SustainCheck

Indicator analysis: ISO/IEC 27001:2022

For the SustainScore

Prepared by: Felix Janssen, CSO, SustainCheck

Indicator: ISO/IEC 27001:2022

Version of this analysis: 1.0

Date of this analysis: 30/08/2026

Contents

How to read this document

ISO/IEC 27001:2022 is an indicator for the SustainScore. An indicator is a label, certificate, standard, commitment, rating or similar instrument that says something about a company's sustainability.

The analysis sets out to determine two things:

- Which ESG subcategories of the SustainScore does ISO/IEC 27001:2022 affect? (chapter 3)
- Which score applies to each possible outcome, per subcategory affected? That follows from the requirements (chapter 3) and the assurance (chapter 4), and is set out in chapter 5.

This is an information security management system (ISMS). It touches S8 mainly on digital security and protection of data, not on all of S8 (product safety, misleading marketing). The 2013 edition is not included here: a different year = a different analysis, and the IAF transition from 2013 ended on 31 October 2025 (source 4).

1. Identity

This chapter says what ISO/IEC 27001:2022 is, what does and does not fall under that name, and which outcomes a company can have.

1.1 Official name

Official name: ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection. Information security management systems. Requirements (source 1). This file does not reproduce ISO's mark. ISO does not certify (source 2, source 3).

1.2 Short name and aliases

- Short name: ISO/IEC 27001:2022
- Also in data or texts: ISO 27001, ISO 27001:2022, ISMS, ISO/IEC 27001:2022/Amd 1:2024
- Confusion: ISO 27002 (guidance for controls), ISO 27701, SOC 2, NIS2, 'GDPR certified'

1.3 Owner / scheme owner

Role	Organisation	Country
Who writes the standard?	ISO/IEC JTC 1/SC 27	international
Who certifies?	Independent certification bodies, not ISO itself	worldwide
Who accredits?	National accreditation bodies under ISO/IEC 17021-1, often with ISO/IEC 27006 as a sector-specific requirement for ISMS certification bodies	per country

1.4 Type of instrument

Possible types:

- label
- certificate
- management system standard
- commitment
- rating
- statutory register
- membership
- charter
- award
- hybrid

Main type: management system standard. SustainCheck uses the certificate against that standard.

1.5 Version

- ISO/IEC 27001:2022, published 25 October 2022 (source 1).
- Amd 1:2024 (climate in the context) belongs to this edition but does not receive an E1 score (3.4, source 8).
- ISO/IEC 27001:2013: transition completed 31 October 2025. 2013 certificates do not fall under this indicator (source 4).

1.6 What this analysis treats as one indicator

One indicator: an active ISO/IEC 27001:2022 certificate on the certified entity. SustainCheck uses, among other sources, IAF CertSearch to see which companies hold this ISO standard (source 5).

1.7 What we do not include under this name

- ISO/IEC 27001:2013 and any other edition or year. A different year = a different ISO standard = a different analysis.
- Implementation without a certificate.
- ISO 27002, ISO 27701, ISO 42001, SOC 2, CyberFundamentals, NIS2-compliance claims without a 27001:2022 certificate.
- Non-accredited certificates.
- Suspended, withdrawn, expired, cancelled or inactive status.
- Sister or subsidiary companies without their own certificate on their certified entity name.

1.8 Possible outcomes for a company

Boolean: present or not.

Outcome	What it is	Score in chapter 5
Active ISO/IEC 27001:2022 certificate	Status Active, standard ISO/IEC 27001:2022, on the certified entity	Yes: S8, G3, G4
Not present	No active 2022 certificate (including leftover 2013, another status, implementation only)	None

2. Scope

2.1 What is assessed

- Object: the ISMS, limited to the scope on the certificate. That scope is often a process or a service ('IT services of entity X', 'customer data in platform Y'), not automatically the whole group (source 1, source 5).
- Own operations plus suppliers insofar as they fall in the ISMS and Annex A.
- Score always on the certified entity name, never on a loose site.

Site versus the whole entity: what we can and cannot see

The scope is free text. There is no closed field for 'whole entity / one service / one site', and the company's share (revenue, data, sites) is not attached (source 5). SustainCheck therefore cannot systematically see whether the ISMS covers the whole legal entity or only an IT island.

One rule, as with Fairtrade: every active 2022 certificate on the certified entity gets the same score. That score already accounts for unknown coverage. We do not read the free text as a second step.

2.2 What the standard does and does not cover

Covered:

- ISMS: risks to confidentiality, integrity, availability; Annex A controls (93 in 2022) (source 1, source 9).
- Protection of information, including personal data if those sit in scope. That is not a GDPR certificate.
- Supplier security via Annex A, where applicable.

Not covered:

- Product safety, misleading marketing, labour rights, environment.
- ISO/IEC 27001:2013.
- Proof that all data or all subsidiaries fall under the ISMS.

2.3 Validity and version transitions

- Three-year cycle with surveillance, ISO/IEC 17021-1 (source 6).
- IAF MD 26: transition from 2013 to 2022 completed 31 October 2025. 2013 certificates are expired or withdrawn after that (source 4).
- Amd 1:2024: climate in the context of the ISMS; not a new edition (source 8).

