TECHNICAL SPECIFICATION

ISO/TS 22317

Second edition
2021-11

Security and resilience — Business continuity management systems — Guidelines for business impact analysis

Sécurité et résilience — Systèmes de management de la continuité d'activité — Lignes directrices pour l'analyse d'impact sur l'activité

Reference number
ISO/TS 22317:2021(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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 of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

This second edition cancels and replaces the first edition (ISO/TS 22317:2015), which has been technically revised. The main changes are as follows:

— the document has been updated to align with ISO 22301:2019;

— the document structure has been updated to improve the description of the business impact analysis (BIA) process;

— more focus has been placed on the BIA process and less on the business continuity programme;

— BIA and the BIA process have been clearly differentiated;

— BIA process roles have been consolidated to BIA leader and activity owners;

— the section "Initial BIA considerations" has been removed and the guidance redistributed;

— the section "Strategy selection" has been removed as it is part of ISO/TS 22331;

— the annex on terminology has been removed;

— the annex on BIA information collection methods has been enhanced;

— a new annex with examples for performing a BIA has been included.

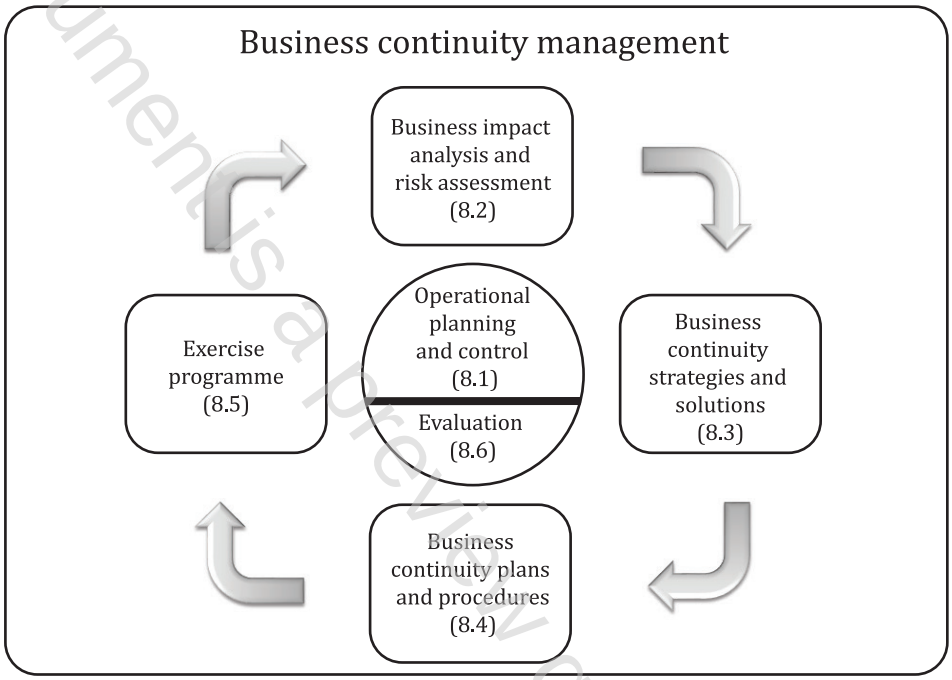
Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document provides detailed guidelines for implementing and maintaining a business impact analysis (BIA) process consistent with ISO 22301. This document is applicable to the performance of any BIA process.

The terminology used is consistent with ISO 22300 and ISO 22301, but an organization can use different terms provided they are clearly understood.

Figure 1 notes the relationship of the BIA process to the business continuity management system (BCMS) as a whole. The organization should complete a cycle of the BIA process before business continuity strategies and solutions are selected.



NOTE Source: ISO 22313:2020, Figure 5.

Figure 1 — Elements of business continuity management

The BIA process analyses the effects of a disruption on the organization. The outcome is a statement and justification of business continuity priorities and requirements.

