ISO/IEC 27001:2022 + Amd 1:2024 Information Security Management Systems (ISMS)

Information security, ISMS, certifiable worldwide

181 requirements. This standard can be certified against by an accredited body. As of 07/2026.

ISO/IEC 27001 sets out the requirements for an information security management system: risk based, documented, and demonstrably effective. An assessment against it is an accredited certification audit in two stages (document review, then on-site effectiveness review), followed by annual surveillance audits and recertification after three years.

Company	Date	Prepared by

4 Context of the organization 8

4.1-1 The external and internal issues that affect the organization's ability to achieve the intended outcomes of the ISMS are determined and kept up to date.

What proves it: Demonstrated through a context analysis, either as a standalone document or as a section of the ISMS manual: market environment, customer and contract situation, legal framework (GDPR, NIS2), technology stack, headcount, dependency on cloud providers. For small organizations a one-page table with a date and a review cycle is enough, provided the management review shows it is actually being updated.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

4.1-2 The organization has determined whether climate change is a relevant issue for it. The determination is justified, whether the answer is yes or no.

What proves it: This requirement was introduced by Amd 1:2024 and auditors ask for it specifically. Keep a dedicated row in the context analysis: heat periods affecting server rooms and availability, extreme weather affecting cloud provider data centres, power grid stability. A justified result of not relevant is acceptable, a missing entry is not.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

4.2-1 The interested parties that are relevant to the ISMS are determined.

What proves it: Stakeholder list covering customers, staff, processors and sub-processors, supervisory authorities, insurers, the certification body and shareholders. In small organizations a table with party, expectation and source of the expectation is sufficient.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

4.2-2 The relevant requirements of these interested parties are determined, including any requirements related to climate change.

What proves it: For each party name the concrete source: contract clause, data processing agreement, customer questionnaire, legal obligation. Amd 1:2024 adds a note that interested parties can have climate change related requirements. It is not a separate shall requirement, but auditors routinely raise it, for example sustainability questions in a major customer's supplier audit. One row in the stakeholder table with the result (including none of that kind) is enough.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

4.2-3 It is decided and traceable which of these requirements are addressed through the ISMS.

What proves it: Add a column to the stakeholder table that points to the rule that addresses the requirement (policy, control, contract annex). This shows that requirements were not merely collected but actually processed.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

4.3-1 **The scope of the ISMS is determined and takes account of the issues from 4.1, the requirements from 4.2 as well as interfaces and dependencies with activities performed by third parties.**

What proves it: The scope names sites, organizational units, products, systems and network boundaries. Outsourced parts (hosting, payment providers, support) are described as interfaces with a clear boundary of responsibility. An artificially narrowed scope that carves out core processes is rejected by certification bodies.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

4.3-2 **The scope is available as documented information and states the boundaries of the ISMS unambiguously.** Document

What proves it: An approved scope document with version, date and sign-off by top management. Its exact wording later appears on the certificate, so phrase it precisely and in a way that can be quoted publicly.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

4.4-1 **The ISMS, including the processes needed and their interactions, is established, implemented, maintained and continually improved.**

What proves it: A process map or process list linking risk management, incident handling, change management, auditing and management review with owners and frequency. Live evidence matters more than the diagram: tickets, minutes, calendar entries.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

5 Leadership 8

5.1-1 **Top management takes accountability for the effectiveness of the ISMS and ensures that the policy and the objectives are established and compatible with the strategic direction.**

What proves it: Evidence includes signed approvals of the policy, the scope and the Statement of Applicability, management review minutes and documented budget decisions. In very small organizations top management is often the same person as the ISMS owner, which is acceptable but must be stated openly in the role definition.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

5.1-2 **The requirements of the ISMS are integrated into the business processes and the importance of effective information security is communicated.**

What proves it: Best shown where security is not a separate binder: a security criterion in the definition of done, a security check in the sales or procurement process, a recurring security item in team meeting minutes.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

5.1-3 **Management provides the necessary resources, supports the people who contribute to the effectiveness of the ISMS and promotes continual improvement.**

What proves it: Approved security budget, time allocated for training, engagement of external auditors or penetration testers. An improvement or action register with entries spanning several quarters shows continuity rather than a one-off effort.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

5.2-1 **An information security policy is established that is appropriate to the purpose of the organization and provides a framework for the information security objectives.** Document

What proves it: A short approved policy document, two to three pages is enough. It names the protection goals, the scope, the responsibilities and the principle of a risk based approach. Generic template text with no link to the actual business stands out in the audit.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

5.2-2 **The policy includes a commitment to satisfy applicable requirements and a commitment to continual improvement of the ISMS.** Document

What proves it: Both commitments must appear as explicit sentences in the policy, and they are read word for word in the stage 1 audit. In addition, refer to the underlying processes (legal register, improvement register).

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

5.2-3 **The policy is communicated within the organization and is available to interested parties as appropriate.** Document

What proves it: Evidence via an intranet or wiki entry with a read requirement, an onboarding checklist with confirmation, or a published summary on the website. A distribution list with acknowledgement receipts is the simplest solid proof.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

5.3-1 **Responsibilities and authorities for security relevant roles are assigned and communicated within the organization.**

What proves it: A role matrix (RACI) covering the ISMS owner, risk owners, asset owners, the incident coordinator and the data protection contact. In one-person or very small teams assign every role to a named individual and document the resulting accumulation of roles openly instead of hiding it.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

5.3-2 **The authority to ensure the ISMS conforms to the standard and to report on ISMS performance to top management is assigned to a role.**

What proves it: An appointment letter or role description for the ISMS owner with an explicit reporting line to management. The reporting line must actually be evidenced by management review minutes.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6 Planning 21

6.1.1-1 **Starting from the issues in 4.1 and the requirements in 4.2, the risks and opportunities that need to be addressed are determined, so that the ISMS achieves its intended outcomes and undesired effects are prevented.**

What proves it: A register linking context issues to risks and opportunities, kept either separately or inside the risk register. What matters is traceability: every issue from the context analysis visibly leads to an assessment or to a justified decision not to consider it.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6.1.1-2 **The actions to address these risks and opportunities are planned, integrated into the ISMS processes, and their effectiveness is evaluated.**

What proves it: Action plan with owner, due date and effectiveness criterion. Keep the effectiveness evaluation as its own column, otherwise the audit lacks proof that the action was not only implemented but also verified.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6.1.2-1 **An information security risk assessment process is defined and applied; it includes risk acceptance criteria and criteria for performing risk assessments.** Document

What proves it: A risk management policy with scales for likelihood and impact, a defined risk matrix and a clear acceptance threshold. The threshold must be a number or a zone, not a phrase such as at our discretion.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6.1.2-2 **The process ensures that repeated risk assessments produce consistent, valid and comparable results.**

