

---

---

**Societal security — Emergency  
management — Requirements for  
incident response**

*Sécurité sociétale — Gestion des urgences — Exigences relatives aux  
réponses aux incidents*

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO 22320:2011](https://standards.iteh.ai/catalog/standards/sist/4c7960a3-e18b-42fb-bde6-25504658e172/iso-22320-2011)

[https://standards.iteh.ai/catalog/standards/sist/4c7960a3-e18b-42fb-bde6-  
25504658e172/iso-22320-2011](https://standards.iteh.ai/catalog/standards/sist/4c7960a3-e18b-42fb-bde6-25504658e172/iso-22320-2011)



## iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO 22320:2011

<https://standards.iteh.ai/catalog/standards/sist/4c7960a3-e18b-42fb-bde6-25504658e172/iso-22320-2011>



### **COPYRIGHT PROTECTED DOCUMENT**

© ISO 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

Foreword .....	iv
Introduction .....	v
1 Scope .....	1
2 Normative references .....	1
3 Terms and definitions .....	1
4 Requirements for command and control .....	3
4.1 General .....	3
4.2 Command and control system .....	4
4.3 Human factors .....	7
5 Requirements for operational information .....	7
5.1 General .....	7
5.2 Operational information process .....	8
5.3 Operational information process criteria .....	10
6 Requirements for cooperation and coordination .....	10
6.1 General .....	10
6.2 Cooperation .....	11
6.3 Coordination .....	11
6.4 Information sharing .....	13
6.5 Human factors .....	14
Annex A (informative) Examples .....	15
Annex B (normative) Operational information process criteria .....	18
Bibliography .....	21

iTech STANDARD PREVIEW  
(standards.iteh.ai)  
<https://standards.iteh.ai/catalog/standards/sist/4c7960a3-e18b-42fb-bde6-25504658e172/iso-22320-2011>

## 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 22320 was prepared by Technical Committee ISO/TC 223, *Societal security*.

## iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO 22320:2011

<https://standards.iteh.ai/catalog/standards/sist/4c7960a3-e18b-42fb-bde6-25504658e172/iso-22320-2011>

## Introduction

In recent years there have been many disasters, terrorist attacks and other major incidents which have shown the importance of effective incident response in order to save lives, mitigate harm and damage, and to ensure a base level of continuity of essential societal functions. Such functions include health and rescue services, water and food supply, and electricity and fuel delivery. While in the past the focus of incident response has been national, regional or within single organizations, today and for the future there is a need for a multinational and multi-organizational approach. This is a result of worldwide governmental, non-governmental, commercial and industrial relationships and dependencies.

This International Standard enables public and private incident response organizations to improve their capabilities in handling all types of emergencies (for example, crisis, disruptions and disasters). The multiple functions of incident response are shared between organizations and agencies, with the private sector and the government having different levels of responsibility. Thus there is a need to guide all involved parties in how to prepare and implement effective incident responses. This International Standard will, based on minimum requirements, enable organizations involved to operate with joint optimum efficiency.

Effective incident response needs structured command and control, and coordination and cooperation, in order to establish coordination and cooperation, carry out command processes and facilitate information flow amongst the involved organizations, agencies and other parties.

Cross-organization, -region or -border assistance during incident response is expected to be appropriate to the needs of the affected population and also to be culturally acceptable. Therefore community participation in the development and implementation of incident response measures is essential. Involved organizations require the ability to share a common approach across geographical and organizational boundaries.

Information requirements, as well as requirements pertaining to the information management process and structure, may enable industry to develop technical solutions which will provide maximal interoperability according to information and communication exchange needs during incident response.

An effective incident preparedness and operational continuity management programme can be implemented using ISO/PAS 22399, and by conducting regular multi-organizational exercises.

This International Standard can be used alone or together with the other standards developed by ISO/TC 223.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

ISO 22320:2011

<https://standards.iteh.ai/catalog/standards/sist/4c7960a3-e18b-42fb-bde6-25504658e172/iso-22320-2011>

# Societal security — Emergency management — Requirements for incident response

## 1 Scope

This International Standard specifies minimum requirements for effective incident response and provides the basics for command and control, operational information, coordination and cooperation within an incident response organization. It includes command and control organizational structures and procedures, decision support, traceability, information management, and interoperability.

It establishes requirements for operational information for incident response which specifies processes, systems of work, data capture and management in order to produce timely, relevant and accurate information. It supports the process of command and control as well as coordination and cooperation, internally within the organization and externally with other involved parties, and specifies requirements for coordination and cooperation between organizations.

This International Standard is applicable to any organization (private, public, governmental or non-profit) involved in preparing or responding to incidents at the international, national, regional or local levels, including organizations

- a) responsible for, and participating in, incident prevention and resilience preparations,
- b) offering guidance and direction in incident response,
- c) developing regulations and plans for command and control,
- d) developing multi-agency/multi-organizational coordination and cooperation for incident response,
- e) developing information and communication systems for incident response,
- f) researching in the field of incident response, information and communication and data interoperability models,
- g) researching in the field of human factors in incident response,
- h) responsible for communication and interaction with the public.

## 2 Normative references

The following referenced documents are indispensable for the application 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, *Societal security — Vocabulary*<sup>1)</sup>

## 3 Terms and definitions

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

---

1) To be published.

**3.1  
command and control**  
activities of target-orientated decision-making, assessing the situation, planning, implementing decisions and controlling the effects of implementation on the incident

NOTE This process is continuously repeated.

**3.2  
command and control system**  
system that supports effective emergency management of all available assets in a preparation, incident-response, continuity and/or recovery process

**3.3  
cooperation**  
process of working or acting together for common interests and values based on agreement

NOTE The organizations agree by contract or by other arrangements to contribute with their resources to the incident response but keep independence concerning their internal hierarchical structure.

