



BSI Standards Publication

Information technology — The safe framework

National foreword

This British Standard is the UK implementation of ISO/IEC 25389:2025.

The UK participation in its preparation was entrusted to Technical Committee ICT/1, Information systems co-ordination.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 33969 7

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2025.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------



**International
Standard**

ISO/IEC 25389

**Information technology — The safe
framework**

**First edition
2025-06**

Reference number
ISO/IEC 25389:2025(en)

Full document details: BS ISO/IEC 25389:2025

© ISO/IEC 2025



Documents

Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Digital trust and safety	3
5 Commitments and practices	4
5.1 Product development	5
5.2 Product governance	6
5.3 Product enforcement	6
5.4 Product improvement	7
5.5 Product transparency	7
6 Assessment framework	8
6.1 Scoping	8
6.2 Tailoring	8
6.2.1 Tailoring methodology	8
6.2.2 Evaluating the organization's size and scale	9
6.2.3 Evaluating the impact of the product or digital service	10
6.2.4 Determine the initial recommended assessment level	10
6.2.5 Factor in additional business landscape considerations	11
6.3 Assessment Execution	12
6.3.1 Assessment Methodology	12
6.3.2 Discover	13
6.3.3 Identify	14
6.3.4 Assess	14
6.3.5 Test	15
6.3.6 Report	15
Annex A (informative) Illustrative examples of the tailoring framework	16
Annex B (informative) Risk Profile Questionnaire	17
Annex C (informative) Summary of differences between L1, L2, and L3 Assessments	19
Annex D (informative) Sample information discovery form	20
Annex E (informative) Question Bank	22
Annex F (informative) Illustrative example: product area report template	25
Bibliography	26

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by the Digital Trust & Safety Partnership (DTSP) (as The Safe Framework Specification) and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

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 and www.iec.ch/national-committees.

Introduction

Digital services are increasingly central to our daily lives, facilitating social discourse, economic activity, and much more. These services provide powerful tools for users across the globe to engage in a wide range of valuable online activity. But like any tool, they can also be misused to facilitate harmful behavior and content. Awareness of and action against this misuse has grown in recent years, which has led to increasing urgency in understanding, supporting, and evaluating effective ways to reduce harms associated with online content and behavior, while also protecting people's ability to express themselves, carry out business, access information, associate, work, study, and participate in their communities through digital services.

Striking this balance presents a considerable challenge. To begin, there is no one-size-fits-all approach to handling online content and associated behavioral risks or, more generally, to organizations' trust and safety operations. Depending on the nature of the digital service, each may face unique risks relative to the various products or features they provide – different threats, different vulnerabilities, and different consequences. Products or features may engage with end users directly or indirectly, as well as with other services or businesses. What is an effective practice for one digital service may not suit another, and highly prescriptive or rigid approaches to defining trust and safety practices are likely to be too broad, too narrow or have negative unintended consequences. Further, risks change over time and so approaches to mitigating them must also have room to evolve.

Given the diversity of digital services, it is important to define an overall framework and set of aims for what constitutes a responsible approach to managing content- and conduct-related risks, to which digital services can then map their specific practices. This flexible approach has been deployed in other domains, such as information security, yet existing frameworks are not sufficiently concrete to be applied when it comes to addressing harmful behavior and content online.

This document aims to fill this need by offering a framework of commitments to address content- and conduct-related risks. While the overarching commitments are uniform, the method by which they are fulfilled – whether by application of the illustrative practices in this document or alternatives – will vary by digital product or feature and evolve with both the challenges faced and advances made in the field of trust and safety.

This document also provides recommendations for organizations to evaluate the maturity of their implementation of these commitments through a rigorous and flexible approach to assessment.

This document is for the internal use of the organization responsible for trust and safety operations for a digital product or service. Recommendations for public reporting about the commitments and their implementation are outside the scope of this document.

This document is neither a management system standard, nor does it consider the issues of information security, privacy, and other aspects of security, privacy, and data management that are addressed by existing international standards.

Information technology — The safe framework

1 Scope

This document provides a framework of recommendations for organizations that offer a public-facing digital product or service for which they conduct trust and safety operations to control or manage content- and conduct-related risks.

This document also includes recommendations for assessing the implementation of practices for addressing content- and conduct-related risks.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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 abuse

use of a product or service in a way that violates the provider's *product governance* (3.13), generally because it creates or increases the risk of harm to a person or group or tends to undermine the purpose, function or quality of the service.