What proves it: Demonstrated through a fixed methodology with defined scales and by comparing two assessment versions: same risks, same rating logic, explainable differences. A dated version of last year's risk register is the strongest evidence here.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6.1.2-3 **Information security risks are identified to detect loss of confidentiality, integrity and availability within the scope, and a risk owner is assigned to each risk.**

What proves it: Risk register referencing assets or processes, the three protection goals and a named risk owner. The risk owner must have the authority to accept the risk; in small organizations this is normally the managing director.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6.1.2-4 **The identified risks are analysed: potential consequences, realistic likelihood and the resulting level of risk are determined.**

What proves it: Columns for impact, likelihood and resulting risk level, each with a short justification. One sentence of reasoning per risk prevents the most common audit finding, namely numbers without derivation.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6.1.2-5 **The risks are compared against the acceptance criteria and prioritized for treatment.**

What proves it: The risk register must show which risks sit above the acceptance threshold and in what order they will be treated. A sorted view or a priority column is enough.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6.1.2-6 **The risk assessment process is available as documented information.** Document

What proves it: The methodology itself is a mandatory document, not just its output. An approved policy with version and approval date, linked from the ISMS document index.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6.1.3-1 **For every risk above the acceptance threshold an appropriate treatment option is selected (reduce, avoid, transfer or accept).**

What proves it: A treatment option column in the risk register. Where a risk is accepted, record the justification and the formal approval of the risk owner; where it is transferred, name the contract or the insurance policy.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6.1.3-2 **All controls that are necessary to implement the chosen risk treatment options are determined.**

What proves it: Formulate controls concretely and verifiably, with an owner and a due date. Referring to technical work already under way (MFA rollout, backup test) is fine as long as it points to a ticket or a configuration artefact.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6.1.3-3 **The determined controls are compared with the controls in Annex A to verify that no necessary control has been overlooked.**

What proves it: The comparison is a distinct, traceable step, not a by-product. Evidenced by a mapping column in the risk register that references Annex A numbers, plus dated minutes of the comparison.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6.1.3-4 **A Statement of Applicability (SoA) exists. It assesses all 93 Annex A controls individually, states applicability with justification for each control, the implementation status, and the justification for every exclusion.** Document

What proves it: The SoA is the central mandatory document and the map of the entire audit. It must be complete: controls that are not applicable also appear with a justification, never as a blank line. Recommended columns: control number, title, applicable yes or no, justification, implementation status, reference to policy or evidence, link to the risk. Version and management approval are mandatory, because the SoA is checked against reality at every surveillance audit.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

6.1.3-5 **A risk treatment plan is produced that brings together controls, responsibilities, due dates and required resources.** Document

What proves it: This can be a tab in the risk spreadsheet or a project board. What counts is that the dates are realistic and that missed dates were visibly re-planned, because that is exactly what the auditor checks.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

6.1.3-6 **The risk treatment plan is approved by the risk owners and the remaining residual risks are formally accepted by them.** Document

What proves it: Signature, electronic approval or a dated decision in minutes. One line in the management review minutes referencing the version of the register is sufficient, provided the version is unambiguous.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

6.1.3-7 **The risk treatment process is available as documented information.** Document

What proves it: Usually covered in the same policy document as the risk assessment. The flow from assessment through option selection to residual risk acceptance must be described.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

6.2-1 **Information security objectives are established for relevant functions and levels, are consistent with the policy, and are measurable where practicable.**

What proves it: An objectives sheet with three to six objectives, each with a metric, a baseline, a target value and a deadline. Example: share of systems with MFA raised from 80 to 100 percent by the end of the quarter. Objectives without a number count as not measurable.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

6.2-2 **The objectives take into account the applicable information security requirements as well as the results of risk assessment and risk treatment.**

What proves it: Add an origin column to the objectives sheet: which risk, which customer requirement or which legal obligation the objective comes from. This prevents objectives that look arbitrary.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

6.2-3 **The objectives are monitored, communicated and updated as needed.**

What proves it: Quarterly progress tracking in the objectives sheet plus communication to the team, for example a short note in the wiki or an agenda item in the team meeting. Historic versions demonstrate that updates happen.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

6.2-4 **The information security objectives are available as documented information.** Document

What proves it: An approved objectives document with a date is enough. It may be part of the management review, but it must exist there as its own retrievable section.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6.2-5 **For each objective it is planned what will be done, which resources are required, who is responsible, when it will be completed and how the results will be evaluated.**

What proves it: These five items are individually verifiable and are asked for individually in the audit. Set them up as five columns in the objectives sheet, then conformity is visible at a glance.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

6.3-1 **Where the organization determines that changes to the ISMS are needed, those changes are carried out in a planned manner.**

What proves it: Evidenced by change requests, minutes or tickets showing the trigger, the impact assessment, the approval and the implementation. Typical triggers in small organizations: switching cloud provider, new sites, the first hire.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

7 Support 15

7.1-1 **The resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS are determined and provided.**

What proves it: A security budget line, tool licences (password manager, MDM, log platform), planned person days for ISMS upkeep and external audit services. An invoice or a budget approval proves this faster than any prose.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

7.2-1 **The necessary competence of the people whose work affects information security performance is determined.**

What proves it: Competence matrix or role profiles listing the knowledge required per role, for example secure development for developers, incident handling for the coordinator. In very small teams one row per person is enough.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

7.2-2 **Competence is ensured on the basis of appropriate education, training or experience.**

What proves it: Certificates, course confirmations, CVs or documented practical experience. Self-study is acceptable if it is evidenced, for example by completion records from online courses or by passed internal knowledge tests.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

7.2-3 **Where competence gaps exist, actions have been taken to close them and the effectiveness of those actions has been evaluated.**

What proves it: Training plan with a target versus actual comparison and an effectiveness check, for example a test score, a phishing simulation click rate or on-the-job observation. The effectiveness check is often forgotten and is a classic minor finding.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

7.2-4 **Appropriate documented information is available as evidence of competence.** Document

What proves it: A competence or training folder per person with evidence and dates. In small organizations a directory of stored PDF records plus an overview table is enough.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

7.3-1 **The people working within the scope are aware of the information security policy.**

What proves it: Acknowledgement at onboarding and after every change to the policy, with date and version. A wiki read-receipt feature or a signed list is sufficient.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

7.3-2 **People know their own contribution to the effectiveness of the ISMS and the benefits of improved information security performance.**

What proves it: Training material and attendance lists in which the link to the person's own work is visible. Auditors interview staff directly, so train with concrete, everyday examples rather than abstract quotations from the standard.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

7.3-3 **People know the consequences of not conforming to the ISMS requirements.**

What proves it: State the consequences in training slides and work instructions and link them to the process under A.6.4. Even organizations without employees must cover this for contractors and freelancers through their contracts.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

7.4-1 **Internal and external communication relevant to the ISMS is determined: what is communicated, when, with whom and by which means.**

