CEN

WORKSHOP

AGREEMENT

CWA 18390

June 2026

ICS 13.200

English version

Guidelines for Disaster Risk Preparedness Solutions - Project tools, platforms and processes - Good practice recommendations

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No.:CWA 18390:2026 E

Contents

Foreword

This CEN Workshop Agreement (CWA 18390:2026) has been developed in accordance with CEN-CENELEC Guide 29 “CEN/CENELEC Workshop Agreements - A rapid way to standardization” and with the relevant provisions of the CEN/CENELEC Internal Regulations – Part 2.

It was approved on 2026-05-12 by the CEN Workshop “Guidelines for Disaster Risk Preparedness Solutions”, the secretariat of which is held by UNI (Italian National Standards Body), consisting of representatives of interested parties, the constitution of which was supported by CEN following the public call for participation made on 2025-07-30. However, this CEN Workshop Agreement does not necessarily include all relevant stakeholders.

The final text of this CEN Workshop Agreement was provided to CEN for publication on 2026-05-21.

This CWA has been developed building upon results from the SYNERGIES and PARATUS projects, which received funding from the European Union’s Horizon Europe research and innovation programme under Grant Agreement numbers 101121172 and 101073954, respectively.

The following organizations and individuals developed and approved this CEN Workshop Agreement:

— HALL Benjamin (Chair) - THE RESILIENCE ADVISORS NETWORK

— MANSI Paolo (Secretary) - UNI ENTE ITALIANO DI NORMAZIONE

— AGORASTOU Zoi - INFORMATION AND TECHNOLOGIES INSTITUTE (ITI), CENTRE FOR RESEARCH AND TECHNOLOGY HELLAS (CERTH)

— AMMELUNG Bernd

— ANTUNES Dalila - THE EQUATOR COMPANY, S.A

— AUMAYR Georg - JOHANNITER ÖSTERREICH AUSBILDUNG UND FORSCHUNG GEMEINNÜTZIGE GMBH

— BISCHOFF Johanna - DEUTSCHES RETTUNGSROBOTIK-ZENTRUM E.V.

— BULLER Stephanie

— CAILLARD Bastien - INERIS DEVELOPPEMENT

— CAPEZZUTO Pasquale - ASSOCIAZIONE ENERGY MANAGERS

— CHASIOTIS Ioannis - SATWAYS LTD.

— CIMINO Monica - ENEA

— DOMINICIS Luigi De - ENEA

— GADSDON Steve - SPARROW EU DRS PROJECT

— GKOTSIS Ilias - INLECOM INNOVATION

— GOLFETTI Alessia - DEEP BLUE

— GUILLOIS Rodolphe - EXAMO

— HABIG Therese - SAFETY INNOVATION CENTER gGMBH

— HALL Jon - THE RESILIENCE ADVISORS NETWORK

— HUANG Chen - STIFTELSEN NORSAR

— JAHO Eva - EXUS AI LABS

— JEDLIČKA Karel - SPARROW EU DRS PROJECT

— KAPASAKALIS Kostis - SPARROW EU DRS Project

— KAZANTZIDOU-FIRTINIDOU Danai

— KERESZTESI Kamilla - SZÉKELY FAMILY & CO. NONPROFIT KFT.

— KIPARAKIS Georgios

— KONTOU Vaso - SINGULARLOGIC

— LAOUDIAS Christos - SPARROW EU DRS PROJECT

— LARRAÑETA Javier - PESI (PLATAFORMA TECNOLÓGICA ESPAÑOLA DE SEGURIDAD INDUSTRIAL)

— LAZAROVA Yana - CS GROUP

— LERBERGHE Daniel Van - EXUS AI LABS

— LI Echo

— MATERA Sonia - DEEP BLUE

— MEJIA-AGUILAR Abraham - EURAC RESEARCH

— MESLEM Abdelghani - STIFTELSEN NORSAR

— MICHAILIDOU Christina - SPARROW EU DRS PROJECT

— MJELVA Arve - STIFTELSEN NORSAR

— NERANTZIS Elizabeth - ALPHA CONSULTANTS

— PACHECO Carla - INESC-ID

— PALMA-OLIVEIRA José - THE EQUATOR COMPANY, S.A

— PANTELI Mathaios - SPARROW EU DRS PROJECT

— PAPADAKIS Nikos - SPARROW EU DRS PROJECT

— PASTOR Raúl - PESI (PLATAFORMA TECNOLÓGICA ESPAÑOLA DE SEGURIDAD INDUSTRIAL)

— PERLEPES Leonidas - SATWAYS LTD.

— PINTO Diogo Miguel - POSTGRADUATE IN GIS AND CIVIL PROTECTION LAW

— POUSTOURLI Aikaterini - INTERNATIONAL HELLENIC UNIVERSITY (IHU)

— POZZI Simone - DEEP BLUE

— ROSA Beatriz - THE EQUATOR COMPANY, S.A

— SALVI Olivier - INERIS DEVELOPPEMENT

— SIMONSEN Sebastian - PROMETECH B.V

— SOUSA Maria Luísa

— ŠPELDOVÁ Eliška - TECHNOLOGICAL PLATFORM ENERGY SECURITY CZECH REPUBLIC (TPEB)

— STŘÍTECKÝ Vit - TECHNOLOGICAL PLATFORM ENERGY SECURITY CZECH REPUBLIC (TPEB)

— STURM Nadine - SPARROW EU DRS PROJECT, JOHANNITER ÖSTERREICH AUSBILDUNG UND FORSCHUNG GEMEINNÜTZIGE GMBH

— SULZER Jean-Francois

— SZÉKELY Zoltán - SZÉKELY FAMILY & CO. NONPROFIT KFT.

— SZÉKELY-KERESZTESI Orsolya - SZÉKELY FAMILY & CO. NONPROFIT KFT.

— SZKLARSKI Łukasz - ITTI

— TSALOUKIDIS John

— VENKATASUBRAMANIAN Balaji - SPARROW EU DRS PROJECT

— VOLLMER Maike

— YANEV Viktor - SPARROW EU DRS PROJECT

— ZAMMIT Allison - COMMISSION ON THE RIGHTS OF PERSONS WITH DISABILITIES (CRPD)

— ZOLTAN Hozbor

Attention is drawn to the possibility that some elements of this document may be subject to patent rights. The CEN-CENELEC policy on patent rights is described in CEN-CENELEC Guide 8 “Guidelines for Implementation of the Common IPR Policy on Patent”. CEN shall not be held responsible for identifying any or all such patent rights.

Although the Workshop parties have made every effort to ensure the reliability and accuracy of technical and non-technical descriptions, the Workshop is not able to guarantee, explicitly or implicitly, the correctness of this document. Anyone who applies this CEN Workshop Agreement shall be aware that neither the Workshop, nor CEN, can be held liable for damages or losses of any kind whatsoever. The use of this CEN Workshop Agreement does not relieve users of their responsibility for their own actions, and they apply this document at their own risk. The CEN Workshop Agreement should not be construed as legal advice authoritatively endorsed by CEN/CENELEC.

Introduction

This CEN Workshop Agreement (CWA) provides guidance relating to solutions, approaches and supporting practices for the preparedness phase of disaster risk management.

