International Standard

ISO/IEC 27028

First edition
2026-11

Information security, cybersecurity and privacy protection — Guidance on using information security control attributes

Sécurité de l'information, cybersécurité et protection de la vie privée — Recommandations sur l'utilisation des attributs de contrôle de la sécurité de l'information

Reference number
ISO/IEC 27028:2026(en)

© ISO/IEC 2026

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **1**
5 Overview on attribute approach ... **2**
5.1 Concept of attribute ... 2
5.1.1 General ... 2
5.1.2 Attributes given in ISO/IEC 27002 ... 2
5.1.3 Additional attributes introduced in this document ... 3
5.2 Custom attributes ... 3
5.2.1 General ... 3
5.2.2 Event-consequence scenario method ... 4
5.3 Benefits from using attributes ... 5
5.3.1 General ... 5
5.3.2 Creating robust risk treatment plans ... 6
5.3.3 Defining the relationship between this document and both ISO/IEC 27002 and ISO/IEC 27005 ... 8
5.3.4 Strengthening information security ... 8
5.3.5 Achieving a balanced suite of controls ... 9
5.3.6 Maximizing the value of existing and proposed controls ... 9
5.3.7 Reviewing and assessing controls ... 9
5.3.8 Viewing controls from the audience's perspective ... 10
5.3.9 Improving privacy through attributes ... 10
6 Additional attributes ... **10**
6.1 General ... 10
6.2 Assurance attribute ... 11
6.3 Complexity attribute ... 11
6.4 Contextual-fit attribute ... 12
6.5 Control environment attribute ... 12
6.6 Failure modes attribute ... 13
6.7 Formality attribute ... 13
6.8 Integration attribute ... 13
6.9 Mature attribute ... 14
6.10 Measurability attribute ... 14
6.11 Multi-functionality attribute ... 15
6.12 Origin attribute ... 15
6.13 Regulation attribute ... 16
6.14 Strength attribute ... 16
6.15 Reduction-focused attribute ... 16
6.16 Transparency attribute ... 17
6.17 Cost attribute ... 17
6.18 Other custom controls and other custom attributes ... 18
Bibliography ... **19**

© ISO/IEC 2026 – All rights reserved

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 the Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

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.

© ISO/IEC 2026 – All rights reserved

Introduction

ISO/IEC 27002:2022, 4.2 and Annex A, define the concept of attributes. ISO/IEC 27002 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, information security controls can also be characterized in other ways which can be relevant and helpful in particular situations when determining or designing controls.

This document provides guidance on the use of information security control attributes. 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 to check if such plans 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 provides a 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;

— 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 and financial controls.

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

© ISO/IEC 2026 – All rights reserved

Information security, cybersecurity and privacy protection — Guidance on using information security control attributes

1 Scope

This document provides guidance on the use of information security control attributes specified in ISO/IEC 27002. The guidance given in this document is generic and is intended to be applicable to all organizations, regardless of type, size, or nature.

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*

Bibliography

[1] ISO 22340, *Security and resilience — Protective security — Guidelines for an enterprise protective security architecture and framework*

[2] ISO 22301, *Security and resilience — Business continuity management systems — Requirements*

[3] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[4] ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[5] ISO/IEC/TS 27008, *Information technology — Security techniques — Guidelines for the assessment of information security controls*

[6] ISO/IEC/TS 27110, *Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines*

[7] Cloud Security Alliance, "Cloud Controls Matrix (CCM)". Cloud Security. [Viewed 12 April 2026]. Available from: https://cloudsecurityalliance.org/research/cloud-controls-matrix/

[8] ISACA, "COBIT". [Viewed 12 April 2026]. Available from: https://www.isaca.org/resources/cobit

[9] National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0. [Viewed 12 April 2026]. Available from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[10] National Institute of Standards and Technology. "NIST Special Publication 800-Series". [Viewed 12 April 2026]. Available from: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

[11] National Institute of Standards and Technology, "The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management." [Viewed 12 April 2026]. Available from: https://www.nist.gov/privacy-framework/privacy-framework

[12] ISO/IEC 21827, *Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)*

[13] ISO/IEC 27701, *Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance*

[14] Information Security Assessment current version (6.0.3) [Viewed 12 April 2026]. Available from: https://www.enx.com/en-US/TISAX/downloads/

[15] National Institute of Standards and Technology, "NIST Risk Management Framework" [Viewed 12 April 2026]. Available from: https://nist.gov/rmf

© ISO/IEC 2026 – All rights reserved