AS ISO 22313:2020
ISO 22313:2020

Australian STANDARD®

STANDARDS Australia

Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301



AS ISO 22313:2020

This Australian Standard® was prepared by MB-025, Security and Resilience. It was approved on behalf of the Council of Standards Australia on 9 September 2020.

This Standard was published on 25 September 2020.

The following are represented on Committee MB-025:

Australian Emergency Management Institute
Australian Institute of Human Resources
Australian Local Government Association
Australian Risk Policy Institute
Australian Security Industry Association
Australian Strategic Policy Institute
Business Continuity Institute Australasia
Engineers Australia
International Association of Privacy Professionals, Australia and New Zealand
Office of the Victorian Information Commissioner
Risk and Insurance Management Society of Australasia
Risk Management Institute of Australasia
Security Professionals Australasia

This Standard was issued in draft form for comment as DR AS ISO 22313:2020.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:
www.standards.org.au

ISBN 978 1 76072 990 5

Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301

Originated as AS ISO 22313:2017.
Second edition 2020.

COPYRIGHT

© ISO 2020 — All rights reserved
© Standards Australia Limited 2020

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

Preface

This Standard was prepared by the Standards Australia Committee MB-025, Security and Resilience, to supersede AS ISO 22313:2017, *Societal security — Business continuity management systems — Guidance.*

The objective of this document is to give guidance and recommendations for applying the requirements of the business continuity management system (BCMS) given in AS ISO 22301. The guidance and recommendations are based on good international practice.

This document is applicable to organizations that —

(a) implement, maintain and improve a BCMS;

(b) seek to ensure conformity with the stated business continuity policy;

(c) need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption; and

(d) seek to enhance their resilience through the effective application of the BCMS.

The guidance and recommendations are applicable to all sizes and types of organizations, including large, medium and small organizations operating in industrial, commercial, public and not-for-profit sectors. The approach adopted depends on the organization's operating environment and complexity.

This document is identical with, and has been reproduced from, ISO 22313:2020, *Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*.

As this document has been reproduced from an International Standard, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

© Standards Australia Limited 2020

Contents

Preface ii
Foreword v
Introduction vi
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Context of the organization 1
4.1 Understanding the organization and its context 1
4.2 Understanding the needs and expectations of interested parties 2
4.2.1 General 2
4.2.2 Legal and regulatory requirements 3
4.3 Determining the scope of the business continuity management system 4
4.3.1 General 4
4.3.2 Scope of the business continuity management system 4
4.3.3 Exclusions to scope 4
4.4 Business continuity management system 5
5 Leadership 5
5.1 Leadership and commitment 5
5.1.1 General 5
5.1.2 Top management 5
5.1.3 Other managerial roles 6
5.2 Policy 6
5.2.1 Establishing the business continuity policy 6
5.2.2 Communicating the business continuity policy 7
5.3 Roles, responsibilities and authorities 7
6 Planning 9
6.1 Actions to address risks and opportunities 9
6.1.1 Determining risks and opportunities 10
6.1.2 Addressing risks and opportunities 10
6.2 Business continuity objectives and planning to achieve them 10
6.2.1 Establishing business continuity objectives 10
6.2.2 Determining business continuity objectives 10
6.3 Planning changes to the business continuity management system 11
7 Support 11
7.1 Resources 11
7.1.1 General 11
7.1.2 BCMS resources 12
7.2 Competence 12
7.3 Awareness 13
7.4 Communication 14
7.5 Documented information 15
7.5.1 General 15
7.5.2 Creating and updating 16
7.5.3 Control of documented information 17
8 Operation 18
8.1 Operational planning and control 18
8.1.1 General 18
8.1.2 Business continuity management 18
8.1.3 Maintaining business continuity 19
8.2 Business impact analysis and risk assessment 20
8.2.1 General 20

