Australian
STANDARD

Societal security—Business continuity management systems—Requirements

STANDARDS
Australia

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

www.saiglobal.com (sales and distribution)

Australian Standard®

Societal security—Business continuity management systems—Requirements

First published as AS ISO 22301:2017.

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

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 22301 was prepared by Technical Committee ISO/TC 223, *Societal security*.

This corrected version of ISO 22301:2012 incorporates the following corrections:

— first list in 6.1 changed from a numbered to an unnumbered list;

— commas added at the end of list items in 7.5.3 and 8.3.2;

— bibliography items [19] and [20] separated, which were merged in the original;

— font size adjusted in several places.

Introduction

0.1   General

This International Standard specifies requirements for setting up and managing an effective Business Continuity Management System (BCMS).

A BCMS emphasizes the importance of

— understanding the organization's needs and the necessity for establishing business continuity management 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, has 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)   documentation providing auditable evidence; and

e)   any business continuity management processes relevant to the organization.

Business continuity contributes to a more resilient society. The wider community and the impact of the organization's environment on the organization and therefore other organizations may need to be involved in the recovery process.

0.2   The Plan-Do-Check-Act (PDCA) model

This International Standard applies the "Plan-Do-Check-Act" (PDCA) model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization's BCMS.

This ensures a degree of consistency with other management systems standards, such as ISO 9001 *Quality management systems*, ISO 14001, *Environmental management systems*, ISO/IEC 27001, *Information security management systems*, ISO/IEC 20000-1, *Information technology — Service management*, and ISO 28000, *Specification for security management systems for the supply chain*, thereby supporting consistent and integrated implementation and operation with related management systems.

Figure 1 illustrates how a BCMS takes as inputs interested parties, requirements for continuity management and, through the necessary actions and processes, produces continuity outcomes (i.e. managed business continuity) that meet those requirements.
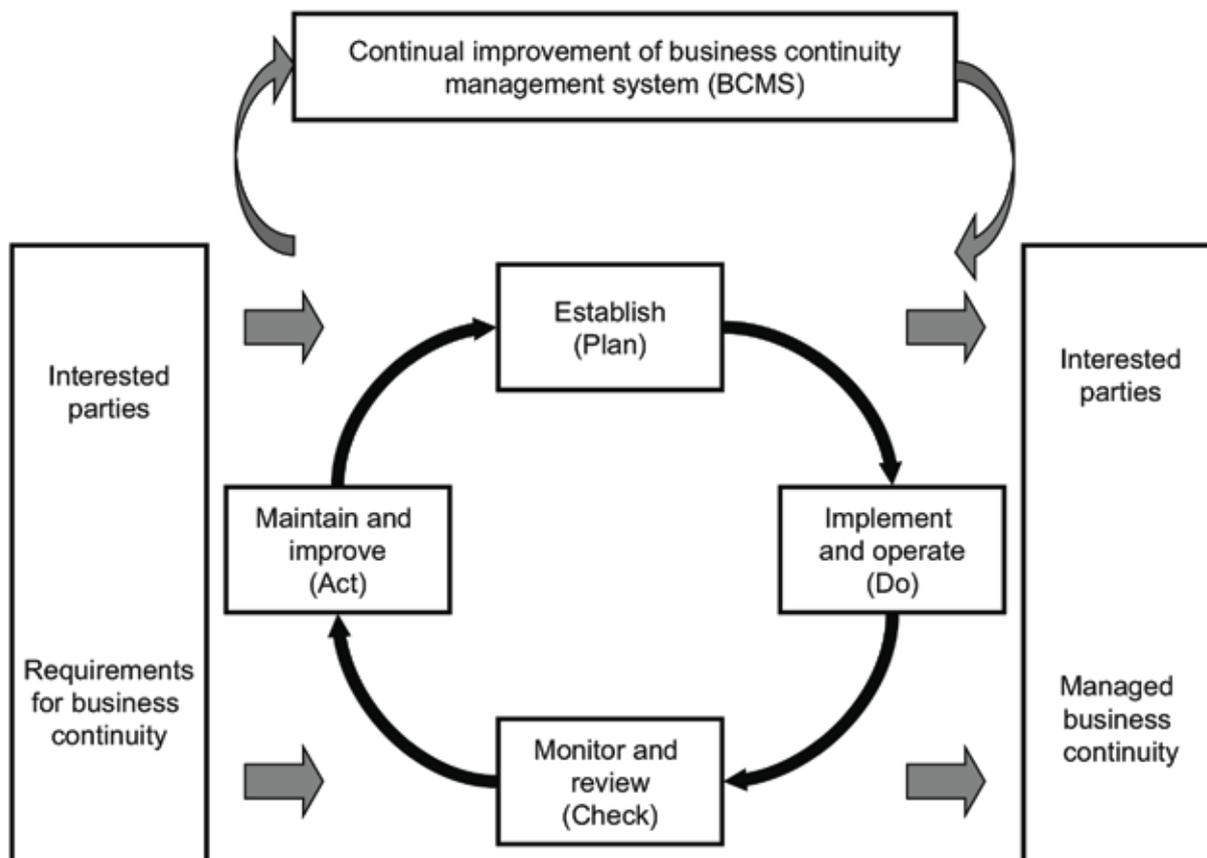
© Standards Australia Limited 2017

Figure 1 — PDCA model applied to BCMS processes

Table 1 — Explanation of PDCA model

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 objectives and policy, 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.

0.3   Components of PDCA in this International Standard

In the Plan-Do-Check-Act model as shown in Table 1, Clause 4 through Clause 10 in this International Standard cover the following components.

— Clause 4 is a component of Plan. It introduces requirements necessary to establish the context of the BCMS as it applies to the organization, as well as needs, requirements, and scope.

— Clause 5 is a component of Plan. It summarizes the requirements specific to top management's role in the BCMS, and how leadership articulates its expectations to the organization via a policy statement.

— Clause 6 is a component of Plan. It describes requirements as it relates to establishing strategic objectives and guiding principles for the BCMS as a whole. The content of Clause 6 differs from establishing risk treatment opportunities stemming from risk assessment, as well as business impact analysis (BIA) derived recovery objectives.

  NOTE   The business impact analysis and risk assessment process requirements are detailed in Clause 8.

— Clause 7 is a component of Plan. It supports BCMS operations as they relate to establishing competence and communication on a recurring/as-needed basis with interested parties, while documenting, controlling, maintaining and retaining required documentation.

— Clause 8 is a component of Do. It defines business continuity requirements, determines how to address them and develops the procedures to manage a disruptive incident.

— Clause 9 is a component of Check. It summarizes requirements necessary to measure business continuity management performance, BCMS compliance with this International Standard and management's expectations, and seeks feedback from management regarding expectations.

— Clause 10 is a component of Act. It identifies and acts on BCMS non-conformance through corrective action.