INTERNATIONAL STANDARD

ISO 22325

First edition
2016-10-15

Security and resilience — Emergency management — Guidelines for capability assessment

Sécurité et résilience — Gestion des situations d'urgence — Lignes directrices pour l'évaluation de la capacité

Reference number
ISO 22325:2016(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

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 documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is Technical Committee ISO/TC 292, *Security and resilience*.

Introduction

This document provides guidelines for an organization in assessing its emergency management capability by using four maturity levels, eight indicators and an assessment process (see Figure 1).

A capability assessment can be used to:

— ensure regulatory compliance, reduce risk and meet the safety expectations of the population;

— improve organizational processes;

— enhance partnership, coordination and cooperation within an organization and with other agencies and sectors;

— share best practices;

— promote continual improvement.

A capability assessment can be performed by the organization itself or by an external organization.

Organizations can define their context to allow for an appropriate assessment of its emergency management capability. This context can be expressed through identifying appropriate activities in relation to prevention, mitigation, preparedness, response and recovery. While most organizations deliver all emergency management functions, some organizations can be responsible for only a single function so not all the indicators will apply.

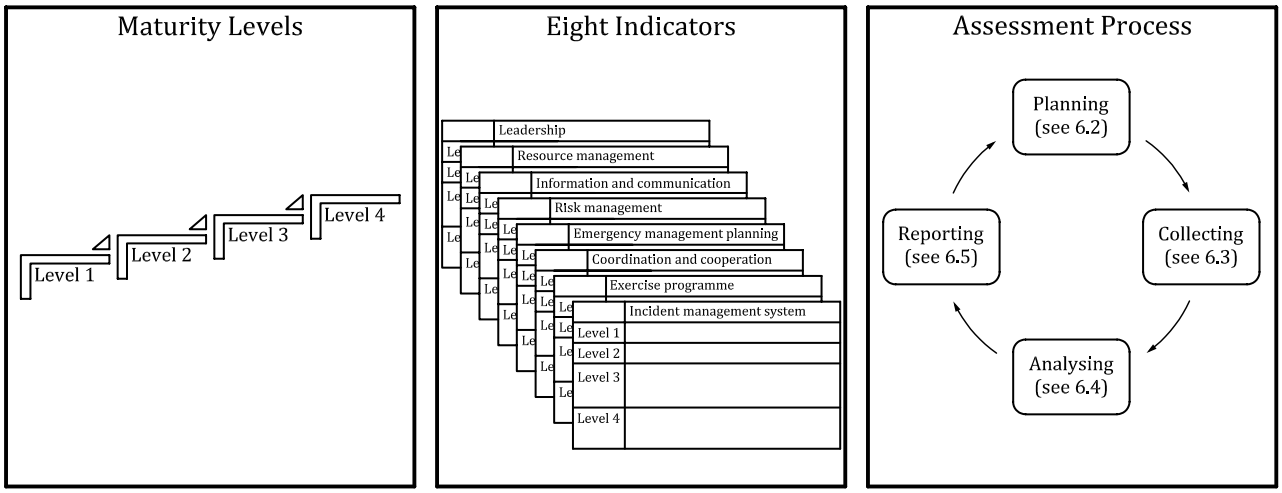

Figure 1 — Emergency capability assessment

Security and resilience — Emergency management — Guidelines for capability assessment

1 Scope

This document provides guidelines for an organization in assessing its emergency management capability. It includes

— an assessment model with a hierarchy of four levels;

— eight indicators;

— an assessment process, explaining how to plan, collect, analyse and report.

This document is intended to be used by organizations responsible and accountable for emergency management. Each organization's context can involve a mix of prevention, mitigation, preparedness, response and recovery activities.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

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

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

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

3.1
context
external and internal factors to be taken into account when undertaking a capability assessment

Note 1 to entry: External context includes the following:

— cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

— key drivers and trends having impact on the objectives of the organizations;

— relationships with, and perceptions and values of external stakeholders.

Note 2 to entry: Internal context includes

— the organization's mandate,

— business sensitivity,

— governance, organizational structure, roles and accountabilities,

— resources and knowledge (e.g. capital, time, people, processes, systems and technologies), and

— organizational culture.

3.2
emergency management capability
overall ability to effectively manage prevention, preparedness, response and recovery before, during and after potentially destabilizing or disruptive events

4 Assessment model

The organization should use the assessment model with four levels to classify its emergency management capability (see Figure 2). This is subject to the role, functions, scope and authority of an organization and the operational context.

Level 1 represents the minimum level of emergency management capability, while Level 4 represents the highest level of emergency management capability.