8.2.2 Business impact analysis 20
8.2.3 Risk assessment 23
8.3 Business continuity strategies and solutions 25
8.3.1 General 25
8.3.2 Identification of strategies and solutions 25
8.3.3 Selection of strategies and solutions 27
8.3.4 Resource requirements 28
8.3.5 Implementation of solutions 34
8.4 Business continuity plans and procedures 35
8.4.1 General 35
8.4.2 Response structure 35
8.4.3 Warning and communication 36
8.4.4 Business continuity plans 37
8.4.5 Recovery 43
8.5 Exercise programme 44
8.5.1 General 44
8.5.2 Design of the exercise programme 44
8.5.3 Exercising business continuity plans 45
8.6 Evaluation of business continuity documentation and capabilities 48
8.6.1 General 48
8.6.2 Measuring effectiveness 49
8.6.3 Outcomes 49

9 Performance evaluation 50
9.1 Monitoring, measurement, analysis and evaluation 50
9.1.1 General 50
9.1.2 Retention of evidence 50
9.1.3 Performance evaluation 50
9.2 Internal audit 51
9.2.1 General 51
9.2.2 Audit programme(s) 51
9.3 Management review 51
9.3.1 General 51
9.3.2 Management review input 51
9.3.3 Management review outputs 52

10 Improvement 52
10.1 Nonconformity and corrective action 52
10.1.1 General 52
10.1.2 Occurrence of nonconformity 53
10.1.3 Retention of documented information 53
10.2 Continual improvement 53

Bibliography 55

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 22313:2012), which has been technically revised. The main changes compared with the previous edition are as follows:

— structural and content alterations have been made to align this document with the latest edition of ISO 22301;

— additional guidance has been added to explain key concepts and terms;

— content has been removed from 8.4 that will be included in ISO/TS 22332 (under development).

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.

© Standards Australia Limited 2020

Introduction

0.1 General

This document provides guidance, where appropriate, on the requirements specified in ISO 22301. It is not the intention of this document to provide general guidance on all aspects of business continuity.

This document includes the same clause headings as ISO 22301 but does not restate the requirements and related terms and definitions.

The intention of the guidance is to explain and clarify the meaning and purpose of the requirements of ISO 22301 and assist in the resolution of any issues of interpretation. Other International Standards and Technical Specifications that provide additional guidance, and to which reference is made in this document, are ISO/TS 22317, ISO/TS 22318, ISO 22322, ISO/TS 22330, ISO/TS 22331 and ISO 22398. The scope of these documents can extend beyond the requirements of ISO 22301. Organizations should therefore always refer to ISO 22301 to verify the requirements to be met.

To provide further clarification and explanation of key points, this document includes several figures. The figures are for illustrative purposes only and the related text in the body of this document takes precedence.

A business continuity management system (BCMS) emphasizes the importance of:

— establishing business continuity policy and objectives that align with the organization's objectives;

— operating and maintaining processes, capabilities and response structures for ensuring the organization will survive disruptions;

— monitoring and reviewing the performance and effectiveness of the BCMS;

— continual improvement based on qualitative and quantitative measurement.

A BCMS, like any other management system, includes the following components:

a) a policy;

b) competent people with defined responsibilities;

c) management processes relating to:

    1) policy;

    2) planning;

    3) implementation and operation;

    4) performance assessment;

    5) management review;

    6) continual improvement;

d) documented information supporting operational control and enabling performance evaluation.

Business continuity is generally specific to an organization. However, its implementation can have far reaching implications on the wider community and other third parties. An organization is likely to have external organizations that it depends upon and there will be others that depend on it. Effective business continuity therefore contributes to a more resilient society.

© Standards Australia Limited 2020

0.2 Benefits of a business continuity management system

A BCMS increases the organization's level of preparedness to continue to operate during disruptions. It also results in improved understanding of the organization's internal and external relationships, better communication with interested parties and the creation of a continual improvement environment. There are potentially many additional benefits to implementing a BCMS in accordance with the recommendations contained in this document and in accordance with the requirements of ISO 22301.

