ICS 35.040 SLOVENSKÁ TECHNICKÁ NORMA September 2014

STN	**Informačné technológie Bezpečnostné metódy Pravidlá dobrej praxe riadenia informačnej bezpečnosti**	**STN ISO/IEC 27002** 36 9784

Information technology. Security techniques. Code of practice for information security controls

Technologies de l'information. Techniques de sécurité. Code de bonne pratique pour le management de la sécurité de l'information

Informationstechnik. IT-Sicherheitsverfahren. Letfaden für das Informationssicherheits. Management

Táto norma obsahuje slovenskú verziu normy ISO/IEC 27002: 2013.

This standard includes Slovak version of ISO/IEC 27002: 2013.

Nahradenie predchádzajúcich noriem

Táto norma nahrádza normu STN ISO/IEC 27002 z októbra 2006 v celom rozsahu.

119075

Národný predhovor

Vysvetlenie k norme

Pri preklade tejto medzinárodnej normy bolo potrebné prijať niektoré jazykové úpravy, pretože slovenčina a angličtina majú určité špecifické vlastnosti a nie vždy je možné urobiť doslovný preklad, aby mala medzinárodná norma rovnaký význam v obidvoch jazykoch.

V angličtine sa používa výraz „risk management“ v jednotnom čísle, v slovenčine sa dlho používa výraz „riadenie rizík“ v množnom čísle. V jednotnom čísle sa výraz používa, len ak ide o jedno konkrétne riziko.

Anglické slovo „party“ označuje fyzickú alebo právnickú osobu. Rozšírenia ako „external party“, „third party“ a „another party“ sa do slovenčiny prekladajú ako „tretia strana“.

Anglické slová „probability“ a „likelihood“ sú v netechnických vedách synonymá a prekladajú sa ako „pravdepodobnosť“. V štatistike však angličtina výrazom „probability“ umožňuje predpovedať výstup založený na známych parametroch, „likelihood“ určuje neznáme parametre na známych výstupoch. Slovenčina takéto rozdiely nerozlišuje, a preto obidva výrazy sa prekladajú ako „pravdepodobnosť“.

Skratka ISMS (Information Security Management System) sa v niektorej literatúre na Slovensku prekladá ako SMIB (systém manažérstva informačnej bezpečnosti). V tejto medzinárodnej norme sme sa priklonili k neprekladaniu tejto skratky, používa sa ako ISMS, pretože by sme sa zákonite museli dostať do situácie, keď jednu skratku preložíme, inú nie. Z princípov slovenčiny o používaní skratiek a následných možných výkladov sa prikláňame k spôsobu neprekladania skratiek.

Anglický výraz „management“ sa v niektorej literatúre prekladá ako „manažérstvo“. V preklade tejto normy sme sa rozhodli držať logiky a anglický výraz „risk management“ prekladáme ako „riadenie rizík“.

Anglický výraz „Act“ v tabuľke činností PDCA je preložený ako „Zlepšuj“, pretože tento výraz v slovenčine oveľa lepšie zodpovedá prekladu a vykonávaným činnostiam ako v niektorej literatúre používaný výraz „Konaj“.

Anglický výraz „cryptography“ sa prekladá ako kryptografia. Metódy, ktoré používajú kryptografiu, nazývajú sa kryptografické metódy. Anglické kryptografické výrazy „cipher“, „encryption“ a „decryption“ sa prekladajú ako „šifrovanie“. Túto poznámku uvádzame preto, lebo v praxi a na odborných prednáškach sa často stretávame s nevhodným výrazom „kryptovanie“.

V normách a ich anglických textoch sa často používa výraz „documented information“. Aby sa udržala univerzálnosť, tento výraz sa prekladá ako „dokumentovaná informácia“, ale v slovenčine sa tým myslí udržiavaná informácia a v prípade preskúmania predložiteľná, v papierovej alebo elektronickej forme.

