



## Expert commentary

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

David Brewer, Director, IMS-Smart Ltd



## 1 Overview

BS EN ISO/IEC 27002:2022, the third edition of this standard, technically revises, cancels and replaces the second edition – BS EN ISO/IEC 27002:2017. The standard provides a reference set of information security controls for use in the context of BS EN ISO/IEC 27001 (the Information Security Management System, or ISMS requirements standard). It can also be used as a guidance document for organizations wishing to develop their own information security control guidelines. The document is intended for use by organizations of all types and sizes.

A requirement of the ISMS standard is to determine, through a process of risk assessment and risk treatment, the information security controls that are necessary to render the organization's exposure to information security risk acceptable. To ensure that no necessary control has been inadvertently omitted, organizations are then required to compare their necessary controls with the reference set of controls in Annex A to that standard. Publication of an anticipated Amendment to BS EN ISO/IEC 27001:2017, will change the second edition of that standard to align its reference set with those in BS EN ISO/IEC 27002:2022. Thus, this third edition of BS EN ISO/IEC 27002 effectively updates the ISMS reference control set.

The level of change incorporated into the revised version of the standard is high. The main changes compared to the previous edition are:

- a radically new layout, grouping controls by whether they concern the organization, people, physical objects or technology
- the introduction of example control attributes, such as whether a control is preventive, corrective or corrective in nature
- an updated control set, reducing the number of controls by merging previous edition controls yet adding new ones to keep pace with changes in the cyber threat landscape
- extensively revised guidance on how the controls can be implemented
- the inclusion of definitions and mapping tables, thereby making the standard self-contained
- added clarification of the purpose and use of the standard as a reference document

BS EN ISO/IEC 27002:2022 is used by other 27000 series standards, such as BS EN ISO/IEC 27011:2020, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations* and BS EN ISO/IEC 27017:2021, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. These standards provided additional control guidance and controls in the context of a given sector. These standards are under revision. Standards that use BS EN ISO/IEC 27002 by way of providing examples will be revised in due course.

### 1.1 Reason for change

The main technical reason for the revision of the standard was to update the control reference set. When the second edition was published the idea of an internet connected world was in its infancy. Since then, many parts of the world have come to enjoy fast broadband connections, electronic banking and commerce is commonplace and with the onset of the pandemic, many people work from home. Alongside these technological and societal changes, the threat landscape has evolved. New threats demand new information security controls. Moreover, to increase cyber resilience it is necessary to reinforce the largely preventive measures traditionally associated with IT with detective and corrective measures.

Another reason for revision was the realization that the effectiveness of an ISMS will degrade over time if the reference set used by BS EN ISO/IEC 27001 is not kept up to date: the process of comparing controls determined as being necessary with those in a reference set cannot discover inadvertently omitted controls, if the omitted control is not in the reference set.

### 1.2 Summary

- a radically new layout, grouping controls by whether they concern the organization, people, physical objects or technology
- the introduction of example control attributes, such as whether a control is preventive, corrective or corrective in nature
- an updated control set, reducing the number of controls by merging previous edition controls yet adding new ones to keep pace with changes in the cyber threat landscape
- extensively revised guidance on how the controls can be implemented
- the inclusion of definitions and mapping tables, thereby making the standard self-contained
- added clarification of the purpose and use of the standard as a reference document

## 2 Main commentary

### 2.1 Scope of BS EN ISO/IEC 27002:2022

The scope of the standard is better aligned with the ISMS standard, pointing out that it is:

- a reference set of generic security controls
- designed for use within the context of an BS EN ISO/IEC 27001 ISMS
- for implementing controls based on internationally recognized best practices and
- for developing organizational information security management guidelines

### 2.2 Terms and definitions

Due to recent changes in the ISO directives, terms, definitions and abbreviated terms are now included in full in Clause 3 of the standard.

### 2.3 Structure

#### 2.3.1 Clauses

Clauses 5–8 present the controls in the order:

- Clause 5, Organizational controls
- Clause 6, People controls
- Clause 7, Physical controls
- Clause 8, Technological controls

There are two informative annexes:

- Annex A explains how an organization can use the control attribute concept and define its own attributes
- Annex B presents the correspondence between the controls in this edition and the previous edition of the standard

#### 2.3.2 Themes and attributes

The categorization of controls given by Clauses 5–8 is referred to as themes.

Each control is associated with five attributes (control types, information security properties, cybersecurity concepts, organizational capabilities and security domains). The purpose of these attributes is to allow the controls to be filtered or otherwise sorted for different audiences. The results of such filtering are referred to as 'views'. However, these attributes and their values are only examples. Organizations may disregard one or more of them and create their own.

#### 2.3.3 Control layout

Each control is presented in a common format:

- name
- attribute values
- control text
- purpose
- guidance
- other information

For some controls the guidance text is subdivided into subheadings. This is done when the text covers several topics. The control text is intended to capture the essence of the control in a form suitable for use in BS EN ISO/IEC 27001 Annex A. However, such conciseness does not always capture all the points or topics covered in the guidance text. This is not a new phenomenon and was present in the previous editions of the standard.

The purpose of Section 5.21 (Managing information security in the ICT supply chain) is identical to the purpose of Section 5.20 (Addressing information security within supplier agreements), whereas all other purposes are distinct. This duplication of purpose is deliberate. Whilst both are intended to ensure the organization's security through the proper provisions in supplier agreements, Section 5.20 considers suppliers in general, whereas Section 5.21 concentrates on ICT and its supply chains. An example of the former is the supply of non-ICT related business consultancy services. An example of the latter is cloud provisioning, where the cloud service provider relies on the software developers, telecommunication service providers and hardware providers.