
**Security and resilience — Crisis
management — Guidelines**

Sécurité et résilience — Gestion de crise — Lignes directrices



This document is a preview generated by EUS



COPYRIGHT PROTECTED DOCUMENT

© ISO 2022

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

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

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Crisis management — Context, core concepts and principles	3
4.1 The nature of crises	3
4.2 Characteristics of a crisis	3
4.3 Potential origins of crises	5
4.4 Readiness to respond and recover	7
4.5 Principles for crisis management	7
4.5.1 General	7
4.5.2 Principle A: Governance	7
4.5.3 Principle B: Strategy	7
4.5.4 Principle C: Risk management	7
4.5.5 Principle D: Decision-making	8
4.5.6 Principle E: Communication	8
4.5.7 Principle F: Ethics	8
4.5.8 Principle G: Learning	8
5 Building a crisis management capability	8
5.1 General	8
5.2 Crisis management framework	9
5.2.1 General	9
5.2.2 Leadership	9
5.2.3 Structure	10
5.2.4 Culture	10
5.2.5 Competence	11
5.3 Crisis management process	11
5.3.1 Anticipation	11
5.3.2 Assessment	11
5.3.3 Prevention and mitigation	11
5.3.4 Preparedness	12
5.3.5 Response	16
5.3.6 Recovery	19
5.3.7 Continual improvement	19
6 Crisis leadership	20
6.1 Core leadership skills and attributes	20
6.1.1 General	20
6.1.2 Role and responsibility of the crisis leader(s)	21
6.2 Well-being and sustainable crisis response	22
6.2.1 Crisis management responders	22
6.2.2 Wider interested-party impact	22
7 Strategic crisis decision-making	23
7.1 General	23
7.2 Why decision-making can be challenging	24
7.3 Dilemmas, decision delay, decision avoidance	25
7.4 Decision-making issues	25
7.5 Effective crisis decision-making	25
8 Crisis communication	26
8.1 General	26
8.2 Pre-crisis preparation	26

8.3	Managing relationships and reputation.....	27
8.4	Key roles.....	27
8.4.1	Communication team.....	27
8.4.2	Spokespeople.....	28
8.4.3	Media relations.....	28
8.5	Crisis communication strategy.....	28
8.6	Key principles and activities of crisis communication.....	29
8.7	Consistency of message.....	30
8.8	Barriers to effective communication.....	30
8.9	Social media — Opportunities and threats.....	31
9	Training, validation and learning from crises.....	31
9.1	General.....	31
9.2	Developing competence.....	32
9.3	Training.....	32
9.4	Exercising.....	33
9.5	Validation.....	34
9.6	Evaluating and learning.....	34
	Bibliography.....	36

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 of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 391, *Societal and Citizen Security*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document has been developed to aid in the design and ongoing development of an organization's crisis management capability. It sets out principles and practices needed by all organizations.

Crises present organizations with complex challenges and, possibly, opportunities that can have profound and far-reaching consequences. An organization's crisis management capability and its ability to manage a changing environment are key factors in determining whether a situation or incident has the potential to pose a serious or existential threat to the organization and its environment. The crisis affecting an organization can be part of a broader crisis.

To ensure the crisis management capability has the desired outcome, the organization should provide:

- committed leadership;
- structures (e.g. funding, communications, relationships and linkages, equipment, facilities, information management, principles, processes and procedures);
- a supportive culture (e.g. values, ethics, code of conduct);
- competent personnel (e.g. knowledge, skills and attitude, flexible thinking).

An organization's crisis management capability will be influenced by its relationship with other interdependent areas such as risk management, business continuity, information security, physical security, safety, civil protection, incident response and emergency management.

The organization should adopt a structured approach to crisis management by applying a set of principles on which a crisis management framework can be developed. These interrelated principles, framework and applicable process elements support the implementation of a crisis management capability in a purposeful, consistent and rigorous manner (see [Figure 1](#)).