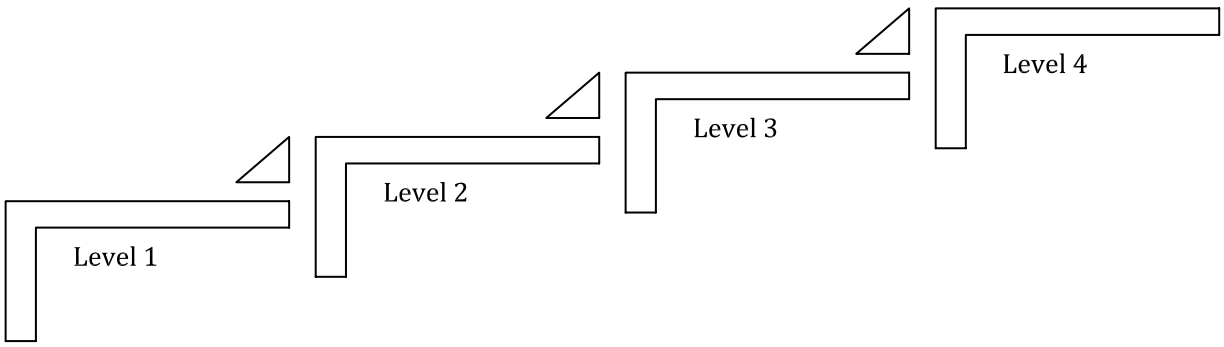

Figure 2 — Levels of emergency management capability

At Level 1, an organization performs its emergency management role at a basic level.

At Level 2, an organization has established detailed plans with the goal of achieving a balance between resource demands and availability. Plans are developed in terms of the knowledge, skills and capabilities to manage incidents and are updated periodically.

At Level 3, an organization has designed an emergency management process to facilitate appropriate measurement and assessment which enables the organization to identify opportunities for improvement. The organization has integrated with other organizations in order to increase the effectiveness and efficiency.

At Level 4, an organization has reached an optimal level of emergency management capability. Critical to this level of performance is the ability to demonstrate organizational learning, adaptive capacity and effective coordination and cooperation with other organizations. It commits to research and best practice and is able to appropriately use technology.

5 Indicators

5.1 General

The organization should assess emergency management capability using the indicators which reflect the scope, function and authority of the organization:

a) leadership;

b) resource management;

c) information and communication;

d) risk management;

e) coordination and cooperation;

f) emergency management planning;

g) exercise programme;

h) incident management system.

The indicators in Tables 1 to 8 are described in accordance with the four levels of the assessment model (see Figure 2).

5.2 Leadership

Effective leadership enables the organization to forge effective communication and collaboration among organizations. It is important for the leadership to be aware of the organization's internal and external context. A clear commitment to the assessment process should be demonstrated.

Table 1 — Indicator for leadership

Level	Criteria
Level 1	The roles and responsibilities of the organization have been defined. An emergency management policy has been approved which includes emergency management objectives.
Level 2	The leadership is aware of the roles and responsibilities of the own organization and commits appropriate resources. The emergency management objectives have been harmonized with objectives of the organization. Leadership approves and supports these objectives. The leadership has demonstrated a commitment to continual improvement.
Level 3	The leadership is aware of the roles and responsibilities of other organizations and demonstrates coordination and cooperation. The leadership has identified strengths and weaknesses of organization and shares opportunities for improvement with other organizations. The leadership ensures alignment between job competences and individuals.
Level 4	Procedures have been implemented to learn from incidents, near misses, exercises and tests. Leadership has been involved in exercises. The leadership has assigned resources to support research and development activities and to improve its capacity to cope with current and future emergencies. Commitment includes identified contingency funding. The organization demonstrates the ability to optimize according to its context.

5.3 Resource management

Resource management is the efficient and effective allocation and deployment of resources when and where they are needed.

Table 2 — Indicator for resource management

Level	Criteria
Level 1	The organization has carried out an analysis of resources (e.g. personnel, facilities, tools, technology, equipment and budget). The basic resources are in place to achieve the organization's emergency management objectives.
Level 2	Resources are updated, documented and tracked, including the identification of resources available for immediate deployment. A policy for resource management regarding emergencies exists. The policy includes routines for: — timely deployment of resources according to predefined priorities; — backup system(s); — maintenance and test of the functionality of the internal material resources.
Level 3	Resources requirements have been defined based on the results of a risk assessment. Resources are available to support coordination and cooperation and agreements are in place. Appropriate procedures are in place for requesting and receiving external resources. Evidence of flexible resource allocation is demonstrated.
Level 4	Resource management is based on research and evidence, which may include benchmarking, lessons learned from real incidents, exercises and stress tests. Lessons learned should be: — documented; — captured as opportunities for improvement (e.g. of personnel, technical equipment); — shared with other organizations. Agreements are periodically reviewed within a multi-organizational setting.

5.4 Information and communication

It is essential for information and communication to be effectively managed in order to support the organization's mission within an emergency management context.

