



DPC: 25 / 30469622 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 21 January 2025

Origin: International

Latest date for receipt of comments: 10 March 2025

Project No. 2023/00316

Responsible committee: IST/33/1 Information Security Management Systems

Interested committees:

Title: BS EN ISO/IEC 27028 Information security, cyber security and privacy protection — Guidance on ISO/IEC 27002 attributes

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 10 March 2025**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: **Mr Delme Stephenson (BSI)**
Direct tel: **020 8996 7213**
E-mail: **delme.stephenson@bsigroup.com**

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

Information security, cyber security and privacy protection — Guidance on ISO/IEC 27002 attributes

ICS: 35.030

ISO/IEC DIS 27028

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2025-01-15

Voting terminates on:
2025-04-09

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

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.

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.

Reference number
ISO/IEC DIS 27028:2025(en)

Full document details: 25/30469622 DC

© 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 Abbreviated terms	2
5 Overview on attribute approach	2
5.1 Concept of attribute and its use	2
5.1.1 General	2
5.1.2 Attributes given in ISO/IEC 27002:2022	2
5.1.3 Additional attributes introduced in this document	2
5.2 Custom attributes	3
5.2.1 General	3
5.2.2 The method	4
5.3 Examples of using attributes	4
5.3.1 General	4
5.3.2 Using attributes to create robust risk treatment plans	5
5.3.3 Other example of using attribute	8
6 Additional attributes	10
6.1 Security architecture attribute	11
6.2 Assurance attribute	11
6.3 Complexity attribute	12
6.4 Contextual-fit attribute	12
6.5 Control environment attribute	13
6.6 Failure modes attribute	13
6.7 Formality attribute	14
6.8 Integration attribute	14
6.9 Mature attribute	14
6.10 Measurability attribute	15
6.11 Multi-functionality attribute	15
6.12 Origin attribute	16
6.13 Regulation attribute	16
6.14 Strength attribute	17
6.15 Target attribute	17
6.16 Transparency attribute	17
6.17 Cost attribute	18
6.18 Other custom controls and other custom attributes	19
Bibliography	20

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 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. 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.

For an explanation on 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: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Introduction

Subclause 4.2 of ISO/IEC 27002:2022, and its Annex A, define the concept of attributes. ISO/IEC 27002:2022 also explains that an organization can develop its own attributes (with the corresponding attribute values) to describe how controls are used or how to determine where they are applicable.

In addition to the attributes and themes presented in ISO/IEC 27002:2022, information security controls can also be characterized in other ways which can be relevant and helpful in particular situations when determining or designing controls.

The document provides guidance on how to develop customized attributes and describes how the attributes can be used. It introduces a method to help organizations develop their own custom attributes based on event-consequence scenarios and describes how attributes can be used to discover gaps within the organization's risk treatment plan(s) and check if the plan(s) is (are) tolerant of control failures.

It also describes how attributes can be used as criteria to set controls to mitigate the risk within an organization's information security management system (ISMS).

ISO/IEC 27002:2022 provides a comprehensive set of information security controls that:

- mitigate risk associated with the preservation of confidentiality, integrity, and availability of information within the scope of the ISMS, that is the stated purpose of ISO/IEC 27001:2022^[3];
- prevent, or detect the occurrence of information security events, or mitigate the effects of such events;
- mitigate risk associated with a variety of risk contexts.

This document is specifically concerned with the attributes of information security controls, but the concept and approach can be applied to attributes of other types of controls, e.g. privacy controls, health and safety controls, environmental protection controls, financial controls.

In principle, such an application of attributes can be applied to other information security issues, whatever they might be. If the attributes given in ISO/IEC 27002:2022 are undesirable for the organization's purpose, the organization can create its own, as exemplified by the guidance provided in this document.

Information security, cyber security and privacy protection — Guidance on ISO/IEC 27002 attributes

1 Scope

This document provides guidance on the use and development of attributes aligned to ISO/IEC 27002:2022. This guidance set out in this document is generic and is intended to be applicable to all organizations, regardless of type, size, or nature.

Excluded from this standard are aspects of conformity assessment.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27002:2022 and the following 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 attribute

quality or feature of something or somebody

Note 1 to entry: Attribute is a quality or feature regarded as a characteristic or inherent part of something.

Note 2 to entry: In the context of this document the term 'attribute' is used within the context of *control attribute* (3.3).

Note 3 to entry: An attribute can include information about the intended use.

3.2 attribute value

particular form or quantity, or a category or range of quantities, for a given attribute

3.3 control attribute

any attribute not included in ISO/IEC 27002:2022

3.4 custom attribute

attribute developed or adopted by the organization or the users which differs from those given in ISO/IEC 27002:2022