ICS 35.040 SLOVENSKÁ TECHNICKÁ NORMA Júl 2022

STN	**Informačné technológie Bezpečnostné metódy Návody pre pripravenosť informačných a komunikačných technológií na zabezpečenie kontinuity činnosti**	**STN ISO/IEC 27031 97 4151**

Information technology
Security techniques
Guidelines for information and communication technology readiness for business continuity

Technologies de l'information
Techniques de sécurité
Lignes directrices pour mise en état des technologies de la communication et de l'information pour continuité des affaires

Informationstechnik
IT-Sicherheitsverfahren
Leitfaden für die Bereitschaft von Informations- und Kommunikationstechnologien für Business Continuity

Táto slovenská technická norma obsahuje anglickú verziu medzinárodnej normy ISO/IEC 27031: 2011 a má postavenie oficiálnej verzie.

This Slovak standard includes the English version of the International Standard ISO/IEC 27031: 2011 and has the status of the official version.

135194

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2022
Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii.

Anotácia

Táto medzinárodná norma opisuje koncepty a princípy pripravenosti informačných a komunikačných technológií (IKT) na kontinuitu podnikania a poskytuje rámec metód a procesov na identifikáciu a špecifikáciu všetkých aspektov (ako sú výkonnostné kritériá, návrh a implementácia) na zlepšenie IKT pripravenosti na zabezpečenie kontinuity podnikania organizácie. Vzťahuje sa na akúkoľvek organizáciu (súkromnú, vládnu a mimovládnu, bez ohľadu na veľkosť), ktorá rozvíja svoj program pripravenosti IKT na kontinuitu podnikania (IRBC) a vyžaduje, aby jej služby/infraštruktúry IKT boli pripravené na podporu obchodných operácií v prípade vzniku udalosti a incidenty a súvisiace prerušenia, ktoré by mohli ovplyvniť kontinuitu (vrátane zabezpečenia) kritických obchodných funkcií. Organizácii tiež umožňuje konzistentným a uznávaným spôsobom merať výkonnostné parametre, ktoré korelujú s jej IRBC.

Rozsah tejto medzinárodnej normy zahŕňa všetky udalosti a incidenty (vrátane bezpečnostných), ktoré by mohli mať vplyv na infraštruktúru a systémy IKT. Zahŕňa a rozširuje postupy riešenia a riadenia incidentov informačnej bezpečnosti a plánovania a služieb pripravenosti IKT.

Národný predhovor

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 27035-1: 2016[1)] prijatá ako STN ISO/IEC 27035-1: 2022 Informačné technológie. Bezpečnostné metódy. Manažment incidentov informačnej bezpečnosti. Časť1: Zásady riadenia incidentov (97 4101)

ISO/IEC 27035-2: 2016[1)] prijatá ako STN ISO/IEC 27035-2: 2021 Informačné technológie. Bezpečnostné metódy. Manažment incidentov informačnej bezpečnosti. Časť 2: Návody na plánovanie a prípravu odozvy na incident (97 4101)

ISO/IEC 27000 prijatá ako STN EN ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000) (36 9789)

ISO/IEC 27001 prijatá ako STN EN ISO/IEC 27001 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky (ISO/IEC 27001) (36 9789)

ISO/IEC 27002 prijatá ako STN EN ISO/IEC 27002 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti (ISO/IEC 27002) (36 9784)

ISO/IEC 27005 prijatá ako STN ISO/IEC 27005 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti (36 9789)

Vypracovanie slovenskej technickej normy

Spracovateľ: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

[1)] ISO/IEC 27035-1 a -2: 2016 nahradili ISO/IEC 27035: 2011, ktorá nahradila ISO/IEC TR 18044: 2004.

Contents

Page

© ISO/IEC 2011 – All rights reserved

© ISO/IEC 2011 – All rights reserved

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 27031 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

© ISO/IEC 2011 – All rights reserved

Introduction

Over the years, information and communication technology (ICT) has become an integral part of many of the activities which are elements of the critical infrastructures in all organizational sectors, whether public, private or voluntary. The proliferation of the Internet and other electronic networking services, and today's capabilities of systems and applications, has also meant that organizations have become ever 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 specific domains of knowledge, expertise, and standards developed and promulgated in recent years, including the BCM International Standard developed by ISO/TC 223.

NOTE ISO/TC 223 is in the process of developing a relevant business continuity management International Standard (ISO 22301).

Failures of ICT services, including the occurrence of security issues such as systems intrusion and malware infections, will impact the continuity of business operations. Thus managing ICT and related continuity and other security aspects form a key part of business continuity requirements. Furthermore, in the majority of cases, the critical business functions 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.