The first step in the BIA is the prioritization of products and services, which is followed by a number of process BIAs (optional) and activity BIAs. The scope of each of these BIAs can be limited, but together they should cover the entire BCMS scope. Organizations should review and perform the BIA process on a periodic basis (e.g. annually) and whenever there are significant changes within the organization or its context.

In this document, the terms “BIA” and “BIA process” are used as well as “result” and “outcome”. Figure 2 depicts how these terms are used.

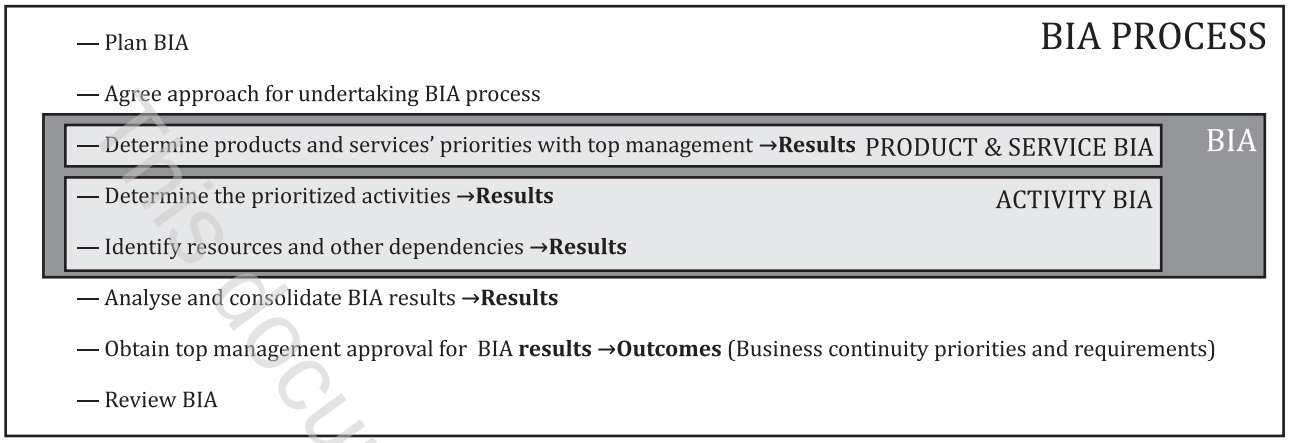


Figure 2 — Understanding BIA, BIA process, results and outcomes

The purpose of this document is to:

— provide a basis for implementing an effective BIA process within an organization;

— assist the organization with planning, conducting and reporting on the BIA process in a consistent manner.

This document provides examples for performing the BIA. It is important to note that these examples, individually or in combination, can help an organization achieve BIA outcomes. The selection of the most appropriate method will be influenced by the organization's size, sector, geography or context.

The outcomes of the BIA process include:

a) endorsement or modification of the organization's BCMS scope;

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

c) evaluation of the impact of a disruption over time on the organization, which serves as the justification for business continuity priorities and requirements;

d) estimation of the time it would take for adverse impacts to products and services to become unacceptable [maximum tolerable period of disruption (MTPD)] following a disruption;

e) identification of the requirements [MTPD and recovery time objective (RTO)] for the prioritized activities;

f) identification of the resources needed to perform prioritized activities following a disruption, including their dependencies, and requirements, specifying RTOs and applicable recovery point objectives (RPOs);

g) identification of dependencies including suppliers, partners and other interested parties;

h) identification of the interdependencies of prioritized activities.

Figure 3 shows the BIA process, along with its prerequisites and its relationship to the selection of business continuity strategies and solutions. The clauses referred to in the diagram correspond to subclauses of this document.

