

ČESKÁ TECHNICKÁ NORMA

ICS 03.100.01 **Listopad 2013**

Ochrana společnosti – Systémy managementu kontinuity podnikání – Požadavky

ČSN
ISO 22301
01 2306

Societal security – Business continuity management systems – Requirements

Sécurité sociétale – Gestion de la continuité des affaires – Exigences

Tato norma je českou verzí mezinárodní normy ISO 22301:2012. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO 22301:2012. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Souvisící ČSN

ČSN EN ISO 9001 (01 0321) Systémy managementu kvality – Požadavky

ČSN EN ISO 14001 (01 0901) Systémy environmentálního managementu – Požadavky s návodem pro použití

ČSN EN ISO 19011 (01 0330) Směrnice pro auditování systémů managementu

ČSN ISO/IEC 20000-1 (36 9074) Informační technologie – Management služeb – Část 1: Požadavky na systém managementu služeb

ČSN ISO/IEC 27001 (36 9790) Informační technologie – Bezpečnostní techniky – systémy managementu bezpečnostních informací – Požadavky

ČSN ISO 31000 (01 0351) Management rizik – Principy a směrnice

ČSN EN 31010 (01 0352) Management rizik – Techniky posuzování rizik

TNI 01 0350 Management rizik – Slovník (Pokyn 73)

Vysvětlivky k textu převzaté normy

K podpoře správného chápání textu je dále uvedeno vysvětlení překladu výrazů, pro které nebylo v normě možné nalézt zcela výstižný český ekvivalent a mohly by být chápány ve zkresleném nebo

omezeném významu, než je

a. **disruption**

Anglický výraz „*disruption*“, který je klíčovým slovem, vyskytujícím se v normě jako podstatné jméno, ale také ve formě přídavného jména „*disruptive*“ lze překládat mnoha výrazy, jako „rozkol“, „rozpad“, „roztržení“, „rozvrat“, „rozvrácení“ a vyjadřuje podstatu jevu, kvůli kterému je třeba budovat systém managementu kontinuity, byl přeložen jako „narušení“, a následně adjektivum bylo kvůli konzistenci překladu přeloženo jako „rušivý“, přestože význam obou slov je třeba chápat v mnohem hrozivějším významu, protože souvisí s možností zániku organizace.

b. disruptive incident

V normě se vyskytuje spojení „disruptive incident“ velmi často při popisu události, která může vést až ke ztrátě schopnosti organizace realizovat své produkty nebo služby. Výraz „rušivý incident“, který byl v překladu použit, je třeba vnímat jako incident, který může vést k rozpadu nebo zničení organizace.

Vypracování normy

Zpracovatel: Asociace technických bezpečnostních služeb Grémium Alarm, o. s., Centrum technické normalizace pro bezpečnostní služby, IČ 63839911, Ing. Miroslav Urban, Ing. Marie Šebestová