— Following the recommendations in Clause 4 ("context of the organization") involves the organization:
  — reviewing its strategic objectives to ensure that the BCMS supports them;
  — reconsidering the needs, expectations and requirements of interested parties;
  — being aware of applicable legal, regulatory and other obligations.
— Clause 5 ("leadership") involves the organization:
  — reconsidering management roles and responsibilities;
  — promoting a culture of continual improvement;
  — allocating responsibility for performance monitoring and reporting.
— Clause 6 ("planning") involves the organization:
  — re-examining its risks and opportunities and identifying actions to address and take advantage of them;
  — establishing effective change management.
— Clause 7 ("support") involves the organization:
  — establishing effective management of its BCMS resources, including competence management;
  — improving employee awareness of matters that are important to management;
  — having effective mechanisms for internal and external communications;
  — managing its documentation effectively.
— Clause 8 ("operation") results in the organization considering:
  — the unintended consequences of change;
  — business continuity priorities and requirements;
  — dependencies;
  — vulnerabilities from an impact perspective;
  — risks of disruption and identifying how best to address them;
  — alternative solutions for running the business with limited resources;
  — effective structures and procedures for dealing with disruptions;
  — responsibilities to the community and other interested parties.
— Clause 9 ("performance evaluation") involves the organization:
  — having effective mechanisms for monitoring, measuring and evaluating performance;

© Standards Australia Limited 2020

  - involving management in monitoring the performance and contributing to the effectiveness of the BCMS.

- Clause 10 ("improvement") involves the organization:
  - having procedures for monitoring performance and improving effectiveness;
  - benefitting from continual improvement of its management systems.

As a result, implementation of the BCMS can:

a) protect life, assets and the environment;

b) protect and enhance the organization's reputation and credibility;

c) contribute to the organization's competitive advantage by enabling it to operate during disruptions;

d) reduce costs arising from disruptions and improving the organization's capability to remain effective during them;

e) contribute to the organization's overall organizational resilience;

f) assist in making interested parties more confident in the organization's success;

g) reduce the organization's legal and financial exposure;

h) demonstrate the organization's ability to manage risk and address operational vulnerabilities.

0.3 Plan-Do-Check-Act (PDCA) cycle

This document applies the Plan-Do-Check-Act (PDCA) cycle to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization's BCMS. An explanation of the PDCA cycle is given in Table 1.

Figure 1 illustrates how the BCMS takes interested parties' requirements as inputs for business continuity management and, through the required actions and processes, produces business continuity outcomes (i.e. managed business continuity) that meet those requirements.

Table 1 — Explanation of PDCA cycle

Plan (Establish)	Establish business continuity policy, objectives, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization's overall policies and objectives.
Do (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMS by taking corrective actions, based on the results of management review and re-appraising the scope of the BCMS and business continuity policy and objectives.