Anglický výraz „authentication“ sa veľmi často v praxi prekladá ako „autentifikácia“. Slovenčina pripúšťa tento preklad, ale tiež pripúšťa aj preklad „autentizácia“. Medzi týmito dvoma výrazmi je však v slovenčine rozdiel. Pri autentifikácii ide o jednorazové zavedenie procesu autentizácie do prevádzkového prostredia pri jeho budovaní alebo programovaní. Obdobný význam majú napr. výrazy „elektrifikácia“ alebo „plynofikácia“. Každodenné používanie procesu overenia identity používateľa sa označuje ako autentizácia. V týchto významoch sa výrazy a ich slovenský preklad nachádzajú aj v tejto norme.

V rôznych normách alebo odborných textoch sa vyskytujú rôzne preklady z anglický výrazov „capacity management“, „change management“ a iné zo skupiny IT služieb. V slovenčine sa stretneme napr. s prekladmi „riadenie kapacít“ alebo „manažment kapacít“, príp. „riadenie zmien“ alebo „manažment zmien“. V týchto prípadoch ide o rovnocenný význam výrazov

Citované normy

STN ISO/IEC 27000 zavedená v STN ISO/IEC 27000: 2014 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (36 9789)

Vypracovanie normy

Spracovateľ: RSN Systems, spol. s r. o., Bratislava, Ing. Miloslav Ďurčík, CISA, CRISC

Technická komisia: TK 37 Informačné technológie

Informačné technológie
Bezpečnostné metódy
Pravidlá dobrej praxe riadenia informačnej bezpečnosti

ISO/IEC 27002
Druhé vydanie
2014-02-28

ICS 35.040

Obsah

strana

Predhovor

ISO (Medzinárodná organizácia pre normalizáciu) a IEC (Medzinárodná elektrotechnická komisia) tvoria špecializovaný systém celosvetovej normalizácie. Národné orgány, ktoré sú členmi ISO alebo IEC zúčastňujú sa na tvorbe medzinárodných noriem prostredníctvom technických komisií ustanovených týmito organizáciami pre jednotlivé oblasti technickej činnosti. Technické komisie ISO a IEC vzájomne spolupracujú. S ISO a IEC spolupracujú aj iné medzinárodné vládne alebo mimovládne organizácie. V oblasti informačných technológií ISO a IEC založili spoločnú technickú komisiu ISO/IEC JTC1.

Medzinárodné normy sa navrhujú podľa pravidiel uvedených v smerniciach ISO/IEC, v časti 2.

ISO/IEC 27002 pripravila subkomisia SC 27 Bezpečnostné metódy IT spoločnej komisie ISO/IEC JTC1 Informačné technológie.

Je potrebné venovať pozornosť tej možnosti, že niektoré ustanovenia (časti) tejto normy môžu byť predmetom patentových práv. ISO nie sú zodpovedné za identifikáciu týchto ľubovoľných alebo všetkých patentových práv.

Toto druhé vydanie ruší a nahrádza prvé vydanie (ISO/IEC 27002: 2005), ktoré bolo po technickej stránke revidované.

0 Úvod

0.1 Prostredie a súvislosti

Táto medzinárodná norma je vytvorená pre organizácie, ktoré potrebujú referenciu na výber opatrení v rámci procesov zavádzania systému riadenia informačnej bezpečnosti (ISMS) založeného na norme ISO/IEC 27001[10] alebo ako dokument návodu na zavádzanie všeobecne uznávaných opatrení informačnej bezpečnosti. Táto norma je určená aj na používanie v rozvíjajúcom sa priemysle a v organizáciách so špecifickými návodmi na riadenie informačnej bezpečnosti, ktoré zohľadňujú špecifické prostredie riadenia rizík informačnej bezpečnosti.

Organizácie všetkých typov a veľkostí (vrátane štátneho a súkromného sektora, komerčných alebo neziskových organizácií) zbierajú, spracúvajú, ukladajú a prenášajú informácie v rôznych formách vrátane elektronickej, fyzickej a verbálnej (napr. rozhovory a prednášky).

Hodnota informácií presahuje hodnoty písaného slova, čísel a obrázkov, vedomostí, konceptov, myšlienok a značiek, pričom sú to príklady nedefinovanej hodnoty informácií. V poprepájanom svete sú informácie a príslušné procesy, systémy, siete a osoby zapojené do prevádzky, spracovania a ochrany aktív, tak ako iné významné aktíva podnikania organizácie, a zaslúžia si alebo vyžadujú ochranu pred rôznymi rizikami.