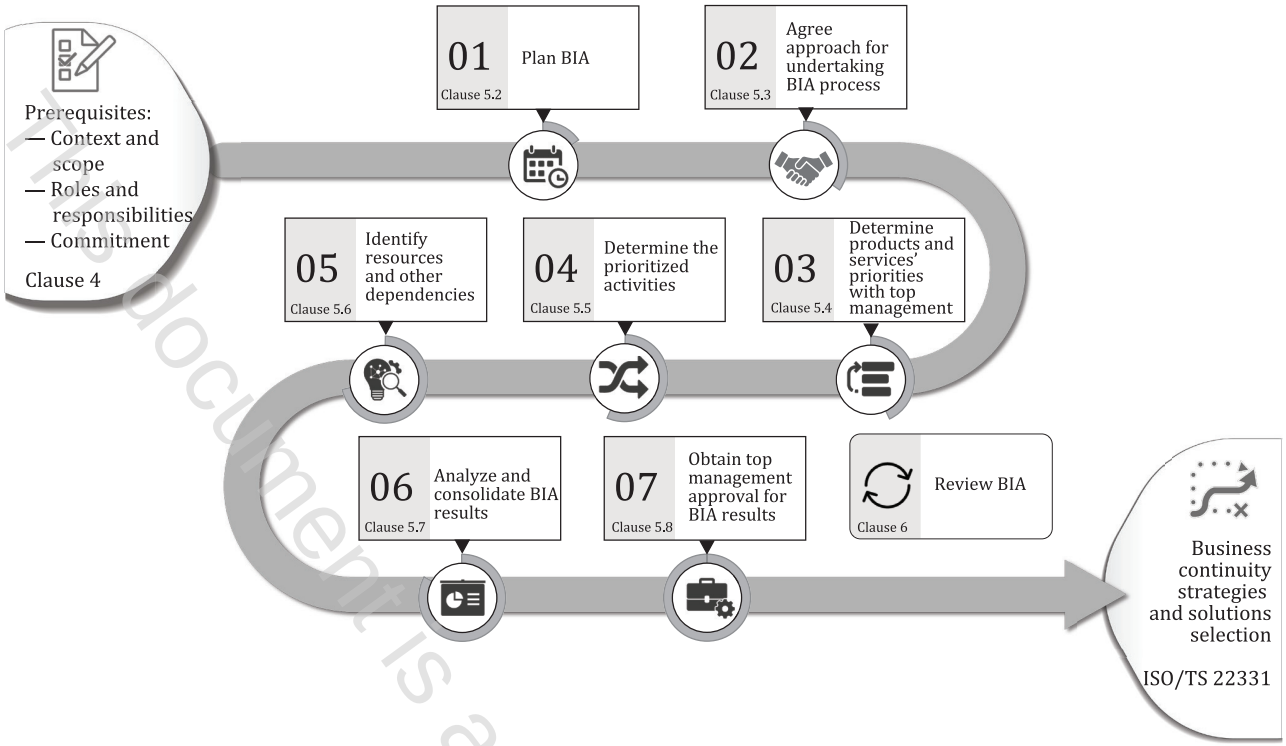


Figure 3 — BIA process

The organization should use the statement of business continuity priorities and requirements to select business continuity strategies and solutions.

The BIA can cause the organization to reconsider how it delivers its products and services.

The BIA depends on information being provided by many people across an organization who can have different perspectives on how the organization operates, what is time-critical or what impacts can occur following a disruption. Commonly, some overstate their requirements, while others understate theirs. This document seeks to define an approach that provides sufficient objectivity and minimizes these issues to produce effective outcomes.

Security and resilience — Business continuity management systems — Guidelines for business impact analysis

1 Scope

This document gives guidelines for an organization to implement and maintain a formal and documented business impact analysis (BIA) process appropriate to its needs. It does not prescribe a uniform process for performing a BIA.

This document 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.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 22300, *Security and resilience — Vocabulary*

ISO 22301, *Security and resilience — Business continuity management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and ISO 22301 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

4 Prerequisites

4.1 General

While this document is consistent with the requirements of ISO 22301, it can be used to implement and review any BIA process.

Before commencing the BIA process, the organization should:

— define the context and scope of the BIA process (see 4.2);

— define and communicate roles and responsibilities (see 4.3);

— obtain leadership commitment and allocate adequate resources (see 4.4).

NOTE See Annex A for a mapping of each clause to ISO 22301.