ČESKÁ TECHNICKÁ NORMA

ICS 03.100.70; 35.030 **Červenec**
2018

Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací

ČSN
ISO/IEC 27007

36 9790

Information Technology – Security techniques – Guidelines for information security management systems auditing

Technologies de l,information – Techniques de sécurité – Lignes directrices pour l,audit des systemes de management
de la sécurité de I,information

Tato norma je českou verzí mezinárodní normy ISO/IEC 27007:2017. 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 27007:2017. 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 2013.

Národní předmluva

Změny proti předchozí normě

Hlavní část této normy byla upravena v souladu s ISO/IEC 27001:2013. Příloha A byla zcela přepracována tak, aby byla v souladu s ISO/IEC 27001:2013.

Informace o citovaných dokumentech

ISO 19011:2011 zavedena v ČSN EN ISO 19011:2012 (01 0330) Směrnice pro auditování systémů manage-
mentu

ISO/IEC 27000:2016 zavedena v ČSN EN ISO/IEC 27000:2017 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ISO/IEC 27001:2013 zavedena v ČSN EN ISO/IEC 27001:2014 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

Souvisící ČSN

ČSN ISO 31000:2010 (01 0351) Management rizik – Principy a směrnice

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 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

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 organizací 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 – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací

ISO/IEC 27007
Druhé vydání
2017-10

ICS 03.100.70; 35.030

Obsah

DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2017, Published in Switzerland
Veškerá práva vyhrazena. Není-li specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně pořizování fotokopií nebo zveřejnění na internetu nebo intranetu, bez předchozího písemného svolení. O písemné svolení lze požádat buď přímo ISO na níže uvedené adrese, nebo členskou organizaci ISO v zemi žadatele.
ISO copyright office
CH. de Blandonnet 8 · CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
copyright@iso.org
www.iso.org

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. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

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 ISO. 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).

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 tomto odkazu URL:
www.iso.org/iso/foreword.html.

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *IT Bezpečnostní techniky.*

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 27007:2011), jehož je technickou revizí.

Hlavní změny oproti předchozímu vydání jsou následující:

- příloha A byla zcela přepracována tak, aby byla v souladu s ISO/IEC 27001:2013;
- hlavní část tohoto dokumentu byla upravena tak, aby byla v souladu s ISO/IEC 27001:2013.

Úvod

Tento dokument poskytuje pokyny pro:

a) řízení programu auditu systému řízení bezpečnosti informací (ISMS);

b) provádění interních a externích auditů ISMS v souladu s ISO/IEC 27001;

c) kompetence a hodnocení auditorů ISMS.

Tento dokument by měl být používán ve spojení s pokyny obsaženými v ISO 19011:2011.

Tento dokument odpovídá struktuře ISO 19011:2011. Další pokyny specifické pro ISMS týkající se aplikace ISO 19011:2011 pro audity ISMS jsou označeny písmeny „IS“.

ISO 19011:2011 poskytuje pokyny týkající se řízení auditních programů, provádění interních nebo externích auditů systémů řízení, jakož i kompetencí a hodnocení auditorů systémů řízení.

POZNÁMKA Pro akreditovanou certifikaci jsou požadavky na auditora uvedeny v ISO/IEC 27006.

Tento dokument nestanovuje požadavky a je určen všem uživatelům, včetně malých a středních organizací.

1 Předmět normy

Tento dokument poskytuje pokyny týkající se řízení programu auditu systému řízení bezpečnosti informací (ISMS), provádění auditů a kompetence auditorů ISMS, nad rámec pokynů obsažených v ISO 19011:2011.

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

Konec náhledu - text dále pokračuje v placené verzi ČSN.