AS ISO 22372:2026
ISO 22372:2025

Australian STANDARD®

STANDARDS Australia

Security and resilience — Community resilience — Guidelines for infrastructure resilience



AS ISO 22372:2026

This Australian Standard® was prepared by MB-025, Security and Resilience. It was approved on behalf of Standards Australia's Standards Development and Accreditation Committee on 12 June 2026.

This Standard was published on 26 June 2026.

The following are represented on Committee MB-025:

- Australian Institute of Human Resources
- Australian Risk Policy Institute
- Australian Security Industry Association
- Business Continuity Institute Australasia
- Department of Defence (Australian Government)
- Engineers Australia
- Office of the Victorian Information Commissioner
- Risk Management Institute of Australasia
- Security Professionals Australasia
- The Risk and Insurance Management Society of Australasia
- Victorian Managed Insurance Authority

This Standard was issued for comment as DR AS ISO 22372:2026

Status of this document

Standards Australia publications are periodically reviewed to ensure their ongoing relevance and accuracy. This document may be withdrawn, revised, or superseded at any time. To verify this document's current status, visit:

www.standards.org.au

ISBN: 978 1 76175 998 7

AS ISO 22372:2026
ISO 22372:2025

Australian Standard®

Security and resilience — Community resilience — Guidelines for infrastructure resilience

First published as AS ISO 22372:2026.

© ISO 2026 — All rights reserved
© Standards Australia Limited 2026

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).

Users must not use the content in this publication in combination with artificial intelligence (AI) tools for any purpose, unless they have the express prior written consent from Standards Australia.

How to read this Standard

This page explains the meaning of the language and structure of this Standard.

Refer to Standards Australia's Standardisation Guide 006 for more details about drafting rules.

Australian and Australian/New Zealand Standards are voluntary unless they are referenced in legislation or called up in contracts.

Requirements

To conform to a Standard, all requirements in the Standard need to be met.

A requirement is any statement in the Standard which uses the word "shall".

Recommendations, permissions and possibilities

The following words are commonly used in Standards, but statements using them do not have to be followed to conform to the Standard:

(a) "should" means that something is recommended.

(b) "may" means that something is permitted.

(c) "can" means that something is possible.

Structure of Standards

A Standard always has the following parts:

(i) The Preface states who developed the Standard, what the Standard is aiming to do, and how it relates to other documents.

(ii) The Scope states what the Standard is about, what it covers and what it does not cover.

(iii) The Normative references clause lists other documents that are referenced in the Standard as part of requirements.

(iv) The Terms and definitions clause defines important terms to help with understanding the Standard.

A Standard may also include other parts, such as the following:

(1) A normative appendix sets additional requirements that need to be conformed to.

(2) An informative appendix provides additional information or guidance. They usually do not contain requirements. If an informative appendix does contain requirements, the Standard will explain when those requirements apply.

(3) A Bibliography lists documents referenced in the Standard but not as part of requirements.

Many Standards include notes. Notes provide recommendations and/or guidance only. They never contain requirements.

Preface

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

The objective of this document is to provide guidelines for establishing, maintaining, monitoring and improving infrastructure resilience to help ensure the continuity and robustness of essential services.

It supports collaborative decision-making across many stakeholders in diverse organizations. It can be used for engaging stakeholders at all levels responsible for, or having influence on, infrastructure resilience matters.

This document is intended to be applicable to all types and sizes of organizations which have a role in infrastructure resilience.

This document is identical to, and has been reproduced from, ISO 22372:2025, *Security and resilience — Community resilience — Guidelines for infrastructure resilience*.

