



FINAL DRAFT Technical Specification

ISO/IEC DTS 27103

Cybersecurity — Guidance on using ISO and IEC standards in a Cybersecurity Framework

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2025-05-26

Voting terminates on:
2025-07-21

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO/IEC DTS 27103](https://standards.iteh.ai/catalog/standards/iso/9428b7e9-db7c-4cc4-ab06-0b20076ab23f/iso-iec-dts-27103)

<https://standards.iteh.ai/catalog/standards/iso/9428b7e9-db7c-4cc4-ab06-0b20076ab23f/iso-iec-dts-27103>

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

ISO/IEC DTS 27103

<https://standards.itih.ai/catalog/standards/iso/9428b7e9-db7c-4cd4-ab06-0b20076ab23f/iso-iec-dts-27103>



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 Document structure	1
5 Background	1
5.1 General	1
5.2 Advantages of a risk-based approach to cybersecurity	2
5.3 Stakeholders	2
5.4 Activities of a cybersecurity framework and programme	2
6 Concepts	2
6.1 Overview of cybersecurity frameworks	2
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

ITeh Standards
(<https://standards.iteh.ai/>)
Document Preview

[ISO/IEC DTS 27103](https://standards.iteh.ai/catalog/standards/iso/9428b7e9-db7c-4cd4-ab06-0b20076ab23f/iso-iec-dts-27103)

<https://standards.iteh.ai/catalog/standards/iso/9428b7e9-db7c-4cd4-ab06-0b20076ab23f/iso-iec-dts-27103>

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. 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.