What proves it: A communication matrix with rows such as security incident to customers, notification to the supervisory authority within 72 hours, monthly status report to management. It is the basis of crisis communication and is reviewed after every incident.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

7.5.1-1 **The ISMS includes the documented information required by the standard as well as the documented information the organization has determined to be necessary for the effectiveness of the ISMS.** Document

What proves it: A document index listing every ISMS document with purpose, owner, version and storage location. It shows that the mandatory documents are complete and is the quickest entry point for the auditor.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

7.5.2-1 **When creating and updating documents, appropriate identification, format and media are ensured, and the documents are reviewed and approved for suitability.**

What proves it: A uniform document header with title, version, date, author and approver. In Git based environments, pull request reviews with approval satisfy the review and approval requirement, provided the history is immutable.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

7.5.3-1 **Documented information is available and suitable for use where and when it is needed.**

What proves it: A central storage location reachable by everyone entitled to it, with a search function. Testable by sampling: any given work instruction must be findable in under a minute.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

7.5.3-2 **Documented information is adequately protected, in particular against loss of confidentiality, improper use and loss of integrity.**

What proves it: Role based access rights to ISMS documents, versioning with history, write protection for approved versions and a backup of the document repository. The backup evidence is the part most often forgotten.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

7.5.3-3 **Distribution, access, retrieval, storage, change control as well as retention and disposition of documented information are governed.**

What proves it: A short document control rule with retention periods and deletion rules. It must be reconciled with legal obligations (commercial law, tax law, GDPR) and is the basis for A.5.33 and A.8.10.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

7.5.3-4 **Documented information of external origin that is necessary for planning and operating the ISMS is identified and controlled.**

What proves it: A list of external documents with version and source: standards, legal texts, vendor hardening guides, cloud security documentation, data processing agreements. Without a version reference, control cannot be demonstrated.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

8 Operation 8

8.1-1 **The processes needed to meet the information security requirements and to implement the actions from clause 6 are planned, implemented and controlled, and criteria for those processes are established.**

What proves it: An operations manual or runbooks with clear criteria, for example the maximum time to deploy critical patches, release criteria for deployments, alert thresholds. Criteria without numbers are worthless in the audit.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

8.1-2 **Documented information is available to the extent necessary to have confidence that the processes have been carried out as planned.** Document

What proves it: Operational records as evidence: ticket history, CI pipeline runs, patch reports, backup logs, access reviews. These records are the actual proof of effectiveness in the stage 2 audit.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

8.1-3 **Planned changes are controlled and the consequences of unintended changes are reviewed; where necessary, adverse effects are mitigated.**

What proves it: A change process with approval and a rollback path, linked to A.8.32. For unintended changes (misconfiguration, accidental privilege escalation) document the incident and evidence the correction.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

8.1-4 **Externally provided processes, products and services that are relevant to the ISMS are determined and controlled.**

What proves it: A supplier list with criticality, contract reference and the state of evidence (the provider's ISO 27001 certificate, SOC 2 report, data processing agreement). For small organizations this is the biggest lever, because most of the IT runs externally anyway.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

8.2-1 **Risk assessments are performed at planned intervals and whenever significant changes or incidents occur, taking the established criteria into account.**

What proves it: A rhythm (typically annual) plus defined triggers for unscheduled assessments. Evidenced by dated versions of the risk register and entries in the calendar or ticket system.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

8.2-2 **The results of the risk assessments are retained as documented information.** Document

What proves it: Historic versions of the risk register with dates, not just the current state. Overwriting the file makes the development impossible to prove; versioning in the file system or in Git solves this.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

8.3-1 **The risk treatment plan is implemented.**

What proves it: Compare plan against reality: completed actions with an implementation date and a concrete artefact (configuration, policy, contract). Open actions need a documented justification and a new target date.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

8.3-2 **The results of the risk treatment are retained as documented information.** Document

What proves it: Status reports or closed action items with a reference to the evidence. The register alone is enough if each row carries a completion date and a link to the evidence.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9 Performance evaluation 21

9.1-1 **It is determined what needs to be monitored and measured, including the information security processes and controls.**

What proves it: A metrics sheet with a manageable number of solid measures: patch backlog, MFA coverage, time to resolve incidents, result of the last restore test, open findings. A few metrics that are actually collected beat a long wish list.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.1-2 **The methods for monitoring, measurement, analysis and evaluation are defined and produce valid results.**

What proves it: Document the data source and the calculation for each metric, for example an export from the vulnerability scanner or from the identity provider report. Traceability of the source is the core of validity.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.1-3 **It is defined when and by whom monitoring and measurement are performed and when the results are analysed and evaluated.**

What proves it: Add columns for frequency and owner to the metrics sheet. A recurring calendar appointment for the evaluation proves regularity better than any description.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.1-4 **The results of monitoring and measurement are retained as documented information.** Document

What proves it: Archived evaluations, exported dashboards or a metrics sheet maintained as a time series. A live view with no history does not satisfy the requirement.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.1-5 **The information security performance and the effectiveness of the ISMS are evaluated on the basis of the measurement results.**

What proves it: A written evaluation, not just figures: trend, causes, need for action. This evaluation text is at the same time an input to the management review.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.2.1-1 **Internal audits are conducted at planned intervals and provide information on whether the ISMS conforms to the organization's own requirements and to the requirements of the standard and is effectively implemented.**

What proves it: Before the certification audit at least one full internal audit cycle covering the entire scope must be completed. Without it, certification is out of reach; this is one of the most common stumbling blocks for first certifications.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.2.2-1 **An audit programme is planned, established and maintained; it defines frequency, methods, responsibilities, planning requirements and reporting, and it considers the importance of the processes concerned and the results of previous audits.**

What proves it: A multi-year audit programme covering all clauses and all applicable controls across the certification cycle, with a higher frequency for critical areas. A simple table spanning three years is entirely sufficient.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.2.2-2 **Audit criteria and audit scope are defined for each audit.**

What proves it: An audit plan per date with the criteria (the standard, internal policies, contracts) and a clear scope. A one-page audit plan per audit is enough and doubles as the basis for the report.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.2.2-3 **Auditors are selected and audits are conducted in a way that ensures objectivity and impartiality. Nobody audits their own work.**

What proves it: Independence is the hard hurdle here: whoever wrote the policies and configured the systems must not audit them. In very small organizations this almost always means an external internal auditor, for example a contracted consultant or a colleague from a partner company; an audit contract plus the auditor's declaration of independence is the evidence. Only in sufficiently large teams can the role be rotated internally to a person with no responsibility for the area under audit, and that then has to be shown in the role matrix.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.2.2-4 **The audit results are reported to relevant management.**

What proves it: An audit report with findings, nonconformities, recommendations and a distribution list, plus evidence of handover to management, for example a minuted item or a dated email handover.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.2.2-5 **Documented information on the audit programme and the audit results is retained.** Document

