ICS 03.080.99; 35.020;
03.100.70; 35.030

SLOVENSKÁ TECHNICKÁ NORMA

Január 2024

STN	**Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Usmernenie k integrovanej implementácii ISO/IEC 27001 a ISO/IEC 20000-1**	**STN ISO/IEC 27013** 97 4128

Information security, cybersecurity and privacy protection
Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

Sécurité de l'information, cybersécurité et protection de la vie privée
Recommandations pour la mise en oeuvre intégrée de l'ISO/IEC 27001 et de l'ISO/IEC 20000-1

Informationssicherheit, Cybersicherheit und Datenschutz
Leitfaden für die integrierte Einführung von ISO/IEC 27001 und ISO/IEC 20000-1

Táto slovenská technická norma je slovenskou verziou medzinárodnej normy ISO/IEC 27013: 2021.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN ISO/IEC 27013 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the International Standard ISO/IEC 27013: 2021.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN ISO/IEC 27013 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza STN ISO/IEC 27013 z marca 2022 v celom rozsahu.

137683

Národný predhovor

Obrázky v tejto STN sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2021 ISO/IEC, ref. č. ISO/IEC 27013: 2021 E.

Táto norma obsahuje sedem národných poznámok.

Preklad medzinárodnej normy musí získať konsolidovaný význam v obidvoch jazykoch. Nie je vždy možné a žiaduce vykonať preklad odborného kontextu doslovným prekladom, spájaním viet a gramatickými zámenami slov. Z toho dôvodu boli pri preklade tejto medzinárodnej normy použité aj lexikálno-gramatické postupy, najmä explikácia (opisný preklad), s cieľom čo najväčšieho zachovania významovej stránky obsahu za cenu zmien jeho výrazovej stránky za použitia primeraných výrazových prostriedkov.

Špecifické technické výrazy, ktoré sú aj v anglickom jazyku používané len okrajovo, nedáva význam prekladať do slovenského jazyka a uvádzajú sa v pôvodnom tvare.

Niektoré termíny sú predmetom iných noriem, ktoré už boli prevzaté do sústavy STN prekladom. Mnohokrát však chybne. Napríklad anglický termín „biznis“ nie je možné doslovne prekladať ako „obchod“ ani ako „podnikanie“. V oblasti informačnej a kybernetickej bezpečnosti sa tento termín do slovenčiny prekladá vo význame, ktorý je myslený a predpokladaný – a to typicky ako „prevádzka“, alebo „činnosť“.

Termíny uvedené tabuľke v prílohe C nie sú doslovným prekladom normy ISO/IEC 27013: 2021 a z dôvodov zaručenia nadväznosti sú použité novšie, medzičasom opravené slovenské preklady termínov, najmä z STN EN ISO/IEC 27000: 2023 ako aj z STN ISO/IEC 20000-1: 2022.

Vzhľadom na viacnásobný význam niektorých anglických termínov preložených do slovenčiny boli do Tabuľky C.1 – Porovnanie pojmov a definícií medzi ISO/IEC 27000 a ISO/IEC 20000-1 ku slovenskému prekladu termínu pridané anglické ekvivalenty príslušných termínov.

ISO/IEC 27001: 2022 má zásadne zmenenú štruktúru oproti pôvodnej verzii ISO/IEC 27001: 2015 použitej vo verzii normy ISO/IEC 27013: 2021. Preto sa Tabuľka A.1 – Zhoda medzi ISO/IEC 27001 a ISO/IEC 20000-1 ako aj Tabuľka B.1 – Zhoda medzi ISO/IEC 27001: 2013, príloha A, a ISO/IEC 20000-1: 2018 odkazujú na ustanovenia noriem, ktoré sú už medzičasom neplatné. Účelné by bolo uviesť ako samostatnú prílohu prevzatej normy STN tabuľku reálneho mapovania ustanovení platných verzií noriem. Mapovanie preložené v tomto dokumente je oproti platným verziám samozrejme nesprávne, z hľadiska autorských práv je však nutné prekladať normu tak, ako znie jej originál – a tým je ISO/IEC 27013: 2021.

Základným cieľom tejto medzinárodnej normy je venovať sa výhodám paralelného prijatia dvoch medzinárodných noriem pre veľmi úzko súvisiace oblasti – manažérstva informačnej bezpečnosti a manažérstva služieb.

