ICS 01.040.35; 35.040 SLOVENSKÁ TECHNICKÁ NORMA Apríl 2014

STN	**Informačné technológie Bezpečnostné metódy Systémy riadenia informačnej bezpečnosti Prehľad a slovník**	**STN ISO/IEC 27000 36 9789**

Information technology. Security techniques. Information security management systems. Overview and vocabulary

Technologies de l'information. Techniques de sécurité. Systèmes de management de la sécurité de l'information. Vue d'ensemble et vocabulaire

Informationstechnik. Sicherheitsverfahren. Informationssicherheits-Managementsysteme. Überblick und Terminologie

Táto norma obsahuje slovenskú verziu normy ISO/IEC 27000: 2012.

This standard includes the Slovak version of ISO/IEC 27000: 2012.

118557

Národný predhovor

Obrázky v tejto norme sú prevzaté z elektronických podkladov dodaných z ISO, © ISO 2012, ref. č. ISO/IEC 27000: 2012 E.

Poznámky k prekladu

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 medzinárodná norma mala rovnaký význam v obidvoch jazykoch.

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 neprekladať skratky.

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

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

Anglické slová „probability“ a „likelihood“ sú pre netechnické vedy 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 sa obidva výrazy prekladajú ako „pravdepodobnosť“.

Anglický výraz „Act“ v rámci 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“.

Citované normy

EN ISO 9000: 2005 zavedená v STN EN ISO 9000: 2006 Systémy manažérstva kvality. Základy a slovník (ISO 9000: 2005) (01 0300)

ISO Guide 73: 2009 dosiaľ nezavedená

ISO/IEC 15939: 2007 dosiaľ nezavedená

ISO/IEC 27001: 2005 zavedená v STN ISO/IEC 27001: 2006 Informačné technológie. Zabezpečovacie techniky. Systémy manažérstva informačnej bezpečnosti. Požiadavky (36 9789)

ISO/IEC 27002: 2005 zavedená v STN ISO/IEC 27002: 2006 Informačné technológie. Zabezpečovacie techniky. Pravidlá dobrej praxe manažérstva informačnej bezpečnosti (36 9787)

ISO/IEC 27003: 2010 dosiaľ nezavedená

ISO/IEC 27004: 2009 dosiaľ nezavedená

ISO/IEC 27005: 2011 zavedená v STN ISO/IEC 27005: 2012 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti (36 9789)

ISO/IEC 27006: 2011 dosiaľ nezavedená

ISO/IEC 27007: 2011 dosiaľ nezavedená

ISO/IEC TR 27008: 2011 dosiaľ nezavedená

ISO/IEC 27010: 2012 dosiaľ nezavedená

ISO/IEC 27011: 2008 dosiaľ nezavedená

ISO/IEC 27013: 2012 dosiaľ nezavedená

ISO/IEC 27014 2013 dosiaľ nezavedená

ISO/IEC TR 27015: 2012 dosiaľ nezavedená

ISO/IEC DTR 27016 dosiaľ nezavedená

EN ISO 27799: 2008 zavedená v STN EN ISO 27799: 2008 Zdravotnícka informatika. Riadenie informačnej bezpečnosti v zdravotníctve s využitím ISO/IEC 27002 (ISO 27799: 2008) (84 8100)

Vypracovanie normy

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

Technická komisia: TK 37 Informačné technológie

Informačné technológie
Bezpečnostné metódy
Systémy riadenia informačnej bezpečnosti
Prehľad a slovník

ISO/IEC 27000
Druhé vydanie
2012-12-01

ICS 01.040.35; 35.040

Obsah

strana

Predhovor ... 5

0 Úvod ... 5

1 Rozsah ... 7

2 Termíny a definície ... 7

3 Systém riadenia informačnej bezpečnosti ... 20
3.1 Úvod ... 20
3.2 Čo je ISMS? ... 21
3.3 Procesný prístup ... 25
3.4 Prečo je ISMS dôležitý ... 25
3.5 Zriadenie, monitorovanie, udržiavanie a zlepšovanie ISMS ... 27
3.6 Kritické faktory úspechu ISMS ... 31
3.7 Výhody súboru noriem ISMS ... 32

4 Súbor noriem ISMS ... 33
4.1 Všeobecné informácie ... 33
4.2 Normy opisujúce prehľad a terminológiu ... 36
4.3 Normy špecifikujúce požiadavky ... 37
4.4 Normy opisujúce všeobecné smernice ... 38
4.5 Normy opisujúce odvetvovo špecifické smernice ... 41

Príloha A (informatívna) – Slovné tvary pre vyjadrenie nariadení ... 43

Literatúra ... 45

Predhovor

ISO (Medzinárodná organizácia pre normalizáciu) a IEC (Medzinárodná elektrotechnická komisia) vytvárajú 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 spolupracujú v oblastiach spoločného záujmu. S ISO a IEC spolupracujú aj iné medzinárodné vládne a mimovládne organizácie. V oblasti informačných technológií ISO a IEC založili spoločnú technickú komisiu ISO/IEC JTC 1.

