ICS 35.080 SLOVENSKÁ TECHNICKÁ NORMA September 2014

STN	**Informačné technológie Bezpečnostné metódy Systémy riadenia informačnej bezpečnosti Požiadavky**	**STN ISO/IEC 27001 36 9789**

Information technology. Security techniques. Information security management systems. Requirements

Technologies de l'information. Techniques de sécurité. Systèmes de management de la sécurité de l'information. Exigences

Informationstechnik. IT-Sicherheitsverfahren. Informationssicherheits-Managementsysteme. Anforderungen

Táto norma obsahuje slovenskú verziu normy ISO/IEC 27001: 2013.

This standard includes Slovak version of ISO/IEC 27001: 2013.

Nahradenie predchádzajúcich noriem

Táto norma nahrádza normu STN ISO/IEC 27001 z októbra 2006 v celom rozsahu.

119076

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 zdravého rozumu 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“.

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 slovenskom jazyku sa tým myslí udržiavaná informácia a v prípade preskúmania predložiteľná v papierovej alebo elektronickej forme.

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

Technická komisia: TK 37 Informačné technológie

Informačné technológie
Bezpečnostné metódy
Systém riadenia informačnej bezpečnosti
Požiadavky

ISO/IEC 27001
Druhé vydanie
2014-03-31

ICS 35.080

Obsah

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.

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.

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

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

Toto druhé vydanie ruší a nahrádza prvé vydanie (ISO/IEC 27001: 2005), ktoré bolo po technickej stránke revidované.

Úvod

0.1 Všeobecne

Táto medzinárodná norma bola pripravená, aby predložila požiadavky na vytvorenie, zavedenie, údržbu a kontinuálne zlepšovanie systému riadenia informačnej bezpečnosti. Prijatie systému riadenia informačnej bezpečnosti je pre organizáciu strategické rozhodnutie. Vytvorenie a zavedenie systému riadenia informačnej bezpečnosti v organizácii ovplyvňuje potreby a ciele organizácie, bezpečnostné požiadavky, používané procesy v organizácii a veľkosť a štruktúru organizácie. Všetky tieto faktory ovplyvňujú organizáciu a očakáva sa, že sa budú časom meniť.

Systém riadenia informačnej bezpečnosti chráni dôvernosť, integritu a dostupnosť informácií zavedením procesu riadenia rizík a poskytnutím dôvery zainteresovaným stranám, že riziká sú dostatočne riadené.

Je dôležité, že systém riadenia informačnej bezpečnosti je súčasťou procesov organizácie a všetkých riadiacich štruktúr a integrovaný do nich. Informačná bezpečnosť je dôležitá pri vytváraní procesov, informačných systémov a opatrení v organizácii. Očakáva sa, že systém riadenia informačnej bezpečnosti sa bude členiť v súlade s potrebami organizácie.

Táto medzinárodná norma sa môže použiť vnútri organizácie alebo ju môže použiť tretia strana, aby sa dosiahla schopnosť organizácie splniť vlastné požiadavky informačnej bezpečnosti.

Poradie, v ktorom sa požiadavky uvádzajú v tejto norme, neznamenajú poradie ich dôležitosti alebo neurčujú poradie, v akom by sa mali zavádzať. Tieto položky sú číslované len z dôvodu referencií.

Norma ISO/IEC 27000 opisuje prehľad a slovník používaný na riadenie informačnej bezpečnosti, odkazuje na ďalšie normy súboru noriem na riadenie informačnej bezpečnosti (vrátane noriem ISO/IEC 27003,[2] ISO/IEC 27004[3] a ISO/IEC 27005[4]), súvisiace výrazy a definície.

0.2 Kompatibilita s inými normami systémov riadenia

Táto medzinárodná norma zavádza štruktúru vysokej úrovne, rovnaké názvy kapitol, rovnaký text, všeobecné výrazy a základné definície, ako ich definuje príloha SL Nariadenia ISO/IEC, Časť 1, Upravený doplnok ISO, a preto udržiava kompatibilitu s inými normami riadiacich systémov, ktoré sa prijali v prílohe SL.

0 Introduction

0.1 General

This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this International Standard does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This International Standard applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

Všeobecný prístup, ktorý sa definuje v prílohe SL, je užitočný pre také organizácie, ktoré si vyberú pre prevádzku jeden systém riadenia, ktorý spĺňa požiadavky dvoch alebo viacerých noriem systémov riadenia.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

1 Predmet normy

Táto medzinárodná norma špecifikuje požiadavky na vytvorenie, zavedenie, údržbu a stále zlepšovanie systému riadenia informačnej bezpečnosti v kontexte organizácie. Táto medzinárodná norma obsahuje aj požiadavky na posúdenie a ošetrenie rizík informačnej bezpečnosti prispôsobených potrebám organizácie. Požiadavky vymedzené v tejto medzinárodnej norme sú všeobecné a sú určené pre všetky organizácie bez rozdielu typu, veľkosti alebo pôvodu. Nesplnenie niektorej z požiadaviek vymenovaných v kapitolách 4 až 10 nie je akceptovateľné, ak organizácia konštatuje dosiahnutie zhody s touto medzinárodnou normou.

1 Scope

This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this International Standard.

2 Normatívne odkazy

Nasledujúce dokumenty, v celosti alebo po častiach, sú normatívne odkazy, na ktoré sa odkazuje v tomto dokumente, a sú nevyhnutné pre ich zavedenie. Pri datovaných odkazoch sú použiteľné len citované vydania. Pri nedatovaných odkazoch je použiteľné len posledné vydanie odkazovaného dokumentu (vrátane všetkých zmien).

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

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