ICS 35.030 SLOVENSKÁ TECHNICKÁ NORMA Máj 2023

STN	**Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Riadenie informačnej bezpečnosti (ISO/IEC 27002: 2022)**	**STN EN ISO/IEC 27002** 97 4172

Information security, cybersecurity and privacy protection
Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée
Moyens de maîtrise de l'information

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre
Informationssicherheitsmaßnahmen

Táto slovenská technická norma je slovenskou verziou európskej normy EN ISO/IEC 27002: 2022.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN EN ISO/IEC 27002 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 27002: 2022.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN EN ISO/IEC 27002 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza STN EN ISO/IEC 27002 z februára 2019 v celom rozsahu.

136380

Národný predhovor

Tento dokument pripravila spoločná technická komisia ISO/IEC JTC 1 Informačné technológie, subkomisia SC 27, Bezpečnosť informácií, kybernetická bezpečnosť a ochrana súkromia.

Toto tretie vydanie ruší a nahrádza druhé vydanie (ISO/IEC 27002: 2013), ktoré bolo technicky revidované. Zahŕňa aj technické opravy ISO/IEC 27002: 2013/Cor. 1: 2014 a ISO/IEC 27002: 2013/Cor. 2: 2015.

Hlavné zmeny sú tieto:

- názov bol upravený;
- štruktúra dokumentu bola zmenená, pričom ovládacie prvky sú prezentované pomocou jednoduchej taxonómie a súvisiacich atribútov;
- niektoré ovládacie prvky boli zlúčené, niektoré odstránené a bolo zavedených niekoľko nových ovládacích prvkov. Úplná korešpondencia sa nachádza v prílohe B.

Normatívne referenčné dokumenty

Táto slovenská technická norma neobsahuje normatívne odkazy.

Vypracovanie slovenskej technickej normy

Spracovateľ: Ing. Lenka Gondová, Pro Excellence, s. r. o., Bratislava

Technická komisia: TK 37 Informačné technológie

EURÓPSKA NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27002

November 2022

ICS 35.030

Nahrádza EN ISO/IEC 27002: 2017

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Riadenie informačnej bezpečnosti (ISO/IEC 27002: 2022)

Information security, cybersecurity
and privacy protection
Information security controls
(ISO/IEC 27002: 2022)

Sécurité de l'information, cybersécurité
et protection de la vie privée
Moyens de maîtrise de l'information
(ISO/IEC 27002: 2022)

Informationssicherheit, Cybersicherheit
und Schutz der Privatsphäre
Informationssicherheitsmaßnahmen
(ISO/IEC 27002: 2022)

Túto európsku normu schválil CEN 30. októbra 2022.

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

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

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 27002: 2022 SK

Obsah

Contents

Európsky predhovor

Text ISO/IEC 27002: 2022 vypracovala technická komisia ISO/IEC JTC 1 „Informačné technológie“ medzinárodnej organizácie pre normalizáciu (ISO) a bola prevzatá ako EN ISO/IEC 27002: 2022 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 identických textu, alebo oznámením najneskoršie do mája 2023 a národné normy, ktoré sú s ňou v rozpore, musia sa zrušiť najneskôr do mája 2023.

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

Tento dokument nahrádza EN ISO/IEC 27002: 2017.

Akákoľvek súpätná väzba a otázky k tomuto dokumentu sa majú adresovať národnému normalizačnému orgánu používateľov. Kompletný z oznam týchto používateľov je na webovom sídle CEN-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 medzinárodnej normy ISO/IEC 27002: 2022 schválil CEN-CENELEC ako EN ISO/IEC 27002: 2022 bez akýchkoľvek modifikácií.

