ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Prosinec 2023**

Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Pokyny pro management rizik informační bezpečnosti	ČSN ISO/IEC 27005 36 9790

Information security, cybersecurity and privacy protection – Guidance on managing information security risks

Sécurité de l,information, cybersécurité et protection de la vie privée – Préconisations pour la gestion des risques liés
a la sécurité de l,information

Tato norma je českou verzí mezinárodní normy ISO/IEC 27005:2022. 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 27005:2022. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

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

Souvisící ČSN a TNI

ČSN EN ISO/IEC 27001:2023 (36 9797) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky

ČSN ISO/IEC 27003 (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 27014 (36 9790) Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Správa a řízení bezpečnosti informací

ČSN EN ISO/IEC 27017 (36 9710) Informační technologie – Bezpečnostní techniky – Soubor postupů

pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002

ČSN EN ISO/IEC 27701 (36 9770) Bezpečnostní techniky – Rozšíření ISO/IEC 27001 a ISO/IEC 27002 pro řízení ochrany soukromí – Požadavky a směrnice

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

ČSN EN IEC 31010 ed. 2:2020 (01 0352) Management rizik – Techniky posuzování rizik

TNI 01 0350:2010 (01 0350) Management rizik – Slovník (Pokyn 73)

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článcích „Informace
o citovaných dokumentech“ a „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

Vysvětlivky k textu převzaté normy

Pro účely této normy byly použity následující anglické termíny v původní podobě, vzhledem k rozšíření těchto termínů v odborné komunitě a/nebo absenci českého ekvivalentu:

0-Day, man-in-the-middle, script-kiddies, shell

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 bezpečnost, kybernetická bezpečnost a ochrana soukromí – Pokyny pro management rizik informační bezpečnosti

ISO/IEC 27005
Čtvrté vydání 2022-10

ICS 35.030

Obsah

Strana

Strana

ISO copyright office
CP 401 · Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Tel.: + 41 22 749 01 11
E-mail: copyright@iso.org
Web: 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 nebo www.iec.ch/members_experts/refdocs).

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 https://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), viz www.iso.org/iso/foreword.html. V IEC viz www.iec.ch/understanding-standards.

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

Toto čtvrté vydání zrušuje a nahrazuje třetí vydání (ISO/IEC 27005:2018), které bylo technicky zrevidováno.

Hlavní změny jsou:

– všechny pokyny byly sladěny s ISO/IEC 27001:2022 a ISO 31000:2018;

– terminologie byla sladěna s terminologií v ISO 31000:2018;

– struktura kapitol byla přizpůsobena uspořádání ISO/IEC 27001:2022;

– byly zavedeny koncepty scénářů rizik;

– přístup k identifikaci rizik založený na událostech je postaven do kontrastu s přístupem k identifikaci rizik založeným na aktivech;

– obsah příloh byl revidován a restrukturalizován do jediné přílohy.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na
www.iso.org/members.html
a www.iec.ch/national-committees.

Úvod

Tento dokument poskytuje pokyny pro:

– implementaci požadavků na rizika informační bezpečnosti uvedených v ISO/IEC 27001;

– základní odkazy v rámci norem vypracovaných ISO/IEC JTC 1/SC 27 na podporu činností managementu rizik informační bezpečnosti;

– činnosti, které se zabývají riziky souvisícími s informační bezpečností (viz ISO/IEC 27001:2022, 6.1 a kapitola 8);

– implementaci pokynů pro management rizik z ISO 31000 v kontextu informační bezpečnosti.

Tento dokument obsahuje podrobné pokyny pro management rizik a doplňuje pokyny v ISO/IEC 27003.

Tento dokument je určen pro:

– organizace, které zamýšlejí zavést a implementovat systém managementu informační bezpečnosti (ISMS) v souladu s ISO/IEC 27001;

– osoby, které provádějí nebo se podílejí na managementu rizik informační bezpečnosti (např. odborníci na ISMS, vlastníci rizik a další zainteresované strany);

– organizace, které zamýšlejí zlepšit svůj proces managementu rizik informační bezpečnosti.

1 Předmět normy

Tento dokument obsahuje pokyny, které mají organizacím pomoci:

– splnit požadavky ISO/IEC 27001 týkající se opatření k řešení rizik v oblasti informační bezpečnosti;

– provádět činnosti v oblasti managementu rizik informační bezpečnosti, zejména posuzování a ošetření rizik informační bezpečnosti.

Tento dokument je použitelný pro všechny organizace bez ohledu na typ, velikost nebo odvětví.