ICT readiness is an essential component for many organizations in the implementation of business continuity management and information security management. As part of the implementation and operation of an information security management system (ISMS) specified in ISO/IEC 27001 and business continuity management system (BCMS) respectively, it is critical to develop and implement a readiness plan for the ICT services to help ensure business continuity.

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

In order for an organization to achieve ICT Readiness for Business Continuity (IRBC), it needs to put in place a systematic process to prevent, predict and manage ICT disruption and incidents which have the potential to disrupt ICT services. This can be best achieved by applying the Plan-Do-Check-Act (PDCA) cyclical steps as part of a management system in ICT IRBC. In this way IRBC supports BCM by ensuring that the ICT services are as resilient as appropriate and can be recovered to pre-determined levels within timescales required and agreed by the organization.

Table 1 — Plan-Do-Check-Act cycle in IRBC

Plan	Establish IRBC policy, objectives, targets, processes and procedures relevant to managing risk and improving ICT readiness to deliver results in accordance with an organization's overall business continuity policies and objectives.
Do	Implement and operate the IRBC policy, controls, processes and procedures.
Check	Assess and, where applicable, measure process performance against IRBC policy, objectives and practical experience, and report the results to management for review.
Act	Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the IRBC.

© ISO/IEC 2011 – All rights reserved

If an organization is using ISO/IEC 27001 to establish an ISMS, and/or using relevant standards to establish a BCMS, 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. Figure 1 summarizes the interaction of IRBC and BCMS.

In the planning and implementation of IRBC, an organization can refer to ISO/IEC 24762:2008 in its planning and delivery of ICT disaster recovery services, regardless of whether or not those services are provided by an outsourced vendor, or internally to the organization.

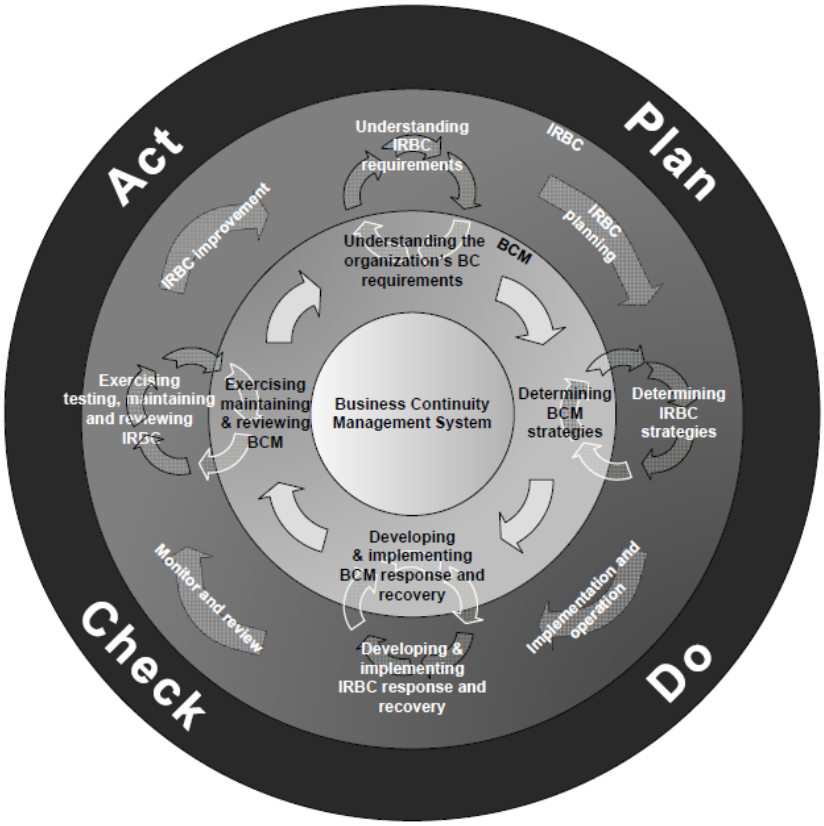

Figure 1 — Integration of IRBC and BCMS

© ISO/IEC 2011 – All rights reserved

INTERNATIONAL STANDARD **ISO/IEC 27031:2011(E)**

Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

1 Scope

This International Standard describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity. It applies to any organization (private, governmental, and non-governmental, irrespective of size) developing its ICT readiness for business continuity (IRBC) program, and requiring its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business functions. It also enables an organization to measure performance parameters that correlate to its IRBC in a consistent and recognized manner.

The scope of this International Standard encompasses all events and incidents (including security related) that could have an impact on ICT infrastructure and systems. It includes and extends the practices of information security incident handling and management and ICT readiness planning and services.

2 Normative references

The following referenced documents are indispensable for the application 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 TR 18044:2004 [1)], *Information technology — Security techniques — Information security incident management*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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

ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN

1) ISO/IEC TR 18044:2004 is to be revised and renumbered as ISO/IEC 27035.

© ISO/IEC 2011 – All rights reserved