

---

---

**Security and resilience — Emergency  
management — Guidelines for  
incident management**

*Sécurité et résilience — Gestion des urgences — Lignes directrices  
pour la gestion des incidents*

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

[ISO 22320:2018](https://standards.iteh.ai/catalog/standards/sist/a5e55918-69ec-4b82-8531-df6523036d5b/iso-22320-2018)

[https://standards.iteh.ai/catalog/standards/sist/a5e55918-69ec-4b82-8531-  
df6523036d5b/iso-22320-2018](https://standards.iteh.ai/catalog/standards/sist/a5e55918-69ec-4b82-8531-df6523036d5b/iso-22320-2018)



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

ISO 22320:2018

<https://standards.iteh.ai/catalog/standards/sist/a5e55918-69ec-4b82-8531-df6523036d5b/iso-22320-2018>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2018

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  
Fax: +41 22 749 09 47  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Principles</b> .....	<b>1</b>
4.1 General.....	1
4.2 Ethics.....	1
4.3 Unity of command.....	1
4.4 Working together.....	2
4.5 All-hazards approach.....	2
4.6 Risk management.....	2
4.7 Preparedness.....	2
4.8 Information sharing.....	2
4.9 Safety.....	2
4.10 Flexibility.....	2
4.11 Human and cultural factors.....	2
4.12 Continual improvement.....	2
<b>5 Incident management</b> .....	<b>2</b>
5.1 General.....	2
5.2 Incident management process.....	3
5.2.1 General.....	3
5.2.2 Different perspectives.....	4
5.2.3 Understanding the importance of time.....	4
5.2.4 Being proactive.....	5
5.3 Incident management structure.....	5
5.3.1 General.....	5
5.3.2 Roles and responsibilities.....	6
5.3.3 Incident management tasks.....	6
5.3.4 Incident management resources.....	7
<b>6 Working together</b> .....	<b>7</b>
6.1 General.....	7
6.2 Prerequisites for achieving coordination and cooperation.....	8
6.2.1 Sharing the same incident management process.....	8
6.2.2 Seeing the whole picture.....	8
6.2.3 Common operational picture.....	8
6.2.4 Establishing communication.....	9
6.2.5 Establishing joint decisions.....	9
6.3 Developing and implementing methods for working together.....	9
6.3.1 General.....	9
6.3.2 Agreements.....	9
6.3.3 Technical equipment.....	10
<b>Annex A (informative) Additional guidance on working together</b> .....	<b>11</b>
<b>Annex B (informative) Additional guidance on incident management structure</b> .....	<b>14</b>
<b>Annex C (informative) Examples of incident management tasks</b> .....	<b>16</b>
<b>Annex D (informative) Incident management planning</b> .....	<b>18</b>
<b>Bibliography</b> .....	<b>20</b>

## 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](http://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](http://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](http://www.iso.org/iso/foreword.html).

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

This second edition cancels and replaces the first edition (ISO 22320:2011), which has been technically revised.

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](http://www.iso.org/members.html).

## Introduction

In recent years, there have been many disasters, both natural and human-induced, and other major incidents which have shown the importance of incident management in order to save lives, reduce harm and damage, and to ensure an appropriate level of continuity of essential societal functions.

Such functions include health, telecommunication, water and food supply, and access to electricity and fuel. While in the past the focus of incident management 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 need is driven by relationships and interdependencies between governments, non-governmental organizations (NGO), civil society organizations (CSO) and the private sector internationally.

Factors such as increased urbanization, critical infrastructure dependencies and interdependencies, socio-economic dynamics, environmental change, animal and human diseases and the heightened movement of people and goods around the world have increased the potential for disruptions and disasters that transcend geographic and political boundaries and impact the incident management capability.

This document provides guidance for organizations to improve their handling of all types of incidents (for example, emergencies, crisis, disruptions and disasters). The multiple incident management activities are often shared between organizations and agencies, with the private sector, regional organizations, and governments, have different levels of jurisdiction. Thus, there is a need to guide all involved parties in how to prepare and implement incident management.

Cross-organization-region or -border assistance during incident management is expected to be appropriate to the needs of the affected population and to be culturally sensitive. Therefore, multi-stakeholder participation, which focuses on community involvement in the development and implementation of incident management, is desirable where appropriate. Involved organizations require the ability to share a common approach across geographical, political and organizational boundaries.