3. Requirements

3.1 Material requirements

- Clauses 4 to 10: set up, maintain and improve an ISMS.
- Annex A: 93 controls, including threat intelligence, cloud, ICT readiness, suppliers (source 9).
- The organisation states applicability (Statement of Applicability). No 'hack-proof' guarantee.

3.2 Mapping to SustainScore subcategories

Scale: strong / moderate / weak.

Requirement	Subcategory	Coupling	Evidence in the standard	Source
ISMS and controls on information and (if in scope) personal data	S8	moderate	Strong on digital/cyber, not on all of S8 (product, marketing)	1, 9
Leadership, internal audit, nonconformities, improvement	G3	moderate	Control of the ISMS	1
Supplier relationships / ICT supply chain in Annex A	G4	weak	Chain security, not broad value-chain management	9

3.3 Primary versus secondary

Primary: S8. Secondary: G3. Weak: G4.

3.4 Limits of coverage

- S8 in the SustainScore is broader than information security. That is why there is no score of 100.
- Privacy is in it if data is in scope, not as ISO 27701 or a GDPR attestation.
- Amd 1:2024 requires determining whether climate is relevant for the ISMS. No E1 score: too little concrete information, impact of the amendment too small (source 8).
- Unknown scope coverage (often an IT service, not the whole entity) is built into the scores.

4. Assurance

4.1 Assurance level

Possible levels:

- 1. Self-declared: the company claims it itself, with no independent check.
- 2. Second party: a check by a customer, a trade body or another interested party.
- 3. Third-party audit: an independent auditor, without accreditation against an international standard.
- 4. Accredited third party: independent certification under accreditation. Typically ISO/IEC 17021-1 for management systems.

Level for this indicator: 4, for an active accredited certificate (17021-1, supplemented where applicable with 27006).

4.2 Audit practice

- Initial certification, annual surveillance, recertification every three years (source 6).

4.3 Accreditation

ISO/IEC 17021-1; for an ISMS often ISO/IEC 27006 as an extra requirement on the certification body (source 6, source 10).

4.4 Verifiability

SustainCheck uses, among other sources, IAF CertSearch to see which companies hold this ISO standard (source 5). Relevant fields: certified entity name, standard name (ISO/IEC 27001:2022 or equivalent), status Active.

4.5 Overclaim risks

- Presenting 27001 as coverage of all of S8 or of the whole group.
- Reading a 2013 certificate as 2022.
- Equating SOC 2 or NIS2 with 27001:2022.
- Amd 1:2024 as a climate certificate.
- Reading a scope of 'IT services' as all of the company's activities.

5. Conclusion: impact on the SustainScore

Boolean. S8 solid but not 100. G3 moderate. G4 thin. Unknown scope coverage included.

5.1 Score per outcome and subcategory

Outcome	Subcategory	Score	Note
Active ISO/IEC 27001:2022 certificate	S8	87	Core on information security; S8 is broader; unknown scope coverage
Active ISO/IEC 27001:2022 certificate	G3	58	ISMS governance and audit
Active ISO/IEC 27001:2022 certificate	G4	47	Annex A supplier security, thin chain link
Not present	all	none	Including 2013, another status, implementation only

5.2 What this indicator does not do

- No score on E1 to E6, S1 to S7, G1, G2.
- No E1 via Amd 1:2024.
- No score for ISO/IEC 27001:2013 or another year.
- No score on sites as separate companies.
- No proof that all data, services or group companies fall under the ISMS.

6. Sources

Every statement in this document that is later used in the SustainScore points to a source below.

6.1 Sources used

Numbering:

1. ISO/IEC. ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection. Information security management systems. Requirements. https://www.iso.org/standard/27001 Accessed: 30/08/2026.

2. ISO. Management system standards. https://www.iso.org/management-system-standards.html Accessed: 30/08/2026.

3. ISO. Certification. https://www.iso.org/certification.html Accessed: 30/08/2026.

4. IAF. IAF MD 26, Transition requirements for ISO/IEC 27001:2022 (client transition completed 31 October 2025). https://iaf.nu/iaf_system/uploads/documents/IAF_MD26_Issue_2_15012023.pdf Accessed: 30/08/2026.

5. IAF. IAF CertSearch. https://www.iafcertsearch.org/ Accessed: 30/08/2026.

6. ISO. ISO/IEC 17021-1. https://www.iso.org/standard/61651.html Accessed: 30/08/2026.

7. ISO. ISO/IEC 27002:2022 (controls guidance, not a certificate). https://www.iso.org/standard/75652.html Accessed: 30/08/2026.

8. ISO/IEC. ISO/IEC 27001:2022/Amd 1:2024, Climate action changes. https://www.iso.org/standard/88435.html Accessed: 30/08/2026.

9. ISO/IEC. ISO/IEC 27001:2022 Annex A (93 controls; via the standard, source 1). Accessed: 30/08/2026.

10. ISO/IEC. ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems. https://www.iso.org/standard/82875.html Accessed: 30/08/2026.

6.2 Looked for but not found

- A standardised field for 'whole entity versus IT scope'.
- The share of data, revenue or services under a given ISMS scope.
- A public Statement of Applicability per listing.