

---

---

## Societal security — Terminology

*Sécurité sociétale — Terminologie*

STANDARDSISO.COM : Click to view the full PDF of ISO 22300:2012



STANDARDSISO.COM : Click to view the full PDF of ISO 22300:2012



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2012

All rights reserved. Unless otherwise specified, 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  
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
<b>Foreword</b> .....	<b>iv</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Terms and definitions</b> .....	<b>1</b>
2.1 Societal security.....	1
2.2 Management of societal security.....	3
2.3 Operational — Risk reduction.....	6
2.4 Operational — Exercise.....	7
2.5 Operational — Recovery.....	8
2.6 Technology.....	9
<b>Bibliography</b> .....	<b>11</b>

STANDARDSISO.COM : Click to view the full PDF of ISO 22300:2012

## 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 22300 was prepared by Technical Committee ISO/TC 223, *Societal security*.

STANDARDSISO.COM : Click to view the full PDF of ISO 22300:2012

# Societal security — Terminology

## 1 Scope

This International Standard contains terms and definitions applicable to societal security to establish a common understanding so that consistent terms are used.

## 2 Terms and definitions

### 2.1 Societal security

#### 2.1.1

##### **societal security**

protection of society from, and response to, incidents, emergencies and disasters caused by intentional and unintentional human acts, natural hazards, and technical failures

#### 2.1.2

##### **stakeholder**

person or group of people that holds a view that can affect the *organization* (2.2.9)

#### 2.1.3

##### **societal security framework**

set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving *societal security* (2.1.1)

Note 1 to entry: The foundations include the policy, objectives, mandate and commitment to manage societal security.

Note 2 to entry: Organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.

#### 2.1.4

##### **civil protection**

measures taken and systems implemented to preserve the lives and health of citizens, their properties and their environment from undesired events

Note 1 to entry: Undesired events can include accidents, emergencies and disasters.

#### 2.1.5

##### **risk**

effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected: positive and/or negative.

Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

Note 3 to entry: Risk is often characterized by reference to potential events, and consequences, or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

[SOURCE: ISO Guide 73]

**2.1.6  
risk management**

coordinated activities to direct and control an *organization* (2.2.9) with regard to *risk* (2.1.5)

[SOURCE: ISO Guide 73]

**2.1.7  
threat**

potential cause of an unwanted incident, which can result in harm to individuals, a system or *organization* (2.2.9), the environment or the community

**2.1.8  
event**

occurrence or change of a particular set of circumstances

Note 1 to entry: An event can be one or more occurrences, and can have several causes.

Note 2 to entry: An event can consist of something not happening.

Note 3 to entry: An event can sometimes be referred to as an "incident" or "accident".

Note 4 to entry: An event without consequences can also be referred to as a "near miss", "incident", "near hit" or "close call".

[SOURCE: ISO Guide 73]

**2.1.9  
consequence**

outcome of an event affecting objectives

Note 1 to entry: An event can lead to a range of consequences.

Note 2 to entry: A consequence can be certain or uncertain and can have positive or negative effects on objectives.

Note 3 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 4 to entry: Initial consequences can escalate through knock-on effects.

[SOURCE: ISO Guide 73]

**2.1.10  
business continuity**

capability of the *organization* (2.2.9) to continue delivery of products or services at acceptable predefined levels following disruptive *incident* (2.1.15)

**2.1.11  
disaster**

situation where widespread human, material, economic or environmental losses have occurred which exceeded the ability of the affected *organization* (2.2.9), community or society to respond and recover using its own resources

**2.1.12  
crisis**

situation with high level of uncertainty that disrupts the core activities and/or credibility of an *organization* (2.2.9) and requires urgent action

**2.1.13  
all-hazards**

naturally occurring events, human induced events (both intentional and unintentional) and technology caused events with potential impact on an *organization* (2.2.9), community or society and the environment on which it depends

**2.1.14****hazard**

source of potential harm

Note 1 to entry: Hazard can be a risk source.

[SOURCE: ISO Guide 73]

**2.1.15****incident**

situation that might be, or could lead to, a disruption, loss, emergency or crisis

**2.1.16****mitigation**

measures taken to prevent, limit and reduce impact of the negative *consequences* (2.1.9) of incidents, emergencies and disasters

**2.1.17****resilience**

adaptive *capacity* (2.2.15) of an *organization* (2.2.9) in a complex and changing environment

Note 1 to entry: Resilience is the ability of an organization to manage disruptive related *risk* (2.1.5).