This document is applicable to any organization responsible for preparing for or responding to incidents at the local, regional, national and, possibly, international level, including those who

- a) are responsible for, and participating in, incident preparation,
- b) offer guidance and direction in incident management,
- c) are responsible for communication and interaction with the public, and
- d) do research in the field of incident management.

Organizations benefit from using a common approach for incident management as this enables collaborative work and ensures more coherent and complementary actions among organizations.

Most incidents are local in nature and are managed at the local, municipal, regional, state or provincial level.

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

ISO 22320:2018

<https://standards.iteh.ai/catalog/standards/sist/a5e55918-69ec-4b82-8531-df6523036d5b/iso-22320-2018>

# Security and resilience — Emergency management — Guidelines for incident management

## 1 Scope

This document gives guidelines for incident management, including

- principles that communicate the value and explain the purpose of incident management,
- basic components of incident management including process and structure, which focus on roles and responsibilities, tasks and management of resources, and
- working together through joint direction and cooperation.

This document is applicable to any organization involved in responding to incidents of any type and scale.

This document is applicable to any organization with one organizational structure as well as for two or more organizations that choose to work together while continuing to use their own organizational structure or to use a combined organizational structure.

## 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*,  
<https://standards.iteh.ai/catalog/standards/sist/a5e55918-69ec-4b82-8531-d16523056d58/iso-22320-2018>

## 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 <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

## 4 Principles

### 4.1 General

An organization dealing with any incident should consider the principles described in 4.2 to 4.12.

### 4.2 Ethics

Incident management respects the primacy of human life and human dignity through neutrality and impartiality.

### 4.3 Unity of command

Incident management requires that every person at any point in time reports to only one supervisor.

#### 4.4 Working together

Incident management requires organizations to work together.

NOTE For additional information, see [Clause 6](#).

#### 4.5 All-hazards approach

Incident management considers both natural and human induced incidents, including those which the organization has not yet experienced.

NOTE For a definition of all-hazards, see ISO 22300.

#### 4.6 Risk management

Incident management is based on risk management.

NOTE Guidance on risk management is given in ISO 31000.

#### 4.7 Preparedness

Incident management requires preparedness.

#### 4.8 Information sharing

Incident management requires the sharing of information and perspectives.

#### 4.9 Safety

Incident management emphasizes the importance of safety for both responders and those impacted.

#### 4.10 Flexibility

Incident management is flexible (e.g. adaptability, scalability, and subsidiarity).

#### 4.11 Human and cultural factors

Incident management takes human and cultural factors into account.

#### 4.12 Continual improvement

Incident management emphasizes continual improvement to enhance organizational performance.

### 5 Incident management

#### 5.1 General

Incident management should consider a combination of facilities, equipment, personnel, organizational structure, procedures and communications.

Incident management is predicated on the understanding that in any and every incident there are certain management functions that should be carried out regardless of the number of people who are available or involved in the responding to the incident.

The organization should implement incident management, including

- a) an incident management process ([5.2](#)), and



- b) an incident management structure, which identifies incident management roles and responsibilities, tasks and the allocation of resources (5.3).

The organization should document the incident management process and structure.

## 5.2 Incident management process

### 5.2.1 General

The incident management process is based on objectives which are developed by gathering and proactively sharing information in order to assess the situation and identify contingencies.

The organization should engage in planning activities as part of preparedness and response, which consider the following:

- a) safety,
- b) incident management objectives,
- c) information about the situation,
- d) monitoring and assessing the situation,
- e) planning function which determine an incident action plan,
- f) allocating, tracking and releasing resources,
- g) communications,
- h) relationships with other organizations, common operational picture,
- j) demobilization and termination,
- k) documentation guidelines.

NOTE 1 [Annex D](#) gives recommendations on incident management planning.

NOTE 2 An incident action plan (verbal or written) includes goals, objectives, strategies, tactics, safety, communications and resource management information.

NOTE 3 Demobilize means to return resources to their original use and status.

NOTE 4 Termination means a formal handover from incident management responsibilities to another organization.

Decisions made among organizations should be shared as appropriate. The incident management process applies to any scale of incident (short-/long-term) and should be applied as appropriate to all levels of responsibility. [Figure 1](#) gives a simple example of the incident management process.

The organization should establish an incident management process that 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 incident management process should not be limited to the actions of the incident commander but should also be applicable to all people involved in the incident command team, at all levels of responsibility.