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Svoboda

MEZINÁRODNÍ NORMA

Ochrana společnosti – Systémy managementu kontinuity podnikání – ISO 22301

Požadavky První vydání

2012-05-15

Opravená verze

2012-06-15

ICS 03.100.01

Obsah

Strana

Contents

Page

Předmluva	6
0 Úvod	7
0.1 Obecně	
0.2 Model Plánuj-Dělej-Kontroluj-Jednej (PDCA)	7
0.3 Součásti PDCA v této mezinárodní normě	10
1 Předmět normy	11
2 Citované normativní dokumenty	11
3 Termíny a definice	12
4 Kontext organizace	20
4.1 Porozumění organizaci a jejímu kontextu	20
4.2 Porozumění potřebám a očekáváním zainteresovaných stran	20
4.2.1 Obecně	20
4.2.2 Požadavky zákonů a předpisů	21
4.3 Určení rozsahu systému managementu kontinuity podnikání	21
4.3.1 Obecně	21
4.3.2 Rozsah působnosti BCMS	21
4.4 Systém managementu kontinuity podnikání	22
5 Vedení a řízení lidí	22
5.1 Vedení a řízení lidí a závazek	22
5.2 Závazek managementu	22
5.3 Politika	23
5.4 Role, odpovědnosti a zmocnění v rámci organizace	23
6 Plánování	24
6.1 Činnosti zaměřené na rizika a příležitosti	24
6.2 Cíle kontinuity podnikání a plány jejich dosažení	24
7 Podpora	25
7.1 Zdroje	25
7.2 Kompetence	25
Strana	
7.3 Povědomí	25
7.4 Komunikace	25
7.5 Dokladovatelné informace	26
7.5.1 Obecně	26
7.5.2 Vytváření a aktualizování	26
7.5.3 Řízení dokumentovaných informací	26
8 Provoz	27
8.1 Plánování a řízení provozu	27
8.2 Analýza dopadů na podnikání a posuzování rizik	28
8.2.1 Obecně	28
8.2.2 Analýza dopadů na podnikání	28
8.2.3 Posuzování rizik	28
8.3 Strategie kontinuity podnikání	29
8.3.1 Určení a výběr	29
8.3.2 Ustavování požadavků na zdroje	29
8.3.3 Ochrana a zmírnění následků	30
8.4 Ustavení a implementování postupů pro kontinuitu podnikání	30
8.4.1 Obecně	30
8.4.2 Struktura reakce na incident	30
8.4.3 Varování a komunikace	31
8.4.4 Plány kontinuity podnikání	31
8.4.5 Obnova	34
8.5 Nácvik a zkoušení	33
9 Vyhodnocení výkonnosti	33
9.1 Monitorování, měření, analýza a vyhodnocení	33
9.1.1 Obecně	33
9.1.2 Vyhodnocení postupů kontinuity podnikání	34
9.2 Interní audit	34
9.3 Přezkoumání managementu	35
10 Zlepšování	37
10.1 Neshoda a nápravné opatření	37
10.2 Neustálé zlepšování	37
Bibliografie	38
Obrázek 1 – PDCA model aplikovaný na procesy BCMS	8
Tabulka 1 – Vysvětlení modelu PDCA	8

Foreword	6
0 Introduction	7
0.1 General	7
0.2 The Plan-Do-Check-Act (PDCA) model	7
0.3 Components of PDCA in this International Standard	10
1 Scope	11
2 Normative references	11
3 Terms and definitions	12
4 Context of the organization	20
4.1 Understanding of the organization and its context	20
4.2 Understanding the needs and expectations of interested parties	20
4.2.1 General	20
4.2.2 Legal and regulatory requirements	21
4.3 Determining the scope of the business continuity management system	21
4.3.1 General	21
4.3.2 Scope of the BCMS	21
4.4 Business continuity management system	22
5 Leadership	22
5.1 Leadership and commitment	22
5.2 Management commitment	22
5.3 Policy	23
5.4 Organizational roles, responsibilities and authorities	23
6 Planning	24
6.1 Actions to address risks and opportunities	24
6.2 Business continuity objectives and plans to achieve them	24
7 Support	25
7.1 Resources	25
7.2 Competence	25
Page	
7.3 Awareness	25
7.4 Communication	25
7.5 Documented information	26
7.5.1 General	26
7.5.2 Creating and updating	26
7.5.3 Control of documented information	26
8 Operation	27
8.1 Operational planning and control	27
8.2 Business impact analysis and risk assessment	28
8.2.1 General	28
8.2.2 Business impact analysis	28
8.2.3 Risk assessment	28
8.3 Business continuity strategy	29
8.3.1 Determination and selection	29
8.3.2 Establishing resource requirements	29
8.3.3 Protection and mitigation	30
8.4 Establish and implement business continuity procedures	30
8.4.1 General	30
8.4.2 Incident response structure	30
8.4.3 Warning and communication	31
8.4.4 Business continuity plans	31
8.4.5 Recovery	32
8.5 Exercising and testing	33
9 Performance evaluation	33
9.1 Monitoring, measurement, analysis and evaluation	33
9.1.1 General	33
9.1.2 Evaluation of business continuity procedures	34
9.2 Internal audit	34
9.3 Management review	35
10 Improvement	37
10.1 Nonconformity and corrective action	37
10.2 Continual improvement	37
Figure 1 – PDCA model applied to BCMS processes	9
Table 1 – Explanation of PDCA model	9



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO 2012

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně fotokopíí a mikrofilmů, bez písemného svolení buď od organizace ISO na níže uvedené adrese, nebo od členské organizace ISO v zemi žadatele.

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětovou federací národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle připravují technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodní organizace, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

Mezinárodní normy se navrhují podle pravidel uvedených ve směrnících ISO/IEC, části 2.

Hlavním úkolem technických komisí je tvorba mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členským orgánům k hlasování. Zveřejnění mezinárodní normy vyžaduje schválení alespoň 75 % hlasujících členů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO není odpovědná za identifikování jakýchkoli nebo všech těchto patentových práv.