What proves it: Keep the audit programme, audit plans, audit reports and the resulting actions in one place. The link from a finding to a corrective action (clause 10.2) must be visible end to end.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.3.1-1 **Top management reviews the ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness.**

What proves it: At least annually and scheduled before the external audit. Even in very small organizations there must be dated, signed minutes, even where management and the ISMS owner are the same person.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.3.2-1 **The management review considers the status of actions from previous management reviews.**

What proves it: The minutes start with a follow-up table of last year's decisions and their current status. Without this back-reference the review counts as incomplete.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.3.2-2 **The management review considers changes in the external and internal issues that are relevant to the ISMS, including relevant aspects of climate change.**

What proves it: A dedicated agenda item referring to the updated context analysis. Climate change is not named explicitly in the text of this clause (Amd 1:2024 only changes 4.1 and 4.2), but it enters here through changes in the 4.1 issues and auditors expect it. Even a result of not relevant, unchanged belongs in the minutes.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.3.2-3 **The management review considers changes in the needs and expectations of interested parties that are relevant to the ISMS.**

What proves it: New customer requirements from contracts and security questionnaires, new legal obligations, requirements from the certification body. Record them as a list with sources in the minutes.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.3.2-4 **The management review considers feedback on information security performance, including nonconformities and corrective actions, monitoring and measurement results, audit results and the fulfilment of the information security objectives.**

What proves it: Handle these four blocks as separate agenda items, otherwise one of them will be missing from the minutes later. Attach the metrics sheet, the audit report and the objectives sheet as annexes.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.3.2-5 **The management review considers feedback from interested parties.**

What proves it: Customer complaints with a security angle, results of customer audits, reports from the whistleblowing channel, feedback from service providers. Record it in the minutes even where the finding is that none were received.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.3.2-6 **The management review considers the results of the risk assessment and the status of the risk treatment plan.**

What proves it: Attach the current risk register and the implementation status of the treatment plan, with explicit confirmation of residual risk acceptance by the risk owners.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.3.2-7 **The management review considers opportunities for continual improvement.**

What proves it: An agenda item with concrete improvement ideas and a decision on each. Accepted ideas move into the improvement register as entries with due dates.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.3.3-1 **The results of the management review include decisions on opportunities for continual improvement and on any need for changes to the ISMS.**

What proves it: The minutes end with a decisions section: decision, owner, due date. Minutes without decisions are a finding in the audit, because the leadership effect is then missing.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

9.3.3-2 **Documented information is retained as evidence of the results of the management review.** Document

What proves it: Signed minutes with date, participants, inputs, evaluation and decisions. It is one of the first documents a certification body asks for in stage 1.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

10 Improvement 7

10.1-1 **The suitability, adequacy and effectiveness of the ISMS are continually improved.**

What proves it: An improvement register fed from several sources (audits, incidents, ideas, metric deviations) with visible progress over time. Continuity over several months is the proof, not the number of entries.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

10.2-1 **When a nonconformity occurs, the organization reacts to it: it controls and corrects it and deals with the consequences.**

What proves it: A nonconformity report with an immediate action and a date. Sources are internal audits, external audits, incidents and observations from daily operations; all of them feed the same register.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

10.2-2 **It is evaluated whether action is needed to eliminate the causes so that the nonconformity does not recur or occur elsewhere; this includes checking whether similar nonconformities exist or could occur.**

What proves it: Document the root cause analysis, for example with 5 Why or Ishikawa, plus an explicit statement on transferability to other systems or processes. The transferability step is the one most often skipped.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

10.2-3 **Any necessary corrective actions are implemented and their effectiveness is reviewed.**

What proves it: For each action record the implementation date, the evidence artefact and a later effectiveness review with its own date. Two date fields per row are the simplest way not to lose the effectiveness review.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

10.2-4 **Where necessary, changes are made to the ISMS as a result of the nonconformity.**

What proves it: If a nonconformity traces back to a gap in a policy, the risk register or the SoA, the change must become visible there. A reference from the nonconformity to the updated document version closes the chain.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

10.2-5 **Corrective actions are appropriate to the effects of the nonconformities encountered.**

What proves it: A severity rating in the register from which the proportionality of the action is evident. Neither trivia handled as a project nor serious deviations answered with a mere reminder email.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

10.2-6 **Documented information is retained on the nature of the nonconformities, the actions taken in response and the results of the corrective actions.** Document

What proves it: A nonconformity and corrective action register with columns for nature, cause, action, owner, due date and the result of the effectiveness review. It is mandatory evidence and is pulled in every surveillance audit.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5 Annex A: Organizational controls 37

A.5.1 **Policies for information security: An overarching information security policy and topic-specific policies are defined, approved by management, communicated, and reviewed at planned intervals and whenever significant changes occur.** Document

What proves it: A policy set with version, approval date and next review date, plus evidence of acknowledgement. For small organizations a framework policy and a handful of topic policies (access, cryptography, remote working, incidents) are enough.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.2 **Information security roles and responsibilities: Information security roles and responsibilities are defined and allocated according to the needs of the organization.**

What proves it: A role matrix with names, deputies and tasks. In very small organizations state openly where several roles accumulate in one person and link this to the compensating controls under A.5.3.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.3 **Segregation of duties: Duties and areas of responsibility that are meant to check one another are not held by a single person. The goal is that nobody can initiate, approve and conceal a change on their own.**

What proves it: In small organizations full segregation is structurally impossible; a blanket claim of compliant collapses immediately in the audit interview. What holds up is an honest analysis: which combinations of duties are critical (develop and release, grant rights and use them, initiate and approve payments), which of them sit with one person, and which compensating controls apply. Proven approaches are immutable audit logs accessible to a third party, MFA on privileged accounts, automated CI gates and branch protection instead of four-eyes review, a periodic log review by an external person, and separate approval for payments. Keep the analysis and the compensating controls as a dated document of its own and link it from the SoA.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.4 **Management responsibilities: Management requires all personnel to apply information security in line with the established policies and procedures.**

What proves it: A commitment in employment and contractor agreements, acknowledgement of the policies at onboarding, and regular reminders from management. Evidence: signed commitment statements and meeting minutes.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.5.5 **Contact with authorities: Appropriate contacts with relevant authorities are maintained and can be reached when needed.**

What proves it: A contact list with the competent data protection authority, the police or cybercrime unit, the national cyber security reporting point and, where in scope, NIS2 reporting channels. Note the deadlines (such as the 72 hours under GDPR) directly in the list.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.5.6 **Contact with special interest groups: Contacts with special interest groups, security forums and professional associations are maintained.**

What proves it: Memberships, subscribed advisories (national CERT, vendor feeds), participation in special interest groups. A simple proof: a list of subscriptions plus one example of how an advisory led to an action.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.5.7 **Threat intelligence: Information about information security threats is collected and analysed to derive appropriate actions from it.**