Aktíva sú cieľom tak cielených, ako aj náhodných hrozieb, zatiaľ čo napojené procesy, systémy, siete a ľudia majú základnú zraniteľnosť. Zmeny do obchodných procesov a systémov alebo iné externé zmeny (ako napr. zákony a nariadenia) môžu vyvolať nové riziká informačnej bezpečnosti. Preto pri existencii množstva spôsobov, kde hrozby môžu využiť zraniteľnosť na ohrozenie organizácie, sú riziká informačnej bezpečnosti vždy prítomné. Efektívna informačná bezpečnosť znižuje tieto riziká ochranou organizácie proti hrozbám a zraniteľnosti a znižuje následky na jej aktíva.

Informačná bezpečnosť sa dosahuje implementáciou vhodného súboru opatrení, ktorými môžu byť politiky, procesy, postupy, organizačné štruktúry a softvérové a hardvérové funkcie. Tieto opatrenia je nevyhnutné ustanoviť, implementovať, monitorovať, preskúmavať a zlepšovať tam, kde je to potrebné, aby sa zabezpečilo splnenie špecifických bezpečnostných a podnikateľských zámerov organizácie. ISMS, tak ako sa definuje v norme ISO/IEC 27001,[10] vytvára holistický, koordinovaný pohľad na riziká informačnej bezpečnosti v organizácii s úsilím implementovať súbor

0 Introduction

0.1 Background and context

This International Standard is designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001[10] or as a guidance document for organizations implementing commonly accepted information security controls. This standard is also intended for use in developing industry- and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s).

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

The value of information goes beyond the written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization's business and consequently deserve or require protection against various hazards.

Assets are subject to both deliberate and accidental threats while the related processes, systems, networks and people have inherent vulnerabilities. Changes to business processes and systems or other external changes (such as new laws and regulations) may create new information security risks. Therefore, given the multitude of ways in which threats could take advantage of vulnerabilities to harm the organization, information security risks are always present. Effective information security reduces these risks by protecting the organization against threats and vulnerabilities, and then reduces impacts to its assets.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. An ISMS such as that specified in ISO/IEC 27001[10] takes a holistic, coordinated view of the organization's information security risks in order to implement a comprehensive suite of information security con-

opatrení informačnej bezpečnosti v celkovom rámci, ktorý je koherentný v systéme riadenia.

Mnohé informačné systémy neboli vytvorené a zabezpečené v zmysle požiadaviek normy ISO/IEC 27001[10] a tejto normy. Bezpečnosť, ktorá sa môže dosiahnuť technickými opatreniami, je obmedzená, a preto by sa mala podporovať vhodným riadením a postupmi. Zistenie, ktoré opatrenia je potrebné použiť, vyžaduje starostlivé plánovanie a venovanie pozornosti detailom. Úspešný ISMS vyžaduje podporu všetkých zamestnancov organizácie. Môže sa požadovať aj spolupráca zainteresovaných strán, dodávateľov alebo tretích strán. Môžu byť potrebné aj odporúčania špecialistov tretích strán.

Vo všeobecnejšom význame efektívna informačná bezpečnosť vyžaduje podporu manažmentu a iných zainteresovaných strán, aby aktíva organizácie boli dostatočne zabezpečené a chránené proti škodám a tým pôsobili na zlepšovanie podmienok obchodu.

0.2 Požiadavky informačnej bezpečnosti

Je povinnosťou organizácie, aby zistila svoje bezpečnostné požiadavky. Existujú tri hlavné zdroje požiadaviek bezpečnosti:

a) posúdenie rizík organizácie, pričom sa zoberú do úvahy celoorganizačné obchodné ciele a stratégie; pomocou posúdenia rizík sa identifikujú hrozby na aktíva, zraniteľnosť a vyhodnocuje sa pravdepodobnosť ich výskytu s odhadom ich možných následkov;

b) zákonné, štatutárne, regulačné a zmluvné požiadavky, ktoré musí organizácia, jej obchodní partneri, zmluvní dodávatelia a poskytovatelia služieb splniť, a sociálne a kultúrne prostredie;

c) súbor princípov, cieľov a obchodných požiadaviek na prácu s informáciami, ich spracúvaním, ukladaním, komunikáciou a archivovaním, ktoré organizácia vytvorila na podporu jej prevádzky.