© Standards Australia Limited 2020

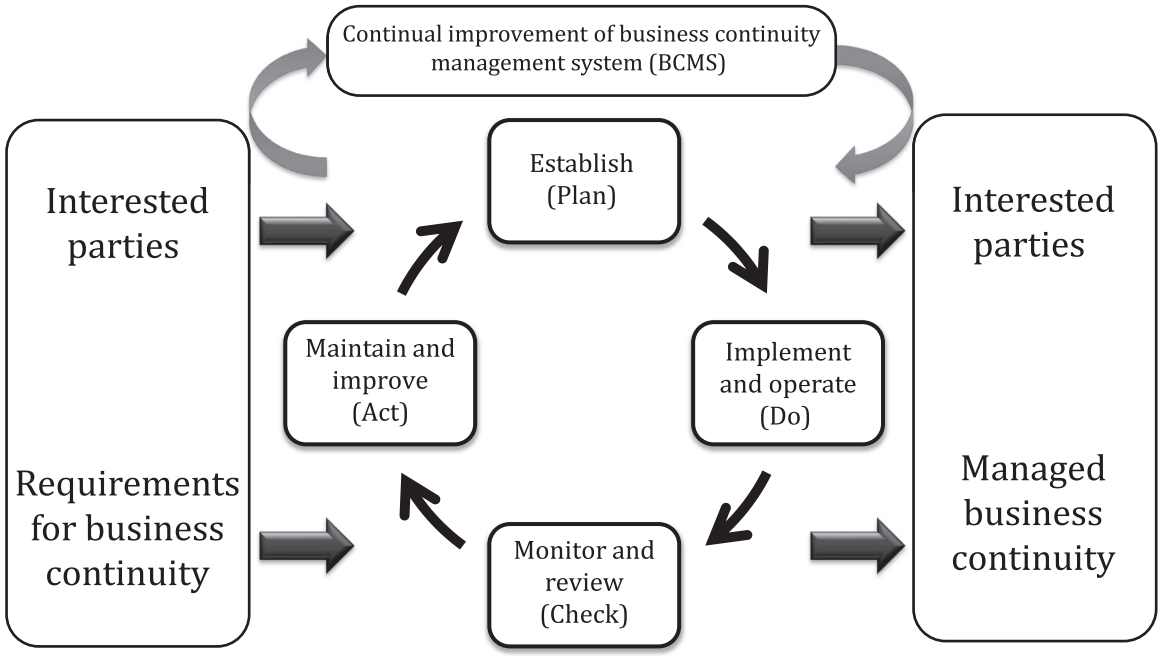


Figure 1 — PDCA cycle applied to BCMS processes

0.4 Components of PDCA in this document

Table 2 shows the direct relationship between the content of Figure 1 and the clauses of this document.

Table 2 — Relationship between the PDCA cycle and Clauses 4 to 10

PDCA component	Clause addressing PDCA component
Plan (Establish)	Clause 4 ("context of the organization") sets out what the organization should do in order to make sure that the BCMS meets its requirements, taking into account all relevant external and internal factors, including: — the needs and expectations of interested parties; — its legal and regulatory obligations; — the required scope of the BCMS.
	Clause 5 ("leadership") sets out the role of management in terms of demonstrating commitment, defining policy and establishing roles, responsibilities and authorities.
	Clause 6 ("planning") describes the actions for establishing strategic objectives and guiding principles for the implementation of the BCMS.
	Clause 7 ("support") identifies the BCMS elements that should be in place, namely: resources, competence, awareness, communication and documented information.
Do (Implement and operate)	Clause 8 ("operation") identifies the processes for establishing and maintaining business continuity.
Check (Monitor and review)	Clause 9 ("performance evaluation") provides the basis for improving the BCMS through measurement and evaluating its performance.
Act (Maintain and improve)	Clause 10 ("improvement") covers the corrective action for addressing nonconformity identified through performance evaluation.

0.5 Contents of this document

© Standards Australia Limited 2020

It is not the intent of this document to imply uniformity in the structure of a BCMS but for an organization to design a BCMS that is appropriate to its needs and that meets the requirements of its interested parties, particularly customers and employees. These needs are shaped by legal, regulatory, organizational and industry requirements, the products and services, the processes employed, the environment in which it operates, the size and structure of the organization and the requirements of its interested parties.

This document is not intended to be used to assess an organization's ability to meet its own business continuity needs, or any customer, legal or regulatory needs. Organizations wishing to do so can use the requirements in ISO 22301.

Clauses 1 to 3 in this document set out the scope, normative references and terms and definitions that apply to the use of this document. Clauses 4 to 10 contain guidance on the requirements given in ISO 22301.

In this document, the following verbal forms are used:

a) "should" indicates a recommendation;

b) "may" indicates a permission;

c) "can" indicates a possibility or a capability.

0.6 Business continuity

Business continuity is the capability of the organization to continue delivery of products or services at acceptable predefined capacities following a disruption. Business continuity management is the process of implementing and maintaining business continuity (see 8.1.2 and Figure 5) in order to prevent loss and prepare for, mitigate and manage disruptions.

Establishing a BCMS enables the organization to control, evaluate and continually improve its business continuity.

In this document, the word "business" is used as an all-embracing term for the operations and services performed by an organization in pursuit of its objectives, goals or mission. As such, it is equally applicable to large, medium and small organizations operating in industrial, commercial, public and not-for-profit sectors.

Disruptions have the potential to interrupt the organization's entire operations and its ability to deliver products and services. However, implementing a BCMS before a disruption occurs, rather than responding in an unplanned manner after the incident, will enable the organization to resume operations before unacceptable levels of impact arise.

Business continuity management involves:

a) identifying the organization's products and services and the activities that deliver them;

b) analysing the impacts of not resuming the activities and the resources they depend on;

c) understanding the risk of disruption;

d) determining priorities, time frames, capacities and strategies for resuming the delivery of products and services;

e) having solutions and plans in place to resume the activities within the required time frames following a disruption;

f) making sure that these arrangements are routinely reviewed and updated so that they will be effective in all circumstances.

