

# INTERNATIONAL STANDARD

**ISO  
31073**

First edition  
2022-02

---

---

## **Risk management — Vocabulary**

*Management du risque — Vocabulaire*

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

ISO 31073:2022

<https://standards.iteh.ai/catalog/standards/sist/da7740a8-790c-4c3b-bb4f-c80a79deb44a/iso-31073-2022>



Reference number  
ISO 31073:2022(E)

© ISO 2022

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

ISO 31073:2022

<https://standards.iteh.ai/catalog/standards/sist/da7740a8-790c-4c3b-bb4f-c80a79deb44a/iso-31073-2022>



**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](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>
3.1 Terms related to risk.....	1
3.2 Terms related to risk management.....	2
3.3 Terms related to the risk management process.....	2
<b>Bibliography</b> .....	<b>9</b>
<b>Index</b> .....	<b>10</b>

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

ISO 31073:2022

<https://standards.iteh.ai/catalog/standards/sist/da7740a8-790c-4c3b-bb4f-c80a79deb44a/iso-31073-2022>

## 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 262, *Risk management*.

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

This document provides basic vocabulary to develop common understanding on risk management concepts and terms among organizations and functions, and across different applications and types.

In the context of risk management terminology applicable to risks faced by organizations, it is intended that preference be given to the definitions provided in this document.

Risk management is application specific. In some circumstances, it can therefore be necessary to supplement the vocabulary in this document. Where terms related to the management of risk are used in a standard, it is imperative that their intended meanings within the context of the standard are not misinterpreted, misrepresented or misused. The terminology in this document may need to be replaced by disciplinary-specific terminology where appropriate.

In addition to managing threats to the achievement of their objectives, organizations are increasingly applying risk management processes and developing an integrated approach to risk management in order to improve the management of potential opportunities. The terms and definitions in this document are, therefore, broader in concept and application than those contained in other documents. Since organizations increasingly adopt a broader approach to the management of risk, this document addresses all applications and sectors.

This vocabulary document represents the current focus of ISO/TC 262 on the management of risks faced by organizations.

This document encourages a mutual and consistent understanding of, and a coherent approach to, the description of activities related to the management of risk, and the use of a uniform risk management terminology in processes and frameworks dealing with the management of the risks faced by organizations.

This document is intended to be used by:

- those engaged in managing risks;
- those who are involved in activities of the ISO and IEC;
- developers of national or sector-specific standards, guides, procedures and codes of practice related to the management of risk.

For principles and guidelines on risk management, see ISO 31000:2018.



# Risk management — Vocabulary

## 1 Scope

This document defines generic terms related to the management of risks faced by organizations.

## 2 Normative references

There are no normative references in this document.

## 3 Terms and definitions

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 Terms related to risk

#### 3.1.1 risk

effect of *uncertainty* (3.1.3) on *objectives* (3.1.2)

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in *opportunities* (3.3.23) and *threats* (3.3.13).

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of *risk sources* (3.3.10), potential *events* (3.3.11), their *consequences* (3.3.18) and their *likelihood* (3.3.16).

#### 3.1.2

#### 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).

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 management system objective, or by the use of other words with similar meaning (e.g. aim, goal, target).

#### 3.1.3

#### uncertainty

state, even partial, of deficiency of information related to understanding or knowledge

Note 1 to entry: In some cases, uncertainty can be related to the *organization's* (3.3.7) context as well as to its *objectives* (3.1.2).

Note 2 to entry: Uncertainty is the root source of *risk* (3.1.1), namely any kind of “deficiency of information” that matters in relation to objectives (and objectives, in turn, relate to all relevant *interested parties'* (3.3.2) needs and expectations).

## 3.2 Terms related to risk management

### 3.2.1

#### **risk management**

coordinated activities to direct and control an *organization* (3.3.7) with regard to *risk* (3.1.1)

### 3.2.2

#### **risk management policy**

statement of the overall intentions and direction of an *organization* (3.3.7) related to *risk management* (3.2.1)

[SOURCE: ISO Guide 73:2009, 2.1.2]

### 3.2.3

#### **risk management plan**

scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of *risk* (3.1.1)

Note 1 to entry: Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities.

Note 2 to entry: The risk management plan can be applied to a particular product, process and project, and part or whole of the *organization* (3.3.7).

