PD ISO/TS 22317:2015

BSI Standards Publication

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

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of ISO/TS 22317:2015.

The UK participation in its preparation was entrusted by Technical Committee CAR/1, Continuity and Resilience, to Panel CAR/1/-/11, Business Impact Analysis.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2015

ISBN 978 0 580 86367 7
ICS 03.100.01

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2015.

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/TS 22317:2015

TECHNICAL SPECIFICATION

ISO/TS 22317

First edition
2015-09-15

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

Reference number
ISO/TS 22317:2015(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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.

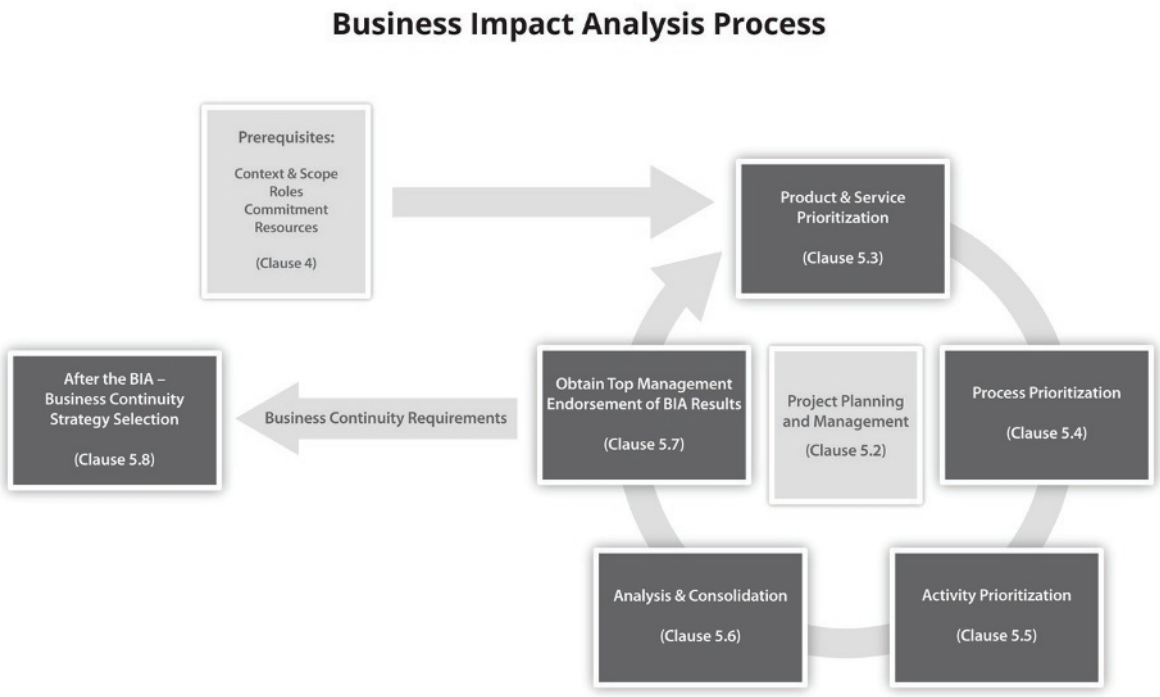

Figure 2 — Business impact analysis process

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions in ISO 22300 apply.

NOTE All terms and definitions contained in ISO 22300 are available on the ISO Online Browsing Platform: www.iso.org/obp.

4 Prerequisites

4.1 General

As noted in the Introduction, this Technical Specification is consistent with ISO 22301, but it could be used to develop, implement, review, maintain, and continually improve a BIA process addressing other standards or regulatory requirements. Whether part of a BCMS or a BC programme, the organization should consider a number of prerequisites before starting the BIA process. Clause 4 summarizes these prerequisites, many of which are from ISO 22301.

The organization should take a number of steps within the BC programme before beginning the BIA process, which include the following:

— define the context and scope (4.2);

— define and communicate roles and responsibilities (4.3);

— obtain leadership commitment (4.4);

— allocate adequate resources (4.5).

NOTE For additional information, see Annex A for a mapping of each step to ISO 22301.