It focuses on preparedness activities that help authorities, organisations, communities and other stakeholders anticipate, plan, coordinate and improve readiness for potential disasters.

The CWA addresses preparedness-related aspects such as planning, coordination, training and exercises, situational awareness and information sharing, and other organisational aspects that contribute to preparedness.

It does not address mitigation or prevention measures intended to reduce hazard exposure or vulnerability, nor does it cover response operations or post-disaster recovery.

Through an inclusive and collaborative approach, this CWA aims to support greater consistency, interoperability and knowledge sharing in disaster preparedness across Europe.

The Workshop engaged a wide range of stakeholders, including projects from the Societal Resilience Cluster (SRC), notably the SYNERGIES and PARATUS projects which initiated this Workshop, as well as contributors from the Responder Technology Cluster (RTC) and the CBRNe and Standardisation Cluster (CSTAC), facilitated through CMINE. Participation also included policymakers, emergency services, humanitarian actors, researchers, and representatives of civil society. This cross-cluster engagement has reinforced knowledge exchange, alignment, and collaboration.

The following is a list of the main projects[1] which participated in the drafting of the CWA:

SYNERGIES, PARATUS, DIREKTION, Driver+, RESILOC, GUARDIANS, MYRIAD-EU, TOGETHER, HARMONY, RiskPACC, SPARROW, DARE, ECHO, UNICORN, OVERWATCH, AGILE, FASTER, EMBRACE, PEERS, B-PREPARED, CARMA, CHIMERA, HURRICANE, INCLUDING, MEDiate, PALAESTRA, STRATEGY, TeamAware, RESILIACT, HARMONI, DYNAMO, MAVRIC-CERT, INTEGRA CBRN.

The resulting CWA has been developed with consideration of the wider European and international policy context for disaster risk management, preparedness, resilience and civil protection, where relevant to its scope and purpose. It also complements relevant standards and ongoing activities within CEN, in particular those of CEN/TC 391 Societal and Citizen Security.

The key elements addressed in this CWA can be understood through the framework illustrated in Figure 1. The framework highlights the relationship between documentation, governance, interoperability and sustainability considerations when developing and maintaining preparedness solutions. Together, these elements support the consistent description, responsible management, discoverability and long-term availability of preparedness solutions.

The development of shared guidance documents, reference frameworks or common descriptive models may itself form part of a sustainability strategy. Such outputs can help retain and transfer knowledge generated by projects, support continuity across successive initiatives, and provide a stable basis for the longer-term use, adaptation and visibility of project outcomes, including tools, platforms and associated processes.

[1] Further information on these projects is available on CORDIS (Community Research and Development Information Service): https://cordis.europa.eu/it

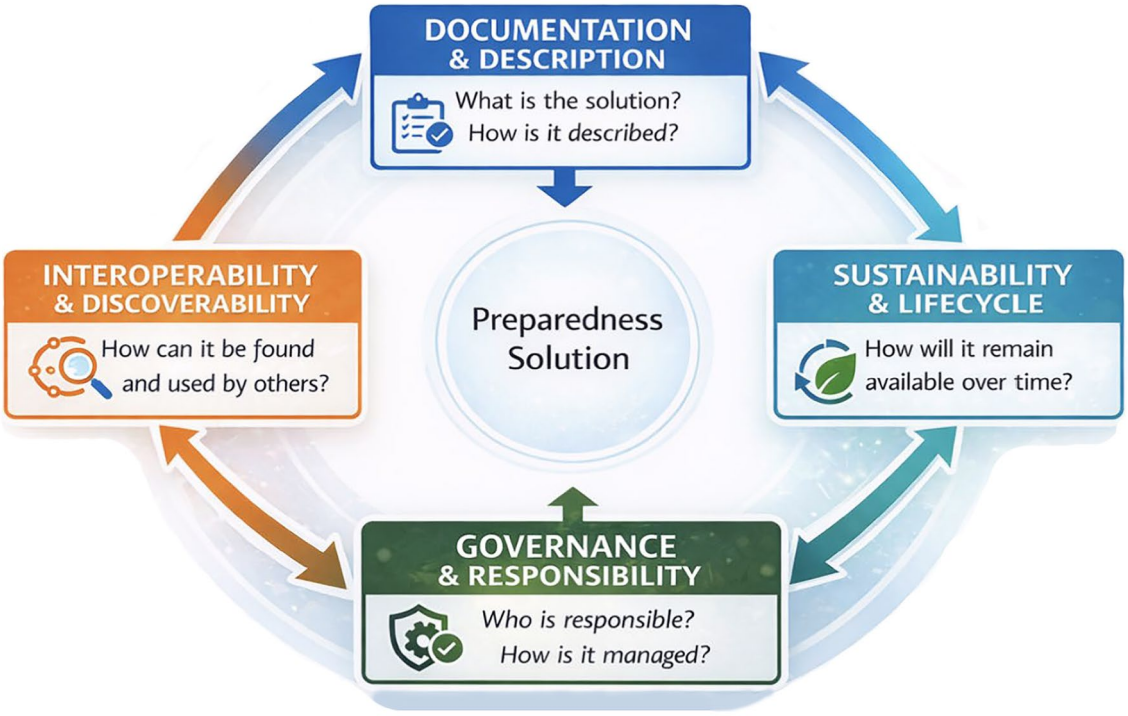

Figure 1 — Conceptual framework for documenting and sustaining disaster preparedness solutions

1 Scope

This CEN Workshop Agreement provides guidance for the preparedness phase of disaster risk management. It focuses on the alignment of how tools, platforms, and processes developed for disaster risk preparedness are presented, organised, maintained, and made discoverable, providing a practical reference of good practices that research and innovation (R&I) projects and other stakeholders can adopt and adapt.

This CWA addresses the documentation and presentation of preparedness solutions developed through research, innovation and operational programmes. It promotes the adoption of shared descriptors and quality practices so that these outputs can be more easily identified, compared and applied by different organisations.

It also covers aspects of governance, sustainability, interoperability and communication that influence how such solutions are developed, accessed and retained.

Examples of preparedness solutions include but are not limited to emergency communications systems, digital twins or other systems to gather data and show the operational picture, risk assessment modules, decision support systems, and training modules.

The recommendations are designed to support:

— teams, organisations or bodies undertaking research and innovation activities that produce preparedness solutions;

— teams, organisations or bodies undertaking initiatives that identify, assess or select preparedness solutions for operational or policy use;

— civil-protection and emergency-management authorities;

— practitioner and responder organisations;

— policy and funding bodies seeking to align or evaluate initiatives; and

— entities responsible for maintaining catalogues, repositories or training material.

This CWA applies to preparedness solutions addressing both rapid-onset and slow-onset hazards, recognising that different hazard dynamics may influence how preparedness activities are documented and presented. It is applicable to both digital and non-digital outputs, ranging from software platforms and data services to operational procedures, training frameworks and collaborative processes.

While primarily intended for European use, the guidance may also inform cooperation and exchange beyond Europe where appropriate.

This CWA does not prescribe any particular technical architecture, management structure or legal arrangement. It provides a voluntary reference that organisations can adopt or adapt to suit their own context. It is not intended to establish conformity assessment, auditing or certification schemes. Users remain responsible for ensuring compliance with applicable legislation, standards and organisational requirements.