Úvod

0.1 Východiská a kontext

Tento dokument je určený pre organizácie všetkých typov a veľkostí. Používa sa ako referencia na určenie a implementáciu opatrení na ošetrenie rizík informačnej bezpečnosti v systéme riadenia informačnej bezpečnosti (ISMS) založenom na ISO/IEC 27001. Môže sa použiť aj ako usmernenie pre organizácie určujúce a implementujúce všeobecne akceptované opatrenia informačnej bezpečnosti. Tento dokument je navyše určený na použitie pri rozvoji priemyselných alebo organizačných návodov riadenia informačnej bezpečnosti, pričom sa zohľadňujú riziká informačnej bezpečnosti vlastné danému prostrediu. Organizačné alebo prostrediu špecifické opatrenia odlišné od opatrení zahrnutých v tomto dokumente, je možné určiť prostredníctvom posúdenia rizík podľa potreby.

Organizácie všetkých typov a veľkostí (vrátane verejného a súkromného sektora, komerčného a neziskového) vytvárajú, zhromažďujú, spracúvajú, ukladajú, prenášajú a likvidujú informácie v mnohých formách vrátane elektronických, fyzických a verbálnych (napr. konverzácie a prezentácie).

Hodnota informácií presahuje písané slová, čísla a obrázky: vedomosti, koncepty, nápady a značky sú príkladmi nehmotných foriem informácií. V prepojenom svete si informácie a ďalšie súvisiace aktíva zaslúžia alebo vyžadujú ochranu pred rôznymi zdrojmi rizika, či už prírodnými, náhodnými alebo úmyselnými.

Informačná bezpečnosť sa dosahuje implementáciou vhodného súboru opatrení vrátane politík, pravidiel, procesov, postupov, organizačných štruktúr a softvérových a hardvérových funkcií. Na splnenie svojich konkrétnych bezpečnostných a obchodných cieľov by organizácia mala v prípade potreby definovať, implementovať, monitorovať, preskúmať a vylepšiť tieto opatrenia. ISMS, ako sa uvádza v ISO/IEC 27001, má holistický, koordinovaný pohľad na riziká informačnej bezpečnosti organizácie s cieľom určiť a implementovať komplexnú sadu opatrení informačnej bezpečnosti v rámci celkového rámca koherentného systému riadenia.

Mnoho informačných systémov, vrátane ich správy a prevádzky, nebolo navrhnutých tak, aby boli bezpečné podľa ISMS, ako je uvedené v ISO/IEC 27001 a v tomto dokumente. Úroveň bezpečnosti, ktorú je možné dosiahnuť iba technologickými opatreniami, je obmedzená a mala by byť podporená vhodnými riadiacimi činnosťami a organizačnými procesmi. Identifikácia, ktoré opatrenia by mali byť zavedené, si vyžaduje starostlivé plánovanie a detailný prístup pri ošetrovaní rizík.

Introduction

0.1 Background and context

This document is designed for organizations of all types and sizes. It is to be used as a reference for determining and implementing controls for information security risk treatment in an information security management system (ISMS) based on ISO/IEC 27001. It can also be used as a guidance document for organizations determining and implementing commonly accepted information security controls. Furthermore, this document is intended for use in developing industry and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s). Organizational or environment-specific controls other than those included in this document can be determined through risk assessment as necessary.

Organizations of all types and sizes (including public and private sector, commercial and non-profit) create, collect, process, store, transmit and dispose of information in many forms, including electronic, physical and verbal (e.g. conversations and presentations).

The value of information goes beyond written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and other associated assets deserve or require protection against various risk sources, whether natural, accidental or deliberate.

Information security is achieved by implementing a suitable set of controls, including policies, rules, processes, procedures, organizational structures and software and hardware functions. To meet its specific security and business objectives, the organization should define, implement, monitor, review and improve these controls where necessary. An ISMS such as that specified in ISO/IEC 27001 takes a holistic, coordinated view of the organization’s information security risks in order to determine and implement a comprehensive suite of information security controls within the overall framework of a coherent management system.

Many information systems, including their management and operations, have not been designed to be secure in terms of an ISMS as specified in ISO/IEC 27001 and this document. The level of security that can be achieved only through technological measures is limited and should be supported by appropriate management activities and organizational processes. Identifying which controls should be in place requires careful planning and attention to detail while carrying out risk treatment.

Úspešné ISMS vyžaduje podporu od všetkých zamestnancov v organizácii. Môže tiež vyžadovať účasť iných zainteresovaných strán, ako sú akcionári alebo dodávatelia. Môžu byť potrebné aj rady od odborníkov.