© Standards Australia Limited 2026

Contents

Page

Preface ..... **v**
National foreword ..... **viii**
Foreword ..... **ix**
Introduction ..... **x**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Framework **2**
4.1 General 2
4.2 Objectives and responsibilities 3
4.3 Identifying and assessing capabilities of infrastructure 3
4.4 Setting priorities 5
4.5 Establishing a strategy and plan 6
5 Principles **7**
5.1 General 7
5.2 Principle 1: Clearly defined accountabilities and shared responsibilities 8
5.3 Principle 2: Proactively protected 9
5.4 Principle 3: Environmentally integrated 10
5.5 Principle 4: Socially engaged 11
5.6 Principle 5: Adaptively transforming 12
5.7 Principle 6: Continually learning and improving 13
6 Operational processes **14**
6.1 General 14
6.2 Plan: developing and sharing understanding 14
6.2.1 General 14
6.2.2 Collecting evidence 14
6.2.3 Working with and sharing information with others 15
6.3 Plan: investing in infrastructure resilience 18
6.3.1 General 18
6.3.2 P1A6 Share hazard, risk and return information 18
6.3.3 P1A7 Invest to enhance resilience 18
6.3.4 P2A12 Devise long-term investments 19
6.4 Do: devising and designing ways to improve infrastructure resilience 19
6.4.1 General 19
6.4.2 P2A1 Increase essential safety requirements 20
6.4.3 P2A2 Exceed basic requirements for critical components 20
6.4.4 P2A3 Consider interdependencies of systems and systemic risks 21
6.4.5 P2A8 Design infrastructure to fail safely 21
6.4.6 P2A10 Design for multiple scales 21
6.4.7 P3A2 Appropriate use of nature-based solutions 21
6.4.8 P3A5 Use environmentally sustainable resources 21
6.4.9 P3A6 Sustainable use of natural resources 22
6.5 Do: implementing ways to improve infrastructure resilience 22
6.5.1 General 22
6.5.2 P2A4 Secure multiple resilience pathways and controls 23
6.5.3 P2A5 Take timely action 23
6.5.4 P2A6 Embed emergency management 23
6.5.5 P2A7 Consider infrastructure users 23
6.5.6 P2A9 Implement strategies to overcome systemic weaknesses found by stress testing 24
6.5.7 P3A1 Minimize environmental exposure and impact 24
6.5.8 P4A4 Focus resources on critical tasks during emergencies 24

© Standards Australia Limited 2026

6.5.9 P5A2 Create and enhance adaptive capacity 24
6.5.10 P6A7 Establish redundancy within any monitoring and analysis system 24
6.6 Check: testing ways to improve resilience 25
6.6.1 General 25
6.6.2 P6A4 Analyse, learn, and formulate improvements 25
6.6.3 P6A5 Develop and test strategies to overcome component vulnerabilities 25
6.7 Check: monitoring infrastructure resilience 26
6.7.1 General 26
6.7.2 P1A8 Manage infrastructure resilience performance 26
6.7.3 P6A3 Monitor and report 26
6.8 Act: improving practices, norms and management approaches 26
6.8.1 General 26
6.8.2 P4A1 Encourage active public participation 27
6.8.3 P4A3 Assess needs and expectations of the public 27
6.8.4 P4A5 Prepare people for disruptive incidents 28
6.8.5 P5A1 Choose manageable solutions 28
6.8.6 P5A3 Develop flexible management 28
6.8.7 P5A4 Enable capacity to extend beyond initial scope 28
6.8.8 P5A5 Allow for human discretion 29
6.8.9 P6A6 Maintain and improve competencies 29
6.9 Act: maintaining operational infrastructure and its natural environment 29
6.9.1 General 29
6.9.2 P2A11 Adopt condition-based maintenance 30
6.9.3 P2A13 Inspect assets after disruptive incidents and near misses 30
6.9.4 P3A4 Maintain the natural environment 30
Annex A (informative) **Example of a governance framework for infrastructure resilience 31**
Bibliography 33

© Standards Australia Limited 2026

National foreword

The application of this document in an Australian context is relevant and of interest to organisations that have a responsibility to ensure the delivery of essential services to communities, cities, regions, states and the nation. These guidelines assist organisations in risk management planning and ongoing monitoring of infrastructure critical to the delivery of those essential services. This guide is also useful for organizations responsible for infrastructure that is currently not covered by the Commonwealth Security of Critical Infrastructure (SOCI) legislation. It is applicable to organisations preparing responses to the SOCI Act risk management program rules.

This guideline's use can provide increased —

(a) local, state and national preparedness for the simultaneous occurrence of distinct multiple crisis events and their effect on essential services;

(b) understanding of the importance of collaboration with various stakeholders in order to fully understand resilience management responsibilities;

(c) proactive measures and versatile decision systems to meet the challenges of current and future complex natural and geopolitical environments;

(d) amplification of national and state regulatory needs;

(e) social engagement and understanding of the criticality of service delivery to communities throughout Australia;

(f) adaptive capacities for transforming the way critical services are delivered; and

(g) promotion of collaborative learning systems at national and state levels other than those Australia currently has.

