AS ISO 22313:2017
ISO 22313:2012

AS ISO 22313:2017

Australian STANDARD

# Societal security—Business continuity management systems—Guidance

STANDARDS Australia

AS ISO 22313:2017

This Australian Standard® was prepared by Committee MB-025, Security and Resilience. It was approved on behalf of the Council of Standards Australia on 31 July 2017.

This Standard was published on 29 August 2017.

The following are represented on Committee MB-025:

Australasian Council of Security Professionals
Australian Security Industry Association
Business Continuity Institute Australasia
Commissioner for Privacy and Data Protection
Engineers Australia
International Commission of Jurists Australia
Risk and Insurance Management Society of Australasia
Security Professionals Registry Australasia
Transport Accident Commission

This Standard was issued in draft form for comment as DR AS ISO 22313:2017.

**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

www.saiglobal.com (sales and distribution)

ISBN 978 1 76035 866 2

AS ISO 22313:2017
ISO 22313:2012

Australian Standard®

# Societal security—Business continuity management systems—Guidance

First published as AS ISO 22313:2017.



Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia.

# Preface

This Standard was prepared by the Standards Australia Committee MB-025, Security and Resilience.

The objective of this Standard is to provide guidance based on effective international practice for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving a documented management system that enables organizations to prepare for, respond to and recover from disruptive incidents when they arise.

This Standard is identical with, and has been reproduced from, ISO 22313:2012, *Societal security—Business continuity management systems—Guidance*.

As this document has been reproduced from an International Standard, the following applies:

(a) Source text 'this International Standard' should read 'this Australian Standard'.

(b) A full point substitutes for a coma 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.

The terms 'normative' and 'informative' are used in Standards to define the application of the appendices or annexes to which they apply. A 'normative' appendix or annex is an integral part of a Standard, whereas an 'informative' appendix or annex is only for information and guidance.

# 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 22313 was prepared by Technical Committee ISO/TC 223, *Societal security*.

**For the purposes of research, users are encouraged to share their views on ISO 22313:2012 and their priorities for changes to future editions of the document. Click on the link below to take part in the online survey:**

**http://www.surveymonkey.com/s/22313**

# Introduction

## General

This International Standard provides guidance, where appropriate, on the requirements specified in ISO 22301:2012 and provides recommendations ('should') and permissions ('may') in relation to them. It is not the intention of this International Standard to provide general guidance on all aspects of business continuity.

This International Standard includes the same headings as ISO 22301 but does not repeat the requirements for business continuity management systems and its related terms and definitions. Organizations wishing to be informed of these must therefore refer to ISO 22301 and ISO 22300.

To provide further clarification and explanation of key points, this International Standard includes a number of figures. All such figures are for illustrative purposes only and the related text in the body of this International Standard takes precedence.

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

— understanding the organization's needs and the necessity for establishing business continuity policy and objectives;

— implementing and operating controls and measures for managing an organization's overall capability to manage disruptive incidents;

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

— continual improvement based on objective measurement.

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

a) a policy;

b) people with defined responsibilities;

c) management processes relating to:

   1) policy;

   2) planning;

   3) implementation and operation;

   4) performance assessment;

   5) management review; and

   6) improvement.

d) a set of documentation providing auditable evidence; and

e) any BCMS processes relevant to the organization.

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.

## The Plan-Do-Check-Act cycle

This International Standard 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.