**3.4  
coordination**  
way in which different organizations (public or private) or parts of the same organization work or act together in order to achieve a common objective

NOTE 1 Coordination integrates the individual response activities of involved parties (including public or private organizations and government) to achieve synergy to the extent that the incident response has a unified objective and to coordinate activities through transparent information sharing regarding their respective incident-response activities.

NOTE 2 All organizations are involved in the process to agree on a common incident-response objective and accept to implement the strategies by this consensus decision-making process.

**3.5  
emergency management** <https://standards.iteh.ai/catalog/standards/sist/4c7960a3-e18b-42fb-bde6-d792156171e3/iso-22320-2011>  
overall approach preventing emergencies and managing those that occur

NOTE In general, emergency management utilizes a risk-management approach to prevention, preparedness, response and recovery before, during and after potentially destabilizing and/or disruptive events.

**3.6  
incident command**  
part of an organized incident response structure

NOTE Incident command is the process that is conducted within the command structures that evolve during the management of an incident.

**3.7  
incident preparedness**  
activities taken in order to prepare incident response

**3.8  
incident response**  
actions taken in order to stop the causes of an imminent hazard and/or mitigate the consequences of potentially destabilizing or disruptive events, and to recover to a normal situation

NOTE Incident response is part of the emergency management process.

**3.9  
information**  
data that are processed, organized and correlated to produce meaning



**3.10****operational information**

information that has been contextualized and analysed to provide an understanding of the situation and its possible evolution

**3.11****organization**

group of people and facilities with an arrangement of responsibilities, authorities and relationships

EXAMPLES Company, corporation, firm, enterprise, institution, charity, sole trader, association, agency or parts or combination thereof.

NOTE 1 The arrangement is generally orderly.

NOTE 2 An organization can be public or private.

NOTE 3 This definition is valid for the purposes of quality management system standards. The term "organization" is defined differently in ISO/IEC Guide 2.

[ISO 9000:2005, definition 3.3.1]

NOTE 4 An organization can be either a standing group or a temporary one established ad-hoc to perform a specific and limited task.

**4 Requirements for command and control****4.1 General**

In general, command and control includes the following tasks:

- a) establishing and updating goals and objectives for the incident response;
- b) determining roles, responsibilities and relationships;
- c) establishing rules, constraints and schedules;
- d) ensuring legal compliance and liability protection;
- e) monitoring, assessing and reporting on the situation and progress;
- f) recording key decisions and assumptions;
- g) managing resources;
- h) dissemination of information;
- i) taking and communicating decisions;
- j) follow-up of decisions taken.

When multiple organizations, or different parts of one organization, are involved in the incident response

- consensus should be sought on overall mission objectives among involved organizations,
- structures and processes should permit operational decisions to be taken at the lowest possible level, and coordination and support offered from the highest necessary level,
- authority and resources shall be appropriate to this mission, and
- organizations shall encourage community participation in the development and implementation of incident response measures.

## 4.2 Command and control system

### 4.2.1 General

The objective of a command and control system is to enable organizations to carry out efficient incident responses, independently as well as jointly, with all other involved parties, in order to support all measures to save lives and limit adverse effects.

For the purpose of incident response the organization shall implement a command and control system which complies with relevant legislation and regulations as well as with the requirements of this International Standard.

Along with the setting up of a command and control system, the organization shall, as quickly as possible, determine the following lines of command both within the organization and with other organizations, actors and involved parties (e.g. designation of an incident commander):

- a) a common understanding of the mission's purpose;
- b) a common operational picture;
- c) relations to other organizations that are not within the line of command;
- d) appointment of persons with appropriate delegated authority to be accountable for leadership.

All of the above issues shall be taken into account during planning and exercises.

The command and control system shall be

- scalable for different incident types and involved organizations,
- adaptable to any type of incident,
- able to integrate different incident response organizations and involved parties, and
- flexible to the evolution of the incident and the outcome of incident responses.

To fulfil these tasks a command and control system shall include

- a command and control structure,
- a command and control process, and
- the resources necessary to implement the command structure and process.

The organizational structure, and the processes of the command and control system, shall be documented.

NOTE The number of persons, roles and responsibilities involved in the command and control organization may differ, depending on the scale of the incident.

### 4.2.2 Roles and responsibilities

One role within the organization, i.e. the incident commander, shall be identified as having the overall responsibility for command and control within that organization. This role shall have responsibility for

- initiating, coordinating and taking responsibility for all measures of incident response,
- setting up an organization,
- considering the activation, escalation and termination processes, and
- identifying and meeting legal and other obligations.

The command and control structure shall be organized in such a way that the incident commander can delegate authority.

#### 4.2.3 Command and control structure

The command and control structure shall be divided into different levels (e.g. tactical, operational, strategic and normative levels) where different types of decisions are taken within different timescales. An example is given in Table A.1.

#### 4.2.4 Levels of incident response

Corresponding to the predefined strategic and tactical command structure, the organization shall categorize a scale of incident severity levels. This is in order to implement, as soon as reasonably practicable, the appropriate level of command and control. An example is given in Table A.2.

#### 4.2.5 Command and control process

The organization shall establish a command and control process which is ongoing and includes the following activities:

- observation;
- information gathering, processing and sharing;
- assessment of the situation, including forecast;
- planning;
- decision-making and the communication of the decisions taken;
- implementation of decisions;
- feedback gathering and control measures.

The command and control process shall not be limited to the actions of the incident commander but shall also be applicable to all persons involved in the incident command team, at all levels of responsibility.

An example of a command and control process for an incident involving organization(s) under a single hierarchy command is given in Figure 1.