Table 3 — Indicator for information and communication

Level	Criteria
Level 1	An information and communication system within the organization has been implemented. The system supports information exchange and communication within the organization.
Level 2	The information and communication system is maintained regularly. Alternative solutions or backup systems are in place.
Level 3	A plan for internal and external information and communication has been implemented. The information and communication system supports the information exchange between organizations and the public and ensures continuity of the information and communication system.
Level 4	Lessons learned from real incidents, exercises, research and stress tests are reflected in the information and communications system. An optimal system has been implemented and integrated with other organizations and considers: — confidentiality, integrity, availability and reliability of the information; — speed, timeliness and relevance of communication; — communication needs of stakeholders; — information analysis for situation awareness; — training needs; — human factors.

5.5 Risk management

Risk management should be an integral to all of the organization's emergency management activities. It is a systematic approach to manage uncertainty to the organization's objectives. It should be consistent with ISO 31000.

Table 4 — Indicator for risk management

Level	Criteria
Level 1	Risks have been identified but have not been analysed or considered in long-term planning.
Level 2	A basic risk management process has been conducted in an ad hoc manner.
Level 3	Risk management includes critical dependencies to other organizations and stakeholders. The risk treatment plan considers other organizations and stakeholders and shares with them. Risk treatment activities are implemented.
Level 4	Risk management is integral to all decision making within the organization and is monitored and regularly reviewed. Risk management reflects research and best practice.

5.6 Coordination and cooperation

Effective and efficient emergency management results from organizations demonstrating a high level of coordination and cooperation.

Table 5 — Indicator for coordination and cooperation

Level	Criteria
Level 1	The organization demonstrates awareness of its roles and responsibilities and is able to communicate them to other organizations or stakeholders.
Level 2	The organization has knowledge of other relevant organization's roles and responsibilities. The organization demonstrates coordinated ability at the operational level.
Level 3	The organization has signed cooperation agreement(s) with other organization(s) according to ISO 22320. Common, agreed to objectives are established to ensure and prioritize effective, sustained coordination and cooperation at the tactical and strategic levels among organizations.
Level 4	Coordination and cooperation has been fully implemented according to ISO 22320. The coordination and cooperation agreement(s) are reviewed and updated. Coordination and cooperation is considered during exercises and during continuous improvement activities. The organization enables integration with cooperation partners by exchanging experts where appropriate. The organization has implemented ISO 22397 where applicable.

5.7 Emergency management planning

The emergency management planning should be driven by organization's internal and external emergency management context.

Table 6 — Indicator for emergency management planning

Level	Criteria
Level 1	Emergency management planning is undertaken.
Level 2	Emergency management planning is known within the own organization and includes — the scope; — objectives which consider human lives and health, societal functionality, economic assets and environment; — roles and responsibilities.
Level 3	Emergency management planning is developed with consideration of other organizations. Planning considers other organizations. After a significant incident or a major change in the organization, planning is updated accordingly.
Level 4	Plans are evaluated and updated reflecting the outcomes of exercises, training, lessons learned and significant changes. An emergency response plan has been integrated with other plans within the organization and also ensures continuity of operations. The organization carefully considers other organization's emergency response plans with the intention to promote coordination and cooperation in accordance with ISO 22397 where applicable. Results from research and best practice are incorporated into the emergency response plan.

5.8 Exercise programme

An exercise programme is essential for driving effective and efficient organizational performance.

Exercises can be used for:

— validating policies, plans, procedures, training, equipment and inter-organizational agreements;

— clarifying and training personnel in roles and responsibilities;

— improving inter-organizational coordination and communications;

— identifying gaps in resources, improving individual performance;

— identifying opportunities for improvement and controlled opportunity to practice improvisation.

Table 7 — Indicator for exercise programme

Level	Criteria
Level 1	The organization does not have a formal exercise programme. Exercises are conducted to meet minimum mandatory requirements.
Level 2	A needs based exercise programme has been established. Exercises are conducted regularly according to the exercise programme.
Level 3	The organizations' needs analysis is regularly monitored and reviewed. The exercise programme is regularly reviewed and updated in line with the needs analysis. Where appropriate, it is developed with other organizations. Exercises are conducted with other organizations according to the programme.
Level 4	An exercise programme has been implemented according to ISO 22398 where applicable. Exercises are evaluated and lessons learned are documented. These learnings are integrated into strategy and continuous improvement. The exercise programme is continuously improved and is based on research and best practice.

5.9 Incident management system

Organizations should be able to establish an effective incident management system or integrate into an existing one. The system should be based on ISO 22320.

