ČSN EN ISO/IEC 17024 (01 5258) Posuzování shody – Všeobecné požadavky na orgány pro certifikaci osob

ČSN EN ISO/IEC 27001:2014 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

ČSN EN ISO/IEC 27002 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

ČSN ISO/IEC 27003:2018 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny

ČSN ISO/IEC 27004 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení

ČSN ISO/IEC 27005 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti
informací

ČSN ISO/IEC 27006:2016 (36 9790) Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

ČSN ISO 31000:2018 (01 0351) Management rizik – Směrnice

Vysvětlivky k textu převzaté normy

Pro účely této normy je anglický termín „guidance“ přeložen jako „pokyny“ vzhledem k jeho používání v oblasti IT a v návaznosti na vydané normy z oblasti 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.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

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.

MEZINÁRODNÍ NORMA

Informační technologie, kybernetická bezpečnost a ochrana soukromí – Směrnice pro audit systémů řízení bezpečnosti informací

ISO/IEC 27007
Třetí vydání
2020-01

ICS 35.030; 03.120.20

Obsah

ISO copyright office
CP 401 · CH. de Blandonnet 8
CH-1214 Vernier, Geneva
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org
Publikováno ve Švýcarsku

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).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržených ISO (viz www.iso.org/patents) nebo v seznamu patentových prohlášení obdržených IEC (viz http://patents.iec.ch).

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) jsou uvedeny na www.iso.org/iso/foreword.html.

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí*.

Toto třetí vydání zrušuje a nahrazuje druhé vydání (ISO/IEC 27007:2017), které bylo technicky zrevidováno.

Hlavní změny oproti předchozímu vydání jsou následující:

- dokument byl sladěn s ISO 19011:2018;
- Úvod byl přeformulován a rozšířen;
- v 5.1 byl celý text vypuštěn;
- v 5.2.2 byla předchozí položka d) vypuštěna;
- v 5.3 byl celý text vypuštěn;
- v 5.5.2.2 byla vypuštěna předchozí položka b) a byl vypuštěn níže uvedený odstavec;
- v 6.5.2.2 byl první odstavec vypuštěn a POZNÁMKA byla přeformulována.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu by měly být směrovány na národní

normalizační orgán uživatele. Úplný seznam těchto orgánů lze nalézt na www.iso.org/members.html.

Úvod

Audit systému řízení bezpečnosti informací (ISMS) lze provádět na základě řady kritérií auditu, samostatně nebo v kombinaci, zahrnující mimo jiné například:

- požadavky definované v ISO/IEC 27001:2013;
- politiky a požadavky stanovené příslušnými zúčastněnými stranami;
- zákonné a regulatorní požadavky;
- procesy a kontrolní opatření ISMS definované organizací nebo jinými stranami;
- plán (plány) systému řízení týkající se poskytování konkrétních výstupů ISMS (například plány pro řešení rizik a příležitostí při stanovování ISMS, plány na dosažení cílů v oblasti bezpečnosti informací, plány ošetření rizik, plány projektů).

Tento dokument poskytuje pokyny pro všechny velikosti a typy organizací a audity ISMS různých předmětů a rozsahů, včetně těch, které provádějí velké auditorské týmy, obvykle větších organizací, a ty, které provádějí jednotliví auditoři, ať už ve velkých nebo malých organizacích. Tyto pokyny by měly být přizpůsobeny podle předmětu, složitosti a rozsahu programu auditu ISMS.

Tento dokument se zaměřuje na interní audity ISMS (audity první stranou) a audity ISMS prováděné organizacemi u jejich externích poskytovatelů a dalších externích zúčastněných stran (audity druhou stranou). Tento dokument může být užitečný také pro externí audity ISMS prováděné pro jiné účely, než je certifikace systému řízení třetích stran. ISO/IEC 27006 poskytuje požadavky na audit ISMS pro certifikaci třetích stran; tento dokument může poskytnout užitečné doplňující pokyny.

Tento dokument je určen pro použití ve spojení s pokyny obsaženými v ISO 19011:2018.

Tento dokument dodržuje strukturu ISO 19011:2018.

ISO 19011:2018 poskytuje pokyny pro řízení programů auditu, provádění interních nebo externích auditů systémů řízení, jakož i pro kompetence a hodnocení auditorů systémů řízení.

Příloha A poskytuje pokyny pro postupy auditorů ISMS spolu s požadavky ISO/IEC 27001:2013, kapitoly 4 až 10.

1 Předmět normy

Tento dokument poskytuje pokyny k řízení programu auditů systému řízení bezpečnosti informací (ISMS), k provádění auditů a kompetence auditorů ISMS, nad rámec pokynů obsažených v ISO 19011.

Tento dokument je použitelný pro ty, kdo potřebují porozumět interním nebo externím auditům ISMS nebo potřebují tyto audity provádět nebo řídit program auditu ISMS.