

STN	Informačné technológie Bezpečnostné metódy Systémy riadenia informačnej bezpečnosti Návod	STN ISO/IEC 27003 36 9794
------------	--	---

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

Technologies de l'information. Techniques de sécurité. Systèmes de management de la sécurité de l'information. Lignes directrices

Informationstechnik. Sicherheitsverfahren. Informationssicherheitsmanagementsysteme. Leitfaden

Táto norma obsahuje anglickú verziu ISO/IEC 27003: 2017.

This standard includes the English version of ISO/IEC 27003: 2017.

126811

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2018

Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii.

Anotácia

Táto norma poskytuje vysvetlenie a rady k systému riadenia informačnej bezpečnosti, ktorý je špecifikovaný normou ISO/IEC 27001: 2013. Poskytuje odporúčania („should“), možnosti („can“) a povolené možnosti („may“), avšak nerozširuje požiadavky, podmienky, či definície systému riadenia informačnej bezpečnosti, ktoré sú primárne určené normami ISO/IEC 27001 a ISO/IEC 27000.

Štruktúra normy v kapitolách 4 až 10 kopíruje štruktúru normy ISO/IEC 27001: 2013 s cieľom jej jednoduchšej aplikovateľnosti a práce s ňou. Každá z týchto kapitol obsahuje požadované aktivity, ich vysvetlenie, návody s podrobnejšími informáciami podporujúcimi implementáciu aktivít s prípadnými príkladmi a ostatné informácie.

Vzhľadom k tomu, že táto norma obsahuje univerzálne a všeobecne použiteľné návody, môže byť ich implementácia zbytočná alebo neprimeraná vzhľadom k veľkosti organizácie, či jej iných špecifik. Je preto potrebné pripomenúť, že ide o súhrn postupov, ktoré sa majú aplikovať primerane, efektívne a zmysluplne tak, aby vznikol funkčný a konzistentný systém bez zjavných slabých miest. Proces realizácie by mal byť uskutočnený v opakovanej postupnosti krokov plánovania, realizácie plánov, overenia realizácie a ich následnej úpravy, či zlepšenia.

Táto norma je základným a všeobecným dokumentom, ktorý je podrobnejšie doplnený konkrétnejšie zameranými normami ako ISO/IEC 27004 a ISO/IEC 27005.

Národný predhovor

Toto druhé vydanie normy ISO/IEC 27003 ruší a nahrádza prvé vydanie (ISO/IEC 27003: 2010), ktoré nebolo prevzaté do sústavy slovenských technických noriem. Pre rýchlejšie prevzatie tejto normy do sústavy STN bol zvolený spôsob prevzatia normy originálom.

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 možno získať na webovej stránke www.unms.sk.

ISO/IEC 27000: 2016 zavedená v STN EN ISO/IEC 27000: 2017 Informačné technológie. Bezpečnostné metódy. Systém riadenia informačnej bezpečnosti. Prehľad a slovník (36 9789)

ISO/IEC 27001: 2013 zavedená v STN ISO/IEC 27001: 2014 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky (36 9789)

Vypracovanie normy

Spracovateľ: DCIT Consulting, organizačná zložka, Ing. Martin Zajíček, CISA, CRISC

Technická komisia: TK 37 Informačné technológie

Contents		Page
Foreword		iv
Introduction		v
1 Scope		1
2 Normative references		1
3 Terms and definitions		1
4 Context of the organization		1
4.1	Understanding the organization and its context	1
4.2	Understanding the needs and expectations of interested parties	3
4.3	Determining the scope of the information security management system	4
4.4	Information security management system	6
5 Leadership		6
5.1	Leadership and commitment	6
5.2	Policy	8
5.3	Organizational roles, responsibilities and authorities	9
6 Planning		10
6.1	Actions to address risks and opportunities	10
6.1.1	General	10
6.1.2	Information security risk assessment	12
6.1.3	Information security risk treatment	15
6.2	Information security objectives and planning to achieve them	18
7 Support		21
7.1	Resources	21
7.2	Competence	22
7.3	Awareness	23
7.4	Communication	24
7.5	Documented information	25
7.5.1	General	25
7.5.2	Creating and updating	27
7.5.3	Control of documented information	28
8 Operation		29
8.1	Operational planning and control	29
8.2	Information security risk assessment	31
8.3	Information security risk treatment	31
9 Performance evaluation		32
9.1	Monitoring, measurement, analysis and evaluation	32
9.2	Internal audit	33
9.3	Management review	36
10 Improvement		37
10.1	Nonconformity and corrective action	37
10.2	Continual improvement	40
Annex A (informative) Policy framework		42
Bibliography		45

ISO/IEC 27003:2017(E)

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition of ISO/IEC 27003 cancels and replaces the first edition (ISO/IEC 27003:2010), of which it constitutes a minor revision.