The scope of this CWA is limited to the preparedness phase of disaster risk management. Certain elements of the recommendations may also prove useful for prevention, mitigation, response or recovery activities; however, those areas lie outside the present Scope.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardisation at the following addresses:

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

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

Note 1 to entry: In this document, the term "critical entities" is used in line with current European legislation, while "critical infrastructure" is retained where relevant to refer to the physical structures, facilities, networks and other assets operated or managed by such entities, and to maintain compatibility with broader international terminology.

3.1
civil protection
measures taken and systems implemented to preserve the lives and well-being of people, properties and environment from undesired events

[Source: EN ISO 22300:2025]

3.2
community resilience
capacities of local communities, as complex systems, to mitigate, withstand and recover from the impacts of a disaster or emergency, and to adapt or transform to be less vulnerable to future events

3.3
critical infrastructure
physical structures, facilities, networks and other assets which provide essential services for the social and economic functioning of a community or society, and which may be operated or managed by critical entities

[Source: UNDRR Terminology, modified – "and which may be operated or managed by critical entities" has been added]

3.4
disaster risk
potential loss of life, injury, or destroyed or damaged assets which could occur to a system, society or community in a specific period of time, determined probabilistically as a function of hazard, exposure, vulnerability and capacity

[Source: UNDRR Terminology]

3.5
disaster risk management
application of disaster risk reduction policies and strategies to prevent new disaster risk, reduce existing disaster risk and manage residual risk, contributing to the strengthening of resilience and reduction of disaster losses

[Source: UNDRR Terminology]

3.6
early warning system
integrated system of hazard monitoring, forecasting and prediction, disaster risk assessment, communication and preparedness activities that enables individuals, communities, governments, businesses and others to take timely action to reduce disaster risks in advance of hazardous events

[Source: UNDRR Terminology]

3.7
exposure
situation of people, infrastructure, housing, production capacities and other tangible human assets located in hazard-prone areas

[Source: UNDRR Terminology]

3.8
hazard
process, phenomenon or human activity that may cause loss of life, injury or other health impacts, property damage, social and economic disruption or environmental degradation

[Source: UNDRR Terminology]

3.9
interoperability
ability of independent systems, organisations and processes to work together

Note 1 to entry: In this CWA, "work together" refers to the exchange, interpretation and use of data and information in a coherent and meaningful way, across technical, semantic, organisational and legal dimensions.

[Source: EN ISO 22300:2025, modified – Note 1 to entry has been added]

3.10
multi-hazard
approach that considers the possibility that multiple hazards may occur simultaneously, cascadingly or cumulatively over time, and the potential interrelated effects of such events on people, systems and communities

3.11
preparedness
knowledge and capacities developed by governments, response and recovery organisations, communities and individuals to effectively anticipate, respond to and recover from the impacts of likely, imminent or current disasters

[Source: UNDRR Terminology]

3.12
preparedness solution
product, tool, methodology, dataset, process, service or other solution that supports activities undertaken in the preparedness phase of disaster risk management, including planning, assessment, training, communication, coordination, early warning and capability development

3.13
risk assessment
overall process of risk identification, risk analysis and risk evaluation

[Source: ISO 31000:2018]

3.14
risk communication
process of exchanging or sharing risk-related data, information and knowledge between and among different groups (for example scientists, regulators, industry and the public)

3.15
solution
<crisis/preparedness management> one or more processes or tools with related procedures contributing to a crisis or preparedness management function

3.16
vulnerability
conditions determined by physical, social, economic and environmental factors or processes which increase the susceptibility of individuals, communities, assets or systems to the impacts of hazards

[Source: UNDRR Terminology]

4 Purpose and guiding Principles

4.1 Purpose

This Workshop Agreement provides recommendations intended to align the way disaster risk preparedness solutions are documented, made accessible and sustained.

It aims to reduce fragmentation, improve comparability and support the long-term use of outputs developed through publicly funded and collaborative initiatives.

This CWA encourages a shared approach so that such solutions can be more easily identified, understood and taken up by a wide range of users. It supports a whole-of-society approach to preparedness, recognising that resilience depends on collaboration across public authorities, practitioners, communities, researchers and private-sector actors.

The document is advisory in nature. It supports alignment and cooperation between ongoing activities and offers a practical foundation for ensuring that knowledge, tools and platforms remain available after the completion of individual projects.

4.2 Intended users and application

These guidelines are designed for use by research and innovation projects, civil-protection and emergency-management authorities, responder organisations, policymakers, funding bodies, practitioners, private enterprises, academic institutions and community actors involved in preparedness.

They may be applied when preparing project deliverables, organising repositories or catalogues, planning post-project maintenance, developing exercises or validation activities, assessing the maturity of existing solutions, designing preparedness solutions, planning their integration with existing systems, or considering interoperability with other solutions.

4.3 Objectives and expected benefits

The main objectives are to:

— improve clarity and comparability by proposing a common descriptive approach;

— strengthen discoverability and access to preparedness solutions;

— enhance interoperability across sectors and systems;

— encourage planning for sustainability and maintenance;

— promote evidence-based development and transparency;

— facilitate collaboration and the exchange of good practices; and

— strengthen cooperation and mutual learning across related initiatives.

Adoption of the guidance is expected to limit duplication of effort, improve coherence, improve visibility of available solutions and increase the collective value of preparedness solutions.

4.4 Scope boundaries

This CWA is limited to the preparedness phase of disaster risk management. It does not establish certification or compliance mechanisms and does not prescribe particular technologies, architectures or legal arrangements.

4.5 Guiding principles

The recommendations in this CWA are based on a set of principles that recognise preparedness as a collective, whole-of-society endeavour:

1. **Public value and openness**: wherever possible, information about preparedness solutions should be accessible, with clear conditions for its use.

2. **Proportionality**: documentation and procedures should remain appropriate to the scale and purpose of the activity.

3. **Clarity of language**: text should be concise and use terminology consistent with recognised sources.

4. **Evidence and transparency**: the origin, testing and validation of a solution should be traceable.

5. **Interoperability by design**: preference should be given to open standards and compatible data formats.

6. **Sustainability**: early planning for long-term viability, including responsible resource use, maintenance, adaptation and hand-over, should be part of every project.

7. **Clear ownership and licensing**: responsibilities and rights of use should be unambiguous.

8. **Inclusiveness and accessibility**: engagement of diverse user groups, including vulnerable populations, and the provision of accessible formats, interfaces and communication should be considered.

9. **Ethical and secure practice**: handling of data and information should comply with relevant legal and ethical requirements.

10. **Feedback and improvement**: mechanisms for user feedback should inform updates and revisions.

4.6 Application of the principles

In practice, the principles can be implemented through clear documentation (see Clause 5), well-defined roles and responsibilities (see Clause 6), sustainable lifecycle planning (see Clause 7), interoperability measures (see Clause 8), inclusive engagement processes (see Clause 9) and continuous review (see Clause 10).

Organisations may apply the guidance incrementally, focusing first on core descriptive information and gradually developing fuller documentation and governance measures.