[SOURCE: ISO Guide 73]

**2.2 Management of societal security****2.2.1****emergency management**

overall approach preventing and managing emergencies that might occur

Note 1 to entry: In general, emergency management utilizes a *risk management* (2.1.6) approach to prevention, preparedness, response and recovery before, during and after potentially destabilizing or disruptive events.

[SOURCE: ISO 22320]

**2.2.2****policy**

intentions and direction of an *organization* (2.2.9) as formally expressed by top management

**2.2.3****objective**

result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels [such as strategic, organization-wide, project, product and process (3.12)]. An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a societal security objective or by the use of other words of similar meaning (e.g. aim, goal, or target).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a societal security objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of societal security management systems standards, societal security objectives are set by the organization, consistent with the societal security policy, to achieve specific results.

#### 2.2.4

##### **top management**

person or group of people that directs and controls an *organization* (2.2.9) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: An organization can for this purpose be identified by reference to the scope of the implementation of a *management system* (2.2.5).

#### 2.2.5

##### **management system**

set of interrelated or interacting elements of an *organization* (2.2.9) that serve to establish policies and objectives, and processes to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning, operation, etc.

Note 3 to entry: The scope of a management system can include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

#### 2.2.6

##### **business impact analysis**

process of analysing activities and the effect that the business disruption might have upon them

#### 2.2.7

##### **sensitive information**

information that must be protected from public disclosure only because it would have an adverse effect on an *organization* (2.2.9), national security or public safety

#### 2.2.8

##### **risk source**

element which alone or in combination has the intrinsic potential to give rise to *risk* (2.1.5)

Note 1 to entry: A risk source can be tangible or intangible.

[SOURCE: ISO Guide 73]

#### 2.2.9

##### **organization**

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to, sole trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

#### 2.2.10

##### **risk owner**

person or entity with the accountability and authority to manage a *risk* (2.1.5)

[SOURCE: ISO Guide 73]

#### 2.2.11

##### **performance**

measurable result

Note 1 to entry: Performance can relate to either quantitative or qualitative findings.

Note 2 to entry: Performance can relate to the management of activities, processes, products (including services), systems, or organizations.

#### 2.2.12

##### **partnership**

organized relationship between two bodies (public-public, private-public, private-private) which establishes the scope, roles, procedures and tools to prevent and manage any *incident* (2.1.15) impacting on *societal security* (2.1.1) with respect to related laws

#### 2.2.13

##### **mutual aid agreement**

pre-arranged understanding between two or more entities to render assistance to each other

#### 2.2.14

##### **exercise programme**

series of exercise events designed to meet an overall objective or goal

#### 2.2.15

##### **capacity**

combination of all the strengths and resources available within an *organization* (2.2.9), community or society that can reduce the level of *risk* (2.1.5), or the effects of a crisis

Note 1 to entry: Capacity can include physical, institutional, social, or economic means as well as skilled personnel or attributes such as leadership and management.

#### 2.2.16

##### **competence**

demonstrated ability to apply knowledge and skills to achieve intended results

#### 2.2.17

##### **nonconformity**

non-fulfilment of a requirement

#### 2.2.18

##### **correction**

action to eliminate a detected *nonconformity* (2.2.17)

#### 2.2.19

##### **corrective action**

action to eliminate the cause of a *nonconformity* (2.2.17) and to prevent recurrence

Note 1 to entry: In the case of other undesirable outcomes, action is necessary to minimize or eliminate causes and to reduce impact or prevent recurrence. Such actions fall outside the concept of “corrective action” in the sense of this definition.

#### 2.2.20

##### **residual risk**

risk remaining after risk treatment

Note 1 to entry: Residual risk can contain unidentified risk.

Note 2 to entry: Residual risk is also known as “retained” risk.

[SOURCE: ISO Guide 73]

#### 2.2.21

##### **conformity**

fulfilment of a requirement

#### 2.2.22

##### **effectiveness**

extent to which planned activities are realized and planned results achieved

2.2.23

**continual improvement**

recurring activity to enhance performance

2.3 Operational — Risk reduction

2.3.1

**work environment**

set of conditions under which work is performed

Note 1 to entry: Conditions include physical, social, psychological and environmental factors such as temperature, recognition schemes, ergonomics and atmospheric composition.

2.3.2

**vulnerability**

intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a *consequence* (2.1.9)

2.3.3

**risk assessment**

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

[SOURCE: ISO Guide 73]

2.3.4

**probability**

measure of the chance of occurrence expressed as a number between 0 and 1 where 0 is impossibility and 1 is absolute certainty

[SOURCE: ISO Guide 73]

2.3.5

**prioritized activities**

activities to which priority must be given following an *incident* (2.1.15) in order to mitigate impacts

Note 1 to entry: Terms in common used to describe activities within this group include: critical, essential, vital, urgent and key.

