ISO/IEC TS 27028

ISO/IEC TS 27028 — Information security, cybersecurity and privacy protection — **Guidance on ISO/IEC 27002 attributes** *[DRAFT]*

Abstract

"[ISO/IEC TS 27028] provides guidance on the use and development of attributes aligned to ISO/IEC 27002:2022."

[Source: ISO/IEC JTC 1/SC 27 Committee Doc 11 May 2025]

Introduction

ISO/IEC 27002:2022 introduced a new structure for the information security controls, based around 'themes' and 'attributes', noting that organisations may prefer to use their own attributes as well or instead. ISO/IEC 27028 will explain how to do that, in practice, suggesting a variety of attributes with which to classify or characterise, select or design information security controls in various ways for various information security and business management purposes.

Scope of the standard

The standard will expand upon the control attributes from ISO/IEC 27002, providing practical guidance on how to use the specified attributes *and* how to develop additional attributes and attribute values where appropriate.

Content of the standard

The standard may cover:

- *"Guidance on the development of customized sets of attributes and their usage;*
- *Attributes can be used to check that an organization's risk treatment plan(s) are tolerant of control failures;*
- *This concept can be used to confirm that controls cover the different aspects an organization has regarding its risks within scope of an ISMS."*

[Source: design specification]

Status of the standard

Work started on this project in 2021.

It will be a **T**echnical **S**pecification rather than a full **I**nternational **S**tandard since the approach is innovative and not yet proven by experience.

New Structural and content comments on the **D**raft **I**nternational **S**tandard, plus revision of the title and scope,

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

mean another DIS version is on the cards, necessitating an extension to the project timescale. The standard is unlikely to be published until the middle of 2026.

Personal comments

There has been significant interest and support for the control attributes concept from ISO/IEC JTC 1/SC 27. When eventually published, I believe ISO/IEC TS 27028 will be a valuable contribution to the field, expanding on the value and utility of ISO/IEC 27002.

Meanwhile, a free guideline in the ISO27k Toolkit explains how control attributes can be used creatively within an ISO27k ISMS, or indeed any other information risk-based framework that involves mitigating unacceptable risks using appropriate information security controls. Thinking about which attributes or characteristics of controls are relevant, plus the importance of the corresponding attribute values, helps round-off the analysis and so select appropriate controls.

< Previous standard ^ Up a level ^ Next standard >

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799