Zdroje vytvorené pri zavádzaní opatrení musia byť v rovnováhe s ohrozeniami obchodných procesov, ako by to vyplynulo z bezpečnostných problémov v prípade absencie týchto opatrení. Výsledok posúdenia rizík napomôže návodom a určeniu vhodných riadiacich aktivít a ich priorít na riadenie rizík informačnej bezpečnosti a na zavedenie opatrení, ktoré sa zvolili na ochranu pred týmito rizikami.

Norma ISO/IEC 27005[11] poskytuje návod na riadenie rizík informačnej bezpečnosti vrátane rád týkajúcich sa posudzovania rizík, ošetrenia rizík,

trols under the overall framework of a coherent management system.

Many information systems have not been designed to be secure in the sense of ISO/IEC 27001[10] and this standard. The security that can be achieved through technical means is limited and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. A successful ISMS requires support by all employees in the organization. It can also require participation from shareholders, suppliers or other external parties. Specialist advice from external parties can also be needed.

In a more general sense, effective information security also assures management and other stakeholders that the organization's assets are reasonably safe and protected against harm, thereby acting as a business enabler.

0.2 Information security requirements

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

a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated;

b) the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, and their sociocultural environment;

c) the set of principles, objectives and business requirements for information handling, processing, storing, communicating and archiving that an organization has developed to support its operations.

Resources employed in implementing controls need to be balanced against the business harm likely to result from security issues in the absence of those controls. The results of a risk assessment will help guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

ISO/IEC 27005[11] provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance,

akceptácie rizík, komunikácie o rizikách, monitorovania rizík a preskúmania rizík.

0.3 Výber opatrení

Opatrenia sa môžu vybrať z tejto normy, z iného súboru opatrení alebo sa môžu vytvoriť úplne nové opatrenia, aby sa splnili špecifické potreby.

Výber opatrení závisí od rozhodnutia organizácie, ktoré je založené na kritériách na akceptovanie rizík, od možností ošetrenia rizík a od všeobecného prístupu k riadeniu rizík, ktorý sa zaviedol v organizácii a mal by byť v súlade so všetkými relevantnými národnými a medzinárodnými zákonmi a nariadeniami. Výber opatrení závisí od spôsobu, akým opatrenia spolupracujú so zavedenou hĺbkovou ochranou.

Niektoré opatrenia uvedené v tejto norme možno považovať za vodiace princípy riadenia informačnej bezpečnosti, aplikovateľné vo väčšine organizácií. Sú detailnejšie vysvetlené ďalej pod nadpisom „Východisko informačnej bezpečnosti". Viac informácií o výbere bezpečnostných opatrení, ako aj o ďalších možnostiach v súvislosti s ošetrovaním rizík možno nájsť v norme ISO/IEC 27005.[11]

0.4 Vytvorenie vlastných návodov

Táto medzinárodná norma sa môže považovať za štartovací bod na vývoj špecifických návodov v organizácii. Nie všetky opatrenia a návody z tohto zoznamu dobrých skúseností sa musia použiť. Môžu sa požadovať dodatočné opatrenia a návody, ktoré nie sú obsiahnuté v tejto norme. Ak sa vytvára dokument, ktorý obsahuje dodatočné návody alebo opatrenia, mohlo by byť užitočné začleniť tabuľku krížových referencií do kapitol tejto normy, ktoré sú použiteľné na dosiahnutie súladu pri kontrole audítormi a obchodnými partnermi.

0.5 Faktory životného cyklu

Informácie majú prirodzený životný cyklus, od vytvorenia cez uloženie, spracúvanie, používanie a prenos až po ich eventuálne zničenie, príp. zostarnutie. Ich hodnota a riziká s nimi spojené môžu kolísať počas ich životného cyklu (napr. neautorizovaným vyzradením alebo krádežou firemných účtovných zložiek, ktorá je oveľa menej významná ako ich zverejnenie), ale informačná bezpečnosť ostáva dôležitá v rozsahu všetkých úrovní.

Informačné systémy majú životný cyklus v rámci toho, ako boli naplánované, špecifikované, navrhnuté, vytvorené, testované, zavedené, používané, udržiavané a zrušené. Informačná bezpečnosť by sa mala venovať každej úrovni. Vývoj nových sys-

risk communication, risk monitoring and risk review.

0.3 Selecting controls

Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate.

The selection of controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations. Control selection also depends on the manner in which controls interact to provide defence in depth.

Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organizations. The controls are explained in more detail below along with implementation guidance. More information about selecting controls and other risk treatment options can be found in ISO/IEC 27005.[11]

0.4 Developing your own guidelines

This International Standard may be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners.

0.5 Lifecycle considerations

Information has a natural lifecycle, from creation and origination through storage, processing, use and transmission to its eventual destruction or decay. The value of, and risks to, assets may vary during their lifetime (e.g. unauthorized disclosure or theft of a company's financial accounts is far less significant after they have been formally published) but information security remains important to some extent at all stages.

Information systems have lifecycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be taken into account

témov a zmeny v existujúcich systémoch vytvárajú príležitosti pre organizáciu aktualizovať a zlepšiť bezpečnostné opatrenia, zohľadňujúc aktuálne incidenty a súčasné a projektované riziká informačnej bezpečnosti.

0.6 Súvisiace normy

Pretože táto norma ponúka návod v širokom rozsahu opatrení informačnej bezpečnosti, ktoré sú všeobecne zavedené v mnohých rozličných organizáciách, zvyšné normy zo súboru noriem ISO/IEC 27000 poskytujú doplňujúce rady alebo požiadavky na iné aspekty celkových procesov riadenia informačnej bezpečnosti.

Všeobecný úvod pre ISMS a súbor noriem riadenia informačnej bezpečnosti poskytuje norma ISO/IEC 27000. Norma ISO/IEC 27000 poskytuje slovník, formálne definovanú väčšinu výrazov, ktoré sa používajú v súbore noriem ISO/IEC 27000 a opisuje rozsah a ciele pre každú normu tohto súboru.

1 Predmet normy

Táto medzinárodná norma poskytuje návod na organizovanie informačnej bezpečnosti a skúsenosti na riadenie informačnej bezpečnosti vrátane výberu, zavedenia a riadenia opatrení, ktoré treba zohľadniť v organizácii v prostredí bezpečnostných rizík.

Táto medzinárodná norma je vytvorená pre organizácie, ktoré majú záujem:

a) vybrať opatrenia v rámci procesov zavedenia riadenia informačnej bezpečnosti podľa normy ISO/IEC 27001[10] ;

b) zaviesť všeobecne platné opatrenia informačnej bezpečnosti;

c) vytvoriť vlastné návody na riadenie informačnej bezpečnosti.

2 Normatívne odkazy

Na nasledujúce dokumenty, v celosti alebo častiach, sú v tomto dokumente vytvorené normatívne odkazy a sú nevyhnutné pre jeho zavedenie. Pri datovaných odkazoch sú relevantné len citované odkazy, pri nedatovaných odkazoch sú relevantné posledné edície z odkazovaného dokumentu (vrátane všetkých príloh).

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

at every stage. New system developments and changes to existing systems present opportunities for organizations to update and improve security controls, taking actual incidents and current and projected information security risks into account.

0.6 Related standards

While this standard offers guidance on a broad range of information security controls that are commonly applied in many different organizations, the remaining standards 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 ISMSs and the family of standards. ISO/IEC 27000 provides a glossary, formally defining most of the terms used throughout the ISO/IEC 27000 family of standards, and describes the scope and objectives for each member of the family.

1 Scope

This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

This International Standard is designed to be used by organizations that intend to:

a) select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001[10];

b) implement commonly accepted information security controls;

c) develop their own information security management guidelines.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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