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.

# 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.

# Contents

# 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.

# 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.

## 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;