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)

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.

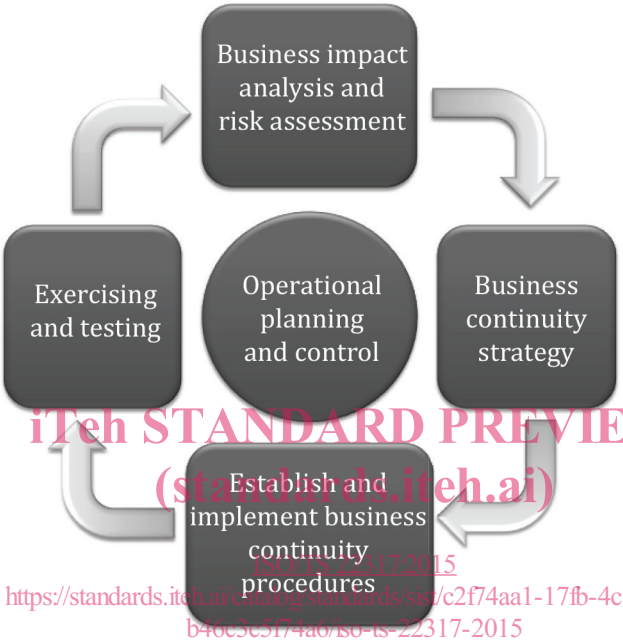

Figure 1 — Elements of business continuity management (Source: ISO 22313)

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.

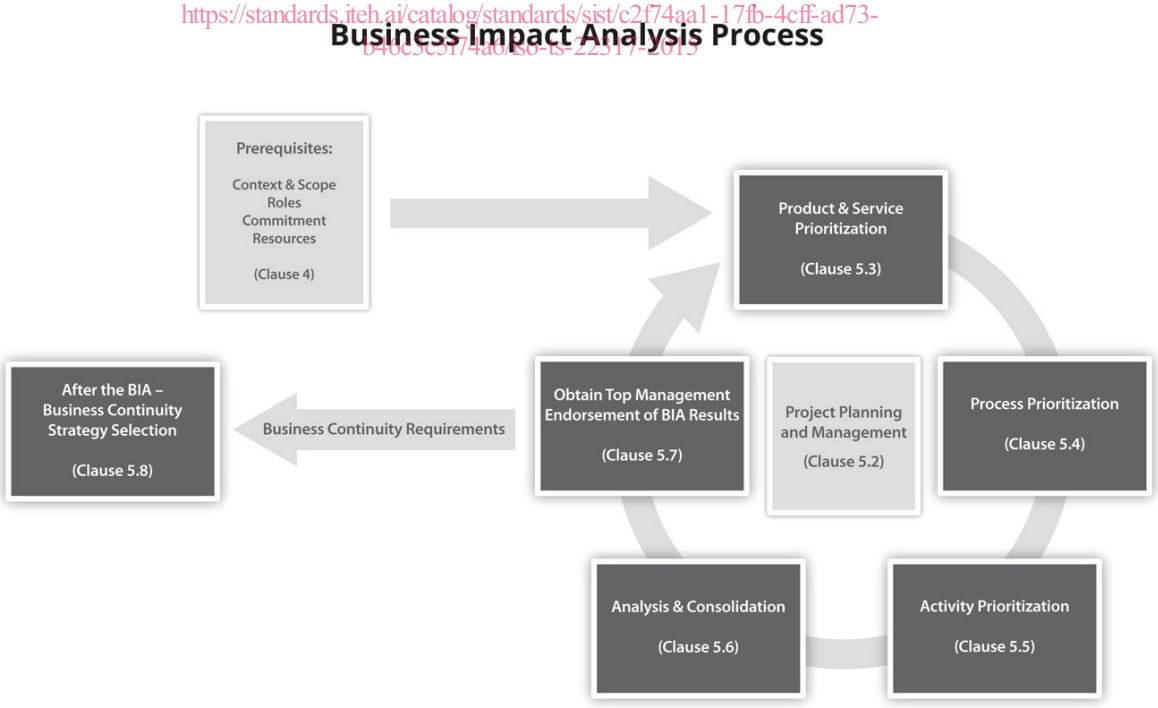

Figure 2 — Business impact analysis process

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.

4.2 BC programme context and scope

4.2.1 BC programme context

Successful BIA process outcomes are dependent on the organization understanding the following:

— the external environment in which it operates so that it can achieve its purpose by delivering its products and services to customers;

— the internal operating environment, inclusive of processes, activities, and resources, as well as the potential impact caused by disrupting the delivery of products and services; and

— laws and regulations mandating the BIA process and how it is performed.