4.7 Measuring progress

Progress can be observed through quantitative and qualitative indicators such as the number of solutions with complete descriptive profiles, visible licensing statements, available validation evidence or established maintenance arrangements.

5 Documentation, common descriptors and quality considerations

5.1 General

Consistent documentation is essential to ensure that preparedness solutions can be understood, compared and reused by others.

Good documentation supports transparency, enables interoperability and assists in maintaining the value of outputs once a project or initiative has concluded.

This clause sets out elements that should be considered when recording and presenting information about preparedness solutions.

5.2 Descriptive information

Each solution should include a concise description that allows users to understand its purpose and context.

As a minimum, it is recommended that documentation provides:

— the title of the solution, version, date and responsible organisation;

— a description of the addressed preparedness need or gap;

— a summary of its intended use, key functions and expected results;

— identification of the principal contact point or maintaining entity;

— references to relevant projects, partners or funding sources;

— where possible, a stable link or identifier to access further information;

— the intended users or target audience for the solution (for example authorities, practitioners, volunteers, researchers or communities);

— references to relevant scientific, technical, policy, operational, or media publications where these support traceability or understanding of the solution;

— information on the maturity of the solution, and, where appropriate, the technology readiness level (TRL);

— references to any available use-cases, exercises, pilots or operational deployments.

Where several related outputs exist within one project, these should be described in a consistent format to support comparability.

A template of descriptive information is provided in Annex A.

5.3 Content and structure

The level of detail should be proportionate to the complexity and potential use of the solution. A clear structure, using sections such as overview, technical details, dependencies and supporting materials, helps future users locate information easily.

Text should be written in plain and neutral language and avoid unnecessary technical or institutional jargon.

Terminology should follow recognised sources such as EN ISO 22300, ISO 31000 and UNDRR Terminology. Where new or alternative terminology is introduced, it is recommended that the reason for diverging from existing definitions be explained briefly, so that users can understand the rationale and context.

5.4 Metadata and identifiers

Where possible, metadata should conform to existing cataloguing or repository standards so that information can be indexed and searched efficiently.

This may include standardised metadata fields describing the solution itself, such as title, keywords, author, date, geographical scope, hazards addressed and maturity level.

Where relevant, associated datasets may require separate metadata appropriate to their own management and use.

Persistent identifiers (for example DOIs or institutional catalogue references) are encouraged to maintain long-term traceability.

As an indicative good practice, where solutions generate or rely on operationally relevant data, metadata may include consistent time information and location information in a form appropriate to the solution's purpose and context (for example, to support correlation between independently captured datasets). The level of detail and method used should remain proportionate and should respect security, privacy and legal constraints.

5.5 Quality assurance

Documentation should indicate whether, and how, the solution has been tested, validated or reviewed. This may include information on:

— methods used for verification or validation, such as exercises, trials or peer review;

— performance indicators or evaluation results, where available; and

— known limitations or conditions under which the solution is effective.

Where formal quality-management systems exist within participating organisations, they may be used to support these processes.

5.6 Version control and change management

Preparedness solutions often evolve over time.

It is therefore recommended that documentation includes a version number, revision date and a short summary of changes.

A clear change-management procedure should describe who is authorised to update content, how updates are recorded and how earlier versions can be retrieved when required.

5.7 Data management and FAIR principles

When the solution involves the use or production of data, documentation should describe the data's origin, format and accessibility.

Data should, where practicable, follow the FAIR principles (Findable, Accessible, Interoperable and Reusable).

Information about data licensing, privacy protection and security measures should be included to support responsible use.

5.8 Accessibility and language

Documents should be prepared in an accessible format and, where feasible, translated or summarised in additional languages relevant to intended users.

Figures, tables and diagrams may be used to aid understanding, provided that textual explanations accompany them.

Digital documents should be compatible with common formats and accessibility standards.

5.9 Relationship to other frameworks

Where relevant, references should be provided to existing standards, regulations, or related initiatives that the solution aligns with.

Documenting these linkages assists in identifying overlaps, complementarities and potential integration opportunities with other preparedness activities.

Where available, existing research dashboards, repositories or mapping tools may be used to identify related initiatives, themes or solutions. Such resources can support shared situational awareness across the preparedness community and help reduce duplication of effort.

5.10 Maintenance of documentation

Responsibility for keeping documentation current should be clearly assigned.

Periodic review at intervals proportionate to the rate of change of the solution helps ensure accuracy and continued usefulness.

Updates should be communicated through the same channels where the documentation is published, ensuring users are aware of revisions.

6 Governance, roles and ethics

6.1 General

Clear and transparent governance supports accountability, quality and continuity in the development and maintenance of preparedness solutions.

Governance structures should be proportionate to the scale and complexity of the activity and should define who is responsible for decision-making, validation, maintenance and communication.

This clause sets out guidance on governance arrangements, role definition, accountability and ethical conduct relating to preparedness solutions.

6.2 Governance framework

Each preparedness solution should have an identifiable governance framework that describes how decisions are made, how responsibilities are shared and how changes are approved.

This should include:

— designation of an overall owner or custodian responsible for oversight and continuity;

— identification of contributors and partners, including their roles in design, testing, deployment and review;

— procedures for risk management, including legal, operational and reputational risks; and

— methods for reporting issues or suggesting improvements;

— procedures for monitoring and evaluation, including responsibilities and methods for assessing the continued relevance, usability and performance of the preparedness solution.

Where several organisations cooperate on a shared solution, the governance arrangements should be recorded in writing and agreed by all parties. This ensures transparency and helps maintain continuity if staff or partners change.

6.3 Roles and responsibilities

Typical roles that may be defined within a governance model include:

— **Owner or custodian:** holds overall responsibility for the solution, including its availability, integrity and maintenance.

— **Contributor or developer:** provides technical, scientific or procedural input to create or improve the solution.

— **Validation or assessment body:** validates the solution and assesses the accuracy, usability or performance of the solution.

— **User or implementer:** applies the solution in operational or policy contexts and provides feedback.

— **Support or maintenance function:** ensures hosting, updates, and user assistance are maintained as needed.

In smaller organisations or projects, one entity may perform several of these roles. It is important that responsibilities are clearly defined and properly documented.

6.4 Decision-making and accountability

Decision-making should follow transparent and traceable processes.

Records should be kept of major decisions, version approvals and governance meetings.

Responsibilities for approving changes, archiving obsolete material and communicating updates should be explicitly assigned.

Where solutions are made available to external users, clear contact points should be provided for feedback, questions or incident reporting.

6.5 Ethical conduct and integrity

Ethical principles underpin the responsible use of preparedness solutions.

Developers and custodians should ensure that their work:

— respects human rights and fundamental freedoms;

— considers accessibility and inclusion of all user groups;

— avoids discrimination, bias or exclusion;

— protects privacy and personal data in line with applicable legislation; and

— promotes trust, transparency and fairness in the way information is shared or decisions are supported.

Where automated or data-driven systems are used, documentation should describe how potential ethical issues such as bias, explainability or accountability have been addressed.

6.6 Legal and regulatory compliance

All activities associated with the creation and operation of preparedness solutions must comply with applicable laws and regulations, including those related to data protection, cybersecurity, intellectual property and accessibility.

Where relevant, reference should be made to the legal basis under which data are collected or processed, and to the ownership and licensing arrangements governing the solution.