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

Hlavnou úlohou spoločnej technickej komisie je príprava medzinárodných noriem. Návrhy medzinárodných noriem prijaté spoločnou technickou komisiou sa rozosielajú národným členom na hlasovanie. Vydanie medzinárodnej normy si vyžaduje súhlas najmenej 75 % hlasujúcich národných členov.

Upozorňuje sa na možnosť, že niektoré časti tohto dokumentu môžu byť predmetom patentových práv. ISO a IEC nezodpovedajú za identifikáciu ktoréhokoľvek ani všetkých takýchto patentových práv.

Normu ISO/IEC 27000 pripravila spoločná technická komisia ISO/IEC JTC 1 *Informačné technológie*, subkomisia SC 27 *Bezpečnostné metódy IT.*

Toto druhé vydanie normy ruší a nahrádza prvé vydanie (ISO/IEC 27000: 2009).

0 Úvod

0.1 Prehľad

Medzinárodné normy pre systémy riadenia poskytujú model, ktorý slúži ako vzor pri zriaďovaní a prevádzke systému riadenia. Tento model zahŕňa vlastnosti, podľa ktorých experti z praxe dosiahli konsenzus ako medzinárodný stav skúseností. Technická komisia ISO/IEC JTC 1 SC 27 udržiava expertnú komisiu venovanú vývoju medzinárodných noriem pre systémy riadenia informačnej bezpečnosti, inak známych ako súbor noriem pre systém riadenia informačnej bezpečnosti (ISMS).

Prostredníctvom používania súboru noriem ISMS môžu organizácie vyvíjať a implementovať rámec pre riadenie bezpečnosti ich informačných aktív vrátane finančných informácií, duševného vlastníctva, detailov o zamestnancoch alebo informácií im zverených od zákazníkov alebo tretích strán. Tieto normy sa môžu používať aj na prípravu nezávislých hodnotení ISMS používaných na ochranu informácií.

0.2 Súbor noriem ISMS

Súbor noriem ISMS[1)] (pozri kapitolu 4) je určený na pomoc organizáciám všetkých typov a veľkostí pri implementácii a prevádzke ISMS. Súbor noriem ISMS pozostáva z nasledujúcich medzinárodných noriem pod všeobecným označením *Informačné technológie – Bezpečnostné metódy:*

ISO/IEC 27000: 2009 *Systémy riadenia informačnej bezpečnosti. Prehľad a slovník*

ISO/IEC 27001: 2005 *Systémy riadenia informačnej bezpečnosti. Požiadavky*

ISO/IEC 27002: 2005 *Pravidlá dobrej praxe riadenia informačnej bezpečnosti*

ISO/IEC 27003: 2010 *Návod na implementáciu systémov riadenia informačnej bezpečnosti*

ISO/IEC 27004: 2009 *Riadenie informačnej bezpečnosti. Meranie*

ISO/IEC 27005: 2011 *Riadenie rizík informačnej bezpečnosti*

ISO/IEC 27006: 2011 *Požiadavky na orgány poskytujúce audit a certifikáciu systémov riadenia informačnej bezpečnosti*

ISO/IEC 27007: 2011 *Smernice na audit systémov riadenia informačnej bezpečnosti*

1) Normy identifikované v tomto článku bez uvedeného roku vydania sú stále vo vývoji.

0 Introduction

0.1 Overview

International Standards for management systems provide a model to follow in setting up and operating a management system. This model incorporates the features on which experts in the field have reached a consensus as being the international state of the art. ISO/IEC JTC 1 SC 27 maintains an expert committee dedicated to the development of international management systems standards for information security, otherwise known as the Information Security Management System (ISMS) family of standards.

Through the use of the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets including financial information, intellectual property, and employees datails, or information entrusted to them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information.

0.2 ISMS family of standards

The ISMS family of standards[1)] (see Clause 4) is intended to assist organizations of all types and sizes to implement and operate an ISMS. The ISMS family of standards consists of the following International Standards, under the general title *Information technology – Security techniques*:

ISO/IEC 27000: 2009, *Information security management systems – Overview and vocabulary*

ISO/IEC 27001: 2005, *Information security management systems – Requirements*

ISO/IEC 27002: 2005, *Code of practice for information security management*

ISO/IEC 27003: 2010, *Information security management system implementation guidance*

ISO/IEC 27004: 2009, *Information security management – Measurement*

ISO/IEC 27005: 2011, *Information security risk management*

ISO/IEC 27006: 2011, *Requirements for bodies providing audit and certification of information security management systems*

ISO/IEC 27007: 2011, *Guidelines for information security management systems auditing*

1) Standards identified throughout this subclause with no release year indicated are still under development.

