



BSI Standards Publication

Security and resilience — Community resilience — Guidelines for infrastructure resilience

National foreword

This British Standard is the UK implementation of ISO 22372:2025.

The UK participation in its preparation was entrusted to Technical Committee CAR/1, Continuity and Resilience.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 25003 9

ICS 03.100.01

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2025.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------



**International
Standard**

ISO 22372

**Security and resilience —
Community resilience — Guidelines
for infrastructure resilience**

*Sécurité et résilience — Résilience collective — Lignes directrices
pour la résilience des infrastructures*

**First edition
2025-11**

Reference number
ISO 22372:2025(en)

Full document details: BS ISO 22372:2025

© ISO 2025  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Framework	3
4.1 General	3
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	13
6.1 General	13
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
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

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.

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.

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)

Note 1 to entry: Infrastructure can include telecommunications; energy systems; banking and finance; defence; food supply chain; IT infrastructure; education systems; transportation; water supply and sanitation; health services; emergency services (including police, fire, and rescue); and other public services.

[SOURCE: ISO 22300:2021, 3.1.128, modified — “people, resources” has been added and “that enable the functioning of society and the operation of an organization” has replaced “needed for the operation of an organization”; note 1 to entry has been added.]

3.4

infrastructure life cycle

stages of an *infrastructure* (3.3) project: initial planning and evaluation of options, design, procurement, construction, operation and maintenance, and decommissioning and re-use

3.5

organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO 22300:2021, 3.1.165, modified — note 2 to entry has been removed.]

3.6

resilience

ability to absorb and adapt in a changing environment

[SOURCE: ISO 22300:2021, 3.1.206, modified — note 1 to entry has been deleted.]

3.7

resilience phase

phase in which infrastructure exists with respect to a disruptive incident, consisting of:

- preparation (proactive measures to anticipate and mitigate potential disruptions),
- absorption (withstanding and minimizing the immediate impact of an adverse event),
- recovery (restoring functionality), and
- adaptation (proactive measures that prepare for future potential disruptions)

3.8

risk

effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential disruptive incidents, their consequences and their likelihood.

[SOURCE: ISO 22300:2021, 3.1.215, modified — note 4 to entry has been deleted.]

4 Framework

4.1 General

Infrastructure resilience is built on clear and concise policy and established procedures that are intended to ensure resilience goals and objectives are met.

There are four broad steps which should be agreed through collaboration and shared commitment, and to establish governance for infrastructure resilience:

- a) define objectives and responsibilities;
- b) identify and assess capabilities;
- c) set priorities; and
- d) establish a strategy and plan.

4.2 Objectives and responsibilities

Relevant organizations who are responsible for infrastructure resilience should be appointed to define strategic goals, priorities and responsibilities, and to deliver collaborative objectives for the resilience of all infrastructure.

These relevant organizations should set resilience objectives for all stakeholder organizations to integrate into their own objectives. The relevant organizations should establish responsibilities for decision making, controls and accountability for the mutual benefit of communities. Such responsibilities should be coordinated and clear, to avoid fragmentation across the various levels within an organization.

Examples of establishing such responsibilities include the following:

- a) nominating a governing body to determine the method of governance;
- b) inviting representatives of infrastructure stakeholders for consultation, clarification of scope and scale, etc; and
- c) ensuring ethical and robust management.

NOTE In this document, the “relevant organizations” have responsibility for resilience across all infrastructure.

4.3 Identifying and assessing capabilities of infrastructure

The relevant organizations should lead the assessment of infrastructure resilience and each organization should contribute to this assessment. Each key action in this document should be reviewed to determine the scale of its adoption in infrastructure. A comprehensive assessment across relevant organisations will highlight gaps and weaknesses and drive planning of the implementation of resilience across all infrastructure delivering essential services.

