

ISO/IEC ~~TS~~ DTS 27103:2025(en)

ISO ~~JTC1~~ /IEC JTC 1/SC_27

Secretariat: DIN

Date: 2025-05-09

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

iTeh Standards

Warning for Drafts

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

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.

© ISO 2014



© ISO 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~~ Copyright Office

~~Case postale 56 • CP 401 • CH-1211~~ 1214 Vernier, Geneva ~~20~~

~~Tel. Phone:~~ + 41 22 749 01 11

~~Fax + 41 22 749 09 47~~

~~E-mail~~ copyright@iso.org

~~Web~~ www.iso.org

Email: copyright@iso.org

Website: www.iso.org

Published in Switzerland.

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>

Foreward

Contents

Foreword	4
Introduction.....	ix
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.....	3
6 Concepts	3
6.1 Overview of cybersecurity frameworks.....	3
6.2 Cybersecurity framework functions.....	4
6.2.1 General.....	4
6.2.2 Identify	5
6.2.3 Protect.....	7
6.2.4 Detect	8
6.2.5 Respond.....	9
6.2.6 Recover.....	10
Annex A (informative) Subcategories	13
Annex B (informative) Three principles of cybersecurity for top management.....	33
Bibliography.....	37

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. ~~In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.~~

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). ~~www.iso.org/directives or www.iec.ch/members_experts/refdocs).~~

~~Attention is drawn~~ ISO and IEC draw attention to the possibility that ~~some of the elements~~ implementation of this document may ~~be involve~~ the subject use of (a) patent ~~rights(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. 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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

ISO/IEC DTS 27103

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

For an explanation ~~on 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 ~~the following URL~~ www.iso.org/iso/foreword.html. ~~www.iso.org/iso/foreword.html.~~ In the IEC, see www.iec.ch/understanding-standards.

~~The committee responsible for this~~ This document is ~~was prepared by Joint Technical Committee ISO/IEC JTC-1, Information technology, Subcommittee SC-27, Information security, cybersecurity and privacy protection.~~

Contents

Foreward	2
Introduction	6
1 Scope	7
2 Normative references	7
3 Terms and definitions	7
4 Document structure	7
5 Background	7
5.1 General	7
5.2 Advantages of a risk-based approach to cybersecurity	8
5.3 Stakeholders	8
5.4 Activities of a cybersecurity framework and programme	8
6 Concepts	9
6.1 Overview of cybersecurity frameworks	9
6.2 Cybersecurity framework functions	9
6.2.1 Overview	9
6.2.2 Identify	10
6.2.3 Protect	12
6.2.4 Detect	13
6.2.5 Respond	13
6.2.6 Recover	14
Annex A	16
A.1 General	16
A.2 Identify Sub-categories	16
A.2.1 Business Environment	16
A.2.2 Risk Assessment	17
A.2.3 Risk Management Strategy	17

A.2.4 Governance	18
A.2.5 Asset Management	18
A3 Protect Categories	19
A.3.1 Access Control	19
A.3.2 Awareness and Training	19
A.3.3 Data Security	20
A.3.4 Information Protection Processes and Procedures	20
A.3.5 Maintenance	21
A.3.6 Protective Technology	22
A4 Detect Categories	22
A.4.1 Anomalies and Events	22
A.4.2 Security Continuous Monitoring	23
A.4.3 Detection Processes	23
A5 Respond Categories	24
A.5.1 Response Planning	24
A.5.2 Communications	24
A.5.3 Analysis	25
A.5.4 Mitigation	25
A.5.5 Improvements	25
A6 Recover Categories	26
A.6.1 Recovery Planning	26
A.6.2 Improvements	26
A.6.3 Communications	26
Annex B	27
Three principles of the cybersecurity for top management	27
B.1 General	27
B2 Three principles of cybersecurity management	27