The main changes compared to the previous edition are as follows:

- the scope and title have been changed to cover explanation of, and guidance on the requirements of, ISO/IEC 27001:2013 rather than the previous edition (ISO/IEC 27001:2005);
- the structure is now aligned to the structure of ISO/IEC 27001:2013 to make it easier for the user to use it together with ISO/IEC 27001:2013;
- the previous edition had a project approach with a sequence of activities. This edition instead provides guidance on the requirements regardless of the order in which they are implemented.

Introduction

This document provides guidance on the requirements for an information security management system (ISMS) as specified in ISO/IEC 27001 and provides recommendations ('should'), possibilities ('can') and permissions ('may') in relation to them. It is not the intention of this document to provide general guidance on all aspects of information security.

[Clauses 4](#) to [10](#) of this document mirror the structure of ISO/IEC 27001:2013.

This document does not add any new requirements for an ISMS and its related terms and definitions. Organizations should refer to ISO/IEC 27001 and ISO/IEC 27000 for requirements and definitions. Organizations implementing an ISMS are under no obligation to observe the guidance in this document.

An ISMS emphasizes the importance of the following phases:

- understanding the organization's needs and the necessity for establishing information security policy and information security objectives;
- assessing the organization's risks related to information security;
- implementing and operating information security processes, controls and other measures to treat risks;
- monitoring and reviewing the performance and effectiveness of the ISMS; and
- practising continual improvement.

An ISMS, similar to any other type of management system, includes the following key components:

- a) policy;
- b) persons with defined responsibilities;
- c) management processes related to:
 - 1) policy establishment;
 - 2) awareness and competence provision;
 - 3) planning;
 - 4) implementation;
 - 5) operation;
 - 6) performance assessment;
 - 7) management review; and
 - 8) improvement; and
- d) documented information.

An ISMS has additional key components such as:

- e) information security risk assessment; and
- f) information security risk treatment, including determination and implementation of controls.

This document is generic and intended to be applicable to all organizations, regardless of type, size or nature. The organization should identify which part of this guidance applies to it in accordance with its specific organizational context (see ISO/IEC 27001:2013, Clause 4).

ISO/IEC 27003:2017(E)

For example, some guidance can be more suited to large organizations, but for very small organizations (e.g. with fewer than 10 persons) some of the guidance can be unnecessary or inappropriate.

The descriptions of Clauses 4 to 10 are structured as follows:

- **Required activity:** presents key activities required in the corresponding subclause of ISO/IEC 27001;
- **Explanation:** explains what the requirements of ISO/IEC 27001 imply;
- **Guidance:** provides more detailed or supportive information to implement “required activity” including examples for implementation; and
- **Other information:** provides further information that can be considered.

ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005 form a set of documents supporting and providing guidance on ISO/IEC 27001:2013. Among these documents, ISO/IEC 27003 is a basic and comprehensive document that provides guidance for all the requirements of ISO/IEC 27001, but it does not have detailed descriptions regarding “monitoring, measurement, analysis and evaluation” and information security risk management. ISO/IEC 27004 and ISO/IEC 27005 focus on specific contents and give more detailed guidance on “monitoring, measurement, analysis and evaluation” and information security risk management.

There are several explicit references to documented information in ISO/IEC 27001. Nevertheless, an organization can retain additional documented information that it determines as necessary for the effectiveness of its management system as part of its response to ISO/IEC 27001:2013, 7.5.1 b). In these cases, this document uses the phrase “Documented information on this activity and its outcome is mandatory only in the form and to the extent that the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b)).”

Information technology — Security techniques — Information security management systems — Guidance

1 Scope

This document provides explanation and guidance on ISO/IEC 27001:2013.

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 27000:2016, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN