ICS 03.100.70; 35.030 SLOVENSKÁ TECHNICKÁ NORMA Marec 2023

STN	**Informačné technológie Bezpečnostné metódy Riadenie rizík informačnej bezpečnosti**	**STN ISO/IEC 27005 97 4175**

Information technology
Security techniques
Information security risk management

Technologies de l'information
Techniques de sécurité
Gestion des risques liés à la sécurité de l'information

Informationstechnik
Sicherheitsverfahren
Risikomanagement für Informationssicherheit

Táto slovenská technická norma je slovenskou verziou medzinárodnej normy ISO/IEC 27005: 2018.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN ISO/IEC 27005 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the International Standard ISO/IEC 27005: 2018.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN ISO/IEC 27005 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza STN ISO/IEC 27005 z februára 2012 v celom rozsahu.

136230

Národný predhovor

Obrázky v tejto STN sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2018 ISO/IEC, ref. č. ISO/IEC 27005: 2018 E.

Normatívne referenčné dokumenty

Nasledujúce dokumenty, celé alebo ich časti, sú v tomto dokumente normatívnymi odkazmi a sú nevyhnutné pri jeho používaní. Pri datovaných odkazoch sa použije len citované vydanie. Pri nedatovaných odkazoch sa použije najnovšie vydanie citovaného dokumentu (vrátane všetkých 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 27000 prijatá ako STN EN ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000) (97 4170)

Vypracovanie slovenskej technickej normy

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

Technická komisia: TK 37 Informačné technológie

Informačné technológie
Bezpečnostné metódy
Riadenie rizík informačnej bezpečnosti

ISO/IEC 27005
Tretie vydanie
2018-07

ICS 03.100.70; 35.030

Obsah

Contents

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 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 alebo mimovládne organizácie. V oblasti informačných technológií vytvorili ISO a IEC spoločnú technickú komisiu, ISO/IEC JTC 1.

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. Tento dokument bol vypracovaný podľa edičných pravidiel smernice ISO/IEC, Časť 2 (pozri www.iso.org/directives).

Upozorňuje sa na možnosť, že niektoré 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).

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

Vysvetlenie dobrovoľnej podstaty noriem, význam špecifických termínov a výrazov týkajúcich sa posudzovania zhody, ako aj informácie o väzbe ISO na princípy Svetovej obchodnej organizácie (WTO) uplatňované pri odstraňovaní technických prekážok obchodu (TBT) pozri na www.iso.org/iso/foreword.html.

Tento dokument vypracovala spoločná technická komisia ISO/IEC JTC 1, *Informačné technológie, Podvýbor SC 27, Techniky bezpečnosti IT.*

Akúkoľvek spätná väzba alebo otázky k tomuto dokumentu sa majú adresovať národnému normalizačnému orgánu používateľa. Úplný zoznam týchto orgánov nájdete na adrese www.iso.org/members.html.

Toto tretie vydanie ruší a nahrádza druhé vydanie (ISO/IEC 27005: 2011), ktoré sa technicky zrevidovalo.

Hlavné zmeny v porovnaní s predchádzajúcim vydaním sú tieto:

- všetky priame odkazy na ISO/IEC 27001: 2005 boli odstránené;
- bola pridaná jasná informácia, že tento dokument neobsahuje priame usmernenie k problematike implementácie požiadaviek ISMS špecifikovaných v ISO/IEC 27001 (pozri Úvod);
- ISO/IEC 27001: 2005 bola odstránená z kapitoly 2;
- ISO/IEC 27001 bola pridaná do literatúry;
- príloha G a všetky odkazy na ňu boli odstránené;
- zodpovedajúco boli vykonané redakčné zmeny.

Úvod

Tento dokument poskytuje usmernenia pre riadenie rizík informačnej bezpečnosti v organizácii. Tento dokument však neposkytuje žiadnu konkrétnu metódu riadenia rizík informačnej bezpečnosti. Je na organizácii, aby definovala svoj prístup k riadeniu rizík, napríklad v závislosti od rozsahu systému riadenia informačnej bezpečnosti (ISMS), kontextu riadenia rizík alebo priemyselného odvetvia. Na implementáciu požiadaviek systému ISMS možno v rámci popísanom v tomto dokumente použiť niekoľko existujúcich metodík. Tento dokument vychádza z metódy identifikácie rizík aktív, hrozieb a zraniteľností, ktorá sa už podľa normy ISO/IEC 27001 nevyžaduje. Existujú aj iné prístupy, ktoré sa dajú použiť.

Tento dokument neobsahuje priame usmernenie k problematike implementácie požiadaviek ISMS špecifikovaných v norme ISO/IEC 27001.

Tento dokument je relevantný pre manažérov a zamestnancov, ktorí sa zaoberajú riadením rizík informačnej bezpečnosti v rámci organizácie, a prípadne aj pre externé strany, ktoré tieto činnosti podporujú.

Introduction

This document provides guidelines for information security risk management in an organization. However, this document does not provide any specific method for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of an information security management system (ISMS), context of risk management, or industry sector. A number of existing methodologies can be used under the framework described in this document to implement the requirements of an ISMS. This document is based on the asset, threat and vulnerability risk identification method that is no longer required by ISO/IEC 27001. There are some other approaches that can be used.

This document does not contain direct guidance on the implementation of the ISMS requirements given in ISO/IEC 27001.

This document is relevant to managers and staff concerned with information security risk management within an organization and, where appropriate, external parties supporting such activities.

1 Predmet

Tento dokument poskytuje návod na riadenie rizík informačnej bezpečnosti.

Tento dokument potvrdzuje všeobecné koncepty špecifikované v norme ISO/IEC 27001 a je určený na pomoc pri uspokojivom zavádzaní informačnej bezpečnosti na základe prístupu riadenia rizík.

Pre úplné pochopenie tohto dokumentu je dôležitá znalosť pojmov, modelov, procesov a terminológie opísaných v normách ISO/IEC 27001 a ISO/IEC 27002.

Tento dokument sa vzťahuje na všetky typy organizácií (napr. komerčné podniky, vládne agentúry, neziskové organizácie), ktoré majú v úmysle riadiť riziká, ktoré môžu ohroziť bezpečnosť informácií organizácie.

1 Scope

This document provides guidelines for information security risk management.

This document supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this document.

This document is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that can compromise the organization's information security.

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 odkazov sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

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

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 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*