Where preparedness activities rely on digital collaboration platforms (for example document-sharing systems, conferencing tools or shared workspaces), organisations should consider the hosting location and applicable jurisdiction of those services. In contexts where legal, regulatory or public-sector requirements apply, preference may be given to configurations that support appropriate data residency and alignment with the geographical scope of the initiative. The selected tooling and any relevant hosting region should be documented in a manner proportionate to the sensitivity of the information being handled.

6.7 Transparency and communication

Governance should include measures to ensure that relevant stakeholders can access information about how a solution is managed and by whom.

Where appropriate, summaries of governance arrangements may be made public to demonstrate openness and build user confidence.

Feedback mechanisms should be in place to allow users to raise issues or contribute to improvements.

6.8 Continuity and handover

Governance arrangements should anticipate the need for continuity after a project or funding period ends.

Plans should specify how ownership, data and documentation will be transferred, and who will assume future responsibility.

Where no long-term custodian is available, consideration should be given to archiving the solution in a recognised repository with sufficient information for others to reuse or maintain it.

6.9 Review and improvement

Governance models should not remain static.

They should be reviewed periodically to ensure they remain effective and aligned with current legislation, organisational policies and stakeholder needs.

Feedback from users, maintainers and partners should inform these reviews, supporting continuous improvement in transparency, quality and alignment with ethical practice.

7 Sustainability, licensing and lifecycle

7.1 General

Preparedness solutions deliver the greatest value when they remain accessible, functional and relevant beyond the lifetime of the project or initiative in which they were developed.

Sustainability depends on clear ownership, adequate resources, appropriate licensing, and a realistic plan for maintenance and evolution.

This clause provides guidance on lifecycle management, long-term sustainability, licensing and responsible custodianship of preparedness solutions.

7.2 Lifecycle approach

A lifecycle approach considers the different stages a preparedness solution passes through, including conception, design, development, integration, testing, validation, operation, maintenance and decommissioning.

Planning for each stage should occur as early as possible to ensure continuity and responsible use of resources. Documentation should also describe the current maturity of the solution and, where relevant, outline any additional steps, resources or conditions required for operational adoption or wider deployment.

When the development of a solution is publicly funded, arrangements for long-term access and maintenance should be addressed explicitly in the project's exit or sustainability plan.

7.3 Ownership and custodianship

Each solution should have a clearly identified owner or custodian who holds overall responsibility for its maintenance and availability.

Ownership may rest with the developing organisation, a consortium partner, or a designated public body. Where ownership is shared, written agreements should specify the respective rights and obligations of all parties.

If a custodian cannot continue maintaining the solution, provisions should exist for transfer of responsibility to another suitable entity, ensuring that access to the solution is not lost.

7.4 Sustainability planning

Sustainability planning should be proportionate to the complexity and expected lifespan of the solution. Considerations may include:

— the availability of financial or institutional support after the end of project funding;

— the need for technical maintenance, security updates or hosting services;

— arrangements for user support and documentation updates; and

— identification of long-term repositories or platforms that can preserve the solution and its associated materials.

Where long-term maintenance is not feasible, it remains good practice to ensure that documentation and source materials are archived in a way that allows others to understand and, where appropriate, replicate or build upon the work.

Sustainability planning should consider, from an early stage, whether project outcomes should be deposited in shared repositories or catalogues so that they remain visible, citable and accessible beyond the project lifecycle and independent of any single

The development of shared guidance documents, reference frameworks or common descriptive models may itself form part of a sustainability strategy. Such outputs can help retain and transfer knowledge generated by projects, support continuity across successive initiatives, and provide a stable basis for the long-term use, adaptation and visibility of project outcomes, including tools, platforms and associated processes.

Sustainability planning should also consider whether long-term commitments can be secured for domain names, web content and principal access points associated with project outcomes, so that visibility and access are not dependent solely on the duration of project funding or on the continued capacity of one delivery partner.

7.5 Licensing and access conditions

Licensing terms should be stated clearly and aligned with the intended use of the solution. Where possible, open or permissive licences (such as Creative Commons or the European Union Public Licence) are encouraged to facilitate reuse and transparency.

Licences should specify the conditions under which materials, software or data may be used, modified or redistributed.

For proprietary or restricted-access solutions, information should still be provided to explain how users can request access or obtain permissions.

Clarity of licensing helps to avoid misunderstandings and supports lawful reuse of publicly funded results.

7.6 Hosting, repositories and archiving

To support continuity and long-term visibility, projects should consider the use of shared, stable and trustworthy repositories for the deposit of documentation, key outputs and, where appropriate, tools, datasets and associated materials. Such arrangements can reduce the risk that valuable results become inaccessible when project funding ends, hosting arrangements change, or the originating organisation is no longer able to maintain them, and can strengthen the visibility and usability of project outcomes.

These may include institutional repositories, national or European research data infrastructures, or recognised domain-specific catalogues and platforms.

Repositories should provide version control, persistent identifiers and clear metadata to enable discovery and citation.

Where digital services are hosted online, arrangements for ongoing maintenance, cybersecurity and disaster recovery should be documented.

When a service is discontinued, users should be informed in advance and given access to archived materials wherever possible.

To support sustainability, projects should seek long-term arrangements for the continuity of domain names and associated web content that provide access to preparedness solutions. This may include the involvement of trusted third-party organisations able to maintain domain availability, hosting, archived content or persistent redirection beyond the lifetime of the project and beyond the continued participation of any individual partner. Such measures can materially strengthen the long-term visibility and usability of project outcomes.

7.7 Capacity and knowledge retention

Effective take-over and continued use of preparedness solutions also depend on people and skills.

Projects should plan for knowledge transfer between developers, maintainers and users, for example through training, documentation, and community engagement.

Establishing a small support network or advisory group can help retain institutional memory and ensure that expertise is not lost when projects or staff change.

7.8 Monitoring and evaluation

The continued relevance and effectiveness of preparedness solutions should be reviewed periodically. As an indicative good practice, solutions may be reviewed at regular intervals (for example every 1–2 years), taking account of their rate of change, user base and operational context.

Monitoring can include the number and type of users, feedback received, performance indicators, or the degree of integration with other systems. Monitoring results should be appropriately documented to inform evaluation.

Evaluation findings should inform updates, maintenance priorities or decisions to retire a solution that is no longer suitable.

7.9 End-of-life and archiving

When a solution reaches the end of its useful life, steps should be taken to archive documentation and related data in an accessible form.

The reasons for decommissioning should be recorded, and lessons learned should be captured for future initiatives.

Where a successor solution exists, documentation should include references to the new version or related systems.

7.10 Continuous improvement

As technologies, risks and user needs evolve, preparedness solutions and their supporting arrangements should be reviewed and adapted accordingly.

Continuous improvement refers to the ongoing review and updating of a preparedness solution and its supporting arrangements throughout its lifecycle. Improvements may arise from user feedback, evaluation activities, operational experience or technological developments. The results of continuous improvement are incremental changes to process and tools, and may concern one or more phases of the solution lifecycle, or licensing updates.

Continuous improvement encourages adaptability and ensures continued value from investments in preparedness.