ISO 22301 byla vypracována Technickou komisí ISO/TC 223, *Ochrana společnosti*.

Do této opravené verze ISO 22301:2012 jsou zapracovány tyto úpravy:

- první seznam v 6.1 byl změněn z číslovaného na nečíslovaný;
- byly přidány uvozovky na konec seznamu v 7.5.3 a 8.3.2;
- bibliografické položky [19] a [20], které byly v původní verzi sloučeny, byly odděleny;
- velikost fontů byla na několika místech upravena.

0 Úvod

0.1 Obecně

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member 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 shall not be held responsible for identifying any or all such patent rights.

ISO 22301 was prepared by Technical Committee ISO/TC 223, *Societal security*.

This corrected version of ISO 22301:2012 incorporates the following corrections:

- first list in 6.1 changed from a numbered to an unnumbered list;
- commas added at the end of list items in 7.5.3 and 8.3.2;
- bibliography items [19] and [20] separated, which were merged in the original;
- font size adjusted in several places.

0 Introduction

0.1 General

V této mezinárodní normě jsou specifikovány požadavky na vytvoření a řízení účinného Systému managementu kontinuity podnikání (BCMS).

BCMS klade důraz na důležitost

- pochopení potřeb organizace a nezbytnosti ustavování politiky a cílů managementu kontinuity podnikání,

implementování kontroly funkčnosti a opatření pro celkové řízení schopnosti organizace zvládat rušivé incidenty,

- monitorování a přezkouvání výkonnosti a efektivnosti BCMS, a neustálého zlepšování založeného na objektivním měření.

BCMS, stejně jako kterýkoli jiný systém managementu, má tyto klíčové součásti:

1. politiku
3. lidi (osoby) s definovanými odpovědnostmi
4. procesy managementu, týkající se
 1. politiky,
 1. plánování,
 3. implementování a provozu
 4. posuzování výkonnosti,
 5. přezkouvání managementu, a
 6. zlepšování;
5. dokumentaci poskytující auditovatelné důkazy; a
6. jakékoliv procesy managementu kontinuity podnikání týkající se organizace

Kontinuita podnikání přispívá ke zvýšení odolnosti společnosti. Širší společenství a dopad prostředí, ve kterém se organizace nachází, na tuto organizaci a proto může být potřeba zapojit další organizace do procesů obnovy.

0.2 Model Plánuj-Dělej-Kontroluj-Jednej (PDCA)

Tato mezinárodní norma využívá model „Plánuj-Dělej-Kontroluj-Jednej“ (PDCA) k plánování, ustavování, implementování, provozování, monitorování, přezkouvání, udržování a kontinuálnímu zlepšování efektivnosti BCMS v organizacích.

To zajišťuje vysokou míru konzistence s dalšími normami pro systémy managementu, jako je ISO 9001, Systémy managementu kvality, ISO 14001, Systémy environmentálního managementu, ISO/IEC 27001, Systémy managementu bezpečnosti informací, ISO/IEC 20 000-1, Informační technologie – *Management služeb*, a ISO 28000, *Specifikace pro systémy managementu bezpečnosti dodavatelského řetězce*, což podporuje její konzistentní a integrovanou implementaci a provozování s příslušnými systémy managementu.

Obrázek 1 ilustruje, jak BCMS přijímá jako vstupy zainteresované strany, požadavky na management kontinuity, a jak prostřednictvím nezbytných působení a procesů vytváří výstupy kontinuity (tj. řízenou kontinuitu podnikání) splňující tyto požadavky.

This International Standard specifies requirements for setting up and managing an effective Business Continuity Management System (BCMS).

A BCMS emphasizes the importance of

understanding the organization's needs and the necessity for establishing business continuity management policy and objectives

implementing and operating controls and measures for managing an organization's overall capability to manage disruptive incidents,

monitoring and reviewing the performance and effectiveness of the BCMS, and

continual improvement based on objective measurement.

A BCMS, like any other management system, has the following key components:

1. a policy
3. people with defined responsibilities
4. management processes relating to
 1. policy,
 1. planning,
 1. implementation and operation,
 1. performance assessment,
 1. management review, and
 1. improvement;
5. documentation providing auditable evidence; and
6. any business continuity management processes relevant to the organization

Business continuity contributes to a more resilient society. The wider community and the impact of the organization's environment on the organization and therefore other organizations may need to be involved in the recovery process.

