ISO/IEC 27001 & 27002.

ISO/IEC 27001:2022 is the requirements standard for an information security management system; ISO/IEC 27002:2022 is the guidance that explains its 93 reference controls. One is audited and certified, the other is read and applied: **certification is to 27001 alone, and 27002 cannot be certified to.**

REQUIREMENTS VS GUIDANCE | CLAUSES 4 TO 10 MANDATORY | 93 CONTROLS, 4 CLAUSES | ISO DOES NOT CERTIFY

01 THE MECHANISM

Requirements, Then Guidance

ISO/IEC 27001:2022 (edition 3, October 2022, 19 pages) specifies ISMS requirements, including assessing and treating risk. ISO/IEC 27002:2022 (February 2022) is a reference set of controls with implementation guidance. **Only 27001 holds requirements an auditor certifies against.** [02] [03]

All of Clauses 4 to 10

The clauses follow the harmonized structure of ISO management system standards. Excluding any requirement in Clauses 4 to 10 is not acceptable when claiming conformity. **Risk is the engine:** assess risks, select controls, compare them with Annex A, record the result in the SoA. [02] [10] [06]

Annex A Is a Reference Set

Annex A is normative, but it is a reference list: 93 controls in 4 clauses from 27002:2022, down from 114 in 14 clauses; 11 are new, 24 merged, 58 updated, each with a purpose and attributes. **The comparison guards against omitting a needed control, not against choosing your own.** [06] [03]

02 THE FLOW

How an ISMS Comes Together BUILD

1. **Scope and context first:** determine the organization's context and its interested parties and, new in 2022 under 4.2 c), which of their requirements the ISMS will address. A one-page Amendment 1:2024 on climate action is published at no charge. [06] [05]
2. **Assess and treat risk:** the standard requires assessing and treating risks tailored to the organization. Treatment selects the necessary controls from any source; 6.1.3 c) then compares them with the Annex A reference set so no necessary control is inadvertently omitted. [02] [06]
3. **Write the Statement of Applicability:** 6.1.3 d) requires the SoA recording the comparison; the risk treatment plan follows, and new subclause 6.3 requires ISMS changes to be carried out in a planned manner. If an omitted necessary control surfaces, update the plan and implement it. [06]

How Certification Works CERTIFY

1. **ISO does not certify anyone.** Certification is written assurance from an independent certification body; accreditation is an accreditation body's recognition that the certifier operates to international standards. Global ACI now holds the former IAF and ILAC roles. [07]
2. **Audit, then surveillance and recertification:** accredited bodies audit the ISMS against 27001, and the audit team as a whole must know every ISO/IEC 27002:2022 control. Surveillance and recertification audits then carry the certificate through its cycle. [06]
3. **Editions expire:** the 2013-to-2022 transition ran 36 months. From April 30, 2024 initial and recertification audits had to be to the 2022 edition only, and all 2013 certifications expired or were withdrawn at the end of the period, October 31, 2025. ISO lists 2013 as withdrawn. [06] [01]

03 WHAT CHANGED IN 2022

CLAUSE	THE 2022 REQUIREMENT
Clause 4	Organizational context and interested parties; 2022 adds 4.2 c), which of their requirements the ISMS addresses.
Clause 6	Risk assessment and treatment, the Annex A comparison (6.1.3 c), the SoA (6.1.3 d) and 6.3 planning for changes.
Clause 8	Where the ISMS runs; 8.1 now says externally provided processes, products or services, not outsourced processes.
Clause 9	Internal audit (9.2) and management review (9.3), reordered in 2022; documented information evidences each.
Clause 10	Improvement; its two subclauses swapped order in 2022. Continually improving the ISMS is in the standard's scope.
Annex A	Normative reference set of 93 controls in 4 clauses from ISO/IEC 27002:2022; feeds the 6.1.3 comparison and SoA.

04 THE 27000 FAMILY COMPARED

DOCUMENT	CERTIFIABLE?	WHAT IT IS
ISO/IEC 27005:2022	No	Guidance on managing information security risks to support an ISMS based on 27001; edition 4, October 2022, aligned with ISO 31000.
ISO/IEC 27002:2022	No	Reference set of generic controls with implementation guidance; best-practice recommendations that cannot be certified to.
ISO/IEC 27701:2025	Yes	Requirements and guidance for a privacy information management system for PII controllers and processors; a standalone MSS since 2025.
ISO/IEC 27001:2022	Yes	ISMS requirements; the one document here organizations are certified to, by accredited bodies and never by ISO; 2013 edition withdrawn.

