STN	Kybernetická bezpečnosť Pripravenosť informačných a komunikačných technológií na kontinuitu podnikania	STN ISO/IEC 27031 97 4151

Cybersecurity
Information and communication technology readiness for business continuity

Cybersécurité
Préparation des technologies de l'information et de la communication pour la continuité d'activité

Informationstechnik
Cybersicherheit
Informations- und Kommunikationstechnologische Bereitschaft für Geschäftskontinuität

Táto slovenská technická norma obsahuje anglickú verziu medzinárodnej normy ISO/IEC 27031: 2025 a má postavenie oficiálnej verzie.

This Slovak standard includes the English version of the International standard ISO/IEC 27031: 2025 and has the status of the official version.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza anglickú verziu STN ISO/IEC 27031 z júla 2022 v celom rozsahu.

141410

Anotácia

Tento dokument opisuje koncepty a princípy informačných a komunikačných technológií (IKT) pripravenosti na kontinuitu podnikania. Poskytuje rámec metód a procesov na identifikáciu a špecifikáciu aspektov zlepšenia pripravenosti IKT organizácie na zabezpečenie kontinuity podnikania.

Tento dokument slúži na dosiahnutie nasledujúcich cieľov kontinuity podnikania pre IKT:

- minimálny cieľ kontinuity podnikania (MBCO);
- cieľ bodu obnovy (RPO);
- cieľ času obnovy (RTO) ako súčasť plánovania kontinuity podnikania v oblasti IKT.

Tento dokument sa vzťahuje na všetky typy a veľkosti organizácií. Tento dokument opisuje, ako sa oddelenia IKT plánujú a pripravujú na prispievanie k cieľom odolnosti organizácie.

V priebehu rokov sa informačné a komunikačné technológie (IKT) stali neoddeliteľnou súčasťou mnohých činností v rámci kritických infraštruktúr vo všetkých sektoroch organizácií, či už verejných alebo súkromných. Rozšírenie internetu a iných elektronických sieťových služieb, ako aj schopností systémov a aplikácií, viedlo tiež k tomu, že organizácie sa stali viac závislé od spoľahlivých, bezpečných a zabezpečených IKT infraštruktúr. Medzitým bola uznaná potreba riadenia kontinuity činností (BCM), vrátane pripravenosti na incidenty, plánovania obnovy po havárii a reakcie na núdzové situácie a ich riadenia, a bola podporená rozvojom a schválením špecifických oblastí znalostí, odborných znalostí a noriem, vrátane ISO 22313.

Poruchy služieb IKT, vrátane tých, ktoré sú spôsobené bezpečnostnými problémami, ako je narušenie systémov a infekcie škodlivým softvérom, majú vplyv na kontinuitu obchodných operácií. Riadenie IKT a súvisiacej kontinuity, ako aj ďalších bezpečnostných aspektov, preto tvorí kľúčovú súčasť požiadaviek na kontinuitu podnikania. Navyše, vo väčšine prípadov sú kritické procesy a činnosti, ktoré vyžadujú kontinuitu podnikania, zvyčajne závislé od IKT. Táto závislosť znamená, že narušenia IKT môžu predstavovať strategické riziká pre reputáciu organizácie a jej schopnosť fungovať. Nástup a rastúca dominancia internetových služieb IKT (cloudové služby IKT) spôsobili, že povaha pripravenosti sa zmenila zo spoliehania sa na interné procesy na spoliehanie sa na kvalitu a robustnosť služieb od iných organizácií a súvisiacich obchodných vzťahov s takýmito organizáciami.

Pripravenosť IKT je pre mnohé organizácie základnou zložkou pri implementácii riadenia kontinuity činnosti a riadenia bezpečnosti informácií. V dôsledku toho je účinné BCM často závislé od účinnej pripravenosti IKT, aby sa zabezpečilo, že ciele organizácie môžu byť naďalej plnené aj počas narušení. To je obzvlášť dôležité, pretože dôsledky narušení IKT sú často komplikovanejšie, pretože sú neviditeľné alebo ťažko zistiteľné.

Národný predhovor

Obrázky a matematické výrazy v tejto STN sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2025 ISO/IEC, ref. č. ISO/IEC 27031: 2025 E.

