

ISO/IEC TS 27103

Cybersecurity — Guidance on using ISO and IEC standards in a cybersecurity framework

*Cybersécurité — Recommandations sur l'utilisation des normes
ISO et IEC dans le cadre de la cybersécurité*

First edition
2026-02



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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

This is a preview of ISO/IEC TS 27103:2026. [Click here to purchase the full version from the ANSI store.](#)

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Document structure	1
5 Background	2
5.1 General	2
5.2 Advantages of a risk-based approach to cybersecurity	2
5.3 Interested parties	2
5.4 Activities of a cybersecurity framework and programme	2
6 Concepts	3
6.1 Overview of cybersecurity frameworks	3
6.2 Cybersecurity framework functions	3
6.2.1 General	3
6.2.2 Identify	4
6.2.3 Protect	5
6.2.4 Detect	6
6.2.5 Respond	6
6.2.6 Recover	7
Annex A (informative) Subcategories	8
Annex B (informative) Three principles of cybersecurity for top management	16
Bibliography	19

This is a preview of ISO/IEC TS 27103:2026. Click here to purchase the full version from the ANSI store.

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. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (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 Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This first edition of ISO/IEC TS 27103 cancels and replaces ISO/IEC TR 27103:2018, which has been technically revised.

The main changes are as follows:

— updated to align with ISO/IEC 27002:2022.

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.

This is a preview of ISO/IEC TS 27103:2026. [Click here to purchase the full version from the ANSI store.](#)

Security on the Internet and other networks is a subject of growing concern. Organizations around the world, in both government and industry sectors, are seeking ways to address and manage cybersecurity risks, including via baseline cybersecurity measures that may be implemented as requirements or guidance. The demonstrated security and economic value of utilizing existing best practices to develop approaches to cyber risk management has led organizations to assess how to use and improve upon existing approaches.

Perspectives, and consequent approaches, to risk management are affected by the terminology used, e.g. “cybersecurity” versus “information security”. Where similar risks are addressed, this different perspective can result in “cybersecurity” approaches focusing on external threats and the need to use information for organizational purposes, while, in contrast, “information security” approaches consider all risks whether from internal or external sources. There can also be a perception that cybersecurity risks are primarily related to antagonistic threats, and that a lack of “cybersecurity” can create worse consequences to the organization than a lack of “information security”. Thus, cybersecurity can be perceived as more relevant to the organization than information security. This perception can cause confusion and also reduces the effectiveness of risk assessment and treatment.

Regardless of perception, the concepts behind information security can be used to assess and manage cybersecurity risks. The key question is how to manage cybersecurity risk in a comprehensive and structured manner, and ensure that processes, governance and controls are addressed. This can be done through a management systems approach. An Information Security Management system (ISMS) as described in ISO/IEC 27001 is a well proven way for any organization to implement a risk-based approach to cybersecurity.

This document demonstrates how a cybersecurity framework can utilize current information security standards to achieve a well-controlled approach to cybersecurity management.