3.2 assessments

methods to evaluate policies and operations for accuracy, changing user practices, emerging harms, effectiveness and process improvement

3.3 best practices

examples of practices embodying the commitments to product development, product governance, enforcement, improvement, and transparency

3.4 commitment

the actions taken by an organization to identify and address *content- and conduct-related risk* (3.8)

3.5 community guidelines

content policy

acceptable use policy

the set of conditions and limitations governing use of a digital service that a user must agree to as a condition of use.

Note 1 to entry: These are generally written in plain and concrete language compared to legal language used in *terms of service* (3.18).

3.6

conduct

user behavior facilitated by a digital product or service

Note 1 to entry: behavior may take place entirely online, or take place offline but is mediated by the use of the digital product or service.

3.7

content

text, images, audio and videos which are accessed by users via a digital product or service

Note 1 to entry: content may be created or generated by other users, AI, publishers or other entities before being made available for a user to access.

3.8

content- and conduct-related risk(s)

the possibility of certain illegal, dangerous, or otherwise harmful content or behavior, including risks to human rights, which are prohibited by relevant policies and terms of service

3.9

control

measure that maintains and/or modifies risk

Note 1 to entry: Risk controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

Note 2 to entry: Risk controls do not always exert the intended or assumed modifying effect.

[SOURCE: ISO 31073:2022, 3.3.33]

3.10

digital product

a product offered by one party to another party by means of digital hardware or software technology, or both, including communication over a network

3.11

digital service

a service offered by one party to another party by means of digital hardware or software technology, or both, including communication over a network

[SOURCE: ISO/IEC TS 5928:2023]

3.12

monthly active registered users

the number of users with a registered account who logged in or otherwise authenticated to visit the product website, mobile website, desktop or mobile application, within the last 30 days, from the date of measurement.

3.13

product governance

the set of agreements, rules, and guidelines mediating user interaction with the digital service and structuring conduct related to the product (examples include terms of service, privacy policy, community guidelines, content policy, acceptable use policy, codes of conduct, and any organizational processes by which these governing statements are created, adopted, or iterated).

3.14

question bank

set of questions that can be used by an organization to understand and identify the specific practices it uses to mitigate content- and conduct-related risks.

3.15

risk

effect of uncertainty on objectives

Note 1 to entry: In the context of this document, risk can be expressed as effect of uncertainty on implementation of commitments

Note 2 to entry: in the context of this document, risk is associated with *content- and conduct-related risk* (3.8)

[SOURCE: ISO/IEC 27000:2018, 3.61]

3.16

risk assessment

overall process of risk identification, risk analysis and risk evaluation

[SOURCE: 31073:2022, 3.3.8]

3.17

risk profile questionnaire

yes/no questions used to measure the extent to which product or service features and policies implicate *content- or conduct-related risks* (3.8).

3.18

terms of service

rules by which users agree to abide in order to use a service

[SOURCE: ISO 32110:2023, 3.4.7]

3.19

trust and safety

The field and practices that manage challenges related to *content- and conduct-related risk* (3.8), including but not limited to consideration of safety-by-design, *product governance* (3.13), *risk assessment* (3.16), detection, and response, quality assurance, and transparency.

Note 1 to entry: “trust and safety” is a term used throughout the digital products and services industry that has a definition that is distinct from ISO/IEC definitions for trustworthiness and safety, which have been referenced in this document for completeness and to avoid confusion.

Note 2 to entry: for the ISO/IEC definition of trustworthiness, see ISO/IEC TS 5723.

Note 3 to entry: for the ISO/IEC definition of safety, see ISO/IEC Guide 51.

3.20

user volume

average monthly active registered users over the past twelve months.

4 Digital trust and safety

For an organization which provides a digital product or service, digital trust and safety refers to the part of that organization that focuses on understanding and addressing the harmful content or conduct potentially associated with that service.

Content- and conduct-related risks are sources of hazard and harm created by user generated content and conduct, which are distinct from other risks in digital products and services, which can be managed through existing international standards. These include but are not limited to information security, privacy, data management, and artificial intelligence.

Each organization is guided by its own values, product aims, digital tools, and human-led processes to make decisions about how to enable a broad range of human expression and conduct, while working to identify and prevent harmful content or conduct. Despite these individual approaches, a shared framework of best practices and assessments can help advance the development of industry best practices to ensure consumer trust and safety when using digital products and services.