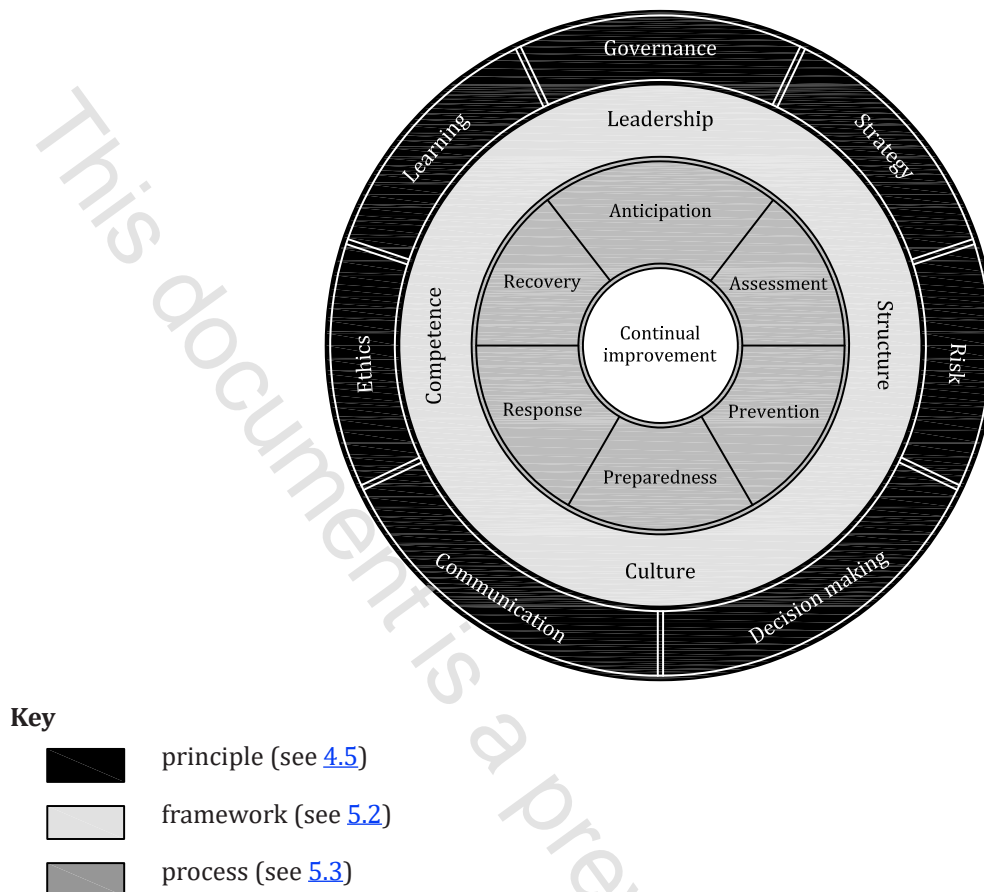


Figure 1 — Building a crisis management capability — Principles, framework and process

The structure of the document is as follows:

- the core concepts of crisis management are described (see [Clause 4](#));
- then the framework and process for building a crisis management capability are outlined (see [Clause 5](#)).

The clauses that follow provide more detail on:

- crisis leadership (see [Clause 6](#));
- strategic crisis decision-making (see [Clause 7](#));
- crisis communication (see [Clause 8](#));
- training, validation and learning from crises (see [Clause 9](#)).

Continual improvement is a component of all elements of this document (see [5.3.7](#)), so that while it is part of the process, it also addresses all capability elements.

Security and resilience — Crisis management — Guidelines

1 Scope

This document provides guidance on crisis management to help organizations plan, establish, maintain, review and continually improve a strategic crisis management capability. This guidance can help any organization to identify and manage a crisis. Elements for consideration include:

- context, core concepts, principles and challenges (see [Clause 4](#));
- developing an organization's crisis management capability (see [Clause 5](#));
- crisis leadership (see [Clause 6](#));
- the decision-making challenges and complexities facing a crisis team in action (see [Clause 7](#));
- crisis communication (see [Clause 8](#));
- training, validation and learning from crises (see [Clause 9](#)).

It is applicable to top management with strategic responsibilities for the delivery of a crisis management capability in any organization. It can also be used by those who operate under the direction of top management.

This document acknowledges the relationship and interdependencies with various disciplines but is distinct from these topics.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Security and resilience — Vocabulary*

3 Terms and definitions

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

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1

capability

ability to accomplish an undertaking with a defined intended outcome and within specified conditions

Note 1 to entry: An organizational capability depends on the available resources and organizational principles, framework (leadership, structure, culture, competences) and processes.