



# **Societal security—Business continuity management systems—Requirements**



AS ISO 22301:2017

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 28 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 Association of Privacy Professionals Australia New Zealand
- 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 22301:2017.

### **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](http://www.standards.org.au)

[www.saiglobal.com](http://www.saiglobal.com) (sales and distribution)

ISBN 978 1 76035 868 6

Australian Standard®

# **Societal security—Business continuity management systems—Requirements**

First published as AS ISO 22301:2017.

## **COPYRIGHT**

© ISO 2017 — All rights reserved  
© Standards Australia Limited 2017

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).

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 specify requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

This Standard is identical with, and has been reproduced from, ISO 22301:2012, *Societal security—Business continuity management systems—Requirements*

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

<b>Preface</b> .....	<b>ii</b>
<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
0.1 General.....	vi
0.2 The Plan-Do-Check-Act (PDCA) model.....	vi
0.3 Components of PDCA in this International Standard.....	vii
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Context of the organization</b> .....	<b>8</b>
4.1 Understanding of the organization and its context.....	8
4.2 Understanding the needs and expectations of interested parties.....	9
4.2.1 General.....	9
4.2.2 Legal and regulatory requirements.....	9
4.3 Determining the scope of the business continuity management system.....	9
4.3.1 General.....	9
4.3.2 Scope of the BCMS.....	10
4.4 Business continuity management system.....	10
<b>5 Leadership</b> .....	<b>10</b>
5.1 Leadership and commitment.....	10
5.2 Management commitment.....	10
5.3 Policy.....	11
5.4 Organizational roles, responsibilities and authorities.....	11
<b>6 Planning</b> .....	<b>12</b>
6.1 Actions to address risks and opportunities.....	12
6.2 Business continuity objectives and plans to achieve them.....	12
<b>7 Support</b> .....	<b>13</b>
7.1 Resources.....	13
7.2 Competence.....	13
7.3 Awareness.....	13
7.4 Communication.....	13
7.5 Documented information.....	14
7.5.1 General.....	14
7.5.2 Creating and updating.....	14
7.5.3 Control of documented information.....	14
<b>8 Operation</b> .....	<b>15</b>
8.1 Operational planning and control.....	15
8.2 Business impact analysis and risk assessment.....	15
8.2.1 General.....	15
8.2.2 Business impact analysis.....	15
8.2.3 Risk assessment.....	16
8.3 Business continuity strategy.....	16
8.3.1 Determination and selection.....	16
8.3.2 Establishing resource requirements.....	16
8.3.3 Protection and mitigation.....	17
8.4 Establish and implement business continuity procedures.....	17
8.4.1 General.....	17
8.4.2 Incident response structure.....	17
8.4.3 Warning and communication.....	18
8.4.4 Business continuity plans.....	18
8.4.5 Recovery.....	19

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

- 
- [Looking for additional Standards? Visit Intertek Inform Infostore](#)
  - [Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation](#)
-