What proves it: New in the 2022 edition. Workable for small organizations: subscribe to national CERT advisories and vendor advisories, then run a short monthly review with a relevance decision and tickets derived from it. The evidence is the analysis, not the subscription.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.5.8 **Information security in project management: Information security is integrated into project management, regardless of the type of project.**

What proves it: Security items in the project checklist: protection needs, risk review, data protection check, security sign-off before go-live. In agile teams anchor them as fixed items in the definition of ready and the definition of done.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.5.9 **Inventory of information and other associated assets: An inventory of information and other associated assets with named owners is created and maintained.**

What proves it: An asset inventory covering hardware, software, cloud services, data stores, domains and accounts, each with an owner and its protection needs. In small organizations it can be assembled automatically from an MDM export, a licence list and the cloud console; a current date is mandatory.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.5.10 **Acceptable use of information and other associated assets: Rules for the acceptable use and handling of information and other associated assets are identified, documented and implemented.** Document

What proves it: An acceptable use policy for devices, networks, cloud accounts and AI tools, with acknowledgement. Personal devices and external AI services should be covered explicitly, because that is where most leakage happens.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.5.11 **Return of assets: When a working relationship ends or changes, it is governed and confirmed in writing that all issued devices, keys, accounts and documents are returned.**

What proves it: An offboarding checklist with a return receipt for laptop, tokens, keys, certificates and storage media, plus account disabling on the same day. This applies to freelancers and interns just as much.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.12 **Classification of information: Information is classified according to its protection needs regarding confidentiality, integrity, availability and legal requirements.**

What proves it: A simple scheme with three or four levels (public, internal, confidential, strictly confidential) and concrete handling rules per level. Record the assignment in the asset inventory or in the record of processing activities.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.13 **Labelling of information: The classification level is recognizable on the document, the file or the message itself, so that recipients know how to handle it without having to ask.**

What proves it: Labelling in the document header, the file name, the email subject or via sensitivity labels in the cloud office suite. Evidence through samples of documents actually labelled, not just through the rule.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.14 **Information transfer: Rules, procedures and agreements for transferring information within the organization and with external parties are in place.**

What proves it: A rule stating which channel is permitted for which classification level: encrypted email or a data room for confidential content, no sending via private messengers. Back confidential transfers with non-disclosure agreements.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.15 **Access control: Rules to control physical and logical access to information and other associated assets are established and implemented based on business and security requirements.**

What proves it: An access control policy following need to know and least privilege, with a role to rights mapping. Evidence through the actual rights configuration in the identity provider, not through the policy alone.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.16 **Identity management: The full life cycle of identities is managed.**

What proves it: A process from creation through change to deactivation, ideally centralized in an identity provider with single sign-on. No shared group accounts; where technically unavoidable, name the account, justify it and log its use.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.17 **Authentication information: The allocation and management of authentication information is controlled by a management process that requires people to handle it properly.**

What proves it: A password manager as a mandatory tool, a policy on password quality and MFA, secure initial access and a reset procedure with identity verification. Evidence through configuration screenshots and the password manager report.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.18 **Access rights: Access rights are provisioned, reviewed, modified and removed in accordance with the access control policy.**

What proves it: A periodic access review, at least annually, with a documented result per account and evidence of rights that were removed. Removal on the day of departure is a point auditors like to trace through a concrete case.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.19 **Information security in supplier relationships: Processes and procedures are defined and implemented to manage the security risks arising from the use of third-party products and services.**

What proves it: A supplier list with a criticality level and the depth of assessment. For critical providers obtain evidence (ISO 27001 certificate, SOC 2 report) rather than running your own audits, which is the only realistic route for small organizations.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.20 **Addressing information security within supplier agreements: Relevant security requirements are agreed with each supplier and set out in the contracts.**

What proves it: An information security contract annex with incident notification duties, rules on sub-processors, deletion obligations and audit rights. For standard services the provider terms plus a data processing agreement are sufficient, provided their content has been reviewed and documented.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.21 **Managing information security in the ICT supply chain: Processes to manage the security risks in the supply chain for information and communication technology are defined and implemented.**

What proves it: This covers software dependencies and the providers' own sub-suppliers. In practice: a software bill of materials (SBOM) or dependency list, automated checks for vulnerable packages in CI, and sourcing software only from signed or official channels.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.22 **Monitoring, review and change management of supplier services: Changes to supplier services are regularly monitored, reviewed and managed.**

What proves it: An annual supplier review looking at incidents, availability reports and certificate validity, plus a channel for the provider's change announcements. Record the result as a short note per supplier.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.23 **Information security for use of cloud services: Processes for acquiring, using, managing and exiting cloud services are established in line with the security requirements.**

What proves it: New in the 2022 edition and the central control for small cloud-based organizations. Evidence through a cloud policy with an approval process for new services, a documented shared responsibility model per service, hardening settings, and an exit strategy including data return and confirmation of deletion.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.24 **Information security incident management planning and preparation: Processes, roles and responsibilities for incident handling are planned and established.** Document

What proves it: An incident response plan with the reporting path, roles, escalation levels, out-of-hours contacts and communication templates. Realistic for small teams: one page, but practised.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.25 **Assessment and decision on information security events: Security events are assessed and a decision is made on whether they are to be classified as information security incidents.**

What proves it: Triage criteria with a severity matrix and an event register in which dismissed events also appear with a justification. The separation between event and incident must be visible in the register.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.26 **Response to information security incidents: Incidents are handled in accordance with the documented procedures.**

What proves it: Incident files with a timeline, the actions taken, the people involved and the closure decision. If there has been no real incident yet, a documented tabletop exercise is the best available evidence.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.27 **Learning from information security incidents: Knowledge gained from incidents is used to strengthen the security controls.**

What proves it: A blameless post-incident review with root cause analysis and derived actions, linked to the improvement register and, where needed, to the risk register.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.28 **Collection of evidence: It is governed how traces relating to a security event are identified, secured and retained so that they remain usable later.**

What proves it: A short evidence preservation procedure: do not rebuild systems prematurely, secure images and logs, document the chain of custody. For small organizations it is enough to define the severity level from which an external forensics provider is called in, together with the contact details.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.29 **Information security during disruption: The organization plans how information security is maintained at an appropriate level during a disruption.**

What proves it: Emergency arrangements must not switch security off. Document that MFA, logging and access restrictions also apply in fallback operation, and that emergency accounts (break-glass accounts) are sealed, documented and reviewed afterwards.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.30 **ICT readiness for business continuity: ICT readiness is planned, implemented, maintained and tested on the basis of business continuity objectives and ICT continuity requirements.**

What proves it: New in the 2022 edition. Evidence through defined recovery time objectives (RTO) and recovery point objectives (RPO) per critical system, a recovery procedure and at least one documented test per year. A successful restore test with date and duration is the strongest single piece of evidence.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.31 **Legal, statutory, regulatory and contractual requirements: The relevant requirements and the approach to meeting them are identified, documented and kept up to date.** Document

What proves it: A legal register covering GDPR, telecommunications law, commercial and tax law, and where applicable NIS2 or sector-specific rules, each with the rule that implements it and the date of review. An annual review is sufficient, but it must be dated.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.32 **Intellectual property rights: Appropriate procedures to protect intellectual property rights are implemented.**

What proves it: A licence inventory for the software in use, a check of open source licences in the product (a licence scanner in CI) and a rule for handling third-party code and generated code. Evidence: the licence report from the build.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.33 **Protection of records: Business and evidential records are stored so that they cannot be lost, cannot be altered unnoticed and cannot fall into the wrong hands, and this holds for the whole retention period.**

What proves it: A retention schedule with the statutory periods, tamper-resistant storage, restricted access and backup. For tax relevant records name the statutory retention periods explicitly, as auditors like to check that specifically.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.34 **Privacy and protection of PII: The requirements for privacy and the protection of personally identifiable information (PII) are identified and met in line with applicable law.**

What proves it: Record of processing activities, data processing agreements, a deletion concept, a process for data subject rights and, where required, a data protection impact assessment. Linking this to the ISMS through a shared asset list avoids maintaining everything twice.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.35 **Independent review of information security: The organization's approach to managing information security is reviewed independently at planned intervals and whenever significant changes occur.**

What proves it: Evidenced by the internal audit performed by an independent auditor, by external penetration tests or by the certification audit itself. Independent means not carried out by the person who is responsible for the area under review.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.36 **Compliance with policies, rules and standards for information security: Compliance with the organization's own security policies and the applicable rules is reviewed regularly.**

What proves it: Compliance checks with date and result, for example a configuration check against your own hardening baseline, sampling of document labelling, automated policy checks in the cloud. Deviations feed into the corrective action register.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.5.37 **Documented operating procedures: Operating procedures for information processing facilities are documented and made available to the people who need them.** Document

What proves it: Runbooks for backup and restore, deployment, user administration, patching and incident handling. Short and current beats extensive and outdated; a last-changed date per runbook is mandatory.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.6 Annex A: People controls 8

A.6.1 **Screening: Candidates who are to work for the organization are screened beforehand, within the limits of the law and proportionate to the protection needs; for sensitive roles the screening is repeated during employment.**

What proves it: With no employees this control can be justified as currently not applicable, but the procedure for the case of hiring should still be defined and recorded in the Statement of Applicability as planned. A workable scope: verification of identity, CV and references, plus certificates; a criminal record check only where the protection needs justify it and the law allows it. Require the same standard from freelancers and contractors through their contracts, otherwise the gap opens exactly there.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.6.2 **Terms and conditions of employment: The contractual agreements state the information security responsibilities of the personnel and of the organization.**

What proves it: A security clause in the employment or service contract referring to the applicable policies. For freelancers the same clause in the service contract, plus a non-disclosure agreement.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.6.3 **Information security awareness, education and training: Personnel and relevant external parties receive appropriate awareness and training as well as regular updates on the organization's policies.**

What proves it: Annual training with attendance evidence and a date, supplemented by phishing simulations with an evaluated click rate. Even solo self-employed people need evidence of their own continuing education, for example course confirmations.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.6.4 **Disciplinary process: A formal and communicated process exists for taking action against people who have violated the security policies.**

What proves it: With no employees this can be justified as currently not applicable, but the process must still be defined for the case of hiring; only its application lapses, not the rule. What is required is a graduated, communicated scale of responses (conversation, reprimand, formal warning, dismissal) in line with employment law and staff representation rules. For contractors reflect the sanction level in the contract, for example a contractual penalty or a right of termination.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.6.5 **Responsibilities after termination or change of employment: Security responsibilities and duties that remain valid after termination or a change of role are defined, enforced and communicated to the people concerned.**

What proves it: An offboarding checklist with removal of rights, return of assets, handover, and an explicit reminder of the continuing confidentiality obligations. A signed exit interview record is the simplest evidence.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.6.6 **Confidentiality or non-disclosure agreements: It is determined who has to sign a confidentiality agreement. The content matches the protection needs of the information, the agreements are signed, filed and reviewed regularly to keep them current.**

What proves it: Signed confidentiality agreements for employees, freelancers, service providers and interns, with a survival period. An overview table with counterparty, date and validity makes the portfolio auditable.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.6.7 **Remote working: Security measures are implemented where people work outside the organization's premises and access organizational information while doing so.**

What proves it: A home office and remote working policy with requirements on disk encryption, screen lock, secure Wi-Fi, use of VPN or zero trust access, privacy screens and a ban on using personal devices without approval. Evidence through the MDM compliance report for the endpoints.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.6.8 **Information security event reporting: A mechanism exists through which people can report observed or suspected security events in a timely manner.**

What proves it: A clearly communicated reporting channel (mailbox, chat channel, phone number) with an assurance of no sanctions for good-faith reports. Evidence: the volume of reports in the event register; a permanently empty register is a warning sign in the audit.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.7 Annex A: Physical controls 14

A.7.1 Physical security perimeters: Security perimeters are defined and used to protect areas that contain information and information processing facilities.

What proves it: A description of the perimeters with a sketch or photos: building, office, server cabinet. In a home office the perimeter is the lockable working room or, failing that, a lockable cabinet; describe it rather than leave it out.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.7.2 Physical entry: Secure areas are protected by appropriate entry controls and access points.

What proves it: A key or badge register with issue and return, and a visitor rule with escorting and a log. If a coworking space or a data centre is used, take the operator's entry controls as evidence and secure them contractually.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.7.3 Securing offices, rooms and facilities: Physical security for offices, rooms and facilities is designed and implemented.

What proves it: Lockable doors, window protection on the ground floor, no confidential screens visible from outside, no company sign on sensitive areas. A short description plus a photo is enough as evidence.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.7.4 Physical security monitoring: Premises are continuously monitored for unauthorized physical access.

What proves it: New in the 2022 edition. Options are an alarm system, motion detectors, video surveillance or entry logs. Video surveillance must be checked for data protection compliance; in a home office the justified alternative is a combination of an alarm system, a locked room and the finding that no sensitive servers are kept there.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.7.5 Protecting against physical and environmental threats: Protection is in place against physical and environmental threats such as natural disasters and intentional or unintentional damage.

What proves it: A review of fire, water, heat, power failure and burglary, together with the measures in place (smoke detectors, fire extinguishers, no equipment under water pipes, backup stored at a different location). This is where the climate change determination from 4.1 connects.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.7.6 Working in secure areas: Measures for working in secure areas are designed and implemented.

What proves it: Rules for the server room or areas of high confidentiality: no unsupervised third-party access, no recording with cameras or mobile devices, logging of the work carried out. If there are no secure areas, that can be justified by referring to cloud-only operation.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.7.7 Clear desk and clear screen: Rules for a clear desk regarding papers and removable media and for locked screens are defined and followed.

What proves it: This applies fully in the home office too and must therefore not be declared not applicable. Evidenced by a short rule (lock away documents, screen lock after five minutes, no sticky notes with credentials) plus the technically enforced lock via device policy, whose configuration can be exported.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.7.8 **Equipment siting and protection: Equipment is sited securely and protected.**

What proves it: Placement away from thoroughfares and public areas, no view from outside, protection against heat and humidity, cable locks for mobile devices. A short description within the home office or office policy is enough.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.7.9 **Security of assets off-premises: Assets located off the premises are protected.**

What proves it: In small organizations this is mainly the laptop, the smartphone and external media, and it cannot be argued away. Evidence: enforced disk encryption, remote wipe enabled through MDM, a rule against leaving devices in vehicles and against using public networks without VPN, plus a loss reporting path. The MDM compliance report showing the encryption status per device is the most solid single piece of evidence.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.7.10 **Storage media: Storage media are managed across their whole life cycle in line with the classification scheme and the handling requirements, from acquisition through use and transport to disposal.**

What proves it: This applies even to purely mobile working, because USB sticks, external drives and backup media exist. Evidence: a media register, encrypted media, a technically enforced ban on unapproved removable media, secure storage in a lockable place, and handover to A.7.14 at end of life.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.7.11 **Supporting utilities: Information processing facilities are protected against failure of the supporting utilities, in particular the power supply.**

What proves it: Where servers are run in house, an uninterruptible power supply with a documented test. In a cloud-only setup the evidence is the reference to the provider's commitments plus a rule on how to keep working during a local power or internet outage (mobile tethering, fallback location).

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.7.12 **Cabling security: Power, data and communications cabling is protected against interception, interference and damage.**

What proves it: Where you own the cabling, protection against damage and against unauthorized access to patch panels. In small offices and home offices the justification is lean, but it has to be given: router and network sockets are not publicly accessible, unused ports are disabled.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.7.13 **Equipment maintenance: Equipment is maintained correctly to ensure the availability, integrity and confidentiality of information.**

What proves it: A maintenance plan or vendor support status per device, and a rule for repairs carried out by third parties (remove the storage device first or wipe the data, and put a confidentiality agreement in place with the provider). Track end-of-support dates in the asset inventory.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.7.14 **Secure disposal or re-use of equipment: Before a device containing storage is passed on, sold or scrapped, it is verified and recorded that no protected data and no licensed software can still be reconstructed on it.**

What proves it: This also applies in the home office and to retired personal devices that were used for work. Evidence: a wipe record per device with serial number, date and method (crypto-erase on encrypted SSDs, overwriting, physical destruction), or a certificate of destruction from a provider. For encrypted devices the documented destruction of the key is enough, provided the procedure is described.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8 Annex A: Technological controls 34

A.8.1 User endpoint devices: Information stored on, processed by or accessible via user endpoint devices is protected.

What proves it: A hardening baseline per operating system, central management via MDM, disk encryption, automatic updates and screen lock. The MDM compliance report with a status per device evidences all of these at once.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.2 Privileged access rights: The allocation and use of privileged access rights is restricted and managed.

What proves it: A list of all administrator accounts with a justification, separate admin accounts not used for daily work, enforced MFA, time-limited elevation where possible, and periodic review. In small organizations this is the most important compensating control for A.5.3.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.3 Information access restriction: Access to information and other associated assets is restricted in accordance with the established access control policy.

What proves it: An authorization concept based on roles and groups rather than individual grants, evidenced by an export of group memberships. Review public sharing links in cloud storage regularly and let them expire.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.4 Access to source code: Read and write access to source code, development tools and software libraries is appropriately managed.

What proves it: Repository permissions by role, protected main branches, enforced reviews or enforced status checks, no direct push to main. Evidence through the branch protection configuration and the organization's member list.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.5 Secure authentication: Secure authentication technologies and procedures are implemented on the basis of the access restrictions and the topic-specific policy.

What proves it: MFA for all external access and all administrator accounts, phishing-resistant methods (passkeys, FIDO2) where possible, and lockout after failed attempts. Evidence through the identity provider's MFA coverage report.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.6 Capacity management: Storage, compute, bandwidth and licences are monitored, and demand is adjusted early enough that bottlenecks never threaten availability.

What proves it: Monitoring of storage, compute load, licence quotas and cloud budgets with threshold alerts. In small organizations an alert on disk usage and on cost limits plus an annual capacity look is enough.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.7 Protection against malware: Technical defences against malware are active and current, and the people who use the devices are trained well enough not to undermine those defences.

What proves it: Active endpoint protection with a central status overview, a mail filter that inspects attachments and links, and a rule against executing unapproved software. The dated status report of the protection solution is the direct evidence.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.8 **Management of technical vulnerabilities: The organization actively learns about vulnerabilities in the technology it uses, decides for each finding how far it is exposed, and closes the gap within defined deadlines or justifies a different response.**

What proves it: Vulnerability management with a source (scanner, dependency check in CI, vendor advisories), a severity rating and defined deadlines per level, for example critical within 7 days. Evidence: scan reports from several points in time showing the decline in open findings.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.8.9 **Configuration management: Configurations of hardware, software, services and networks, including security configurations, are established, documented, implemented, monitored and reviewed.**

What proves it: New in the 2022 edition. Evidence through documented baseline configurations (hardening baselines) and their enforcement, ideally as infrastructure as code in version control or through MDM profiles. Drift detection and a periodic configuration comparison round it off.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.8.10 **Information deletion: Information stored in information systems, on devices and on storage media is deleted once it is no longer required.**

What proves it: New in the 2022 edition and closely tied to the GDPR. Evidence through a deletion concept with retention periods per data category, technically implemented retention policies in cloud services and databases, and deletion logs. Backups and log archives need a retention period too.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.8.11 **Data masking: Data masking is applied in accordance with the topic-specific policy on access control and with the business and legal requirements.**

What proves it: New in the 2022 edition. In practice: no production data in test and development environments, but anonymized or synthetic data instead; pseudonymization in analytics; masking of account numbers and credentials in logs and support interfaces. Evidence through the script or procedure that generates the test data.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.8.12 **Data leakage prevention: Data leakage prevention measures are applied to systems, networks and devices that process, store or transmit sensitive information.**

What proves it: New in the 2022 edition. Realistic in small organizations: control of sharing links in cloud storage, blocking of unapproved removable media, rules against forwarding to private mailboxes, checks on entering confidential data into external AI services, and secret scanning in source code. Evidence through the configuration and through reviews of the hits.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.8.13 **Information backup: Backups of data, software and systems exist according to a defined rule (scope, frequency, retention, location), and restoring from them is actually tested at regular intervals.**

What proves it: A backup policy with frequency, retention and an offsite copy following the 3-2-1 principle, encryption of the backups, and protection against overwriting by ransomware (immutable backups). What is decisive is the documented restore test with date and result, because an untested backup counts as non-existent in the audit.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.8.14 **Redundancy of information processing facilities: Information processing facilities are implemented with enough redundancy to meet the availability requirements.**

What proves it: Redundancy has to match the availability objectives, not the maximum possible. Evidence through an architecture description with redundant instances or zones, spare devices, and a justified decision on where redundancy is deliberately absent.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.8.15 **Logging: Security relevant activities leave a trace. Logs are produced, retained, protected against alteration and actually analysed, not merely collected.**

What proves it: At a minimum log sign-ins and failed attempts, permission changes, administrative actions and access to confidential data. The logs are protected against alteration and carry a defined retention period; in small organizations immutable logs are at the same time the compensation for the missing segregation of duties under A.5.3.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.8.16 **Monitoring activities: Networks, systems and applications are monitored for anomalous behaviour and appropriate action is taken to evaluate potential security incidents.**

What proves it: New in the 2022 edition. Workable without a security team of your own: identity provider alerts on impossible travel and on series of failed attempts, cloud platform alerts on unusual spend or permission changes, forwarded to a monitored mailbox with a defined response time. Evidence through the alert rules plus examples of alerts that were handled.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.8.17 **Clock synchronization: All systems that write logs take their time from a defined, trusted source, so that events can be put in the correct order across systems.**

What proves it: NTP configuration on servers and endpoints, and a uniform time zone in the logs (ideally UTC). Without synchronized time, reconstructing an incident under A.5.28 does not hold up; a configuration extract is enough as evidence.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.8.18 **Use of privileged utility programs: The use of utility programs that can override system protections is restricted and tightly controlled.**

What proves it: A list of approved administration tools, restriction of local administrator rights, application control (allowlisting) where possible, and logging of use. Evidence: the policy plus the configuration of the rights management.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.8.19 **Installation of software on operational systems: Procedures and measures for securely managing software installation on operational systems are implemented.**

What proves it: Only approved software from trusted sources, installation through central distribution or a package manager, a rollback path and retention of the previous version. Evidence through the approval list and deployment logs.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.8.20 **Networks security: Networks and active network devices have a named owner, a hardened configuration and a traceable rule set defining which traffic is permitted at all.**

What proves it: A firewall rule set following deny by default, documented open ports with a justification, a secure Wi-Fi configuration, and changed default credentials on network devices. Evidence through a rule set export and an external port scan.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.8.21 **Security of network services: Security mechanisms, service levels and management requirements of network services are identified, implemented and monitored.**

What proves it: For each network service in use (VPN, DNS, mail, CDN) document the security commitments and your own configuration, including encryption in transit and the provider's service level commitments. Evidence: a configuration overview plus the contract or the service description.

◯ Open ◯ In progress ◯ Met ◯ Not applicable

Evidence / justification

A.8.22 **Segregation of networks: The network is divided into zones so that services, user groups and systems with different protection needs cannot reach each other unfiltered.**

What proves it: Separate network segments or VLANs for guests, administration and production; in the cloud, separate accounts or virtual networks with security groups. In a home office the workable implementation is a separate network or VLAN for work devices, kept apart from personal devices and smart home technology.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.23 **Web filtering: Access to external websites is managed to reduce exposure to malicious content.**

What proves it: New in the 2022 edition. Achievable with little effort through a filtering DNS service or the web filtering included in the endpoint protection, with blocked categories and logging of blocked requests. Evidence through the filter configuration and a reporting extract.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.24 **Use of cryptography: It is bindingly defined where encryption is applied, with which algorithms, and how keys are generated, stored, rotated and destroyed across their whole life cycle.** Document

What proves it: A cryptography policy with approved algorithms and minimum key lengths, encryption in transit (TLS) and at rest, plus a key management procedure covering generation, storage, rotation and destruction. Evidence through the policy plus the configuration of the key service or vault.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.25 **Secure development life cycle: Rules for the secure development of software and systems are established and applied.**

What proves it: A description of the development process with security touchpoints per phase: requirements, design, implementation, testing, release, operation. For small teams a single page referring to the concrete CI gates and the review obligation is enough.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.26 **Application security requirements: Security requirements for applications are identified, specified and approved during development and acquisition.**

What proves it: Security requirements as explicit items in the requirements list or as a reusable checklist, oriented for example on common application security verification standards. Evidence through tickets or requirements documents with a security angle.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.27 **Secure system architecture and engineering principles: Principles for secure system engineering are established, documented and applied to development activities.**

What proves it: Documented principles such as least privilege, defence in depth, secure defaults, data minimization and a zero trust approach, together with visible application of them in architecture sketches or decision records.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.28 **Secure coding: Secure coding principles are applied in software development.**

What proves it: New in the 2022 edition. Evidence through binding coding rules, static code analysis and secret scanning as mandatory CI gates, use of vetted libraries, and documented code reviews. Where segregation of duties is impossible, enforced automated gates take the place of four-eyes review; justify this and evidence it with the pipeline configuration.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.29 **Security testing in development and acceptance: Security testing processes are defined and implemented within the development life cycle.**

What proves it: Automated security tests in the pipeline (dependency checks, static and dynamic analysis) plus a periodic penetration test where protection needs are elevated. Evidence through dated test reports and the tracking of the findings.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.30 **Outsourced development: Outsourced development activities are directed, monitored and reviewed.**

What proves it: Where development is outsourced, set the security requirements in the contract, secure ownership of the code and the right to review, and run code reviews and security tests before acceptance. Without outsourced development, non-applicability must be justified coherently in the SoA.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.31 **Separation of development, test and production environments: Development, test and production environments are separated and protected.**

What proves it: Separate accounts, projects or namespaces, separate credentials and separate data sets. In combination with A.8.11, ensure that no production data ends up in non-production environments. Evidence through the environment overview and the rights assignment.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.32 **Change management: Changes to information processing facilities and information systems are subject to change management procedures.**

What proves it: A change process with request, impact assessment, testing, approval, implementation and a rollback path. In development teams a pull request pipeline with enforced checks and logged deployments satisfies this point, provided the history is immutable.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.33 **Test information: Test information is appropriately selected, protected and managed.**

What proves it: The principle: no real personal data in test systems. Where that is unavoidable, document the approval, the masking, the access restriction and the deletion after the test. Evidence through the test data concept and the deletion logs.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification

A.8.34 **Protection of information systems during audit testing: Audit tests that involve access to operational systems are planned and agreed with management to avoid disruption to operations.**

What proves it: An audit agreement with a time window, a scope, read-only access where possible, logging of the audit access and approval by management. This applies to penetration tests as well: a written test authorization with a time window and an emergency contact is the evidence.

○ Open ○ In progress ○ Met ○ Not applicable

Evidence / justification