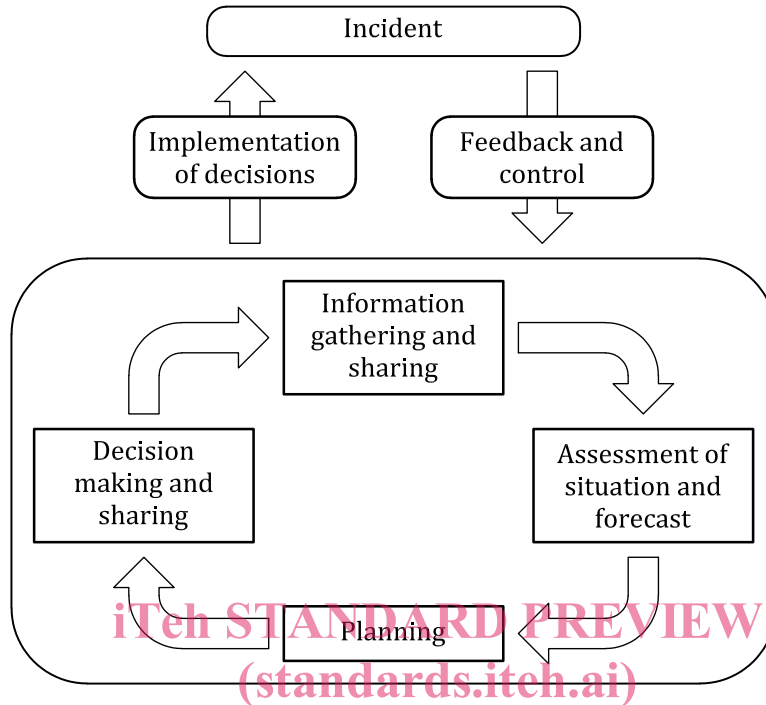


Figure 1 — Incident management process

<https://standards.itech.ai/catalog/standards/sist/a5e55918-69ec-4b82-8531-df6523036d5b/iso-22320-2018>

### 5.2.2 Different perspectives

The organization should strive to understand other perspectives such as

- a) within and outside the organization,
- b) various response scenarios,
- c) differing needs,
- d) various required actions, and
- e) different organizational cultures and objectives.

### 5.2.3 Understanding the importance of time

The organization should

- a) anticipate cascading effects,
- b) take the initiative to do something sooner, rather than later,
- c) consider other organization’s timelines,
- d) determine the impact of different timelines, and
- e) modify its timeline accordingly.

The organization should consider the needs and effects in both the short- and long-term. This includes anticipating

- how the incident will develop,
- when different needs will arise, and
- how long it takes to meet these needs.

#### 5.2.4 Being proactive

The organization should take the initiative to

- a) assess risks and align the response to increase response effectiveness,
- b) anticipate how incidents can change and use resources effectively,
- c) make decisions concerning various measures early enough for decisions to be effective when they are actually needed,
- d) manage the incident early,
- e) initiate a joint response instead of waiting for someone else to do so,
- f) find out what shared information is required, and
- g) inform and instruct involved parties, e.g. in order to build up new resources.

### 5.3 Incident management structure (standards.iteh.ai)

#### 5.3.1 General

ISO 22320:2018

<https://standards.iteh.ai/catalog/standards/sist/a5e55918-69ec-4b82-8531-1a2100000000>

The organization should implement an incident management structure to carry out the tasks relevant to the incident objectives.

An incident management structure should include the following basic functions.

- a) Command: authority and control of the incident; incident management objectives structure and responsibilities; ordering and release of resources.
- b) Planning: collection, evaluation and timely sharing of incident information and intelligence; status reports including assigned resources and staffing; development and documentation of incident action plan; information gathering, sharing and documentation.
- c) Operations: tactical objectives; hazard reduction; protection of people, property and environment; control of incident and transition to recovery phase.
- d) Logistics: incident support and resources; facilities, transportation, supplies, equipment maintenance, fuel, food service and medical services for incident personnel; communications and information technology support.
- e) Finance and administration: compensation and claims; procurement; costs and time. (Depending on the scale of an incident, a separate financial and administrative function may not be necessary.)

Planning, operations, logistics and finance and administration should be considered for each level of incident management, e.g. sections and subsections of the whole incident management system.

The organization should define and document the minimum staffing requirements to immediately initiate and continuously maintain the organization's incident management.

[Annexes B, C and D](#) provide additional information and examples of an incident management structure for one or more collaborating organizations with internal hierarchal structures.