ISO/IEC 27001 & 27002.

ASSESS · TREAT · CERTIFY

05 PROGRAM OPERATIONS

Scope the ISMS before buying anything. Record the context, interested parties and which of their requirements the ISMS addresses (4.2 c), then set boundaries you can defend to an auditor. ISO's framing: a system to manage risks to data the organization owns or handles, scaled to its size. [01] [06]

Let risk choose controls, then reconcile to Annex A. Select controls from the risk treatment, from 27002 or elsewhere, compare the set with the 93 Annex A controls, record the outcome in the SoA, and update the risk treatment plan whenever a necessary control proves to have been omitted. [06] [03]

Use 27002 as the implementation manual. Each 2022 control has a purpose and attributes, not a shared objective; sort controls by attribute into views your teams use, and watch for ISO/IEC 27028, guidance on control attributes, which ISO lists as under publication for November 2026. [06] [04]

Treat certification as a cycle, not an event. Choose an accredited certification body (verify it in CertSearch), budget for surveillance and recertification audits, and track edition transitions: the 2013-to-2022 switch allowed 36 months, and unconverted certificates ended October 31, 2025. [07] [06]

06 CONTROL MAPPING

ISO/IEC 27002 INTO ANNEX A

Annex A of 27001:2022 references the 27002:2022 controls by title and control text; the implementation guidance stays in 27002. Because the audit team as a whole must know all 27002:2022 controls and their implementation, the guidance shapes every certification audit even though no one is certified to it. [06] [03]

HARMONIZED STRUCTURE

Clauses 4 to 10 follow Annex SL, the harmonized structure and identical core text shared across ISO management system standards, which is why an ISMS can run as one integrated system alongside other MSS. The 2022 edition also fixed 2013 deviations from that structure, for example in 6.2 d). [10] [06]

AMENDMENT 1:2024 (CLIMATE)

ISO/IEC 27001:2022/Amd 1:2024, "Climate action changes," is a one-page amendment published February 2024 and priced at zero, part of the climate action amendments ISO issued to new and existing management system standards that month. ISO lists the 2022 standard as having one amendment. [05] [10] [01]

27005 & 27701 NEIGHBORS

ISO/IEC 27005:2022 (edition 4) gives guidance on managing information security risks to support an ISMS based on 27001 and aligns with ISO 31000. ISO/IEC 27701:2025 (edition 2, October 2025) sets requirements and guidance for a privacy information management system and now stands alone as its own MSS. [08] [09]

07 WHAT THIS DOES NOT SOLVE

Not a Control Rating
Conformity means a system to manage risks is in place. **A management-system claim, not a per-control grade.** [01]

Not Certified by ISO
ISO writes the standard, performs no certification and issues no certificates. **Accredited bodies certify.** [07]

No 27002 Certificate
27002 is best-practice guidance and cannot be certified to. **A 27002 certificate is wrong by definition.** [03]

Not Forever
Certificates need surveillance and recertification; editions expire. **2013 ones ended October 31, 2025.** [06]

08 MYTHS VS. REALITY

MYTH	REALITY
"ISO certified our company."	ISO does not perform certification or issue certificates; **an external, accredited certification body does**. [07]
"All 93 Annex A controls are mandatory."	Annex A is a reference set for the comparison and the SoA; **risk treatment determines the controls**. [06]
"We are ISO 27002 certified."	ISO/IEC 27002 gives best-practice recommendations and **cannot be certified to**; certification is to ISO/IEC 27001. [03]
"A 2013 certificate is still good enough."	The 36-month transition ended October 31, 2025, when **all 2013 certifications expired or were withdrawn**. [06]
"The 2022 edition was a full rewrite."	IAF judged the impact need not be significant: **new Annex A, new 6.3, harmonized-structure edits**. [06]

09 SPEAK THE PROGRAM — KEY TERMS

ISMS
The system 27001 specifies: **establish, implement, maintain, continually improve**.

SOA (6.1.3 D)
The Statement of Applicability, **the record of controls compared against Annex A**.

ANNEX A
Normative reference list of 93 controls drawn from ISO/IEC 27002:2022, in four clauses.

CONTROL ATTRIBUTES
Tags on each 27002:2022 control; **ISO/IEC 27028 guidance on them is under publication**.

ACCREDITATION
An accreditation body's recognition that **a certifier works to international standards**.

CERTIFICATION CYCLE
The life of a certificate: **initial audit, then surveillance and recertification audits**.