Ako pravopisné zdroje boli pri preklade použité Krátky slovník slovenského jazyka a Slovenský národný korpus zo Slovníkového portálu Jazykovedného ústavu Ľ. Štúra SAV, a terminologické databázy, najmä Terminologický portál Jazykovedného ústavu Ľ. Štúra SAV a Terminologická databáza Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

Normatívne referenčné dokumenty

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 odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek 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 20000-1: 2018 prijatá ako STN ISO/IEC 20000-1: 2022 Informačné technológie. Manažérstvo služieb. Časť 1: Požiadavky na systém manažérstva služieb (36 9788)

ISO/IEC 27000: 2018 prijatá ako STN EN ISO/IEC 27000: 2023 Informačné technológie. Bezpečnostné metódy. Systémy manažérstva informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000: 2018) (97 4170)

ISO/IEC 27001: 2013 prijatá ako STN EN ISO/IEC 27001: 2019, zrušená a nahradená STN EN ISO/IEC 27001: 2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Systémy manažérstva informačnej bezpečnosti. Požiadavky (ISO/IEC 27001: 2022) (97 4171)

Vypracovanie slovenskej technickej normy

Spracovateľ: Ing. Ivan Makatura, CIRISC, CDPSE

Technická komisia: TK 37 Informačné technológie

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia
Usmernenie k integrovanej implementácií ISO/IEC 27001 a ISO/IEC 20000-1

ISO/IEC 27013
Tretie vydanie
2021-11

ICS 03.080.99; 35.020; 03.100.70; 35.030

Obsah

strana

Contents

Predhovor

ISO (medzinárodná organizácia pre normalizáciu) a IEC (Medzinárodná elektrotechnická komisia) tvoria špecializovaný systém celosvetovej normalizície. Národné orgány, ktoré sú členmi ISO alebo IEC, zúčastňujú sa 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 a 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 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 vyhlásení o patentoch IEC (pozri patenty.iec.ch).

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

Vysvetlenie dobrovoľného charakteru noriem, významu špecifických termínov a výrazov týkajúcich sa posudzovania zhody, ako aj informácií 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 IEC si pozrite www.iec.ch/understanding-standards.

Tento dokument vypracovala spoločná technická komisia ISO/IEC JTC 1 *Informačné technológie*, subkomisia 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 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 tretie vydanie ruší a nahrádza druhé vydanie (ISO/IEC 27013: 2015), ktoré bolo technicky revidované. Hlavnou zmenou v porovnaní s predchádzajúcim vydaním je zosúladenie s ISO/IEC 20000-1: 2018.

Zoznam všetkých častí zo série ISO/IEC 27000 možno nájsť na webových stránkach ISO a IEC.

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

This third edition cancels and replaces the second edition (ISO/IEC 27013: 2015), which has been technically revised. The main change compared with the previous edition is the alignment with ISO/IEC 20000-1: 2018.

A list of all parts in the ISO/IEC 27000 series can be found on the ISO and IEC websites.

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

Vzťah medzi riadením informačnej bezpečnosti a riadením služieb je taký blízky, že mnohé organizácie už uznávajú výhody prijatia dvoch medzinárodných noriem pre tieto oblasti: ISO/IEC 27001 pre manažérstvo informačnej bezpečnosti a ISO/IEC 20000-1 pre manažérstvo služieb. Je bežné, že organizácia zlepšuje spôsob svojej činnosti, aby dosiahla zhodu s požiadavkami špecifikovanými v jednej medzinárodnej norme a potom robí ďalšie zlepšenia, aby dosiahla zhodu s požiadavkami inej.

Organizácia má množstvo výhod, pretože zabezpečuje, že jej systém riadenia zohľadňuje životný cyklus služby aj ochranu informácií organizácie. Tieto výhody je možné získať bez ohľadu na to, či je jedna medzinárodná norma implementovaná pred druhou, alebo či sú ISO/IEC 27001 a ISO/IEC 20000-1 implementované súčasne. Predovšetkým riadiace a organizačné procesy môžu ťažiť zo vzájomne sa posilňujúcich koncepcií a podobností medzi týmito medzinárodnými normami a ich spoločnými cieľmi.

Kľúčové výhody integrovanej implementácie manažérstva informačnej bezpečnosti a manažérstva služieb zahŕňajú nasledovné:

a) dôveryhodnosť efektívnych a bezpečných služieb pre interných a externých zákazníkov a iné zainteresované strany organizácie;

Introduction

The relationship between information security management and service management is so close that many organizations already recognize the benefits of adopting the two International Standards for these domains: ISO/IEC 27001 for information security management and ISO/IEC 20000-1 for service management. It is common for an organization to improve the way it operates to achieve conformity with the requirements specified in one International Standard and then make further improvements to achieve conformity with the requirements of another.

There are a number of advantages for an organization in ensuring its management system takes into account both the service lifecycle and the protection of the organization's information. These benefits can be experienced whether one International Standard is implemented before the other, or ISO/IEC 27001 and ISO/IEC 20000-1 are implemented simultaneously. Management and organizational processes, in particular, can derive benefit from the mutually reinforcing concepts and similarities between these International Standards and their common objectives.