2.3.6

**contingency**

possible future event, condition or eventuality

2.3.7

**training**

activities designed to facilitate the learning and development of knowledge, skills, and abilities, and to improve the performance of specific tasks or roles

2.3.8

**test**

exercise whose aim is to obtain an expected, measurable pass/fail outcome

Note 1 to entry: A test is a unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the aim or objectives of the exercise being planned.

2.3.9

**testing**

procedure for determining the presence, quality, or veracity of something

Note 1 to entry: Assessing a capability with the result being either pass or fail.

Note 2 to entry: Testing may be referred to as a "trial".

Note 3 to entry: Testing is often applied to supporting plans.

Note 4 to entry: Testing should start with simple component testing, building toward system testing.

## 2.4 Operational — Exercise

### 2.4.1

#### **scenario**

pre-planned storyline that drives an exercise; the stimuli used to achieve exercise objectives

### 2.4.2

#### **inject**

scripted piece of information inserted into the exercise and designed to elicit a response or decision and facilitate the flow of the exercise

### 2.4.3

#### **script**

story of the exercise as it develops, which allows directing staff to understand how events will develop during exercise play as the various elements of the master events list are introduced

Note 1 to entry: The script is often written as a narrative of simulated events.

### 2.4.4

#### **exercise co-ordinator**

person responsible for planning, coordinating, and implementing exercises

Note 1 to entry: This person is also responsible for the cooperation among entities, divisions, and external organizations in large-scale exercises.

### 2.4.5

#### **observer**

exercise participant who watches selected segments as they unfold while remaining separate from role player activities

Note 1 to entry: Observers play a crucial role in the debriefing and reporting process after an exercise. The term is also used for “VIP observers”, who usually visit the exercise for only a short time, largely for internal or external PR purposes, and do not take part in the debrief.

### 2.4.6

#### **monitoring**

determining the status of a system, a process or an activity

Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.

### 2.4.7

#### **drill**

activity which practices a particular skill and often involves repeating the same thing several times

EXAMPLE A fire drill to practice safely evacuating a building on fire.

### 2.4.8

#### **exercise**

process to train for, assess, practice, and improve performance in an organization

Note 1 to entry: 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 and identifying opportunities for improvement; and a controlled opportunity to practice improvisation.

Note 2 to entry: A test is a unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the goal or objectives of the exercise being planned.

#### 2.4.9

##### **exercise safety officer**

person tasked with ensuring that any actions during the exercise and testing are performed safely

Note 1 to entry: Usually relevant to a “live play” exercise.

Note 2 to entry: The exercise safety officer should be involved from the planning of the exercise and testing through to the debriefing.

#### 2.4.10

##### **functional exercise**

exercise to train for, assess, practice, and improve performance of single functions designed to respond to and recover from an unwanted event

Note 1 to entry: Functions can include an emergency operations centre (EOC) team or crisis management team or fire-fighters decontaminating mock victims.

#### 2.4.11

##### **full-scale exercise**

exercise which involves multiple *organizations* (2.2.9) or functions and includes actual activities

#### 2.4.12

##### **strategic exercise**

exercises involving top management at a strategic level

Note 1 to entry: Strategic-level top management typically includes inter-ministerial crisis personnel, political-administrative personnel, cross-sector and cross-departmental management personnel, and the crisis management organization of the corporate management team.

Note 2 to entry: Strategic exercises are designed to assess reactions to crisis in extreme situations.

Note 3 to entry: Strategic exercises are designed to develop a comprehensive coordination and decision-making culture in organizations in the public, private, and not-for-profit sectors.

#### 2.4.13

##### **after-action report**

document which records, describes and analyses the exercise, drawing on debriefs and reports from observers, and derives lessons from it

#### 2.4.14

##### **exercise annual plan**

document in which the exercise policy plan has been translated to exercise goals, and exercises, and in which an exercise agenda or exercise calendar for a certain year are reflected

### 2.5 Operational — Recovery

#### 2.5.1

##### **incident response**

actions taken in order to stop the causes for the imminent hazard and to mitigate the *consequences* (2.1.9) of potentially destabilizing or disruptive events and to recover to a normal situation

[SOURCE: ISO 22320]

#### 2.5.2

##### **incident command**

part of an organized *incident* (2.1.15) response structure

Note 1 to entry: Incident command is the process that is conducted within the command structures that evolve during the management of an incident.

[SOURCE: ISO 22320]