The organization's approach to business continuity management and its documented information should be appropriate to its context (e.g. operating environment, complexity, needs, resources).

© Standards Australia Limited 2020

Business continuity can be effective in dealing with both sudden disruptions (e.g. explosions) and gradual ones (e.g. pandemics).

Activities can be disrupted by a wide variety of incidents, many of which are difficult to predict or analyse. By focusing on the impact of disruption rather than the cause, business continuity enables an organization to identify activities that are essential to it being able to meet its obligations. Through business continuity, an organization can recognize what is to be done to protect its resources (e.g. people, premises, technology, information), supply chain, interested parties and reputation before a disruption occurs. With that recognition, the organization can put in place a response structure, so that it can be confident of managing the impacts of a disruption.

Figure 2 and Figure 3 illustrate conceptually how business continuity can be effective in mitigating impacts in certain situations. No particular timescales are implied by the relative distance between the stages depicted in either diagram.

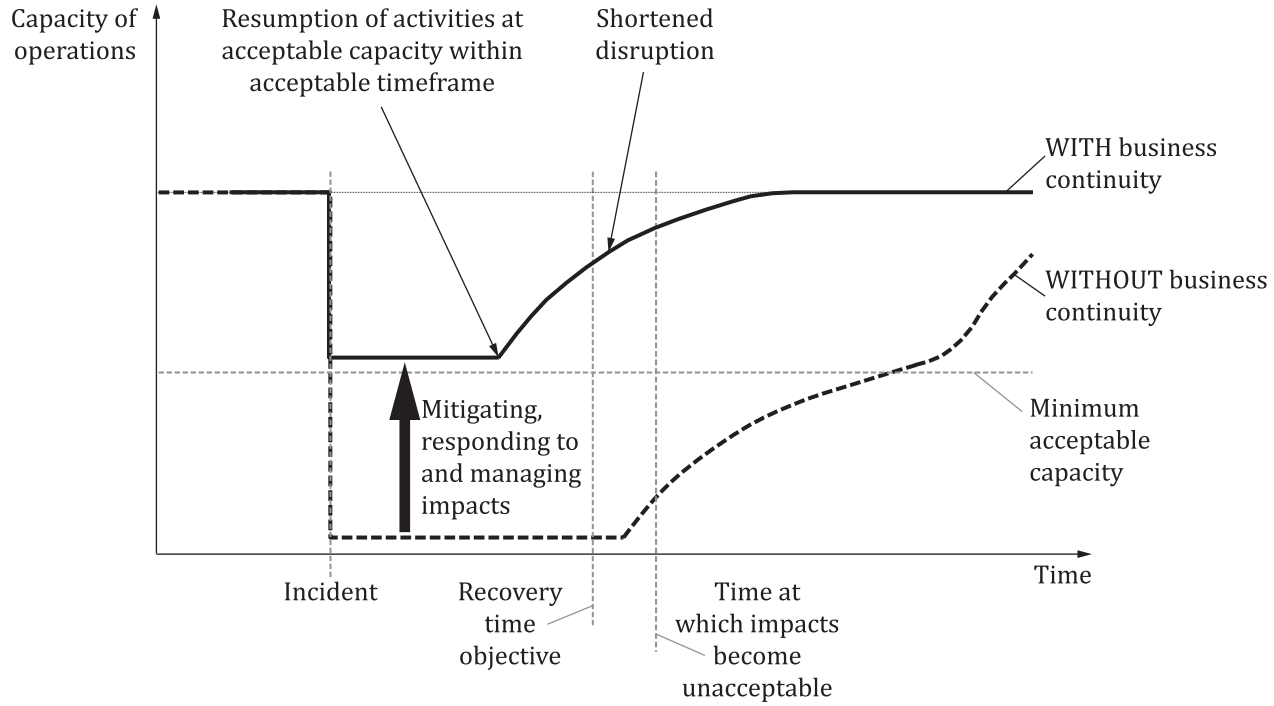


Figure 2 — Illustration of business continuity being effective for sudden disruption