The assessment should be holistic recognizing that infrastructure is a system of systems and considering all essential services as an integrated system rather than relying solely on sector-specific evaluations. This approach helps to identify the weakest links across infrastructure, allowing for prioritization of actions with the greatest impact on systemic resilience of infrastructure. This is intended to ensure that infrastructure resilience is strengthened where it is most needed to maintain uninterrupted service delivery. The assessment should consider the whole infrastructure life cycle, new infrastructure projects and infrastructure still to be decommissioned. The assessment should also consider significant and emerging trends that change the services and resilience required from the infrastructure and changes to the means to deliver them. Objectives and targets for improvements of infrastructure resilience should be set and based on the assessment.

The relevant organizations should identify stakeholders in all infrastructure, ensure participation in the identification and assessment process, manage the assessment and collect the evidence.

Stakeholders of infrastructure resilience can have various roles, including:

a) Governments who:

- initiate changes to policy, subsidy, and penalty for infrastructure resilience,
- appoint or identify relevant organizations with responsibility for infrastructure resilience,
- allocate necessary funding to resilience-building activities,
- balance short and long-term objectives,
- require that the tendering process for infrastructure projects gives appropriate weighting to resilience considerations, and
- act on assessments and adjust policy priorities, update legal requirements and amend regulations for infrastructure resilience.

b) Infrastructure regulators who:

- introduce obligations on infrastructure operators to develop and maintain long-term resilience strategies,
- require asset management of infrastructure,
- require operators to improve their resilience and,
- monitor for disruptive incidents to essential services.

c) Infrastructure operators who:

- collect information on operational resilience of infrastructure,
- incorporate resilience information into the asset management plans to support decision making,
- monitor for disruptive incidents caused by different types of hazards,
- implement retrofit improvements that improve their ability to absorb future incidents, and,
- monitor their capacity to absorb and adapt to disruptive incidents.

d) Infrastructure owners who:

- invest in skills and capacity to achieve infrastructure resilience,
- incorporate risk and resilience measures in the management plans of the whole infrastructure life cycle,
- require operators to assess potential hazards,
- highlight risks, and
- increase adoption and continual improvement of infrastructure-resilience.

e) Emergency responders who:

- plan for diversity of incidents related to infrastructure disruptions,
- contribute and advise on infrastructure resilience plans,
- support stakeholders and assets when disruptions occur, and
- provide feedback for future planning and lessons learned.

f) Financial partners and insurers who:

- collect data on hazards and vulnerabilities to better understand their financial risks,

- improve risk management,
 - integrate resilience considerations into their decision-making processes, and
 - identify the willingness to fund/finance investment for reduced disruptive incidents.
- g) Planners, designers and engineers who:
- establish initial infrastructure resilience through appropriate plans and designs,
 - provide handover documents and models that inform operational decisions for maintaining resilience, and
 - design ways to collect operational data for monitoring resilience during the operational stage.
- h) Suppliers who:
- develop and implement tools that anticipate future needs and generate infrastructure resilience,
 - create tools to collect operational data, and
 - collect information on the resilience of infrastructure during their construction.
- i) Academia who:
- support innovation through research in engineering, architecture, planning, construction and other topics, and
 - provide evidence including research from international sources.
- j) Professional, industry and sectoral associations who:
- support resilience by sharing their knowledge and the experience of their industry members,
 - provide training for updating knowledge and skills, and
 - collect information on environmental and social hazards.
- k) Civil society and non-governmental organizations who:
- mediate relations with communities by improving local people's capacity to understand infrastructure resilience; communicating the needs of vulnerable groups; providing a stronger context in communities to support infrastructure resilience; and representing and being the voice of people in the community,
 - help engage the public at large, for instance by promoting responsible practices that are intended to increase infrastructure resilience,
 - engage in decision-making, planning and monitoring of infrastructure (e.g. through stakeholder consultations), and
 - capture the concerns and potential concerns of the public.

4.4 Setting priorities

The relevant organizations should identify and prioritize interventions aligning with the infrastructure resilience assessment and the agreed objectives.

However, the ability to deliver on the identified priorities depends on the infrastructure resilience capabilities of the organizations. To make progress on delivering infrastructure resilience, it should be necessary for organizations to increase the maturity of their capabilities.