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)

ISO/IEC 27002 prijatá ako STN EN ISO/IEC 27002 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Riadenie informačnej bezpečnosti (ISO/IEC 27002) (97 4172)

ISO/IEC 27005 prijatá ako STN EN ISO/IEC 27005 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Usmernenie k riadeniu rizík informačnej bezpečnosti (ISO/IEC 27005) (97 4175)

ISO/IEC 27035-1: 2023 dosiaľ neprijatá

ISO 22300 prijatá ako STN EN ISO 22300 Ochrana a prispôsobilosť spoločnosti. Terminológia (ISO 22300) (83 0001)

ISO 22301 prijatá ako STN EN ISO 22301 Ochrana spoločnosti. Systémy manažérstva kontinuity podnikania. Požiadavky (ISO 22301) (83 0002)

Vypracovanie

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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document 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 27031:2011), which has been technically revised.

The main changes are as follows:

- the structure of the document has been changed;
- the scope has been changed for clarification;
- technical content has been added in 6.4, 6.5, 6.6, 9.2 and 10.1.5.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Over the years, information and communication technology (ICT) has become an integral part of many of the activities within the critical infrastructures in all organizational sectors, whether public or private. The proliferation of the internet and other electronic networking services, as well as the capabilities of systems and applications, has also resulted in organizations becoming more reliant on reliable, safe and secure ICT infrastructures.

Meanwhile, the need for business continuity management (BCM), including incident preparedness, disaster recovery planning, and emergency response and management, has been recognized and supported with the development and endorsement of specific domains of knowledge, expertise, and standards, including ISO 22313.

Failures of ICT services, including those caused by security issues such as systems intrusion and malware infections, impact the continuity of business operations. Thus, managing ICT and related continuity, as well as other security aspects, form a key part of business continuity requirements. Furthermore, in the majority of cases, the critical processes and activities that require business continuity are usually dependent upon ICT. This dependence means that disruptions to ICT can constitute strategic risks to the reputation of the organization and its ability to operate.

The advent and increasing dominance of Internet-based ICT services (cloud ICT services) has caused the nature of preparedness to change from relying on internal processes to a reliance on the quality and robustness of services from other organizations and the associated business relationships with such organizations.

ICT readiness is an essential component for many organizations in the implementation of business continuity management and information security management.

As a result, effective BCM is frequently dependent upon effective ICT readiness to ensure that the organization's objectives can continue to be met during disruptions. This is particularly important as the consequences of disruptions to ICT often have the added complication of being invisible or difficult to detect.

For an organization to achieve ICT readiness for business continuity (IRBC), it should put in place a systematic process to prevent, predict and manage ICT disruptions and incidents which have the potential to disrupt ICT services. This can be achieved by coordinating IRBC with the information security and BCM processes. In this way, IRBC supports BCM by ensuring that the ICT services can be recovered to pre-determined levels within timescales required and agreed by the organization.

If an organization is using relevant information security and business continuity standards, the establishment of IRBC should preferably take into consideration existing or intended processes linked to these standards. This linkage can support the establishment of IRBC and also avoid any dual processes for the organization.

This document describes the concepts and principles of ICT readiness for business continuity (IRBC) and provides a framework of methods and processes to identify and specify aspects for improving an organization's ICT readiness to ensure business continuity.

This document complements the information security controls relating to business continuity in ISO/IEC 27002. It also supports the information security risk management process specified in ISO/IEC 27005.

Based upon ICT readiness objectives, this document also extends the practices of information security incident management into ICT readiness planning, training and operation.

Cybersecurity — Information and communication technology readiness for business continuity

1 Scope

This document describes the concepts and principles of information and communication technology (ICT) readiness for business continuity (IRBC). It provides a framework of methods and processes to identify and specify aspects for improving an organization's ICT readiness to ensure business continuity.

This document serves the following business continuity objectives for ICT:

- minimum business continuity objective (MBCO),
- recovery point objective (RPO),
- recovery time objective (RTO) as part of the ICT business continuity planning.

This document is applicable to all types and sizes of organizations.

This document describes how ICT departments plan and prepare to contribute to the resilience objectives of the organization.

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*

ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

ISO/IEC 27035-1:2023, *Information technology — Information security incident management — Part 1: Principles and process*

ISO 22300, *Security and resilience — Vocabulary*

ISO 22301, *Security and resilience — Business continuity management systems — Requirements*