ISO/IEC TR 27008: 2011 *Smernice pre audítorov na audit opatrení systémov riadenia informačnej bezpečnosti*

ISO/IEC 27010: 2012 *Smernice na riadenie informačnej bezpečnosti pre medziodvetvovú a medziorganizačnú komunikáciu*

ITU-T X.1051 | ISO/IEC 27011: 2008 *Smernice* na *riadenie informačnej bezpečnosti pre telekomunikačné organizácie založené na ISO/IEC 27002*

ISO/IEC FDIS 27013 *Smernice na integrovanú implementáciu ISO/IEC 27001 a ISO/IEC 20000-1*

ITU-T X.1054 | ISO/IEC FDIS 27014 *Governancia informačnej bezpečnosti*

ISO/IEC TR 27015 *Smernice na riadenie informačnej bezpečnosti pre finančné služby*

ISO/IEC WD 27016 *Riadenie informačnej bezpečnosti. Ekonomika v organizáciách*

POZNÁMKA. – Všeobecný názov „*Informačné technológie. Bezpečnostné metódy*“ naznačuje, že tieto normy pripravila spoločná technická komisia ISO/IEC JTC 1 *Informačné technológie,* subkomisia SC 27 *Bezpečnostné metódy IT*.

Medzinárodné normy, ktoré nie sú pod rovnakým všeobecným názvom a sú aj súčasťou súboru noriem ISMS, sú tieto:

ISO 27799: 2008 Zdravotnícka informatika. Riadenie informačnej bezpečnosti v zdravotníctve použitím ISO/IEC 27002

0.3 Účel tejto medzinárodnej normy

Medzinárodná norma poskytuje prehľad systémov riadenia informačnej bezpečnosti a definuje súvisiace pojmy.

POZNÁMKA. – Príloha A poskytuje vysvetlenie, ako sa slovné tvary používajú na vyjadrenie požiadaviek alebo návodov v súbore noriem ISMS.

Súbor noriem ISMS zahŕňa normy, ktoré:

a) definujú požiadavky na ISMS a na tých, ktorí certifikujú takéto systémy;

b) poskytujú priamu podporu, podrobné pokyny alebo interpretáciu pre procesy a požiadavky cyklu Plánuj – Urob – Kontroluj – Zlepšuj (PDCA);

c) riešia smernice pre ISMS špecifické pre jednotlivé odvetvia;

d) riešia posudzovanie zhody ISMS.

ISO/IEC TR 27008: 2011, *Guidelines for auditors on information security management systems controls*

ISO/IEC 27010: 2012, *Information security management guidelines for inter-sector and inter-organisational communications*

ITU-T X.1051 | ISO/IEC 27011: 2008, *Information security management guidelines for telecommunications organisations based on ISO/IEC 27002*

ISO/IEC FDIS 27013, *Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*

ITU-T X.1054 | ISO/IEC FDIS 27014, *Governance of information security*

ISO/IEC TR 27015, *Information security management guidelines for financial services*

ISO/IEC WD 27016, *Information security management – Organisational economics*

NOTE The general title “*Information technology – Security techniques*” indicates that these standards were prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

International Standards not under the same general title that are also part of the ISMS family of standards are as follows:

ISO 27799: 2008, Health informatics – Information security management in health using ISO/IEC 27002

0.3 Purpose of this International Standard

This International Standard provides an overview of information security management systems, and defines related terms.

NOTE Annex A provides clarification on how verbal forms are used to express requirements and/or guidance in the ISMS family of standards.

The ISMS family of standards includes standards that:

a) define requirements for an ISMS and for those certifying such systems;

b) provide direct support, detailed guidance and/or interpretation for the overall Plan-Do-Check-Act (PDCA) processes and requirements;

c) address sector-specific guidelines for ISMS; and

d) address conformity assessment for ISMS.

Termíny a definície uvedené v tejto medzinárodnej norme:

– pokrývajú bežne používané termíny a definície v súbore noriem ISMS;

– nepokryjú všetky termíny a definície používané v rámci súboru noriem ISMS;

– neobmedzujú súbor noriem ISMS v definovaní termínov na vlastné používanie.

The terms and definitions provided in this International Standard:

– cover commonly used terms and definitions in the ISMS family of standards;

– will not cover all terms and definitions applied within the ISMS family of standards; and

– do not limit the ISMS family of standards in defining terms for own use.

1 Rozsah

Táto medzinárodná norma opisuje prehľad a definíciu systémov riadenia informačnej bezpečnosti, ktoré tvoria súbor noriem ISMS, a opisuje príslušné termíny a definície.

Táto medzinárodná norma je použiteľná pre všetky typy organizácií (napr. obchodné spoločnosti, vládne agentúry, neziskové organizácie).

1 Scope

This International Standard describes the overview and the vocabulary of information security management systems, which form the subject of the ISMS family standards, and defines related terms and definitions.

This International Standard is applicable to all types of organization (e.g. commercial enterprises, government agencies, non-profit organizations).