© Standards Australia Limited 2026

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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*.

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 2026

Introduction

Infrastructure in this document refers to interdependent systems that deliver essential services to communities, cities, regions and nations. Infrastructure is the backbone of every society. Individuals depend on the effective and efficient operation of infrastructure to support businesses and deliver public services. For that reason, the provision, reliability, performance, continuous operation, safety, maintenance, and protection of infrastructure are national and local priorities around the world. Infrastructure, or components of it, can be critical or become critical over time.

Infrastructure resilience needs cooperative action by organizations. Changes to society and technology create significant challenges for delivering resilient essential services to the end user. The increase in scale, complexity and interconnectedness of infrastructure amplifies and propagates disruptive incidents. This can have a severe human and economic impact.

Investment, innovation and novel approaches are needed to update and establish infrastructure resilience. However, most current approaches to infrastructure planning, financing, design, development, operations and decommissioning do not fully take into account either the interdependence of infrastructure and services, or the increasingly complex nature of risk and the cascading impacts that a disruptive incident can have across infrastructure.

There is a need to address disruption-related risk amplified by increasing complexity, age, and interdependency within and across infrastructure. As infrastructure becomes more reliable, end users may lose the memory of coping with interruptions and become more reliant on it. Therefore, infrastructure resilience is increasingly important to society. To address significant change in societies' characteristics (e.g. demographic change) and in the context of infrastructure (e.g. climate and technical change), a systematic approach is required to ensure infrastructure resilience.

This document aims to inform stakeholders on potential strategic and operational issues and assist in the development of an effective approach to infrastructure resilience. To help avoid conflict between and within organizations, the approach should include resilience principles that are aligned at all levels. Using a collaborative approach as recommended in this document, stakeholders can better understand their roles and responsibilities and create direct value through their work that contributes to the overall infrastructure resilience and inter-dependent infrastructure.

Stakeholders can be in the private and public sectors including but not limited to professional associations, donors, infrastructure operators, regulators, policy makers, investors and owners, designers and suppliers, service providers and international organizations including trading blocs.

This document sets out core principles for infrastructure resilience. The principles are informed by the United Nations Office for Disaster Risk Reduction's (UNDRR) Principles for Resilient Infrastructure[1] which were developed in consultation with United Nations member states and experts. It provides guidelines to inform policies, strategies, and regulatory frameworks that are based on evidence of risks and the vulnerabilities of infrastructure. It aims to help decision-makers and provide options to improve infrastructure resilience against clear goals while strengthening governance and assurance.

This document is not intended to provide guidelines on emergency management and response, which are also important considerations in building infrastructure resilience. These guidelines cover all infrastructure and are not limited to critical infrastructure as defined by legal requirements such as the European Commission's Directive on the resilience of critical entities.[2]

NOTE For information on emergency management and response, refer to ISO 22320.

© Standards Australia Limited 2026

Australian Standard®

Security and resilience — Community resilience — Guidelines for infrastructure resilience

1 Scope

This document provides guidelines for establishing, maintaining, monitoring and improving infrastructure resilience to help ensure the continuity and robustness of essential services.

It supports collaborative decision-making across many stakeholders in diverse organizations. It can be used for engaging stakeholders at all levels responsible for, or having influence on, infrastructure resilience matters.

This document is intended to be applicable to all types and sizes of organizations which have a role in infrastructure resilience.

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 22300:2021, *Security and resilience — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
adaptive capacity
ability of a system, *organization* (3.5), region or community to adjust to the effects of change

Note 1 to entry: The effects of change can be related to responding to potential disruptive incidents and damages, or to taking advantage of opportunities.

Note 2 to entry: Examples include spare resources, availability of required information, disaster-relevant competencies.

3.2
hazard
source of potential harm

Note 1 to entry: Hazard can be a risk source.

[SOURCE: ISO 22300:2021, 3.1.110]

3.3
infrastructure
system of people, resources, facilities, equipment and services that enable the functioning of society and the operation of an *organization* (3.5)

© Standards Australia Limited 2026