© Standards Australia Limited 2020

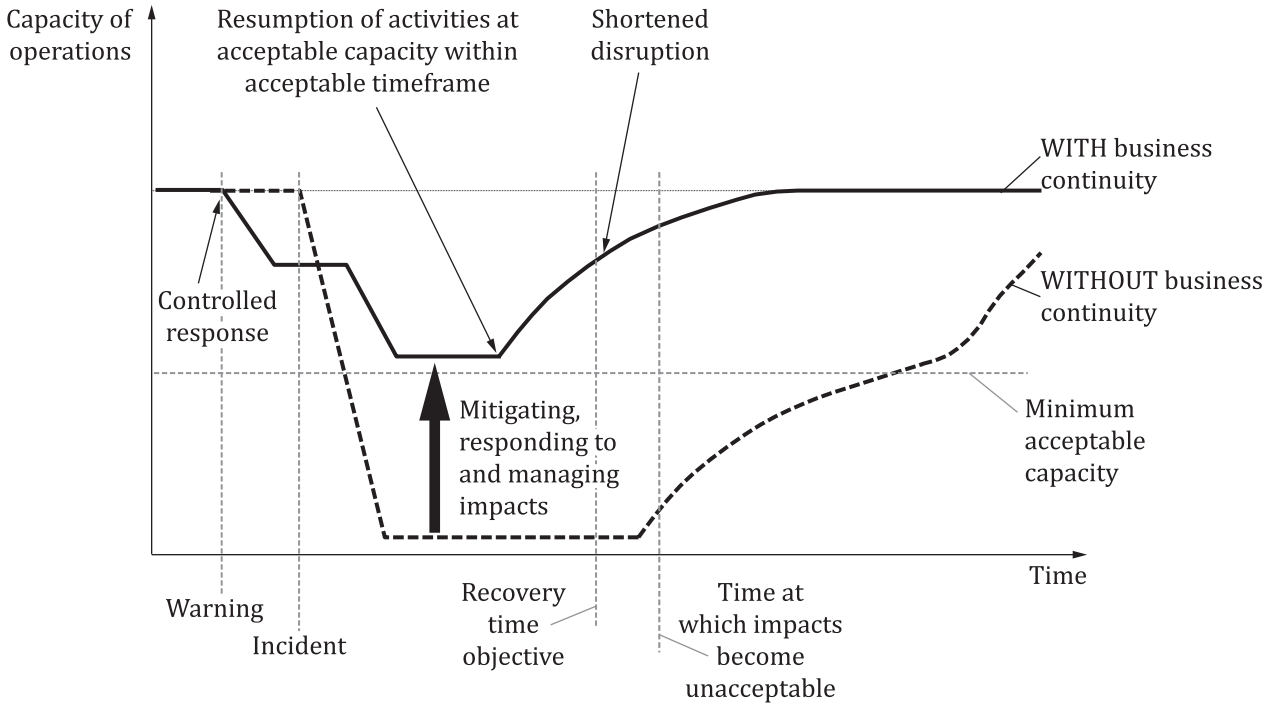


Figure 3 — Illustration of business continuity being effective for gradual disruption (e.g. approaching pandemic)

© Standards Australia Limited 2020

Australian Standard®

Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301

1 Scope

This document gives guidance and recommendations for applying the requirements of the business continuity management system (BCMS) given in ISO 22301. The guidance and recommendations are based on good international practice.

This document is applicable to organizations that:

a) implement, maintain and improve a BCMS;

b) seek to ensure conformity with stated business continuity policy;

c) need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption;

d) seek to enhance their resilience through the effective application of the BCMS.

The guidance and recommendations are applicable to all sizes and types of organizations, including large, medium and small organizations operating in industrial, commercial, public and not-for-profit sectors. The approach adopted depends on the organization's operating environment and complexity.

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, ISO 22301 and the following 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 http://www.electropedia.org/

3.1
business continuity management
process of implementing and maintaining business continuity

4 Context of the organization

4.1 Understanding the organization and its context

This clause provides recommendations for understanding the context of the organization in relation to the BCMS. Recommendations for establishing and maintaining business continuity are addressed in 8.1.

© Standards Australia Limited 2020