8 Interoperability, discoverability and access

8.1 General

Interoperability and discoverability are essential to ensure that preparedness solutions developed across different projects, sectors and regions can work together effectively.

They enable solutions to be located, compared and integrated, supporting collaboration and reducing duplication of effort.

This clause addresses technical, semantic and organisational interoperability, discoverability of solutions, access arrangements and related security and validation considerations.

8.2 Interoperability

Interoperability refers to the ability of independent systems, organisations and processes to exchange, interpret and use data and information in a coherent and meaningful way, across technical, semantic, organisational and legal dimensions. Projects and organisations developing preparedness solutions should consider interoperability from the outset and throughout the lifecycle of their work.

Key considerations include:

— the use of open standards, protocols and interfaces to enable data exchange;

— alignment with existing European and international interoperability frameworks, such as INSPIRE, EN ISO 19115 series or CWA 17513;

— clear definition of data formats, structures and access methods;

— mapping of terminologies and taxonomies to recognised reference vocabularies; and

— documentation of dependencies, assumptions and limitations that may affect interoperability.

Efforts to achieve interoperability should remain proportionate to the scale and intended use of the solution. Where direct interoperability cannot be achieved, documentation should explain the reasons and identify possible pathways for future integration.

8.3 Semantic and organisational coherence

Semantic interoperability ensures that shared information is interpreted in the same way by all users. This may be supported by the use of controlled vocabularies, ontologies or thesauri, developed in alignment with established international frameworks.

In the European context, preparedness solutions may also be mapped using recognised classification systems, such as the EU Civil Security Taxonomy developed under the EU Security Market Study. This taxonomy provides a structured, multi-level classification of security domains (Level 1–3), including disaster risk resilience, critical infrastructure sectors and related thematic areas.

Referencing such structured taxonomies can enhance semantic consistency across projects, facilitate cross-sector comparison, and support alignment with European research, funding and policy frameworks.

Organisational interoperability relates to the ability of institutions to collaborate through compatible policies, processes and governance structures.

Preparedness solutions should therefore describe not only their technical interfaces but also the organisational procedures that enable cooperation, data sharing and joint decision-making.

8.4 Discoverability

Discoverability refers to the ease with which users can find relevant preparedness solutions and information. To improve discoverability, it is recommended that:

— metadata be published in a structured and searchable form, using recognised standards;

— keywords, thematic categories and geographical tags be applied consistently;

— solutions be listed in catalogues, repositories or knowledge platforms that:

  - are accessible to the intended audience;
  - are capable of coupling the need of the repository or platform user to the solution;
  - are actively maintained and designed to support long-term visibility and use;

— persistent identifiers (such as DOIs or stable URLs) be used to ensure reliable referencing.

Where possible, metadata should include concise descriptions, contact information, licence type, and the level of validation or maturity.

A consistent descriptive approach helps users identify and assess the relevance of solutions across multiple domains.

The deposit of project outcomes in shared and trustworthy repositories is encouraged as a means of preserving long-term visibility, discoverability and access, including beyond the end of project funding and beyond the continued capacity of any individual partner to host or maintain the materials.

Long-term discoverability can be strengthened where stable domain names, persistent URLs or managed redirection arrangements are maintained beyond the end of project funding, including through trusted third-party custodians where appropriate.

8.5 Access conditions

Preparedness solutions should be made accessible according to transparent and clearly communicated conditions.

Three broad categories of access can be considered:

— **Open access:** freely available without registration, suitable for information intended for wide public use.

— **Restricted access:** available only to specific authorised users or groups, typically where sensitive or proprietary information is involved.

— **Controlled or managed access:** limited to registered and authorised users, typically when operational or security-sensitive data are included.

Each solution should specify the applicable access level, along with contact details or procedures for obtaining permission where required.

Access arrangements should comply with relevant legal frameworks, including data protection, intellectual property and national security considerations.

8.6 Accessibility and usability

Preparedness information and tools should be presented in formats that are usable by a wide range of audiences, including persons with disabilities, meaning they follow recognised accessibility principles such as clear structure, alternative text for images, readable typography, compatibility with assistive technologies, and use of plain, understandable language.

Digital materials should comply with recognised accessibility standards such as EN 301549 or WCAG guidelines where applicable.

Usability testing with intended user groups can help ensure that solutions are intuitive, reliable and suited to operational contexts.

Language accessibility should also be considered; where feasible, key materials may be provided in more than one European language.

8.7 Security and resilience

Ensuring interoperability and access should not compromise security or system integrity. Preparedness solutions may be exposed to both physical and cybersecurity risks, and appropriate protective measures should be applied to manage these risks. Developers and custodians should implement appropriate cybersecurity measures to protect systems from unauthorised access, tampering or data loss.

Continuity planning should include procedures for backup, recovery and incident response. Users should be informed of any security classifications, encryption requirements or data-handling protocols relevant to the solution.

8.8 Validation and confidence

To support trust and adoption, information about the validation status of a preparedness solution should be made available.

This may include references to field exercises, peer reviews, or technical evaluations that demonstrate the solution’s effectiveness and reliability.

Transparent communication of the validation process allows potential users to assess suitability for their context and promotes confidence in shared outputs.

8.9 Interlinking and federation of resources

Preparedness solutions and catalogues should, where possible, be linked to each other through standardised interfaces or shared identifiers.

This federation of resources enables users to discover complementary tools, datasets or procedures across multiple initiatives.

Efforts to interlink solutions should respect ownership and licensing conditions while promoting visibility and reuse.

8.10 Continuous improvement

Interoperability and discoverability should evolve in step with technological and organisational change. Regular review of descriptors, metadata schemas and repositories ensure that preparedness information remains compatible with emerging systems and standards.

Feedback from users and custodians should guide improvements, ensuring that access to preparedness solutions remains both secure and effective over time.

9 Stakeholder engagement, inclusion and communication

9.1 General

Effective stakeholder engagement and inclusive communication are central to the success and long-term value of preparedness solutions.

Experience across disaster preparedness contexts suggests that effectiveness depends not only on technical solutions but also on territorial variability, community engagement, institutional capacity and the prioritisation of interventions according to local risk conditions.

Disaster risk preparedness depends on the cooperation of many actors - from authorities and practitioners to researchers, communities and private-sector partners.

This clause provides recommendations on stakeholder identification, engagement, inclusion, communication, feedback and knowledge-sharing across the lifecycle of preparedness solutions.

9.2 Stakeholder identification and mapping

Events across Europe have highlighted the critical role of local-level preparedness in managing disaster impacts. Preparedness solutions should therefore remain applicable at the municipal or community scale, where implementation and coordination are frequently carried out in practice. Projects and organisations should begin by identifying relevant stakeholder groups that may influence, or be affected by, the preparedness solution.

These may include:

— public authorities and civil-protection agencies at local, regional, national or international levels;

— responder organisations and emergency service providers, for example police, fire and rescue services, and coast guard authorities;

— research and innovation partners, including universities and technical institutes;

— private-sector entities developing or using technologies relevant to preparedness;

— community groups, NGOs, and civil-society organisations;

— policymakers, funding bodies, and standardisation organisations;

— citizens and end-users who may benefit directly or indirectly from the solution;

— critical infrastructure operators and essential service providers;

— underrepresented or vulnerable groups whose needs may require specific consideration.

