TECHNICAL SPECIFICATION

ISO/TS 22332

First edition
2021-05

Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures

Reference number
ISO/TS 22332:2021(E)

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.*

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 guidelines for developing and maintaining business continuity plans and procedures. This document is consistent with the requirements in ISO 22301 and the guidance in ISO 22313, and is applicable to the performance of any business continuity plan development, or as part of a business continuity management system (BCMS).

A business continuity plan provides guidance and information to assist teams responding to a disruption (ISO 22301:2019, 8.4.1) in order to meet expectations regarding delivery of products and services. The organization should create plans and procedures to address communications, emergency management, incident response, crisis management, recovery and restoration.

Business continuity plans and procedures should be consistent with organizational goals and objectives and business continuity objectives (see ISO 22301:2019, 3.4) and detail the actions that teams will take during a disruption in order to:

— activate the response;

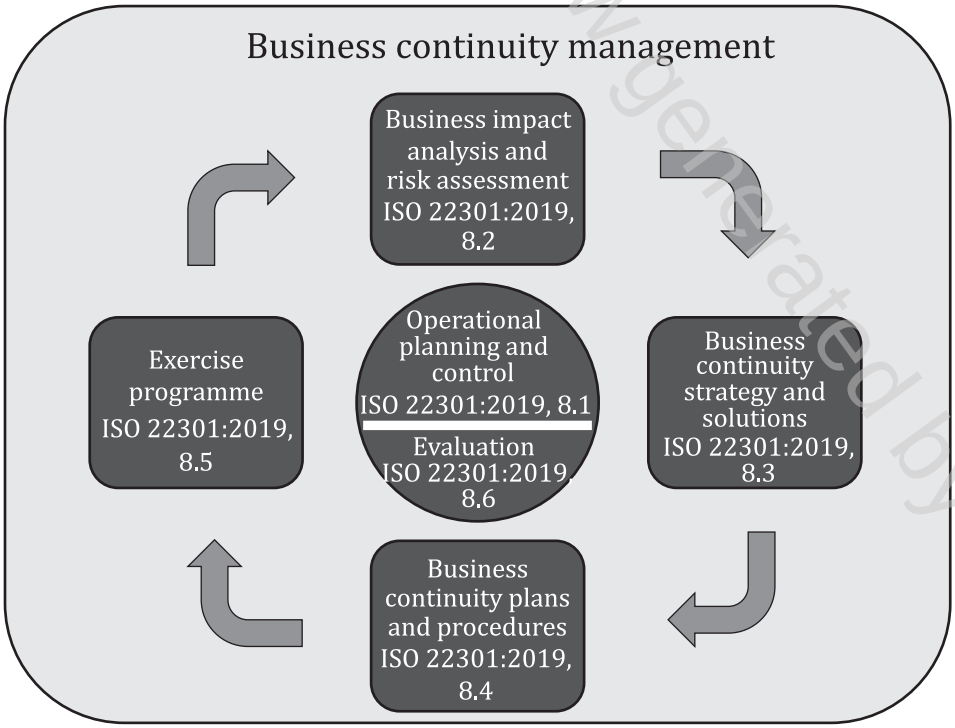
— manage the immediate consequences of a disruption;

— continue or recover prioritized activities within predetermined time frames utilizing, if appropriate, the agreed business continuity strategies and solutions;

— monitor the impact of the disruption and the organization's response to it;

— deliver products and services at agreed capacity.

Figure 1 presents the flow between the different components that constitute business continuity management. The business continuity strategy and solutions process (ISO 22301:2019, 8.3) provides the input for identifying, developing and maintaining business continuity plans and procedures (ISO 22301:2019, 8.4). In turn, the business continuity plans and procedures are a prerequisite for coordinating and performing business continuity exercises and tests (ISO 22301:2019, 8.5).



SOURCE ISO 22313:2020.

Figure 1 — Elements of business continuity management

The purpose of this document is to provide organizations with:

— detailed methods to develop business continuity plans and procedures;

— a structured approach to collect and organize information to develop plans and procedures;

— advice for maintaining plans and procedures over time to establish a continual improvement environment.

Following these guidelines will lead to the:

— establishment of a management structure to respond to a disruption, appointing competent and responsible personnel and teams with the authority to manage the response;

— implementation and maintenance of response processes addressing the protection of life and assets;

— establishment of command and control of the recovery effort following the onset of the disruption;

— implementation and maintenance of communication and warning procedures, including those necessary to manage the media response and coordination with other interested parties throughout a disruption;

— continuity or recovery of disrupted business activities and unavailable resources within predetermined time frames, including procedures necessary to return business activities from the temporary measures adopted during the incident to normal operations;

— recovery of disrupted technology assets;

— establishment of procedures to maintain capabilities and response readiness such as cross-training and exercising.

Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures

1 Scope

This document provides guidelines for developing and maintaining business continuity plans and procedures. It is applicable to all organizations regardless of type, size and nature, whether in the private, public, or not-for-profit sectors, that wish to develop effective business continuity plans and procedures in a consistent manner.

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*

3 Terms and definitions

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

ISO and IEC maintain terminological 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

Although these guidelines are consistent with ISO 22301, they can be used to develop and maintain business continuity plans and procedures when aligning or subscribing to other standards, obligations or regulatory requirements. Regardless of approach, several prerequisites need to be addressed. The organization should:

— understand the needs and expectations of interested parties (4.2);

— complete strategy determination and selection (4.3);

— define and communicate roles and responsibilities of those required to develop plans (4.4);

— allocate adequate resources to develop and maintain plans (4.5).

4.2 Interested parties

Business continuity should address the needs and expectations of interested parties. Therefore, the organization should identify its interested parties and determine their requirements for the response and recovery effort during a disruption.