[SOURCE: ISO Guide 73:2009, 2.1.3]

## 3.3 Terms related to the risk management process

### 3.3.1

#### **risk management process**

systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, *monitoring* (3.3.40) and reviewing *risk* (3.1.1)

[SOURCE: ISO Guide 73:2009, 3.1]

### 3.3.2

#### **interested party**

stakeholder

person or *organization* (3.3.7) that can affect, be affected by, or perceives itself to be affected by a decision or activity

### 3.3.3

#### **risk perception**

*interested party's* (3.3.2) view on *risk* (3.1.1)

Note 1 to entry: Risk perception reflects the interested party's needs, issues, knowledge, beliefs and values.

[SOURCE: ISO Guide 73:2009, 3.2.1.2, modified — “interested party” has replaced “stakeholder”, and “risk” has replaced “a risk” in the definition.]

### 3.3.4

#### **external context**

external environment in which the *organization* (3.3.7) seeks to achieve its *objectives* (3.1.2)

Note 1 to entry: External context can include:

- the 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 organization; and



- relationships with, and perceptions and values of, external *interested parties* (3.3.2).

[SOURCE: ISO Guide 73:2009, 3.3.1.1, modified — “interested parties” has replaced “stakeholders”.]

### 3.3.5

#### **internal context**

internal environment in which the *organization* (3.3.7) seeks to achieve its *objectives* (3.1.2)

Note 1 to entry: Internal context can include:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
- the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- information systems, information flows and decision-making processes (both formal and informal);
- relationships with, and perceptions and values of, internal *interested parties* (3.3.2);
- the organization’s culture;
- standards, guidelines and models adopted by the organization; and
- form and extent of contractual relationships.

[SOURCE: ISO Guide 73:2009, 3.3.1.2, modified — “interested parties” has replaced “stakeholders”.]

### 3.3.6

#### **risk criteria**

terms of reference against which the significance of *risk* (3.1.1) is evaluated

Note 1 to entry: Risk criteria are based on *organizational objectives* (3.1.2), and *external* (3.3.4) and *internal context* (3.3.5).

Note 2 to entry: Risk criteria can be derived from standards, laws, policies and other requirements.

[SOURCE: ISO Guide 73:2009, 3.3.1.3, modified — “risk” has replaced “a risk” in the definition.]

### 3.3.7

#### **organization**

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.1.2)

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.

### 3.3.8

#### **risk assessment**

overall process of *risk identification* (3.3.9), *risk analysis* (3.3.15) and *risk evaluation* (3.3.25)

[SOURCE: ISO Guide 73:2009, 3.4.1]

### 3.3.9

#### **risk identification**

process of finding, recognizing and describing *risks* (3.1.1)

Note 1 to entry: Risk identification involves the identification of *risk sources* (3.3.10), *events* (3.3.11), their causes and their potential *consequences* (3.3.18).

Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and *interested party’s* (3.3.2) needs.

[SOURCE: ISO Guide 73:2009, 3.5.1, modified — “interested party” has replaced “stakeholder”.]

### 3.3.10

#### **risk source**

element which alone or in combination has the potential to give rise to *risk* (3.1.1)

### 3.3.11

#### **event**

occurrence or change of a particular set of circumstances

Note 1 to entry: An event can have one or more occurrences, and can have several causes and several *consequences* (3.3.18).

Note 2 to entry: An event can also be something that is expected which does not happen, or something that is not expected which does happen.

Note 3 to entry: An event can be a *risk source* (3.3.10).

### 3.3.12

#### **hazard**

source of potential harm

Note 1 to entry: Hazard can be a *risk source* (3.3.10).

[SOURCE: ISO Guide 73:2009, 3.5.1.4]

### 3.3.13

#### **threat**

potential source of danger, harm, or other undesirable outcome

Note 1 to entry: A threat is a negative situation in which loss is likely and over which one has relatively little control.

Note 2 to entry: A threat to one party may pose an *opportunity* (3.3.23) to another.

### 3.3.14

#### **risk owner**

person or entity with the accountability and authority to manage *risk* (3.1.1)

[SOURCE: ISO Guide 73:2009, 3.5.1.5, modified — “risk” has replaced “a risk” in the definition.]

### 3.3.15

#### **risk analysis**

process to comprehend the nature of *risk* (3.1.1) and to determine the *level of risk* (3.3.22)

Note 1 to entry: Risk analysis provides the basis for *risk evaluation* (3.3.25) and decisions about *risk treatment* (3.3.32).

[SOURCE: ISO Guide 73:2009, 3.6.1, modified — Note 2 to entry has been deleted.]

### 3.3.16

#### **likelihood**

chance of something happening

Note 1 to entry: In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically [such as a *probability* (3.3.19) or a *frequency* (3.3.20)].

Note 2 to entry: The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.