0.2 The Plan-Do-Check-Act (PDCA) model

This International Standard applies the “Plan-Do-Check-Act” (PDCA) model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving the effectiveness of an organization's BCMS.

This ensures a degree of consistency with other management systems standards, such as ISO 9001, Quality management systems, ISO 14001, Environmental management systems, ISO/IEC 27001, Information security management systems, ISO/IEC 20000-1, Information technology – *Service management*, and ISO 28000, *Specification for security management systems for the supply chain*, thereby supporting consistent and integrated implementation and operation with related management systems.

Figure 1 illustrates how a BCMS takes as inputs interested parties, requirements for continuity management and, through the necessary actions and processes, produces continuity outcomes (i.e. managed business continuity) that meet those requirements.



Obrázek 0A1 - PDCA model aplikovaný na procesy BCMS

Tabulka 1 - Vysvětlení modelu PDCA

Plánování (ustavení BCMS))	Ustavení politiky kontinuity podnikání, dlouhodobých a krátkodobých cílů, opatření, procesů a postupů týkajících se zlepšování kontinuity podnikání tak, aby poskytovaly výsledky, které jsou v souladu s celkovou politikou a cíli organizace.
Provádění (implementace a provoz BCMS)	Implementace a provozování politiky, opatření, procesů a postupů kontinuity podnikání.
Kontrola (monitorování a přezkoumání BCMS)	Monitorování a přezkoumání výkonnosti oproti politice managementu kontinuity podnikání a cílům, hlášení výsledků pro přezkoumání managementu a určení a autorizování činností pro obnovu po narušení a zlepšování.
Činnost (udržování a zlepšování BCMS)	Udržování a zlepšování BCMS přijímáním nápravných opatření založených na výsledcích přezkoumání managementu a přehodnocení rozsahu BCMS včetně politiky a cílů kontinuity podnikání.



Figure 1 - PDCA model applied to BCMS processes

Table 1 - Explanation of PDCA model

Plan (Establish)	Establish business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization's overall policies and objectives.
Do (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMS by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.

0.3 Součásti PDCA v této mezinárodní normě

V modelu Plánuj-Dělej-Kontroluj-Jednej, jak je ukázáno v tabulce 1, jsou jednotlivé části PDCA pojednány v této mezinárodní normě v kapitolách 4 až 10.

- Kapitola 4 je součástí modelu týkající se plánování (Plánuj). Zavádějí se v ní požadavky nezbytné pro ustavení kontextu BCMS, které se vztahují na organizaci, jakož i potřeby, požadavky a rozsah platnosti.

Kapitola 5 je součástí modelu týkající se plánování (Plánuj). Jsou v ní souhrnně uvedeny požadavky specifické pro úlohu vrcholového vedení v rámci BCMS, a jak vedení vyjadřuje svá očekávání pro organizaci prostřednictvím deklarování politiky.

- Kapitola 6 je součástí modelu týkající se plánování (Plánuj). Popisují se v ní požadavky vztahující se k ustavení strategických cílů a základních principů pro BCMS jako celek. V obsahu kapitoly 6 se rozlišuje ustavování příležitostí pro ošetření rizik na základě posouzení rizik, jakož i na základě analýzy dopadů na podnikání (BIA) odvozené od cílů pro obnovu.

POZNÁMKA Požadavky na procesy analýzy dopadu na podnikání a posouzení rizik jsou podrobně pojednány v kapitole 8.

Kapitola 7 je součástí modelu týkající se plánování (Plánuj). Podporuje prováděcí postupy BCMS týkající se ustavení kompetencí a komunikace se zainteresovanými stranami, která se podle potřeby opakuje při dokumentování, řízení, udržování a uchovávání požadované dokumentace.

Kapitola 8 je součástí modelu týkající se implementace a provozování systému (Dělej). Definuje požadavky na kontinuitu podnikání a určuje, jak je uchopit, a rozvíjí postupy pro zvládnutí rušivých incidentů.

0.3 Components of PDCA in this International Standard

In the Plan-Do-Check-Act model as shown in Table 1, Clause 4 through Clause 10 in this International Standard cover the following components.

Clause 4 is a component of Plan. It introduces requirements necessary to establish the context of the BCMS as it applies to the organization, as well as needs, requirements, and scope.

Clause 5 is a component of Plan. It summarizes the requirements specific to top management's role in the BCMS, and how leadership articulates its expectations to the organization via a policy statement.

