ICS 03.100.01 PREDBEŽNÁ SLOVENSKÁ TECHNICKÁ NORMA August 2021

STN P	**Ochrana spoločnosti Systémy riadenia kontinuity podnikania Návod na analýzu vplyvov na podnikanie (BIA)**	**STN P ISO/TS 22317** 97 4140

Societal security
Business continuity management systems
Guidelines for business impact analysis (BIA)

Sécurité sociétale
Systèmes de management de la continuité en affaires
Lignes directrices pour l'analyse d'impact en affaires

Sicherheit und Schutz des Gemeinwesens
Business Continuity Management Systems
Richtlinien für die Business Impact Analyse (BIA)

Táto norma obsahuje anglickú verziu ISO/TS 22317: 2015.

This standard includes the English version of ISO/TS 22317: 2015.

133067

Anotácia

Táto technická špecifikácia poskytuje organizácii návod na vytvorenie, implementáciu a údržbu procesu formálnej a dokumentovanej analýzy dopadov na podnikanie (BIA). Táto technická špecifikácia nepredpisuje jednotný postup vykonávania BIA, ale pomôže organizácii navrhnúť proces BIA, ktorý zodpovedá jej potrebám.

Táto technická špecifikácia je použiteľná pre všetky organizácie bez ohľadu na typ, veľkosť a povahu, či už v súkromnom, verejnom alebo neziskovom sektore. Poradenstvo je možné prispôsobiť potrebám, cieľom, zdrojom a obmedzeniam organizácie.

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 možno získať na webovej stránke www.unms.sk.

ISO 22300 zavedená v STN EN ISO 22300 Ochrana a prispôsobilosť spoločnosti. Terminológia (ISO 22300) (83 0001)

Vypracovanie 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) 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.

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 ISO documents 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 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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 292, *Security and resilience*.

Introduction

This Technical Specification provides detailed guidance for establishing, implementing, and maintaining a business impact analysis (BIA) process consistent with the requirements in ISO 22301. This Technical Specification is applicable to the performance of any BIA process, whether part of a business continuity management system (BCMS) or business continuity programme (BC programme). Hereinafter, BC programme means either BCMS or BC programme.

Figure 1 notes the relationship of the BIA process to the BC programme as a whole. The organization should complete a cycle of the BIA process before business continuity strategies are selected.

Figure 1 — Elements of business continuity management (Source: ISO 22313)

The BIA process analyses the consequences of a disruptive incident on the organization. The outcome is a statement and justification of business continuity requirements.

The BIA process consists of a number of individual BIAs, each focusing of a sub-set of the BC programme scope. The BIA process prioritizes products and services, and continues with prioritizing processes and activities that together cover the entire scope of the BC programme. After a period of time determined by the organization, individual BIAs are repeated to ensure that the BC requirements remain current.

NOTE In this Technical Specification, business continuity requirements has the same meaning as continuity and recovery priorities, objectives, and targets (ISO 22301:2012, 8.2.2).

The purposes of this Technical Specification are the following:

— provide a basis for understanding, developing, implementing, reviewing, maintaining, and continually improving an effective BIA process within an organization;

— provide guidance for planning, conducting, and reporting on a BIA;

— assist the organization with conducting a BIA in a consistent manner that reflects good practices;

— enable proper coordination between the BIA process and the overarching BC programme.

The outcomes of the BIA process include the following:

— endorsement or modification of the organization's BC programme scope;

— identification of legal, regulatory, and contractual requirements (obligations) and their effect on business continuity requirements;

— evaluation of impacts on the organization over time, which serves as the justification for business continuity requirements (time and capability);

— identification and confirmation of product/service delivery requirements following a disruptive incident, which then sets the prioritized timeframes for activities and resources;

— identification and establishment of the relationships between products/services, processes, activities, and resources;

— determination of the resources needed to perform prioritized activities (e.g. facilities; people; equipment; information, communication and technology assets; supplies; and financing);

— understanding of the dependencies on other activities, supply chains, partners, and other interested parties;

— determination of how up to date the information needs to be.

NOTE For purposes of this Technical Specification, supply chains produce supplies of goods, works, and services, which are referred to as 'supplies' throughout the remainder of this document.

The following diagram displays the BIA process, together with prerequisites and its relationship to strategy identification. The clauses referenced in the diagram are subsections of this Technical Specification.

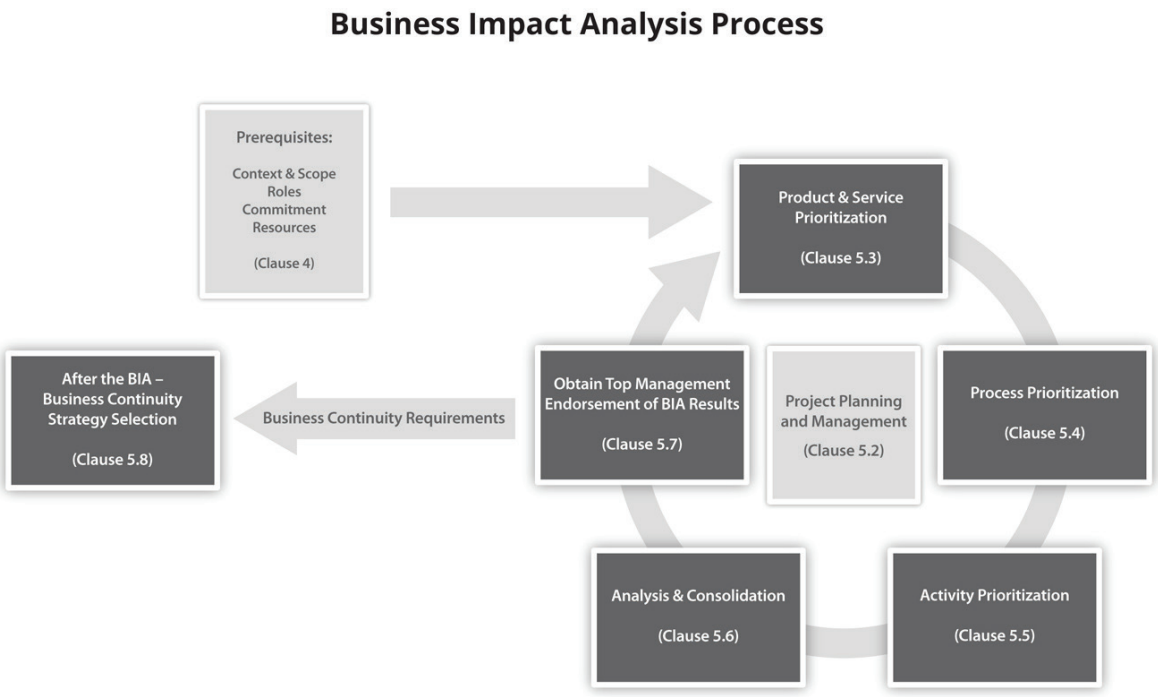

Figure 2 — Business impact analysis process

TECHNICAL SPECIFICATION ISO/TS 22317:2015(E)

Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)

1 Scope

This Technical Specification provides guidance for an organization to establish, implement, and maintain a formal and documented business impact analysis (BIA) process. This Technical Specification does not prescribe a uniform process for performing a BIA, but will assist an organization to design a BIA process that is appropriate to its needs.

This Technical Specification is applicable to all organizations regardless of type, size, and nature, whether in the private, public, or not-for-profit sectors. The guidance can be adapted to the needs, objectives, resources, and constraints of the organization.

It is intended for use by those responsible for the BIA process.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Societal security — Terminology*