Stakeholder mapping should be revisited periodically to reflect changes in the operational environment or project partnerships.

9.3 Principles of engagement

Stakeholder engagement should be conducted in an open, transparent and inclusive manner. Engagement processes should aim to:

— ensure that a range of perspectives, including underrepresented or vulnerable groups, are heard and considered;

— promote co-creation and participatory approaches during design, testing and evaluation;

— maintain regular communication channels for feedback, queries and updates; and

— document key inputs and decisions resulting from engagement activities.

Engagement should be proportional to the scale and scope of the solution and should respect ethical, legal and cultural considerations.

9.4 Inclusion and diversity

Cultural factors across different European contexts, including varying risk perceptions, governance traditions and community engagement practices, may influence preparedness approaches. Documentation of preparedness solutions should remain sensitive to these differences, recognising that levels and forms of preparedness may vary between countries and regions.

Preparedness planning and solution development should take account of gender, age, disability, socioeconomic and cultural diversity, without unnecessary bias.

Inclusive practices help ensure that solutions are relevant and accessible to all segments of society. Where appropriate, materials should be tested with or reviewed by representatives of different user groups to verify accessibility, language clarity and usability.

Training and awareness materials should reflect diverse needs and contexts.

9.5 Community-based preparedness

Community-level organisations, volunteer groups, municipal structures and local associations often play an important role in disaster preparedness. Engagement with community stakeholders can support local ownership, strengthen risk awareness and ensure that preparedness solutions reflect social and territorial realities. Inclusive and participatory approaches may help align community initiatives with municipal and national arrangements while respecting local contexts and capacities.

9.6 Contextual diversity

Preparedness solutions are implemented across diverse social, territorial and cultural settings, including urban and rural areas, remote and low-density regions, multilingual and migrant communities and areas with significant visitor populations. Developers are encouraged to consider these contextual factors so that preparedness solutions remain inclusive, usable and appropriate to differing European settings.

9.7 Communication and dissemination

Communication and dissemination strategies should support the clear and timely sharing of information about preparedness solutions with relevant stakeholders.

Clear and consistent communication strengthens stakeholder confidence and supports adoption of preparedness solutions. Information about the purpose, benefits and limitations of a solution should be communicated in language appropriate to the audience.

Technical details may be shared through professional networks, workshops, or publications, while general information may be disseminated through public websites, newsletters or events.

Projects should ensure that communication products are factual, balanced and verifiable, and that the level of confidence or validation associated with the solution is communicated clearly.

Claims about performance or impact should be proportionate to the available evidence and should avoid implying operational readiness where this has not been demonstrated.

9.8 Knowledge sharing and collaboration

Open exchange of knowledge promotes innovation and learning across the preparedness community. Where possible, projects should share results, lessons learned, and good practices through recognised European or international networks, repositories, and thematic communities.

Joint activities such as webinars, training sessions or collaborative exercises can help validate solutions and increase their practical uptake.

Collaborative mechanisms should respect intellectual property rights and confidentiality obligations while promoting mutual benefit and transparency.

9.9 Feedback and user support

Mechanisms should be established to allow users and stakeholders to provide feedback on functionality, usability, and applicability.

Feedback should be reviewed systematically and, where feasible, used to inform updates or improvements.

Users should have access to a clearly identified contact point, helpdesk or issue-tracking system, together with information on expected support arrangements, including response times or availability where relevant, to support ongoing communication between users and custodians.

9.10 Communication during the lifecycle

Engagement and communication should continue beyond the initial development phase. During the operational phase, regular updates should inform stakeholders of changes, new versions or decommissioning plans. When a solution approaches the end of its lifecycle, users should be given advance notice and clear information on how to access archived materials and, where applicable, on any successor systems or alternative options.

9.11 Transparency and trust

Transparent engagement and communication help build trust in preparedness solutions. Openness should extend to the objectives of the solution, the sources and quality of data used, the governance arrangements under which it is managed, and any known limitations or uncertainties. Proactive communication during both normal operations and periods of change, uncertainty, or crisis events supports stakeholder confidence and ensures continued relevance of the solution.

9.12 Evaluation of engagement

Projects and organisations may periodically monitor and evaluate their stakeholder engagement and communication processes.

Evaluation criteria and key performance indicators (KPIs) can include participation rates, diversity of input, satisfaction of stakeholders, and evidence that feedback has influenced outcomes.

Such evaluations contribute to continuous improvement and to a culture of openness and accountability within the preparedness community.

10 Alignment and continuous improvement

10.1 General

Preparedness solutions should not exist in isolation.

Their long-term effectiveness depends on alignment with relevant policies, standards, and ongoing initiatives, as well as on a process of continuous learning and improvement.

This clause provides guidance on alignment with wider frameworks, coherence across initiatives, organisational integration, continuous learning and revision processes.

This complements the lifecycle-oriented review and maintenance processes described in Clause 7.

10.2 Alignment with standards and policy frameworks

Solutions developed under this CWA should take account of existing international, European and national standards, as well as relevant policy frameworks.

These may include, among others, the Sendai Framework for Disaster Risk Reduction, the Union Civil Protection Mechanism, the European Green Deal, and related ISO and CEN standards addressing risk management, crisis management, and emergency response.

Preparedness solutions may also consider alignment with the EU Civil Security Taxonomy to facilitate coherence with EU-level market analysis, funding programmes and policy development.

In the geospatial domain, the EU INSPIRE Directive provides a framework to support interoperability and sharing of spatial data across Europe.

Alignment does not imply conformity or duplication; rather, it seeks to ensure that concepts, definitions, and approaches are consistent with established references.

This facilitates interoperability between initiatives and helps ensure that preparedness efforts contribute to broader European and global objectives.

This CWA is complementary to CWA 17513:2020, which focuses primarily on interoperability in crisis and disaster response, whereas the present document addresses the documentation, governance, discoverability and sustainability of preparedness solutions.

10.3 Coherence across projects and initiatives

Preparedness solutions frequently originate within time-limited projects.

To avoid fragmentation, developers are encouraged to consider how their outputs relate to other existing or emerging initiatives, including national-level programmes, strategies and platforms as well as European and international projects.

This may include cross-referencing complementary tools or datasets, sharing results through collaborative platforms, and using common descriptors and metadata.

Where projects address similar challenges, cooperation in the exchange of lessons learned and technical experience helps reduce redundancy and enhances the collective maturity of the preparedness community.

Furthermore, structured collaboration with other relevant initiatives can increase the value and long-term usability of preparedness solutions. Such collaboration can support peer learning, alignment of terminology and approaches, identification of complementarities, and earlier visibility of solutions beyond the originating

project or organisation. It can also help to reduce duplication of effort, strengthen coherence across related activities, and create wider communities of practice able to support validation, uptake and sustainability over time.

10.4 Integration into organisational processes

To achieve sustained benefit, preparedness solutions should be embedded into the operational and planning processes of the organisations that use them. Depending on the context, integration may take place at local, regional, national or cross-border level, and may involve multiple organisations working within a shared framework.

Integration ensures that tools and procedures remain active and relevant, and that learning from their application informs broader risk management practices.