NOTE In organizations operating within a non-commercial environment, the 'customer' can be the public or an overseeing authority, such as government.

4.2.2 Scope of the BC programme

Before determining the BIA process scope, the organization should define and document the scope of the BC programme in terms of its products and services.

The BIA process may assist the organization to review the scope of the BC programme.

Following the definition of the BC programme scope, the organization can determine the BIA process scope which may be conducted as a single BIA to cover the whole scope of the BC programme; or undertaken in a number of phases that, over time, covers the whole scope of the BC programme.

NOTE If the organization chooses to undertake the BIA process in phases, it should first determine the prioritization of all products and services (see 5.2) and then continue with the remaining individual BIAs.

4.3 BC programme roles

4.3.1 BC programme roles and responsibilities

Prior to performing the BIA process, top management should ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

4.3.2 BIA process-specific roles and competencies

Following the assignment of BC programme roles, top management should provide resources necessary to perform the BIA process, which may include appointing the following roles:

— the person sponsoring the BIA process;

— BIA steering committee;

— the person leading the BIA process;

— the person managing the BIA project (project manager);

— process owners;

— activity managers.

The person sponsoring the BIA process should

— be an executive representing top management,

— be well respected within the organization by other members of top management,

— have an organization-wide perspective,

— have the authority to commit the organization to action, and

— make final decisions regarding the BIA process.

The BIA steering committee should

— represent top management,

— provide ongoing advice and guidance on the conduct of the BIA process,

— agree on the methods and outcomes,

— make decisions regarding business continuity requirements, and

— assist the person leading the BIA process and project manager in determining the competences required for BIA process-specific roles and responsibilities and the awareness, knowledge, understanding, skills, and experience needed to fulfil them.

The person leading the BIA process should

— have an understanding of the organization, in particular products, services, processes, and activities, and

— have experience in conducting a BIA process.

The person managing the BIA project should

— plan for and manage the BIA process,

— have an understanding of project planning tasks, and

— be familiar with the BIA process.

Process owners should have a relatively detailed understanding of the process they represent in order to assist the project manager in identifying subject matter experts, organizational units, and impacts of downtime.

Activity managers should

— have very detailed understanding of the activity in which they represent, including all of the resources that enable the activity to operate, and

— be aware of alternate processes and resources that could be available in the event of a loss of primary resources.

NOTE In smaller organizations, these roles can be combined.

The organization should ensure the competence of persons leading or participating in the BIA process. Competences should include skills and abilities related to the following:

— project/programme planning and management;

— information gathering;

— analysis;

— effective communication and collaboration;

— translating organizational objectives to business continuity requirements and resource needs;

— applying BIA concepts in the specific organization's context;

— knowledge of the organization, its products and services, processes, activities, and resources.

4.4 BC programme commitment

Top management commitment to the BIA process is necessary to ensure effective participation. To obtain this support, the organization may consider communicating the BIA process' value that includes the following:

— ensuring the appropriate and most cost effective strategies are selected by determining the correct business continuity requirements;

— providing evidence to management that business continuity requirements align with organizational objectives;

— ensuring the organization meets its legal, contractual, and customer requirements during a disruptive incident;

— identifying linkages between products and services and process, activities, and resources;

— providing an overview of the organization that can be used to improve its efficiency or explore new opportunities (see Annex D).

4.5 BC programme resources

The organization should provide resources to the BIA process that are sufficient to the following:

— achieve its BC policy and objectives;

— make adequate provision for people and people-related resources, including the time to fulfil BIA process-specific roles and responsibilities, and training and awareness;

— meet the changing requirements of the organization;

— provide for ongoing operation and continual improvement of the BC programme, as well as the BIA process.

5 Performing the business impact analysis

5.1 General

The BIA process prioritizes the various organizational components so that product and service delivery can be resumed in a predetermined timeframe following a disruptive incident to the satisfaction of interested parties. For purposes of this Technical Specification and consistent with ISO 22301, products and services are created by processes that are made up of activities.

The products and services are prioritized first; this sets the time and service level parameters for process prioritization. If required by the complexity of the organization, the processes can then be separated into their constituent activities for prioritization.

Suitable, adequate, and effective outcomes of subsequent phases of the BC programme depend on the accuracy of the BIA process. Each BIA should be completed consistently, carefully, and thoroughly.

Figure 3 shows how the various elements of the BIA process relate to each other. The diagram illustrates that there can be overlap between the timing of these constituent phases of the process.

