ICS 35.030 SLOVENSKÁ TECHNICKÁ NORMA Júl 2023

STN	**Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Usmernenie k riadeniu rizík informačnej bezpečnosti**	**STN ISO/IEC 27005** 97 4175

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 à la sécurité de l'information

Informationssicherheit, Cybersicherheit und Datenschutz
Leitfaden zur Handhabung von Informationssicherheitsrisiken

Táto slovenská technická norma je slovenskou verziou medzinárodnej normy ISO/IEC 27005: 2022.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN ISO/IEC 27005 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the International Standard ISO/IEC 27005: 2022.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN ISO/IEC 27005 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza STN ISO/IEC 27005 z marca 2023 v celom rozsahu.

136907

Národný predhovor

Obrázky v tejto norme sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2022 ISO/IEC, ref. č. ISO/IEC 27005: 2022 E.

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 a TNI možno získať na webovom sídle www.unms.sk.

ISO/IEC 27000 prijatá ako STN EN ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000) (97 4170)

Vypracovanie slovenskej technickej normy

Spracovateľ: Ing. Lenka Gondová, Mgr. Natália Bosnyaková, SynCo s. r. o., Bratislava

Technická komisia: TK 37 Informačné technológie

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia
Usmernenie k riadeniu rizík informačnej bezpečnosti

ISO/IEC 27005
Štvrté vydanie
2022-10

ICS 35.030

Obsah

Contents

Prehovor

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

Postupy použité pri tvorbe tohto dokumentu, ako aj tie, ktoré sú určené na jeho ďalšie udržiavanie, sú opísané v smernici ISO/IEC, Časť 1. Do úvahy sa majú zobrať najmä rozdielne kritériá schvaľovania pri rôznych typoch dokumentov ISO. Tento dokument bol vypracovaný podľa edičných pravidiel smernice ISO/IEC, Časť 2 (pozri www.iso.org/directives alebo www.iec.ch/members_experts/refdocs).

Upozorňuje sa na možnosť, že niektoré časti tohto dokumentu môžu byť predmetom patentových práv. ISO a IEC nezodpovedajú za identifikáciu ktoréhokoľvek alebo všetkých takýchto patentových práv. Podrobnosti o akýchkoľvek patentových právach identifikovaných počas tvorby dokumentu sú uvedené v úvode dokumentu a/alebo v zozname vyhlásení o patentoch ISO (pozri www.iso.org/patents) alebo v zozname prijatých patentových vyhlásení IEC (pozri https://patents.iec.ch).

Akýkoľvek obchodný názov použitý v tomto dokumente slúži len na informáciu pre používateľa a neznamená jeho schválenie.

Vysvetlenie dobrovoľnej podstaty noriem, význam špecifických termínov a výrazov týkajúcich sa posudzovania zhody, ako aj informácie o väzbe ISO na princípy Svetovej obchodnej organizácie (WTO) uplatňované pri odstraňovaní technických prekážok obchodu (TBT) pozri na www.iso.org/iso/foreword.html. V časti IEC si pozrite www.iec.ch/understanding-standards.

Tento dokument vypracovala spoločná technická komisia ISO/IEC JTC 1, *Informačné technológie, Podvýbor SC 27, Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia.*

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information Technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Toto štvrté vydanie ruší a nahrádza tretie vydanie (ISO/IEC 27005: 2018), ktoré bolo technicky revidované.

Hlavné zmeny sú tieto:

- celý text usmernenia bol zosúladený s normami ISO/IEC 27001: 2022 a ISO 31000: 2018;
- terminológia bola zosúladená s terminológiou v norme ISO 31000: 2018;
- štruktúra kapitol bola prispôsobená štruktúre normy ISO/IEC 27001: 2022;
- boli zavedené koncepty rizikových scenárov;
- prístup založený na udalostiach je v kontraste s prístupom k identifikácii rizík založeným na aktívach;
- obsah príloh bol revidovaný a reštrukturalizovaný do jednej prílohy.

Akákoľvek spätná väzba alebo otázky k tomuto dokumentu sa majú adresovať národnému normalizačnému orgánu používateľa. Úplný zoznam týchto orgánov nájdete na adrese www.iso.org/members.html a www.iec.ch/national-committees.

This fourth edition cancels and replaces the third edition (ISO/IEC 27005: 2018), which has been technically revised.

The main changes are as follows:

- all guidance text has been aligned with ISO/IEC 27001: 2022, and ISO 31000: 2018;
- the terminology has been aligned with the terminology in ISO 31000: 2018;
- the structure of the clauses has been adjusted to the layout of ISO/IEC 27001: 2022;
- risk scenario concepts have been introduced;
- the event-based approach is contrasted with the asset-based approach to risk identification;
- the content of the annexes has been revised and restructured into a single annex.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Úvod

Tento dokument obsahuje usmernenia týkajúce sa:

- implementácie požiadaviek na riziká informačnej bezpečnosti špecifikovaných v norme ISO/IEC 27001;
- základných odkazov v rámci noriem vypracovaných ISO/IEC JTC 1/SC 27 na podporu činností riadenia rizík informačnej bezpečnosti;
- činností, ktoré sa týkajú rizík súvisiacich s informačnou bezpečnosťou (pozri ISO/IEC 27001: 2022, článok 6.1 a kapitola 8);
- implementácie usmernení na riadenie rizík v norme ISO 31000 v súvislostiach informačnej bezpečnosti.

Tento dokument obsahuje podrobné usmernenie k riadeniu rizík a dopĺňa usmernenie v norme ISO/IEC 27003.

Tento dokument je určený na použitie:

- organizáciami, ktoré majú v úmysle vytvoriť a zaviesť systém manažérstva informačnej bezpečnosti (ISMS) v súlade s normou ISO/IEC 27001;
- osobami, ktoré vykonávajú alebo sa podieľajú na riadení rizík informačnej bezpečnosti (napr. odborníci na ISMS, vlastníci rizík a iné zainteresované strany);
- organizáciami, ktoré majú v úmysle zlepšiť svoj proces riadenia rizík informačnej bezpečnosti.

Introduction

This document provides guidance on:

- implementation of the information security risk requirements specified in ISO/IEC 27001;
- essential references within the standards developed by ISO/IEC JTC 1/SC 27 to support information security risk management activities;
- actions that address risks related to information security (see ISO/IEC 27001: 2022, 6.1 and Clause 8);
- implementation of risk management guidance in ISO 31000 in the context of information security.

This document contains detailed guidance on risk management and supplements the guidance in ISO/IEC 27003.

This document is intended to be used by:

- organizations that intend to establish and implement an information security management system (ISMS) in accordance with ISO/IEC 27001;
- persons that perform or are involved in information security risk management (e.g. ISMS professionals, risk owners and other interested parties);
- organizations that intend to improve their information security risk management process.

1 Predmet normy

Tento dokument poskytuje usmernenia, ktoré pomôžu organizáciám:

- splniť požiadavky normy ISO/IEC 27001 týkajúce sa opatrení na riešenie rizík informačnej bezpečnosti;
- vykonávať činnosti riadenia rizík informačnej bezpečnosti, konkrétne posudzovanie a ošetrovanie rizík informačnej bezpečnosti.

Tento dokument sa vzťahuje na všetky organizácie bez ohľadu na ich typ, veľkosť alebo odvetvie.

1 Scope

This document provides guidance to assist organizations to:

- fulfil the requirements of ISO/IEC 27001 concerning actions to address information security risks;
- perform information security risk management activities, specifically information security risk assessment and treatment.

This document is applicable to all organizations, regardless of type, size or sector.

2 Normatívne odkazy

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazov sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy manažérstva informačnej bezpečnosti. Prehľad a slovník.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary.