cycore

FREE DOWNLOAD

2026 EDITION

ISO 27001

ISO 27001 Gap Assessment

Cycore's 115-prompt ISO 27001 self-assessment. Score each prompt 0 to 3, record the evidence and the owner, and find your gaps before you talk to an auditor.

PREPARED BY

Cycore

ONLINE

cycoresecure.com

Cycore built this gap assessment for teams preparing for an ISO 27001 audit, or tightening an information security management system (ISMS) they already run. It's a self-assessment based on ISO/IEC 27001:2022, the same foundation we use with clients. Work through the 115 prompts with the people who own each area, score each one from 0 to 3, and write down the evidence and the owner. You'll end with a score out of 345 and a list of gaps with a name next to each one, ready for your first conversation with an auditor or certification body.

How to use this assessment

ISO/IEC 27001:2022 has two parts that matter here. Clauses 4 through 10 hold the requirements, all of them apply, and none can be excluded (ISO/IEC JTC 1/SC 27 Journal, volume 3, issue 4). Annex A is a reference set of 93 controls. You determine the controls you need through risk treatment, then compare them with Annex A to check that nothing necessary has been left out (ISO/IEC JTC 1/SC 27 Auditing Practices Note on Annex A).

This assessment scores the requirements only. The 115 prompts below cover clauses 4 through 10, and the Annex A section at the end is an unscored overview.

Score every prompt with one of four values:

- **0, not addressed.** No control exists, no plan is in place, or nobody has looked at this area yet.
- **1, planned.** The work hasn't started, and there's a concrete plan with an owner and a date. Vague intentions don't count.
- **2, partly implemented.** Something exists and it's incomplete: documentation is missing, execution is inconsistent, or there's no evidence it works.
- **3, fully implemented.** Documented, implemented, working, backed by evidence, and reviewed at least once.

Add up each clause, then total your score. Each prompt is worth up to 3 points, so the 115 prompts make a maximum of 345. The score is a Cycore planning

signal. It shows you where to focus first and who owns what. It isn't an ISO certification status, and it doesn't predict how long the work will take or how an audit will go.

Next to each prompt there's space for the evidence behind your score and the person who owns the gap. Write both. When an auditor asks what supports a 3, the evidence column is the answer, and the owner column is who closes anything under 3.

If you run a GRC platform, it'll list many of these as tasks and pull in evidence for them. Use this assessment to decide, with the owner in the room, whether each requirement is actually met and what supports the score. Carry the owners and dates back into the platform when you're done.

The numbers next to each prompt, such as 4.1.1, are Cycore assessment IDs. They group the prompts inside each clause so you can refer to one when you hand it off. They aren't ISO subclause numbers.

Score honestly. Auditors test controls, and if you mark something fully implemented you'll need to show the evidence on the spot.

Clause 4: Context of the organization

Everything else in the ISMS rests on this clause. If the scope is wrong or an interested party is missing, the risk assessment and the controls built on them are off too. Since February 2024 (Amendment 1), clause 4 also requires you to decide whether climate change is a relevant issue for the ISMS (IAF/ISO Joint Communiqué, February 2024).

Your organization and its context

0 1 2 3 **Internal issues relevant to information security have been identified.** Business objectives, organizational structure, capabilities, and culture, written into a context document or the opening section of your ISMS manual. Assessment ID 4.1.1

Evidence: _____

Owner: _____

---

0 1 2 3 **External issues relevant to information security have been identified.** The regulatory environment, market conditions, current threats, and technology trends that affect you. Assessment ID 4.1.2

Evidence: _____

Owner: _____

---

0 1 2 3 **Issues are documented and reviewed at defined intervals.** A dated document, a review cadence, and a record of the last review. Assessment ID 4.1.3

Evidence: _____

Owner: _____

---

0 1 2 3 **The relationship between business strategy and information security strategy is documented.** A short statement of how security supports what the business is trying to do. Assessment ID 4.1.4

Evidence: _____

Owner: _____

Interested parties and what they need

0 1 2 3 **Interested parties relevant to the ISMS have been identified.** Customers, regulators, employees, investors, and partners, in one list. Assessment ID 4.2.1

Evidence: _____

Owner: _____

---

0 1 2 3 **Requirements of each interested party have been determined.** Contractual, legal, regulatory, and security expectations, recorded next to each party. Assessment ID 4.2.2

Evidence: _____

Owner: _____

0 1 2 3 **Requirements are documented and reviewed periodically.** The list has an owner and a review date. Assessment ID 4.2.3

Evidence: _____

Owner: _____

0 1 2 3 **Customer security requirements are tracked and addressed.** Questionnaires and contractual clauses logged with a status, so nothing is answered once and forgotten. Assessment ID 4.2.4

Evidence: _____

Owner: _____

The scope of your ISMS

0 1 2 3 **The ISMS scope is clearly defined and documented.** A written scope statement, approved and dated. Assessment ID 4.3.1

Evidence: _____

Owner: _____

0 1 2 3 **The scope considers internal and external issues and the requirements of interested parties.** The scope statement refers back to the issues and parties you identified above. Assessment ID 4.3.2

Evidence: _____

Owner: _____

0 1 2 3 **Scope boundaries are defined.** Locations, assets, technologies, and organizational units, with what's in and what's out. Assessment ID 4.3.3

Evidence: _____

Owner: _____

0 1 2 3 **Interfaces and dependencies with activities performed by other organizations are identified.** Cloud providers, outsourced development, payroll, support, and anything else that touches in-scope information. Assessment ID 4.3.4

Evidence: _____

Owner: _____

---

0 1 2 3 **Justification for any exclusions from scope is documented and defensible.** Each exclusion has a written reason you could explain to an auditor without hesitating. Assessment ID 4.3.5

Evidence: _____

Owner: _____

The management system itself

0 1 2 3 **An ISMS has been established that includes the required processes and their interactions.** A process map or manual that shows how the pieces fit together. Assessment ID 4.4.1

Evidence: _____

Owner: _____

---

0 1 2 3 **The ISMS is implemented and maintained.** Records show the processes running over time. Assessment ID 4.4.2

Evidence: _____

Owner: _____

---

0 1 2 3 **The ISMS is continually improved in accordance with the standard.** A log of improvements, with dates. Assessment ID 4.4.3

Evidence: _____

Owner: _____

Your subtotal: ___ of 48

Clause 5: Leadership

Auditors look for leadership involvement they can see: decisions, resources, and attendance at management reviews. A signature on the policy on its own won't carry this clause.

Leadership and commitment

0 1 2 3 **Top management demonstrates active commitment to the ISMS.** Budget decisions, attendance at management reviews, and direction given in writing. Assessment ID 5.1.1

Evidence: _____

Owner: _____

0 1 2 3 **The information security policy and objectives are aligned with strategic direction.** You can point to the business goal each objective supports. Assessment ID 5.1.2

Evidence: _____

Owner: _____

0 1 2 3 **ISMS requirements are integrated into business processes.** Security steps sit inside onboarding, procurement, development, and change management, where the work happens. Assessment ID 5.1.3

Evidence: _____

Owner: _____

0 1 2 3 **Resources needed for the ISMS are available and allocated.** People, budget, and tools, with names and numbers. Assessment ID 5.1.4

Evidence: _____

Owner: _____

0 1 2 3 **Top management communicates the importance of effective information security.** All-hands notes, internal announcements, or recorded messages that show it. Assessment ID 5.1.5

Evidence: _____

Owner: _____

0 1 2 3 **Top management makes sure the ISMS achieves its intended outcomes.** Leadership sees the results and acts on them, and the management review minutes show it. Assessment ID 5.1.6

Evidence: _____

Owner: _____

0 1 2 3 **Top management directs and supports the people contributing to ISMS effectiveness.** Clear direction to the people doing the work, and backing when they need it. Assessment ID 5.1.7

Evidence: _____

Owner: _____

The information security policy

0 1 2 3 **An information security policy exists and is appropriate to the organization's purpose.** Written for this company, at a length people will read. Assessment ID 5.2.1

Evidence: _____

Owner: _____

0 1 2 3 **The policy includes information security objectives or a framework for setting them.** Either the objectives themselves or how they get set. Assessment ID 5.2.2

Evidence: _____

Owner: _____

0 1 2 3 **The policy includes a commitment to satisfy applicable requirements.** Legal, regulatory, and contractual. Assessment ID 5.2.3

Evidence: _____

Owner: _____

0 1 2 3 **The policy includes a commitment to continual improvement of the ISMS.** A stated commitment, in the policy text. Assessment ID 5.2.4

Evidence: _____

Owner: _____

0 1 2 3 **The policy is available as documented information.** A controlled document with a version and an approval date. Assessment ID 5.2.5

Evidence: _____

Owner: _____

0 1 2 3 **The policy is communicated within the organization.** People can find it, and you can show it was shared. Assessment ID 5.2.6

Evidence: _____

Owner: _____

0 1 2 3 **The policy is available to interested parties as appropriate.** Customers or partners can get it when they ask. Assessment ID 5.2.7

Evidence: _____

Owner: _____

Roles, responsibilities, and authorities

0 1 2 3 **Roles and responsibilities for information security are assigned and communicated.** Named people, and they know. Assessment ID 5.3.1

Evidence: _____

Owner: _____

0 1 2 3 **Responsibility for keeping the ISMS in conformance with the standard is assigned.** One named owner for conformance.

Assessment ID 5.3.2

Evidence: _____

Owner: _____

0 1 2 3 **Responsibility for reporting on ISMS performance to top management is assigned.** Who reports, how often, and in what form. Assessment ID 5.3.3

Evidence: _____

Owner: _____

0 1 2 3 **A RACI or equivalent matrix exists for key ISMS activities.** Risk assessment, internal audit, management review, incident response, and access reviews, each with a responsible and an accountable name. Assessment ID 5.3.4

Evidence: _____

Owner: _____

Your subtotal: ___ of 54

Clause 6: Planning

Risk assessment drives the rest of the standard. Every control, policy, and procedure should trace back to a risk you identified, so a shallow risk assessment shows up everywhere else.

Risks and opportunities

0 1 2 3 **Risks and opportunities that need to be addressed have been determined.** Starting from the issues and interested parties in clause 4. Assessment ID 6.1.1

Evidence: _____

Owner: _____

0 1 2 3 **A documented risk assessment methodology exists.** Criteria for likelihood, impact, and risk acceptance, written down before the assessment starts. Assessment ID 6.1.2

Evidence: _____

Owner: _____

0 1 2 3 **The risk assessment methodology produces consistent, valid, and comparable results.** Two people assessing the same risk would land close to each other. Assessment ID 6.1.3

Evidence: _____

Owner: _____

0 1 2 3 **Information security risks have been identified.** Threats to confidentiality, integrity, and availability, in a risk register.

Assessment ID 6.1.4

Evidence: _____

Owner: _____

---

0 1 2 3 **Risk owners have been assigned for each identified risk.** A name on every row of the register. Assessment ID 6.1.5

Evidence: _____

Owner: _____

---

0 1 2 3 **Risks have been analyzed.** Likelihood and impact assessed against your criteria. Assessment ID 6.1.6

Evidence: _____

Owner: _____

---

0 1 2 3 **Risks have been evaluated.** Prioritized against your risk criteria, so you know which ones need treatment. Assessment ID 6.1.7

Evidence: _____

Owner: _____

---

0 1 2 3 **A risk treatment plan exists with a selected treatment option for each risk.** Each risk has a chosen treatment and the controls that go with it.

Assessment ID 6.1.8

Evidence: _____

Owner: _____

---

0 1 2 3 **Controls from Annex A have been compared against the selected treatment options.** The comparison confirms no necessary control was overlooked, and it's recorded. Assessment ID 6.1.9

Evidence: _____

Owner: _____

---

0 1 2 3 **A Statement of Applicability has been produced.** Every Annex A control, whether it applies, why, and its implementation status.

Assessment ID 6.1.10

Evidence: _____

Owner: _____

0 1 2 3 **Risk owners have approved the risk treatment plan and accepted the residual risks.** Sign-off recorded, with dates. Assessment ID 6.1.11

Evidence: _____

Owner: _____

Information security objectives

0 1 2 3 **Information security objectives are established at relevant functions and levels.** Company-level objectives, plus team-level ones where a team carries specific risk. Assessment ID 6.2.1

Evidence: _____

Owner: _____

0 1 2 3 **Objectives are consistent with the information security policy.** You can trace each objective to a commitment in the policy. Assessment ID 6.2.2

Evidence: _____

Owner: _____

0 1 2 3 **Objectives are measurable, or at minimum evaluable.** A number, or a clear yes-or-no test. Assessment ID 6.2.3

Evidence: _____

Owner: _____

0 1 2 3 **Objectives consider applicable requirements and risk assessment results.** The objectives respond to the risks and requirements you found. Assessment ID 6.2.4

Evidence: _____

Owner: _____

0 1 2 3 **Objectives are communicated and updated as needed.** The people who have to hit them know about them, and they change when the risks change. Assessment ID 6.2.5

Evidence: _____

Owner: _____

---

0 1 2 3 **Plans to achieve objectives cover what will be done, the resources, the responsibility, the timeline, and the evaluation method.** One plan per objective, with all five in it. Assessment ID 6.2.6

Evidence: _____

Owner: _____

Planning changes to the ISMS

0 1 2 3 **Changes to the ISMS are carried out in a planned manner.** A change record, with what changed and why. Assessment ID 6.3.1

Evidence: _____

Owner: _____

---

0 1 2 3 **The purpose of changes and their potential consequences are considered.** Written down before the change, including what could go wrong. Assessment ID 6.3.2

Evidence: _____

Owner: _____

---

0 1 2 3 **The impact on ISMS integrity is evaluated before changes are implemented.** Someone checks that the change doesn't break scope, roles, or existing controls. Assessment ID 6.3.3

Evidence: _____

Owner: _____

Your subtotal: ___ of 60

Clause 7: Support

Most of this clause is records: who's competent, who's been trained, and which document is current.

Resources

0 1 2 3 **Resources needed for the ISMS are determined and provided.** People, tools, and time, listed and funded. Assessment ID 7.1.1

Evidence: _____

Owner: _____

---

0 1 2 3 **Budget is allocated for information security activities.** A line in the budget, with an amount. Assessment ID 7.1.2

Evidence: _____

Owner: _____

---

0 1 2 3 **Staffing levels are adequate for ISMS maintenance and operation.** Named people with the hours to do it. Assessment ID 7.1.3

Evidence: _____

Owner: _____

Competence

0 1 2 3 **Competence requirements for people affecting information security performance are determined.** What each security-relevant role needs to know and be able to do. Assessment ID 7.2.1

Evidence: _____

Owner: _____

---

0 1 2 3 **People are competent based on education, training, or experience.** Matched against the requirements above. Assessment ID 7.2.2

Evidence: _____

Owner: _____

---

0 1 2 3 **Where gaps exist, actions are taken to acquire competence.** Training, hiring, or outsourcing, with the action recorded. Assessment ID 7.2.3

Evidence: _____

Owner: _____

0 1 2 3 **Evidence of competence is retained.** Certificates, training records, or CVs on file. Assessment ID 7.2.4

Evidence: _____

Owner: _____

Awareness

0 1 2 3 **People are aware of the information security policy.** They've read it, and there's a record. Assessment ID 7.3.1

Evidence: _____

Owner: _____

0 1 2 3 **People are aware of their contribution to ISMS effectiveness.** They can say what their role does for security. Assessment ID 7.3.2

Evidence: _____

Owner: _____

0 1 2 3 **People are aware of the implications of not conforming to ISMS requirements.** They know what happens when the rules are broken. Assessment ID 7.3.3

Evidence: _____

Owner: _____

0 1 2 3 **Security awareness training is conducted regularly and tracked.** Completion records, by person and date. Assessment ID 7.3.4

Evidence: _____

Owner: _____

Communication

0 1 2 3 **Internal and external communication needs are determined.** What gets communicated, when, with whom, by whom, and how.

Assessment ID 7.4.1

Evidence: _____

Owner: _____

---

0 1 2 3 **A communication plan or matrix exists for security-related communications.** Incidents, policy changes, and customer notifications at a minimum. Assessment ID 7.4.2

Evidence: _____

Owner: _____

Documented information

0 1 2 3 **All documented information required by the standard is maintained.** The documents and records the standard calls for, current and controlled. Assessment ID 7.5.1

Evidence: _____

Owner: _____

---

0 1 2 3 **Documented information needed for ISMS effectiveness is maintained.** The procedures and records your own ISMS depends on, which the standard leaves to you. Assessment ID 7.5.2

Evidence: _____

Owner: _____

---

0 1 2 3 **Document control exists for identification, format, review, and approval.** Each document has an ID, an owner, a version, and an approver. Assessment ID 7.5.3

Evidence: _____

Owner: _____

---

0 1 2 3 **Documents are available and suitable for use where and when needed.** People can find the current version when they need it.

Assessment ID 7.5.4

Evidence: _____

Owner: _____

0 1 2 3 **Documents are adequately protected.** Access control, integrity, storage, retention, and disposal. Assessment ID 7.5.5

Evidence: _____

Owner: _____

0 1 2 3 **Version control and change history are maintained.** You can see what changed, when, and who approved it. Assessment ID 7.5.6

Evidence: _____

Owner: _____

Your subtotal: ___ of 57

Clause 8: Operation

This clause is where the plans from clause 6 get carried out. Auditors want records that the risk assessment and treatment happened on schedule.

Operational planning and control

0 1 2 3 **Processes needed to meet ISMS requirements are planned, implemented, and controlled.** The processes run as designed, and records show it. Assessment ID 8.1.1

Evidence: _____

Owner: _____

0 1 2 3 **Criteria for security processes have been established.** A written standard for each process, so people know what acceptable looks like. Assessment ID 8.1.2

Evidence: _____

Owner: _____

0 1 2 3 **Processes are controlled in accordance with the criteria.** Records show the criteria being applied. Assessment ID 8.1.3

Evidence: _____

Owner: _____

0 1 2 3 **Outsourced processes that affect the ISMS are identified and controlled.** A list of outsourced processes, with the controls you apply to each. Assessment ID 8.1.4

Evidence: _____

Owner: _____

0 1 2 3 **Changes are controlled, and unintended consequences are reviewed and mitigated.** Change records include a review of what the change caused. Assessment ID 8.1.5

Evidence: _____

Owner: _____

Risk assessment in operation

0 1 2 3 **Risk assessments are performed at planned intervals or when significant changes occur.** A schedule, and a list of the changes that trigger a reassessment. Assessment ID 8.2.1

Evidence: _____

Owner: _____

0 1 2 3 **Risk assessment results are documented and retained.** Dated results, kept. Assessment ID 8.2.2

Evidence: _____

Owner: _____

0 1 2 3 **Risk assessment results are consistent with your documented methodology.** The same criteria, applied the same way each time. Assessment ID 8.2.3

Evidence: _____

Owner: _____

Risk treatment in operation

0 1 2 3 **The risk treatment plan is implemented.** Controls in place, and the plan updated as items complete. Assessment ID 8.3.1

Evidence: _____

Owner: _____

0 1 2 3 **Results of risk treatment are documented and retained.** Evidence of each treatment, kept with the plan. Assessment ID 8.3.2

Evidence: _____

Owner: _____

Your subtotal: ___ of 30

Clause 9: Performance evaluation

This is the largest clause in the assessment, 23 prompts, and nearly every one of them asks for a record: measurement results, audit reports, and management review minutes.

Monitoring, measurement, analysis, and evaluation

0 1 2 3 **What needs to be monitored and measured is determined.** A list of what you measure, tied to your objectives and controls. Assessment ID 9.1.1

Evidence: _____

Owner: _____

0 1 2 3 **Methods for monitoring, measurement, analysis, and evaluation are defined.** How each measurement is taken, so the results are repeatable. Assessment ID 9.1.2

Evidence: _____

Owner: _____

0 1 2 3 **When monitoring and measuring are performed is defined.** A frequency for each measurement. Assessment ID 9.1.3

Evidence: _____

Owner: _____

0 1 2 3 **Who monitors and measures is defined.** A name for each measurement. Assessment ID 9.1.4

Evidence: _____

Owner: _____

0 1 2 3 **When results are analyzed and evaluated is defined.** A cadence for looking at the numbers. Assessment ID 9.1.5

Evidence: _____

Owner: _____

0 1 2 3 **Who analyzes and evaluates the results is defined.** Who reads the numbers and decides what they mean. Assessment ID 9.1.6

Evidence: _____

Owner: _____

0 1 2 3 **Evidence of monitoring and measurement results is retained.** Dashboards, reports, or a log you can show for each measurement. Assessment ID 9.1.7

Evidence: _____

Owner: _____

Internal audit

0 1 2 3 **Internal audits are conducted at planned intervals.** A schedule, and audits that happened on it. Assessment ID 9.2.1

Evidence: _____

Owner: _____

0 1 2 3 **Audits assess conformity to your own ISMS requirements and to ISO 27001.** Both, written into the audit criteria. Assessment ID 9.2.2

Evidence: _____

Owner: _____

0 1 2 3 **An audit programme is planned considering the importance of processes and the results of previous audits.** The programme explains what gets audited when, and why. Assessment ID 9.2.3

Evidence: _____

Owner: _____

0 1 2 3 **Audit criteria, scope, frequency, and methods are defined.** In the programme or in each audit plan. Assessment ID 9.2.4

Evidence: _____

Owner: _____

0 1 2 3 **Auditor objectivity and impartiality are maintained.** Auditors don't audit their own work. Assessment ID 9.2.5

Evidence: _____

Owner: _____

0 1 2 3 **Audit results are reported to relevant management.** A report, and a record of who received it. Assessment ID 9.2.6

Evidence: _____

Owner: _____

0 1 2 3 **Evidence of the audit programme and results is retained.** The programme, each audit plan, the reports, and the findings, filed together. Assessment ID 9.2.7

Evidence: _____

Owner: _____

Management review

0 1 2 3 **Top management reviews the ISMS at planned intervals.** Minutes, with attendees and dates. Assessment ID 9.3.1

Evidence: _____

Owner: _____

0 1 2 3 **The review considers the status of actions from previous reviews.** An action log carried from one review to the next. Assessment ID 9.3.2

Evidence: _____

Owner: _____

0 1 2 3 **The review considers changes in external and internal issues relevant to the ISMS.** An agenda item, with notes against it.

Assessment ID 9.3.3

Evidence: _____

Owner: _____

0 1 2 3 **The review considers information security performance feedback.** Nonconformities, monitoring results, audit results, and progress on objectives. Assessment ID 9.3.4

Evidence: _____

Owner: _____

0 1 2 3 **The review considers feedback from interested parties.** Customer questionnaires, regulator contact, and employee reports, summarized. Assessment ID 9.3.5

Evidence: _____

Owner: _____

0 1 2 3 **The review considers the results of risk assessment and the status of the risk treatment plan.** Both on the agenda, with current numbers.

Assessment ID 9.3.6

Evidence: _____

Owner: _____

0 1 2 3 **The review considers opportunities for continual improvement.** Recorded each time, including when nothing is proposed.

Assessment ID 9.3.7

Evidence: _____

Owner: _____

0 1 2 3 **Review outputs include decisions related to improvement and resource needs.** The minutes record the decisions, with owners.

Assessment ID 9.3.8

Evidence: _____

Owner: _____

0 1 2 3 **Evidence of management review results is retained.** Minutes and decisions from every review, filed where the next review can find them. Assessment ID 9.3.9

Evidence: _____

Owner: _____

Your subtotal: ___ of 69

Clause 10: Improvement

Nonconformities will happen. Auditors check whether you catch them, fix the cause, and keep the record.

Nonconformity and corrective action

0 1 2 3 **When a nonconformity occurs, the organization reacts to control and correct it.** A record of what happened and what was done right away.

Assessment ID 10.1.1

Evidence: _____

Owner: _____

0 1 2 3 **The organization evaluates the need for action to eliminate root causes.** A root-cause note on each nonconformity, even a short one.

Assessment ID 10.1.2

Evidence: _____

Owner: _____

0 1 2 3 **Corrective actions are appropriate to the effects of the nonconformities.** The fix matches the size of the problem.

Assessment ID 10.1.3

Evidence: _____

Owner: _____

---

0 1 2 3 **The organization reviews the effectiveness of corrective actions taken.** A dated follow-up check that says whether the fix worked.

Assessment ID 10.1.4

Evidence: _____

Owner: _____

---

0 1 2 3 **Changes to the ISMS are made if necessary based on corrective actions.** When a fix changes a process, the ISMS documents change with it. Assessment ID 10.1.5

Evidence: _____

Owner: _____

---

0 1 2 3 **Evidence of nonconformities, actions taken, and results is retained.** A nonconformity log with all three. Assessment ID 10.1.6

Evidence: _____

Owner: _____

Continual improvement

0 1 2 3 **The organization continually improves the suitability, adequacy, and effectiveness of the ISMS.** Improvements you can point to, with dates. Assessment ID 10.2.1

Evidence: _____

Owner: _____

---

0 1 2 3 **Improvement actions are tracked, assigned, and followed through.** An improvement log with owners and closure dates. Assessment ID 10.2.2

Evidence: _____

Owner: _____

---

0 1 2 3 **Lessons learned from incidents, audits, and reviews feed back into the ISMS.** You can show a change that came from a lesson.

Assessment ID 10.2.3

Evidence: _____

Owner: _____

Your subtotal: ___ of 27

Your score

CLAUSE	ITEMS	MAXIMUM	YOUR SUBTOTAL
4. Context of the organization	16	48	
5. Leadership	18	54	
6. Planning	20	60	
7. Support	19	57	
8. Operation	10	30	
9. Performance evaluation	23	69	
10. Improvement	9	27	
Total	115	345	

Whatever your total, start with the prompts you scored 0 or 1 that sit on your highest risks. Scope and risk assessment feed everything else, so gaps in clauses 4 and 6 come first. Give each prompt under 3 an owner and a date, and bring the list to your first conversation with an auditor.

Unscored Annex A overview

ISO/IEC 27001:2022 Annex A is a reference set of 93 controls in four themes: organizational (37), people (8), physical (14), and technological (34). You determine the controls you need through risk treatment, then compare those

controls with Annex A to check that nothing necessary has been omitted (ISO/IEC JTC 1/SC 27 Auditing Practices Note on Annex A). Being listed in Annex A doesn't by itself make a control necessary for you.

The 38 controls below are a sample of the 93, for orientation: 10 organizational, all 8 people controls, 8 physical, and 12 technological. There's no score column, and none of them count toward your 345. The third column is what Cycore commonly finds when we assess technology companies. Use the table to check your own control set against familiar trouble spots, and use the full Annex A for the comparison itself.

CONTROL	TITLE	COMMON GAP
A.5.1	Policies for information security	Policies haven't been reviewed in over a year, or employees can't find them.
A.5.2	Information security roles and responsibilities	Responsibilities are assumed and never written down or communicated. No RACI matrix.
A.5.3	Segregation of duties	Developers have production database access. One person can approve and deploy a code change.
A.5.8	Information security in project management	Security reviews happen after launch, if they happen at all, and never during planning or development.
A.5.10	Acceptable use of information and other associated assets	Employees never acknowledged the policy, and nothing enforces or monitors it.
A.5.15	Access control	Access is broader than the job needs, and nobody reviews it on a schedule.
A.5.23	Information security for use of cloud services	No cloud security policy, no inventory of cloud services, and the shared responsibility model isn't understood.
A.5.24	Information security incident management planning and preparation	The incident response plan has never been tested. No severity levels or escalation paths.
A.5.29	Information security during disruption	Business continuity plans don't address information security, and DR testing isn't performed.
A.5.34	Privacy and protection of PII	Privacy is treated as a legal function only, and technical controls for PII aren't mapped to privacy obligations.

CONTROL	TITLE	COMMON GAP
A.6.1	Screening	Screening covers full-time employees only. Contractors and remote international hires are skipped.
A.6.2	Terms and conditions of employment	Security clauses are generic or missing from contractor agreements. NDA and IP clauses aren't security-specific.
A.6.3	Information security awareness, education and training	Training is a one-time onboarding event. No role-based training and no measurement of whether it worked.
A.6.4	Disciplinary process	The process sits in HR policy with no link to the information security policy and no examples of violations.
A.6.5	Responsibilities after termination or change of employment	The offboarding checklist skips security items: key return, access revocation confirmation, NDA reminders.
A.6.6	Confidentiality or non-disclosure agreements	NDAs are signed at hire and never reviewed, so they don't cover current data types or processing activities.
A.6.7	Remote working	No remote work security policy. No requirements for home network security, screen locks, or secure Wi-Fi.
A.6.8	Information security event reporting	A reporting channel exists and employees don't know about it. No protection against retaliation for reporting.
A.7.1	Physical security perimeters	Fully remote companies haven't documented their approach to physical security or justified reduced physical controls.
A.7.2	Physical entry	No visitor logs, tailgating goes unchallenged, and badge access isn't reviewed.
A.7.4	Physical security monitoring	Cloud-first companies assume physical security is entirely the cloud provider's job without verifying it.
A.7.7	Clear desk and clear screen	The policy exists with no enforcement, no spot checks, and no coverage of remote workers.
A.7.8	Equipment siting and protection	Laptops and phones used in public spaces without privacy screens. No asset tracking.
A.7.9	Security of assets off-premises	No policy for devices taken off-site, and no encryption requirement for portable storage.
A.7.10	Storage media	Hard drives and USB media are disposed of without a documented wiping or destruction procedure.

CONTROL	TITLE	COMMON GAP
A.7.14	Secure disposal or re-use of equipment	Old laptops are reassigned without verified data wiping. No disposal certificates for decommissioned hardware.
A.8.1	User endpoint devices	No endpoint detection and response. BYOD devices are unmanaged, and there's no mobile device management.
A.8.2	Privileged access rights	Admin accounts are shared, privileged access isn't time-limited, and there are no separate admin accounts.
A.8.3	Information access restriction	Role-based access control is applied inconsistently. API keys have overly broad permissions.
A.8.5	Secure authentication	MFA isn't enforced everywhere. Service accounts use static credentials. No password manager mandate.
A.8.8	Management of technical vulnerabilities	Scans run and findings sit untriaged, with no fix deadline and no patch management policy.
A.8.9	Configuration management	No hardened baseline configurations, no drift detection, and cloud resource configurations aren't audited.
A.8.15	Logging	Logs are collected and never reviewed. Retention periods are undefined, and there's no central log management.
A.8.16	Monitoring activities	Monitoring covers availability and misses security events. No thresholds or alerts for suspicious activity.
A.8.20	Networks security	A flat network with no segmentation and no network access control. VPN split tunneling leaves a path for data to leak.
A.8.24	Use of cryptography	Encryption is in place and key management is ad hoc: no rotation schedule, and keys stored in source code.
A.8.25	Secure development life cycle	No secure coding guidelines, no mandatory security code review, and no SAST or DAST in the CI/CD pipeline.
A.8.28	Secure coding	Developers haven't had secure coding training. The OWASP Top 10 isn't referenced. No pre-commit security checks.

More Cycore guides and checklists

- SOC 2 Readiness Checklist

- HIPAA Compliance Checklist
- HITRUST Readiness Guide
- AI Governance Starter Kit

Next step

Talk to Cycore about your ISO 27001 gaps

This is a Cycore diagnostic and does not replace ISO/IEC 27001:2022, an accredited certification audit, or qualified interpretation of the standard.