SVENSK STANDARD
SS-EN ISO/IEC 27001:2023

Informationssäkerhet- Cybersäkerhet och integritetsskydd – Ledningssystem för informationssäkerhet – Krav (ISO/IEC 27001:2022,

Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022)

Svenska Institutet för Standarder

Language: engelska/English
Edition: 2

Denna standard är såld av
SEK Svensk Elstandard som även lämnar
allmänna upplysningar om svensk och utländsk standard.
Postadress: SEK, Box 1284, 164 29 Kista
Telefon: 08-444 14 00.
E-post: sek@elstandard.se Internet: www.elstandard.se

Svenska Institutet för Standarder

Den här standarden kan hjälpa dig att effektivisera och kvalitetssäkra ditt arbete. SIS har fler tjänster att erbjuda dig för att underlätta tillämpningen av standarder i din verksamhet.

SIS Abonnemang
Snabb och enkel åtkomst till gällande standard med SIS Abonnemang, en prenumerationstjänst genom vilken din organisation får tillgång till all världens standarder, senaste uppdateringarna och där hela din organisation kan ta del av innehållet i prenumerationen.

Utbildning, event och publikationer
Vi erbjuder även utbildningar, rådgivning och event kring våra mest sålda standarder och frågor kopplade till utveckling av standarder. Vi ger också ut handböcker som underlättar ditt arbete med att använda en specifik standard.

Vill du delta i ett standardiseringsprojekt?
Genom att delta som expert i någon av SIS 300 tekniska kommittéer inom CEN (europeisk standardisering) och/eller ISO (internationell standardisering) har du möjlighet att påverka standardiseringsarbetet i frågor som är viktiga för din organisation. Välkommen att kontakta SIS för att få veta mer!

Kontakt
Skriv till kundservice@sis.se, besök sis.se eller ring 08 - 555 523 10

Upplysningar om sakinnehållet i standarden lämnas av Svenska institutet för standarder, telefon 08 - 555 520 00. Standarder kan beställas hos SIS som även lämnar allmänna upplysningar om svensk och utländsk standard.

Standarden är framtagen av kommittén för LIS, SIS/TK 318/AG 11.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

Fastställd: 2023-08-14
ICS: 01.140.30; 03.100.70; 04.050; 33.040.40; 35.020; 35.030; 35.040; 35.080

Svenska Institutet för Standarder

Europastandarden EN ISO/IEC 27001:2023 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av EN ISO/IEC 27001:2023.

Denna standard ersätter SS-EN ISO/IEC 27001:2017, utgåva 1

The European Standard EN ISO/IEC 27001:2023 has the status of a Swedish Standard. This document contains the official version of EN ISO/IEC 27001:2023.

This standard supersedes the SS-EN ISO/IEC 27001:2017, edition 1

Svenska Institutet för Standarder

LÄSANVISNINGAR FÖR STANDARDER

I dessa anvisningar behandlas huvudprinciperna för hur regler och yttre begränsningar anges i standardiseringsprodukter.

Krav
Ett krav är ett uttryck i ett dokuments innehåll som anger objektivt verifierbara kriterier som ska uppfyllas och från vilka ingen avvikelse tillåts om efterlevnad av dokumentet ska kunna åberopas. Krav uttrycks med hjälpverbet **ska** (eller **ska inte** för förbud).

Rekommendation
En rekommendation är ett uttryck i ett dokuments innehåll som anger en valmöjlighet eller ett tillvägagångssätt som bedöms vara särskilt lämpligt utan att nödvändigtvis nämna eller utesluta andra. Rekommendationer uttrycks med hjälpverbet **bör** (eller **bör inte** för avrådanden).

Instruktion
Instruktioner anges i imperativ form och används för att ange hur något görs eller utförs. De kan underordnas en annan regel, såsom ett krav eller en rekommendation. De kan även användas självständigt, och är då att betrakta som krav.

Förklaring
En förklaring är ett uttryck i ett dokuments innehåll som förmedlar information. En förklaring kan uttrycka tillåtelse, möjlighet eller förmåga. Tillåtelse uttrycks med hjälpverbet **får**. Inom standardiseringen saknas rekommenderad nekande motsats till hjälpverbet får, förbud uttrycks med **ska inte** enligt reglerna för krav. Möjlighet och förmåga uttrycks med hjälpverbet **kan** (eller motsatsen **kan inte**).

READING INSTRUCTIONS FOR STANDARDS

These instructions cover the main principles for the use of provisions and external constraints in standardization deliverables.

Requirement
A requirement is an expression, in the content of a document, that conveys objectively verifiable criteria to be fulfilled, and from which no deviation is permitted if conformance with the document is to be claimed. Requirements are expressed by the auxiliary **shall** (or **shall not** for prohibition).

Recommendation
A recommendation is an expression, in the content of a document, that conveys a suggested possible choice or course of action deemed to be particularly suitable, without necessarily mentioning or excluding others. Recommendations are expressed by the auxiliary **should** (or **should not** for dissuasion).

Instruction
An instruction is expressed in the imperative mood and is used in order to convey an action to be performed. It can be subordinated to another provision, such as a requirement or a recommendation. It can also be used independently and is then to be regarded as a requirement.

Statement
A statement is an expression, in the content of a document, that conveys information. A statement can express permission, possibility or capability. Permission is expressed by the auxiliary **may**. There is no recommended opposite expression for the auxiliary may in standardization, prohibition is expressed by the use of **shall not** in accordance with the rules for requirements. Possibility and capability are expressed by the auxiliary **can** (its opposite being **cannot**).

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 27001

July 2023

ICS 03.100.70; 35.030

Supersedes EN ISO/IEC 27001:2017

English Version

Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences (ISO/IEC 27001:2022)

Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2022)

This European Standard was approved by CEN on 23 July 2023.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN ISO/IEC 27001:2023: E

Innehåll

Sida

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).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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

This third edition cancels and replaces the second edition (ISO/IEC 27001:2013), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 27001:2013/Cor 1:2014 and ISO/IEC 27001:2013/Cor 2:2015.

The main changes are as follows:

— the text has been aligned with the harmonized structure for management system standards and ISO/IEC 27002:2022.

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.

European foreword

The text of ISO/IEC 27001:2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 27001:2023 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by January 2024, and conflicting national standards shall be withdrawn at the latest by January 2024.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO/IEC 27001:2017.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27001:2022 has been approved by CEN-CENELEC as EN ISO/IEC 27001:2023 without any modification.

Introduction

0.1 General

This document has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The adoption of an information security management system is a strategic decision for an organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time.

The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

This document can be used by internal and external parties to assess the organization's ability to meet the organization's own information security requirements.

The order in which requirements are presented in this document does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.

ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3] and ISO/IEC 27005[4]), with related terms and definitions.

0.2 Compatibility with other management system standards

This document applies the high-level structure, identical sub-clause titles, identical text, common terms, and core definitions defined in Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement, and therefore maintains compatibility with other management system standards that have adopted the Annex SL.

This common approach defined in the Annex SL will be useful for those organizations that choose to operate a single management system that meets the requirements of two or more management system standards.

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

1 Scope

This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.

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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*