Key benefits of an integrated implementation of information security management and service management include the following:

a) credibility to internal and external customers, and other interested parties of the organization, of effective and secure services;

b) nižšie náklady na implementáciu, údržbu a audit integrovaného manažérskeho systému, kde efektívne a účinné manažérstvo služieb a informačnej bezpečnosti je súčasťou stratégie organizácie;

c) skrátenie času implementácie vďaka integrovanému rozvoju procesov podporujúcich manažérstvo služieb aj manažérstvo informačnej bezpečnosti;

d) lepšia komunikácia, zvýšená spoľahlivosť a lepšia prevádzková efektívnosť odstránením zbytočnej duplicity;

e) lepšie pochopenie vzájomných názorov zo strany manažmentu služieb a personálu informačnej bezpečnosti;

f) organizácia certifikovaná pre ISO/IEC 27001 môže ľahšie splniť požiadavky na informačnú bezpečnosť špecifikované v ISO/IEC 20000-1: 2018, 8.7.3, keďže ISO/IEC 27001 a ISO/IEC 20000-1 sa v požiadavkách navzájom dopĺňajú.

Tento dokument je založený na normách ISO/IEC 27001: 2013 a ISO/IEC 20000-1: 2018.

Tento dokument je určený na použitie osobami, ktoré majú v úmysle integrovať ISO/IEC 27001 a ISO/IEC 20000-1 a ktoré poznajú obe, jednu alebo žiadnu z týchto medzinárodných noriem.

Tento dokument nereprodukuje obsah ISO/IEC 27001 alebo ISO/IEC 20000-1. Rovnako nepopisuje komplexne všetky časti každej medzinárodnej normy. Podrobne sú popísané iba tie časti, ktorých predmet sa prekrýva alebo líši. Predpokladá sa, že používatelia tohto dokumentu majú prístup k normám ISO/IEC 20000-1 a ISO/IEC 27001.

POZNÁMKA. – Môžu existovať špecifické právne predpisy, ktoré môžu ovplyvniť plánovanie systému riadenia organizácie.

b) lower cost of implementing, maintaining and auditing an integrated management system, where effective and efficient management of both services and information security are part of an organization's strategy;

c) reduction in implementation time due to the integrated development of processes supporting both service management and information security management;

d) better communication, increased reliability and improved operational efficiency through elimination of unnecessary duplication;

e) a greater understanding by service management and information security personnel of each other's viewpoints;

f) an organization certified for ISO/IEC 27001 can more easily fulfil the requirements for information security specified in ISO/IEC 20000-1: 2018, 8.7.3, as ISO/IEC 27001 and ISO/IEC 20000-1 are complementary in requirements.

This document is based on ISO/IEC 27001: 2013 and ISO/IEC 20000-1: 2018.

This document is intended for use by persons who intend to integrate ISO/IEC 27001 and ISO/IEC 20000-1, and who are familiar with both, either or neither of those International Standards.

This document does not reproduce content of ISO/IEC 27001 or ISO/IEC 20000-1. Equally, it does not describe all parts of each International Standard comprehensively. Only those parts where subject matter overlaps or differs are described in detail. It is assumed that users of this document have access to ISO/IEC 20000-1 and ISO/IEC 27001.

NOTE: Specific legislations can exist, which can impact the planning of an organization's management system.

1 Predmet

Tento dokument poskytuje návod na integrovanú implementáciu ISO/IEC 27001 a ISO/IEC 20000-1 pre organizácie, ktoré majú v úmysle:

a) implementovať ISO/IEC 27001, keď je ISO/IEC 20000-1 už implementovaný, alebo naopak;

b) spoločne implementovať ISO/IEC 27001 aj ISO/IEC 20000-1; alebo

c) integrovať existujúce manažérske systémy založené na ISO/IEC 27001 a ISO/IEC 20000-1.

Tento dokument sa zameriava výlučne na integrovanú implementáciu systému manažérstva informačnej bezpečnosti (ISMS) špecifikovaného v ISO/IEC 27001 a systému manažérstva služieb (SMS) špecifikovaného v ISO/IEC 20000-1.

1 Scope

This document gives guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 for organizations intending to:

a) implement ISO/IEC 27001 when ISO/IEC 20000-1 is already implemented, or vice versa;

b) implement both ISO/IEC 27001 and ISO/IEC 20000-1 together; or

c) integrate existing management systems based on ISO/IEC 27001 and ISO/IEC 20000-1.

This document focuses exclusively on the integrated implementation of an information security management system (ISMS) as specified in ISO/IEC 27001 and a service management system (SMS) as specified in ISO/IEC 20000-1.

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 odkazoch sa použije najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

ISO/IEC 20000-1: 2018 Informačné technológie. Manažérstvo služieb. Časť 1: Požiadavky na systém manažérstva služieb

ISO/IEC 27000: 2018 Informačné technológie. Bezpečnostné metódy. Systémy manažérstva informačnej bezpečnosti. Prehľad a slovník

ISO/IEC 27001: 2013 Informačné technológie. Bezpečnostné metódy. Systémy manažérstva informačnej bezpečnosti. Požiadavky

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 20000-1: 2018, Information technology – Service management – Part 1: Service management system requirements

ISO/IEC 27000: 2018, Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27001: 2013, Information technology – Security techniques – Information security managementsystems – Requirements