Adoption at organisational level should be supported by clear responsibilities, training, and appropriate resource allocation.

10.5 Continuous improvement and learning

Continuous improvement relies on structured feedback from owners or custodians, contributors or developers, validation or assessment bodies, and users or implementers.

Evaluation findings, exercise results, and operational experience should be used to update documentation, correct deficiencies, and identify opportunities for enhancement. These learning processes are intended to complement, and not replace, established preparedness or risk-management cycles already in use within organisations or jurisdictions.

Regular review cycles, whether annual or event-driven, help ensure that solutions evolve in step with changing risks, technologies, and user needs.

Improvements should be documented and communicated to stakeholders to maintain transparency and encourage broader learning.

10.6 Monitoring and evaluation

Organisations may adopt monitoring indicators to assess the performance and relevance of preparedness solutions.

Indicators can address areas such as uptake, interoperability, sustainability, user satisfaction, or contribution to policy goals. Monitoring and evaluation processes should remain proportionate to the scale and criticality of the solution and should be designed primarily to support learning and improvement.

Evaluation should be proportionate and focus on lessons learned rather than compliance.

Where appropriate, results may be shared with partners or within relevant communities to inform future development and coordination.

Periodic reflection on the strengths, limitations, opportunities and potential gaps associated with preparedness solutions may support learning and adaptation over time. Such reflective approaches can help identify areas for improvement without implying formal evaluation or compliance mechanisms.

10.7 Knowledge management and institutional memory

Capturing and sharing knowledge generated during the development and use of preparedness solutions supports collective resilience. Good practice includes maintaining repositories of lessons learned, after-action reports and evaluation summaries that can inform future projects. It is particularly important to record the rationale for key decisions, along with the underlying assumptions and relevant contextual factors, so that this knowledge remains meaningful even when personnel or organisational structures change.

10.8 Innovation and adaptability

Preparedness is a dynamic field influenced by technological innovation, social change and emerging risks. Solutions should therefore be designed with adaptability in mind, so that updates or enhancements can be made when justified by user needs or evidence. Adaptability does not imply continual change, but rather the capacity to evolve in a measured and proportionate way. Engagement with research communities, innovation clusters and user networks can facilitate the flow of new ideas and the identification of good practices.

Annex A
(informative)

Example template for documenting a preparedness solution

A.1 General

This Annex provides an illustrative template for documenting a preparedness solution in accordance with the descriptive information recommended in Clause 5.2.

The template is intended as guidance only and may be adapted by organisations or projects according to the scale, complexity and intended use of the solution being documented.

The following structure illustrates the types of information that may be included when describing a preparedness solution.

A.2 Use of the template

The template presented in this Annex illustrates a structured approach for describing preparedness solutions in a consistent and comparable way.

This annex provides illustrative examples of preparedness solution metadata aligned with the considerations described in Clause 5.4.

Organisations and projects may adapt the structure according to their needs; however, maintaining a consistent set of descriptive elements can support the discoverability, comparison and reuse of solutions across different initiatives and domains.

When documenting a preparedness solution, it is recommended that the information provided is proportionate to the maturity and complexity of the solution. Early-stage concepts may require only high-level descriptions, while operational or validated solutions may include more detailed technical, governance and validation information.

A.3 Example of a preparedness solution profile

Title of solution:
[Insert title]

Version and date:
[Insert version number and publication/update date]

Responsible organisation / custodian:
[Insert organisation name]

Primary contact:
[Insert name or role and contact details]

Summary description:
Brief description of the solution, its purpose, and its main functions and expected results.

Intended use and scope:
Description of the preparedness context in which the solution is intended to be applied.

Operational context or use scenario:

(Short description of the operational or planning context in which the solution may be used (for example risk assessment, early warning, training, decision support, coordination, community preparedness)

Target users:
(e.g. civil-protection authorities, responders, policymakers, infrastructure operators, researchers, community organisations).

Hazards addressed:
(e.g. floods, earthquakes, wildfires, multi-hazard)

Security Areas (EU Civil Security Taxonomy):
Indication of the relevant Level 1 security domain

Functional Areas (EU civil security Taxonomy):
Relevant functional classification

Product or service category (EU civil security Taxonomy):
Relevant product or service classification

Geographical scope:
(e.g. local, national, cross-border, European)

Maturity level:
(e.g. concept, prototype, pilot, operational)
Where applicable, the Technology Readiness Level (TRL) of the solution may be indicated.

Operational Status:

(e.g. research concept, prototype, tested in exercises, pilot deployment, operational use)

Key components:
Short description of main elements (tools, processes, datasets, training materials, etc.).

Interoperability considerations:
Summary of relevant standards, interfaces, data formats or integration mechanisms supporting interoperability.

Validation and testing:
Description of exercises, pilots, peer review, or operational deployments.

Evidence of operational use (if available):

Description of any real-world use, adoption by organisations, integration into operational procedures, or use in exercises or training programmes.

Access conditions and licensing:
Description of licence type and access arrangements (open, restricted, controlled).

Sustainability and maintenance:
Identification of the custodian, maintenance arrangements, update responsibilities and any provisions supporting long-term availability.

Related projects or initiatives:
References to funding sources, partner projects, or aligned frameworks.

References:
References or links to documentation, repositories, scientific publications or other supporting materials.

Bibliography

[1] EN ISO 19115-1, *Geographic information — Metadata — Part 1: Fundamentals (ISO 19115-1)*

[2] EN ISO 19115-2, *Geographic information — Metadata — Part 2: Extensions for acquisition and processing (ISO19115-2)*

[3] EN ISO 19115-3, *Geographic information — Metadata — Part 3: XML schema implementation for fundamental concepts (ISO 19115-3)*

[4] EN ISO 22300:2025, *Security and resilience — Vocabulary (ISO 22300:2025)*

[5] EN ISO 22361:2022, *Security and resilience — Crisis management — Guidelines (ISO 22361:2022)*

[6] ISO 22320:2018, *Security and resilience — Emergency management — Guidelines for incident management*

[7] ISO 31000:2018, *Risk management — Guidelines*

[8] CWA 17513:2020 *Crisis and disaster management — Semantic and syntactic interoperability*

[9] EN 301549, *Accessibility requirements for ICT products and services*

[10] UNDRR, 2016, Report of the Open-ended Intergovernmental Expert Working Group on Indicators and Terminology Relating to Disaster Risk Reduction

[11] United Nations, 2015, Sendai Framework for Disaster Risk Reduction 2015–2030

[12] European Union, 2013, Decision No 1313/2013/EU on a Union Civil Protection Mechanism

[13] European Union, 2021, Regulation (EU) 2021/836 amending Decision No 1313/2013/EU

[14] European Commission, 2021, EU Strategy on Adaptation to Climate Change

[15] European Commission, 2019, The European Green Deal

[16] UNDRR/ISC, 2021, Hazard definition and classification review — Technical report

[17] RESILOC, Glossary of terms

[18] European Commission, 2025, EU Preparedness Union Strategy

[19] European Commission, 2022, EU Civil Security Taxonomy

[20] European Union, 2007, Directive 2007/2/EC establishing an Infrastructure for Spatial Information in the European Community (INSPIRE)

[21] Web Content Accessibility Guidelines (WCAG)