Vhodný, primeraný a efektívny systém riadenia informačnej bezpečnosti poskytuje uistenie vedeniu organizácie a iným zainteresovaným stranám, že ich informácie a ďalšie súvisiace aktíva sú primerane zabezpečené a chránené pred hrozbami a škodami, čím umožňujú organizácii dosiahnuť stanovené obchodné ciele.

A successful ISMS requires support from all personnel in the organization. It can also require participation from other interested parties, such as shareholders or suppliers. Advice from subject matter experts can also be needed.

A suitable, adequate and effective information security management system provides assurance to the organization's management and other interested parties that their information and other associated assets are kept reasonably secure and protected against threats and harm, thereby enabling the organization to achieve the stated business objectives.

0.2 Požiadavky na informačnú bezpečnosť

Je nevyhnutné, aby organizácia určovala svoje požiadavky na informačnú bezpečnosť. Existujú tri hlavné zdroje požiadaviek na informačnú bezpečnosť:

a) posúdenie rizík organizácie, pričom sa zohľadňuje celková obchodná stratégia a ciele organizácie. To sa dá uľahčiť alebo podporovať prostredníctvom hodnotenia rizík informačnej bezpečnosti. Výsledkom by malo byť určenie opatrení potrebných na zabezpečenie toho, aby zostatkové riziko organizácie spĺňalo jej kritériá pre akceptáciu rizika;

b) právne, zákonné, regulačné a zmluvné požiadavky, ktoré organizácia a jej zainteresované strany (obchodní partneri, poskytovatelia služieb atď.) musia dodržiavať a ich sociálno-kultúrne prostredie;

c) súbor zásad, cieľov a obchodných požiadaviek pre všetky kroky životného cyklu informácií, ktoré organizácia vyvinula na podporu svojej prevádzky.

0.2 Information security requirements

It is essential that an organization determines its information security requirements. There are three main sources of information security requirements:

a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. This can be facilitated or supported through an information security-specific risk assessment. This should result in the determination of the controls necessary to ensure that the residual risk to the organization meets its risk acceptance criteria;

b) the legal, statutory, regulatory and contractual requirements that an organization and its interested parties (trading partners, service providers, etc.) have to comply with and their socio-cultural environment;

c) the set of principles, objectives and business requirements for all the steps of the life cycle of information that an organization has developed to support its operations.

0.3 Opatrenia

Opatrenie je definovaná ako opatrenie, ktoré modifikuje alebo zachováva riziko. Niektoré z opatrení v tomto dokumente sú opatrenia, ktoré modifikujú riziko, zatiaľ čo iné zachovávajú riziko. Napríklad politika informačnej bezpečnosti môže zachovávať iba riziko, zatiaľ čo súlad s politikou informačnej bezpečnosti môže modifikovať riziko. Niektoré opatrenia navyše opisujú rovnaké generické opatrenie v rôznych rizikových kontextoch. Tento dokument poskytuje všeobecnú kombináciu organizačných, ľudských, fyzických a technologických opatrení informačnej bezpečnosti odvodených z medzinárodne uznávaných osvedčených postupov.

0.3 Controls

A control is defined as a measure that modifies or maintains risk. Some of the controls in this document are controls that modify risk, while others maintain risk. An information security policy, for example, can only maintain risk, whereas compliance with the information security policy can modify risk. Moreover, some controls describe the same generic measure in different risk contexts. This document provides a generic mixture of organizational, people, physical and technological information security controls derived from internationally recognized best practices.

0.4 Určenie opatrení

Určenie opatrení závisí od rozhodnutí organizácie po posúdení rizika s jasne definovaným rozsahom. Rozhodnutia týkajúce sa identifikovaných rizík by sa mali zakladať na kritériách pre prijatie rizika, možnosti ošetrenia rizika a prístupu k riadeniu rizika, ktorý organizácia uplatňuje. Určenie opatrení by malo zohľadniť aj všetky príslušné národné a medzinárodné právne predpisy a nariadenia. Určenie opatrení tiež závisí od spôsobu, akým opatrenia vzájomne pôsobia, aby poskytovali obranu do hĺbky.