Clause 6 is a component of Plan. It describes requirements as it relates to establishing strategic objectives and guiding principles for the BCMS as a whole. The content of Clause 6 differs from establishing risk treatment opportunities stemming from risk assessment, as well as business impact analysis (BIA) derived recovery objectives.

NOTE The business impact analysis and risk assessment process requirements are detailed in Clause 8.

Clause 7 is a component of Plan. It supports BCMS operations as they relate to establishing competence and communication on a recurring/as-needed basis with interested parties, while documenting, controlling, maintaining and retaining required documentation.

Clause 8 is a component of Do. It defines business continuity requirements, determines how to address them and develops the procedures to manage a disruptive incident.

Kapitola 9 je součástí modelu týkající se kontroly (Kontroluj). Shrnuje požadavky nezbytné k měření výkonnosti managementu kontinuity podnikání, shody BCMS s touto mezinárodní normou a očekáváním managementu, a usiluje o zpětnou vazbu managementu ohledně jeho očekávání.

- Kapitola 10 je součástí modelu týkající se udržování a zlepšování BCMS (Jednej). Identifikuje neshody BCMS a způsoby vypořádání prostřednictvím nápravných opatření.

Ochrana společnosti – Systémy managementu kontinuity podnikání – Požadavky

1 Předmět normy

V této mezinárodní normě pro management kontinuity podnikání jsou specifikovány požadavky pro plánování, ustavení, implementaci, provozování, monitorování, přezkoumávání, udržování a kontinuální zlepšování dokumentovaného systému managementu k ochraně před rušivými incidenty, snižování pravděpodobnosti jejich výskytu, přípravě, reagování, a obnově, pokud se vyskytnou.

Požadavky uvedené v této mezinárodní normě jsou obecné povahy a mají být použitelné pro všechny organizace nebo jejich části, bez ohledu na typ, velikost a typ organizace. Rozsah použití těchto požadavků závisí na prostředí, ve kterém se organizace pohybuje, a na její složitosti.

Záměrem této mezinárodní normy není zavádět jednotnost struktury systému managementu kontinuity podnikání (BCMS), ale navrhnout pro organizaci systém BCMS, který odpovídá jejím potřebám, a který splňuje požadavky jejich zainteresovaných stran. Tyto potřeby jsou formovány právními, správními, organizačními a průmyslovými požadavky, výrobky a službami, používanými procesy, velikostí a strukturou organizace a požadavky zainteresovaných stran.

Tuto mezinárodní normu lze použít pro všechny typy a velikosti organizací, které chtějí

stanovit, implementovat, udržovat a zlepšovat BCMS,

1. zajistit shodu se stanovenou politikou kontinuity podnikání,

1. prokázat shodu s ostatními,

1. usilovat o certifikaci/registraci svého systému BCMS akreditovaným certifikačním orgánem, třetí stranou, nebo

1. z vlastního rozhodnutí učinit prohlášení o shodě s touto mezinárodní normou.

Tato mezinárodní norma může být použita k posouzení schopnosti organizace splňovat vlastní potřeby kontinuity a z ní vyplývající závazky.

Clause 9 is a component of Check. It summarizes requirements necessary to measure business continuity management performance, BCMS compliance with this International Standard and management's expectations, and seeks feedback from management regarding expectations.

Clause 10 is a component of Act. It identifies and acts on BCMS non-conformance through corrective action.

Societal security – Business continuity management systems – Requirements

1 Scope

This International Standard for business continuity management specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

The requirements specified in this International Standard are generic and intended to be applicable to all organizations or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity.

It is not the intent of this International Standard to imply uniformity in the structure of a Business Continuity Management System (BCMS), but for an organization to design a BCMS that is appropriate to its needs and that meets its interested parties' requirements. These needs are shaped by legal, regulatory, organizational and industry requirements, the products and services, the processes employed, the size and structure of the organization, and the requirements of its interested parties.

This International Standard is applicable to all types and sizes of organizations that wish to

1. establish, implement, maintain and improve a BCMS,

3. ensure conformity with stated business continuity policy,

4. demonstrate conformity to others,

5. seek certification/registration of its BCMS by an accredited third party certification body, or

6. make a self-determination and self-declaration of conformity with this International Standard.

This International Standard can be used to assess an organization's ability to meet its own continuity needs and obligations.

Konec náhledu - text dále pokračuje v placené verzi ČSN.