Table 8 — Indicator for incident management system

Level	Criteria
Level 1	An incident management system has been implemented and the organization is capable of a basic incident response.
Level 2	Incident management system roles and responsibilities are defined and assigned. The incident management system is updated regularly.
Level 3	The incident management system is able to integrate with other organizations. The efficiency of the incident response is measured against objectives.
Level 4	The incident management system ensures optimal use of scarce resources, including: — tests and reviews its incident management system regularly; — considers the entire incident response in the learning process; — prepares an incident response evaluation report after each incident to assist in the improvement of the incident management system. The organization is capable of a sustained response to deal with an escalating incident. The organization demonstrates a commitment to achieving system to system integration.

6 Assessment process

6.1 General

The assessment process involves planning, collecting, analysing and reporting activities.

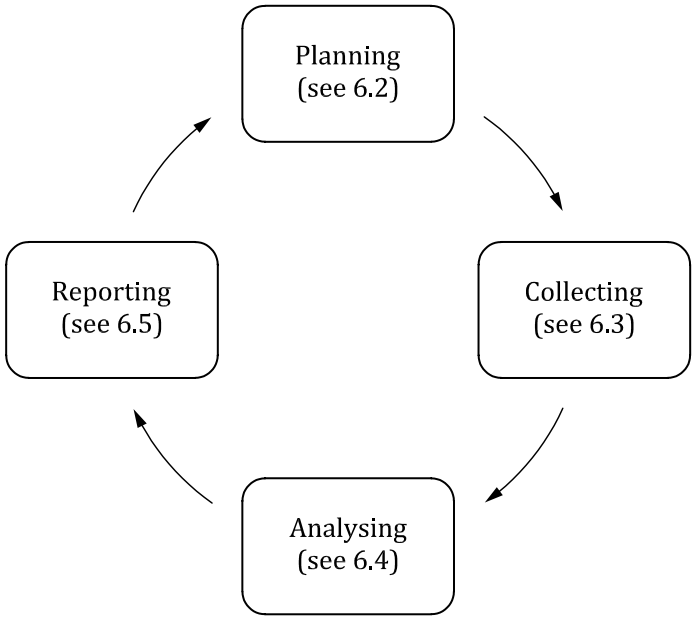

Figure 3 — Assessment process

An assessment should be conducted:

— at regular intervals or when deemed appropriate by the organization;

— to determine what has changed since the last assessment;

— after a major change in or around the organization has occurred;

— following a significant event or incident.

The assessment may be conducted by:

— self-review;

— on-site review by an external organization;

— benchmarking (peer organization – by sector and size);

— regulatory review;

— a combination of above methods.

The assessment should be performed by people:

— with relevant education, training, experience and competence;

— who are able to perform the assessment in accordance with this document;

— who have been provided sufficient resources and authority.

When designating the assessment, the following should be considered in relation to the organization's goals and objectives:

— identification of current, emerging or future threats;

— determination of how regularly the assessment should be conducted;

— how confidentiality/sensitivity is maintained/considered.

6.2 Planning

The assessment process should be documented. The planning process addresses the following:

— assessment purpose and scope, including constraints;

— identification of key roles and responsibilities;

— recording of the results.

6.3 Collecting

The assessment should obtain detailed, accurate data. Key inputs to the assessment may include:

— policies;

— budgets;

— management reports;

— risk and asset registers;

— exercise and test reports;

— training records;

— incident reports;

— meeting records;

— audit reports.

6.4 Analysing

The criteria in Clause 5 are used to evaluate each indicator (for template, see Annex A).

Analysis should be based on evidence as listed in 6.3.

6.5 Reporting

The report includes:

— the results of the assessment;

— identified opportunities for improvement;

— recommendations.

Annex A
(informative)

Assessment template

Table A.1 — Assessment template

Indicators	Level				
Indicator 1: Leadership	(1)	(2)	(3)	(4)	
Comments/Reference					
Indicator 2: Resource management	(1)	(2)	(3)	(4)	
Comments/Reference					
Indicator 3: Information and communication	(1)	(2)	(3)	(4)	
Comments/Reference					
Indicator 4: Risk management	(1)	(2)	(3)	(4)	
Comments/Reference					
Indicator 5: Coordination and cooperation	(1)	(2)	(3)	(4)	
Comments/Reference					
Indicator 6: Emergency management planning	(1)	(2)	(3)	(4)	
Comments/Reference					
Indicator 7: Exercise programme	(1)	(2)	(3)	(4)	
Comments/Reference					
Indicator 8: Incident management system	(1)	(2)	(3)	(4)	
Comments/Reference					

Bibliography

[1] ISO 22300, *Societal security — Terminology*

[2] ISO 22320, *Societal security — Emergency management — Requirements for incident response*

[3] ISO 22397, *Societal security — Guidelines for establishing partnering arrangements*

[4] ISO 22398, *Societal security — Guidelines for exercises*

[5] ISO 31000, *Risk management — Principles and guidelines*

ICS 03.100.01

Price based on 11 pages