Organizácia môže podľa potreby navrhnúť opatrenia alebo ich identifikovať z akéhokoľvek zdroja. Pri špecifikovaní takýchto opatrení by organizácia mala zvážiť zdroje a investície potrebné na implementáciu a prevádzku opatrení s realizovanou obchodnou hodnotou. Pre usmernenie o rozhodnutiach týkajúcich sa investície do ISMS a ekonomických dôsledkov týchto rozhodnutí v kontexte konkurenčných požiadaviek na zdroje odporúčame prejsť normu ISO/IEC TR 27016.

Mala by existovať rovnováha medzi zdrojmi nasadenými na implementáciu opatrení a potenciálnym vplyvom bezpečnostných incidentov pri absencii týchto opatrení na podnikanie. Výsledky posúdenia rizík by mali pomôcť usmerňovať a určiť vhodné kroky, priority pre riadenie rizík informačnej bezpečnosti a na implementáciu opatrení nevyhnutných na ochranu pred týmito rizikami.

Niektoré z opatrení v tomto dokumente možno považovať za hlavné zásady pre riadenie informačnej bezpečnosti a platné pre väčšinu organizácií. Viac informácií o určovaní opatrení a iných možností ošetrenia rizík je možné nájsť v ISO/IEC 27005.

0.5 Tvorba špecifického návodu pre organizáciu

Tento dokument možno považovať za východiskový bod pre tvorbu špecifického návodu pre organizáciu. Nie všetky opatrenia a usmernenia v tomto dokumente sa môžu vzťahovať na všetky organizácie. Na riešenie konkrétnych potrieb organizácie a identifikovaných rizík, ktoré boli identifikované, je možné tiež vyžadovať ďalšie opatrenia a usmernenia, ktoré nie sú zahrnuté v tomto dokumente. Ak sa vypracúvajú dokumenty obsahujúce ďalšie usmernenia alebo opatrenia, môže byť užitočné zahrnúť do kapitol krížové odkazy pre budúce použitie.

0.4 Determining controls

Determining controls is dependent on the organization's decisions following a risk assessment, with a clearly defined scope. Decisions related to identified risks should be based on the criteria for risk acceptance, risk treatment options and the risk management approach applied by the organization. The determination of controls should also take into consideration all relevant national and international legislation and regulations. Control determination also depends on the manner in which controls interact with one another to provide defence in depth.

The organization can design controls as required or identify them from any source. In specifying such controls, the organization should consider the resources and investment needed to implement and operate a control against the business value realized. See ISO/IEC TR 27016 for guidance on decisions regarding the investment in an ISMS and the economic consequences of these decisions in the context of competing requirements for resources.

There should be a balance between the resources deployed for implementing controls and the potential resulting business impact from security incidents in the absence of those controls. The results of a risk assessment should help guide and determine the appropriate management action, priorities for managing information security risks and for implementing controls determined necessary to protect against these risks.

Some of the controls in this document can be considered as guiding principles for information security management and as being applicable for most organizations. More information about determining controls and other risk treatment options can be found in ISO/IEC 27005.

0.5 Developing organization-specific guidelines

This document can be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this document can be applicable to all organizations. Additional controls and guidelines not included in this document can also be required to address the specific needs of the organization and the risks that have been identified. When documents are developed containing additional guidelines or controls, it can be useful to include cross-references to clauses in this document for future reference.

0.6 Úvahy o životnom cykle

Informácie majú životný cyklus, od vytvorenia po likvidáciu. Hodnota informácií a riziká s nimi súvisiace, sa môžu v rámci tohto životného cyklu líšiť (napr. neoprávnené zverejnenie alebo krádež finančných účtov spoločnosti nie sú po zverejnení významné, ale integrita zostáva kritická), preto je informačná bezpečnosť do istej miery dôležitá vo všetkých etapách.

Informačné systémy a iné aktíva relevantné pre informačnú bezpečnosť majú životné cykly, v rámci ktorých sú koncipované, špecifikované, navrhnuté, vyvinuté, testované, implementované, používané, udržiavané a prípadne vyraden z používania a zlikvidované. Informačná bezpečnosť by sa mala brať do úvahy v každej fáze. Nové projekty vývoja systému a zmeny v existujúcich systémoch poskytujú príležitosti na zlepšenie bezpečnostných opatrení a zároveň zohľadňujú riziká a ponaučenia organizácie získané z incidentov.

0.6 Life cycle considerations

Information has a life cycle, from creation to disposal. The value of, and risks to, information can vary throughout this life cycle (e.g. unauthorized disclosure or theft of a company's financial accounts is not significant after they have been published, but integrity remains critical) therefore, information security remains important to some extent at all stages.

Information systems and other assets relevant to information security have life cycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be considered at every stage. New system development projects and changes to existing systems provide opportunities to improve security controls while taking into account the organization's risks and lessons learned from incidents.

0.7 Súvisiace medzinárodné normy

Aj keď tento dokument ponúka usmernenie týkajúce sa širokého spektra opatrení informačnej bezpečnosti, ktoré sa bežne uplatňujú v rôznych organizáciách, ďalšie dokumenty z radu noriem ISO/IEC 27000 poskytujú doplňujúce informácie alebo požiadavky na ďalšie aspekty celkového procesu riadenia informačnej bezpečnosti.

Všeobecný úvod do ISMS a príbuzných dokumentov nájdete v ISO/IEC 27000. ISO/IEC 27000 poskytuje slovník, ktorý definuje väčšinu výrazov používaných v rámci dokumentov ISO/IEC 27000 a opisuje predmet a ciele pre každú normu z tohto radu.

Existujú normy špecifické pre odvetvie, ktoré obsahujú ďalšie opatrenia, ktorých cieľom je riešiť konkrétne oblasti (napr. ISO/IEC 27017 pre cloudové služby, ISO/IEC 27701 pre ochranu osobných údajov, ISO/IEC 27019 pre energetický priemysel, ISO/IEC 27011 pre telekomunikačné služby a ISO 277999 pre oblasť zdravotníctva). Takéto normy sú zahrnuté v použitej literatúre a niektoré z nich sú uvedené v usmerneniach a ďalších informačných sekciách v kapitolách 5-8.

0.7 Related International Standards

While this document offers guidance on a broad range of information security controls that are commonly applied in many different organizations, other documents in the ISO/IEC 27000 family provide complementary advice or requirements on other aspects of the overall process of managing information security.

Refer to ISO/IEC 27000 for a general introduction to both ISMS and the family of documents. ISO/IEC 27000 provides a glossary, defining most of the terms used throughout the ISO/IEC 27000 family of documents, and describes the scope and objectives for each member of the family.

There are sector-specific standards that have additional controls which aim at addressing specific areas (e.g. ISO/IEC 27017 for cloud services, ISO/IEC 27701 for privacy, ISO/IEC 27019 for energy, ISO/IEC 27011 for telecommunications organizations and ISO 27799 for health). Such standards are included in the Bibliography and some of them are referenced in the guidance and other information sections in Clauses 5-8.

1 Predmet

Tento dokument poskytuje referenčný súbor všeobecných opatrení informačnej bezpečnosti vrátane návodu na implementáciu. Tento dokument je určený na použitie organizáciami:

a) v kontexte systému riadenia informačnej bezpečnosti (ISMS) založeného na norme ISO/IEC 27001;

b) na implementáciu opatrení informačnej bezpečnosti na základe medzinárodne uznávaných osvedčených postupov;

c) na vypracovanie návodov pre riadenie informačnej bezpečnosti špecifických pre danú organizáciu.

1 Scope

This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

a) within the context of an information security management system (ISMS) based on ISO/IEC 27001;

b) for implementing information security controls based on internationally recognized best practices;

c) for developing organization-specific information security management guidelines.

2 Normatívne odkazy

V tomto dokumente nie sú žiadne normatívne odkazy.

2 Normative references

There are no normative references in this document.