ICS 35.030 SLOVENSKÁ TECHNICKÁ NORMA Júl 2024

STN	**Kyberbezpečnosť Vzťahy s dodávateľmi Časť 1: Prehľad a koncepty**	**STN ISO/IEC 27036-1** 97 4131

Cybersecurity
Supplier relationships
Part 1: Overview and concepts

Cybersécurité
Relations avec le fournisseur
Partie 1: Aperçu général et concepts

Cybersecurity
Lieferantenbeziehungen
Teil 1: Überblick und Konzepte

Táto slovenská technická norma obsahuje anglickú verziu medzinárodnej normy ISO/IEC 27036-1: 2021 a má postavenie oficiálnej verzie.

This Slovak standard includes the English version of the International standard ISO/IEC 27036-1: 2021 and has the status of the official version.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza STN ISO/IEC 27036-1 z júna 2021 v celom rozsahu.

138740

Anotácia

Tento dokument je úvodnou časťou ISO/IEC 27036. Poskytuje prehľad návodov určených na pomoc organizáciám pri zabezpečovaní ich informácií a informačných systémov v kontexte dodávateľských vzťahov. Zavádza tiež pojmy, ktoré sú podrobne opísané v iných častiach ISO/IEC 27036. Tento dokument sa zaoberá perspektívami nadobúdateľov aj dodávateľov.

Toto druhé vydanie ruší a nahrádza prvé vydanie (ISO/IEC 27036-1: 2014). Hlavné zmeny v porovnaní s predchádzajúcim vydaním sú nasledovné:

- zmena názvu;
- revízia kapitoly 2;
- zosúladenie s pravidlami navrhovania;
- ISO/IEC 27036 (všetky časti) pridaná do bibliografie.

Väčšina (ak nie všetky) organizácie na celom svete, bez ohľadu na ich veľkosť alebo oblasti činnosti, majú vzťahy s dodávateľmi rôznych druhov, ktorí dodávajú produkty alebo služby.

Takíto dodávatelia môžu mať buď priamy alebo nepriamy prístup k informáciám a informačným systémom nadobúdateľa, alebo poskytnú prvky (softvér, hardvér, procesy alebo ľudské zdroje), ktoré sa budú podieľať na spracovaní informácií. Nadobúdatelia môžu mať aj fyzický a logický prístup k informáciám dodávateľa, keď riadia alebo monitorujú výrobné a dodávateľské procesy dodávateľa.

Nadobúdatelia a dodávatelia si tak môžu navzájom spôsobovať riziká informačnej bezpečnosti. Tieto riziká musia byť hodnotené a ošetrené tak nadobúdateľskými, ako aj dodávateľskými organizáciami prostredníctvom vhodného riadenia informačnej bezpečnosti a implementácie príslušných kontrol. V mnohých prípadoch organizácie prijali normy ISO/IEC 27001 a ISO/IEC 27002 na riadenie svojej informačnej bezpečnosti. Takéto medzinárodné normy by sa mali prijať aj pri riadení dodávateľských vzťahov, aby sa účinne kontrolovali riziká informačnej bezpečnosti, ktoré sú s týmito vzťahmi spojené.

Tento dokument poskytuje ďalšie podrobné implementačné usmernenia týkajúce sa kontrol týkajúcich sa dodávateľských vzťahov, ktoré sú opísané ako všeobecné odporúčania v ISO/IEC 27002.

Dodávateľ aj nadobúdateľ by mali prevziať zodpovednosť za dosiahnutie cieľov vo vzťahu medzi dodávateľom a nadobúdateľom a za primerané riešenie rizík informačnej bezpečnosti, ktoré sa môžu vyskytnúť.

Národný predhovor

Normatívne referenčné dokumenty

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 odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek 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: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

Contents

Page

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27036-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity, and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27036-1:2014), of which this constitutes a minor revision.

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

— change of title;

— revision of Clause 2;

— alignment with drafting rules;

— ISO/IEC 27036 (all parts) added in Bibliography.

A list of all parts in the ISO/IEC 27036 series can be found on the ISO website

Introduction

Most (if not all) organizations around the world, whatever their size or domains of activities, have relationships with suppliers of different kinds that deliver products or services.

Such suppliers can have either a direct or indirect access to the information and information systems of the acquirer, or will provide elements (software, hardware, processes, or human resources) that will be involved in information processing. Acquirers can also have physical and logical access to the information of the supplier when they control or monitor production and delivery processes of the supplier.

Thus, acquirers and suppliers can cause information security risks to each other. These risks need to be assessed and treated by both acquirer and supplier organizations through appropriate management of information security and the implementation of relevant controls. In many instances, organizations have adopted ISO/IEC 27001 and ISO/IEC 27002 for the management of their information security. Such International Standards should also be adopted in managing supplier relationships in order to effectively control the information security risks inherent in those relationships.

This document provides further detailed implementation guidance on the controls dealing with supplier relationships that are described as general recommendations in ISO/IEC 27002.

Supplier relationships in the context of this document include any supplier relationship that can have information security implications, e.g. information technology, healthcare services, janitorial services, consulting services, R&D partnerships, outsourced applications (ASPs), or cloud computing services (such as software, platform, or infrastructure as a service).

Both the supplier and acquirer should take responsibility for achieving the objectives in the supplier-acquirer relationship and adequately addressing the information security risks that can occur. It is expected that they implement the requirements and guidelines of this document. Furthermore, fundamental processes should be implemented to support the supplier-acquirer relationship (e.g. governance, business management, and operational and human resources management). These processes will provide support in terms of information security as well as the accomplishment of business objectives.

INTERNATIONAL STANDARD **ISO/IEC 27036-1:2021(E)**

Cybersecurity — Supplier relationships —

Part 1: Overview and concepts

1 Scope

This document is an introductory part of ISO/IEC 27036. It provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships. It also introduces concepts that are described in detail in the other parts of ISO/IEC 27036. This document addresses perspectives of both acquirers and suppliers.

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*