ICS 35.030 SLOVENSKÁ TECHNICKÁ NORMA Jún 2025

| STN | **Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Usmernenie k riadeniu rizík informačnej bezpečnosti (ISO/IEC 27005: 2022)** | **STN EN ISO/IEC 27005**<br><br>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 európskej normy EN ISO/IEC 27005: 2024.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN EN ISO/IEC 27005 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 27005: 2024.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN EN ISO/IEC 27005 has the same status as the official versions.

**Nahradenie predchádzajúcich dokumentov**

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

**140606**

## Národný predhovor

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

Norma obsahuje jednu národnú poznámku.

### Zmeny oproti predchádzajúcej STN

Toto štvrté vydanie medzinárodnej normy ISO/IEC 27005: 2022 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.

### Upozornenie k vydaniu STN EN ISO/IEC 27005

Text STN EN ISO/IEC 27005 z júna 2025 je **identický** s STN ISO/IEC 27005 z júla 2023. Ide len o zmenu označenia z STN ISO/IEC 27005 na **STN EN ISO/IEC 27005**, pridanie európskej titulnej strany a európskeho predhovoru, a to z dôvodu, že medzinárodná norma ISO/IEC 27005: 2022 bola prevzatá európskou technickou komisiou CEN-CENELEC/JTC 13 *Kybernetická bezpečnosť a ochrana údajov* ako EN ISO/IEC 27005: 2024.

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

**Technická komisia:** TK 37 Informačné technológie

**EURÓPSKA NORMA** **EN ISO/IEC 27005**
**EUROPEAN STANDARD**
**NORME EUROPÉENNE**
**EUROPÄISCHE NORM** August 2024

ICS 35.030

# Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Usmernenie k riadeniu rizík informačnej bezpečnosti (ISO/IEC 27005: 2022)

Information security, cybersecurity and privacy protection
Guidance on managing information security risks
(ISO/IEC 27005: 2022)

Sécurité de l'information, cybersécurité et protection de la vie privée
Préconisations pour la gestion des risques liés à la sécurité de l'information
(ISO/IEC 27005: 2022)

Informationssicherheit, Cybersicherheit und Datenschutz
Leitfaden zur Handhabung von Informationssicherheitsrisiken
(ISO/IEC 27005: 2022)

Túto európsku normu schválil CEN 1. augusta 2024.

Členovia CEN a CENELEC sú povinní plniť vnútorné predpisy CEN/CENELEC, v ktorých sú určené podmienky, za ktorých sa tejto európskej norme bez akýchkoľvek zmien priznáva postavenie národnej normy. Aktualizované zoznamy a bibliografické odkazy týkajúce sa takýchto národných noriem možno na požiadanie dostať od Riadiaceho strediska CEN-CENELEC alebo od každého člena CEN a CENELEC.

Táto európska norma existuje v troch oficiálnych verziách (anglickej, francúzskej, nemeckej). Verzia v akomkoľvek inom jazyku, ktorú na vlastnú zodpovednosť vydal člen CEN a CENELEC v preklade do národného jazyka a ktorá bola oznámená Riadiacemu stredisku CEN-CENELEC, má rovnaké postavenie, ako majú oficiálne verzie.

Členmi CEN a CENELEC sú národné normalizačné organizácie Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédska, Talianska a Turecka.

**CEN**

Európsky výbor pre normalizáciu
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

**CENELEC**

Európsky výbor pre normalizáciu v elektrotechnike
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

**Riadiace stredisko CEN-CENELEC: Rue de la Science 23, B-1040 Brusel**



Ref. č. EN ISO/IEC 27005: 2024 SK

## Obsah



## Contents

## Európsky prehovor

Text ISO/IEC 27005: 2022 vypracovala technická komisia ISO/IEC JTC 1 *Informačné technológie* medzinárodnej organizácie pre normalizáciu (ISO) a bol prevzatý ako EN ISO/IEC 27005: 2024 technickou komisiou CEN-CENELEC/JTC 13 *Kybernetická bezpečnosť a ochrana údajov*, ktorej sekretariát je v DIN.

Tejto európskej norme sa musí priznať postavenie národnej normy buď vydaním identického textu, alebo oznámením najneskoršie do februára 2025 a národné normy, ktoré sú s ňou v rozpoore sa musia zrušiť najneskoršie do februára 2025.

Upozorňuje sa na možnosť, že niektoré časti tohto dokumentu môžu byť predmetom patentových práv. CEN-CENELEC nezodpovedajú za identifikáciu ktoréhokoľvek alebo všetkých takýchto patentových práv.

Akákoľvek spätná väzba a otázky k tejto európskej norme majú byť adresované národnému normalizačnému orgánu používateľov. Kompletný zoznam týchto orgánov možno nájsť na webovej stránke CEN a CENELEC.

V súlade s vnútornými predpismi CEN-CENELEC sú túto európsku normu povinné prevziať národné normalizačné organizácie týchto krajín: Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédska, Talianska a Turecka.

### Oznámenie o schválení

Text ISO/IEC 27005: 2022 schválil CEN-CENELEC ako EN ISO/IEC 27005: 2024 bez akýchkoľvek modifikácií.

## Euroepan foreword

The text of ISO/IEC 27005: 2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 27005:2024 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2025, and conflicting national standards shall be withdrawn at the latest by February 2025.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

### Endorsement notice

The text of ISO/IEC 27005: 2022 has been approved by CEN-CENELEC as EN ISO/IEC 27005: 2024 without any modification.

## 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.