

Requirements to Documents Map

ISO/IEC 27001:2022+A1:2024 and ISO/IEC 42001:2023

Every requirement of both standards — each clause and every Annex A control — matched to the kind of document that typically satisfies it and the evidence it produces. Use it to check your existing documentation for gaps, or as a reference while planning what to build.

This map names document types and evidence generically — it is not tied to any specific template set. "Documented information required" marks where the standard requires something to be retained or available, not merely done.

Compiled by Docply · docply.io — audit-ready compliance documentation for NIS-2, the AI Act, ISO 27001 and ISO 42001.

ISO/IEC 27001 — Clauses 4 to 10

Requirement by requirement. Every management-system clause, matched to the document type that typically satisfies it.

Clause	Requirement	Documented info required	Typical document	Evidence it produces
4 Context of the organization				
4.1	External and internal issues determined	No	Context, scope and management system overview	Context, scope and management system overview
4.1 (A1:2024)	Whether climate change is a relevant issue determined	No	Context, scope and management system overview	Context, scope and management system overview
4.2	Interested parties and their requirements determined	No	Context, scope and management system overview	Context, scope and management system overview
4.2 note (A1:2024)	Climate-related requirements of interested parties considered	No	Context, scope and management system overview	Context, scope and management system overview
4.3	Scope determined and documented	Yes	Context, scope and management system overview	Approved scope statement
4.4	ISMS established and its processes and interactions determined	No	Context, scope and management system overview; Operational planning and control procedure	Operational planning and control procedure
5 Leadership				
5.1	Leadership and commitment demonstrated, a) to h)	No	Context, scope and management system overview	Context, scope and management system overview
5.2	Policy established and documented, communicated, available	Yes	Information security policy	Information security policy
5.3	Roles assigned and communicated; two authorities assigned	No	Context, scope and management system overview	Role assignment record
6 Planning				
6.1.1	Risks and opportunities determined and addressed	No	Risk management procedure	Risk register and treatment plan
6.1.2	Risk assessment process defined	Yes	Risk management procedure	Risk criteria, approved
6.1.3 a-c	Treatment options selected, controls determined, compared with Annex A	Yes	Risk management procedure	Risk register and treatment plan
6.1.3 d	Statement of Applicability produced	Yes	Risk management procedure	Statement of Applicability
6.1.3 e	Risk treatment plan formulated	Yes	Risk management procedure	Risk register and treatment plan

Clause	Requirement	Documented info required	Typical document	Evidence it produces
6.1.3 f	Risk owners approve the plan and accept residual risk	Yes	Risk management procedure	Risk register and treatment plan
6.2	Objectives established, measurable, monitored, communicated, documented	Yes	Objectives and change-planning procedure	Objectives register
6.3	Changes to the ISMS carried out in a planned manner	No	Objectives and change-planning procedure	Change planning record
7 Support				
7.1	Resources determined and provided	No	Competence, awareness and resources procedure	Resource determination
7.2 a-c	Competence determined, ensured, and acquired where lacking	No	Competence, awareness and resources procedure	Competence, awareness and resources procedure
7.2 d	Evidence of competence retained	Yes	Competence, awareness and resources procedure	Competence register
7.3	Awareness of the policy, contribution and implications	No	Competence, awareness and resources procedure	Attendance and content of the activity
7.4	Communications determined: on what, when, with whom, how	No	Document and record control procedure	Communication plan; evidence per line
7.5.1	Documented information required by the standard and by the organization	Yes	Document and record control procedure	Master document list
7.5.2	Creating and updating: identification, format, review and approval	No	Document and record control procedure	Approvals on each document
7.5.3	Control: availability, protection, distribution, storage, versioning, retention; external origin	No	Document and record control procedure	Master list; external-origin list, Annex D
8 Operation				
8.1	Processes planned, criteria established, control implemented	Yes	Operational planning and control procedure	Process inventory and its output records
8.1	Confidence that processes were carried out as planned	Yes	Operational planning and control procedure	The records named per process
8.1	Planned changes controlled; unintended changes reviewed	No	Operational planning and control procedure	Change planning record
8.1	Externally provided processes controlled	No	Operational planning and control procedure; Supplier and cloud security procedure	Supplier and cloud security procedure
8.2	Risk assessments performed at planned intervals; results retained	Yes	Risk management procedure	Risk assessment record; Risk register and treatment plan

Clause	Requirement	Documented info required	Typical document	Evidence it produces
8.3	Treatment plan implemented; results retained	Yes	Risk management procedure	Risk register and treatment plan
9 Performance evaluation				
9.1	What is monitored and measured, by what method, when, by whom, analysed when and by whom	Yes	Performance, audit and management review procedure	Measurement set and its results
9.1	Performance and effectiveness evaluated	Yes	Performance, audit and management review procedure	Evaluation presented at the review
9.2.1	Internal audits at planned intervals	No	Performance, audit and management review procedure	Internal audit programme and report
9.2.2	Programme established: frequency, methods, responsibilities, planning, reporting	Yes	Performance, audit and management review procedure	Internal audit programme and report
9.2.2	Auditors objective and impartial; results reported	Yes	Performance, audit and management review procedure	Independence arrangement; audit reports
9.3.1	Management review at planned intervals	No	Performance, audit and management review procedure	Management review minutes
9.3.2	The ten required inputs considered	No	Performance, audit and management review procedure	Management review minutes
9.3.3	Results include decisions on improvement and change; retained	Yes	Performance, audit and management review procedure	Management review minutes
10 Improvement				
10.1	Continual improvement of suitability, adequacy and effectiveness	No	Nonconformity and improvement procedure	Nonconformity and corrective action register
10.2 a	React: control and correct; deal with the consequences	No	Nonconformity and improvement procedure	Nonconformity and corrective action register
10.2 b	Evaluate the need to eliminate the cause; determine whether it exists elsewhere	No	Nonconformity and improvement procedure	Cause and 'exists elsewhere' columns
10.2 c-e	Implement action; review effectiveness; change the ISMS if needed	No	Nonconformity and improvement procedure	Action and effectiveness columns
10.2 f-g	Evidence of the nature of nonconformities and of the results of corrective action	Yes	Nonconformity and improvement procedure	Nonconformity and corrective action register; Corrective action record

ISO/IEC 27001 — Annex A controls (93)

Grouped by theme. Whether a control is applicable to you is a separate decision, recorded in your Statement of Applicability — this sheet shows where an applicable control is typically implemented.

Control(s)	Subject	Typical document	Record it produces
A.5 Organizational controls (37)			
A.5.1–A.5.4	Policies, roles, segregation of duties, management responsibilities	Information security policy; Context, scope and management system overview; Access control and identity procedure	Approved policy; role assignment
A.5.5–A.5.6	Contact with authorities and with special interest groups	Incident management procedure; Vulnerability and configuration management procedure	Incident management procedure
A.5.7	Threat intelligence	Vulnerability and configuration management procedure	Review records and resulting actions
A.5.8	Security in project management	Secure development and change procedure	Security requirements per project
A.5.9–A.5.11	Inventory, acceptable use, return of assets	Asset and information classification procedure	Asset inventory; Onboarding and exit record
A.5.12–A.5.14	Classification, labelling, transfer	Asset and information classification procedure	Classification decisions; transfer logs
A.5.15–A.5.18	Access control, identity, authentication information, access rights	Access control and identity procedure	Access review record
A.5.19–A.5.23	Supplier relationships, agreements, ICT supply chain, monitoring, cloud	Supplier and cloud security procedure	Supplier and cloud security procedure; Supplier security clauses
A.5.24–A.5.28	Incident planning, assessment, response, learning, evidence	Incident management procedure	Incident record; Incident management procedure
A.5.29–A.5.30	Security during disruption; ICT readiness	Continuity and resilience procedure	Exercise and test records
A.5.31–A.5.34	Legal requirements, intellectual property, records, privacy	Legal and contractual requirements procedure	Legal and contractual requirements register
A.5.35–A.5.37	Independent review, compliance, operating procedures	Performance, audit and management review procedure; Document and record control procedure; Operations security procedure	Audit reports; the procedures themselves
A.6 People controls (8)			
A.6.1–A.6.2	Screening; terms of employment	Human resources security procedure	Onboarding and exit record
A.6.3	Awareness, education and training	Competence, awareness and resources procedure	Competence register
A.6.4–A.6.5	Disciplinary process; responsibilities after termination	Human resources security procedure	Onboarding and exit record

Control(s)	Subject	Typical document	Record it produces
A.6.6	Confidentiality agreements	Human resources security procedure; Confidentiality statement	Accepted terms; signed statements
A.6.7	Remote working	Human resources security procedure	Device compliance reports
A.6.8	Event reporting	Incident management procedure	Incident record
A.7 Physical controls (14)			
A.7.1–A.7.4	Perimeters, entry, securing facilities, monitoring	Physical and environmental security procedure	Physical and environmental security procedure
A.7.5–A.7.7	Environmental threats, secure areas, clear desk and screen	Physical and environmental security procedure	Threat assessment; walkthrough findings
A.7.8–A.7.10	Siting, assets off premises, storage media	Physical and environmental security procedure	Siting decisions; media disposal records
A.7.11–A.7.14	Utilities, cabling, maintenance, disposal of equipment	Physical and environmental security procedure	Resilience tests; maintenance and disposal records
A.8 Technological controls (34)			
A.8.1	User endpoint devices	Human resources security procedure	Device management compliance report
A.8.2–A.8.5	Privileged access, access restriction, source code, secure authentication	Access control and identity procedure	Access review record
A.8.6–A.8.7	Capacity; malware	Operations security procedure	Capacity reviews; detection events
A.8.8–A.8.9	Vulnerabilities; configuration	Vulnerability and configuration management procedure	Configuration baselines register
A.8.10–A.8.12	Deletion, masking, leakage prevention	Operations security procedure	Deletion records; DLP alerts
A.8.13–A.8.14	Backup; redundancy	Continuity and resilience procedure	Restore test records
A.8.15–A.8.17	Logging, monitoring, clock synchronisation	Logging and monitoring procedure	Logs; alert triage records
A.8.18–A.8.19	Privileged utilities; software on operational systems	Operations security procedure; Vulnerability and configuration management procedure	Utility inventory; installation records
A.8.20–A.8.23	Networks, network services, segregation, web filtering	Operations security procedure	Operations security procedure
A.8.24	Cryptography	Operations security procedure	Key management logs
A.8.25–A.8.31	Secure development through separation of environments	Secure development and change procedure	Review evidence; test results
A.8.32	Change management	Secure development and change procedure	Change records
A.8.33–A.8.34	Test information; protection during audit testing	Secure development and change procedure; Operations security procedure	Authorisations for production data and for testing

ISO/IEC 42001 — Clauses 4 to 10

Requirement by requirement, for the AI management system standard.

Clause	What you need to have	Must be written down	Typical document	Where it's recorded
4.1	A record of the internal and external issues that affect your AI management system, including whether climate change is a relevant issue for you, and your role with respect to each AI system (provider, deployer, or both)	No	AI management system manual and scope	AI management system manual and scope
4.2	The interested parties relevant to your AI systems, what they require of you, and which of those requirements you will address through the management system	No	AI management system manual and scope; Legal, regulatory and contractual requirements procedure	AI management system manual and scope
4.3	A defined scope: which parts of the organisation, which activities and which AI systems the management system covers	Yes	AI management system manual and scope	AI management system manual and scope
4.4	The management system itself, established and documented, including the processes and how they interact	No	AI management system manual and scope	The kit as a whole
5.1	Evidence that top management is actually leading this: resources made available, the system integrated into how the business runs, direction given	No	AI management system manual and scope	Management review minutes
5.2	An AI policy approved by top management, appropriate to what you do, communicated internally and available to interested parties	Yes	AI policy	AI policy
5.3	Roles and responsibilities assigned and communicated, including who reports on the system's performance to top management	No	AI management system manual and scope	AI management system manual and scope
6.1.1	Risk criteria that let you tell an acceptable risk from an unacceptable one, plus the actions you decided to take on risks and opportunities	Yes	AI risk management procedure	AI risk register and treatment plan
6.1.2	A defined AI risk assessment process that produces consistent, comparable results when repeated	Yes	AI risk management procedure	AI risk management procedure
6.1.3	A risk treatment process, a Statement of Applicability covering all 38 Annex A controls with your reasons for including or excluding each, and a risk treatment plan approved by management	Yes	AI risk management procedure	AI risk register and treatment plan; Statement of Applicability
6.1.4	A process for assessing the consequences your AI systems can have on individuals, groups and society — and the documented result of each assessment	Yes	AI system impact assessment procedure	AI system impact assessment record
6.2	AI objectives that are measurable where practicable, monitored, communicated and updated, with a plan saying what will be done, by whom, by when and how it will be evaluated	Yes	AI objectives and change-planning procedure; Legal, regulatory and contractual requirements procedure	Objectives register

Clause	What you need to have	Must be written down	Typical document	Where it's recorded
6.3	Changes to the management system carried out in a planned way, not improvised	No	AI objectives and change-planning procedure	AI objectives and change-planning procedure
7.1	The resources the system needs, determined and provided	No	Competence and AI resources procedure	AI resources register
7.2	The competence needed for work that affects AI performance, and evidence that the people doing it have it	Yes	Competence and AI resources procedure	Competence register
7.3	People aware of the AI policy, of how their work contributes, and of what happens if the system is not followed	No	Competence and AI resources procedure	Competence register
7.4	Decisions on what you communicate about the system, when, to whom and how	No	Document and record control procedure	Document and record control procedure
7.5	Documented information controlled: identified, in a usable format, reviewed and approved, protected, versioned and retained	Yes	Document and record control procedure	Document and record control procedure
8.1	Operational planning and control: criteria for the processes, control applied against those criteria, and enough evidence to be confident they were followed	Yes	AI system life cycle procedure	AI system life cycle record
8.2	AI risk assessments performed at planned intervals and whenever something significant changes, with the results kept	Yes	AI risk management procedure	AI risk register and treatment plan
8.3	The risk treatment plan implemented and its effectiveness verified, with the results kept	Yes	AI risk management procedure	AI risk register and treatment plan
8.4	Impact assessments performed at planned intervals and on significant change, with the results kept	Yes	AI system impact assessment procedure	AI system impact assessment record
9.1	What you monitor and measure, by which method, when, and who analyses it — with the results kept as evidence	Yes	Performance, audit and management review procedure	Objectives register
9.2	An internal audit programme covering frequency, methods, responsibilities and reporting, with auditors chosen to be objective, and the audit results kept	Yes	Performance, audit and management review procedure	Internal audit programme and report
9.3	Management review at planned intervals covering the required inputs, with decisions on improvement and on changes to the system, and the results kept	Yes	Performance, audit and management review procedure	Management review minutes
10.1	Continual improvement of the suitability, adequacy and effectiveness of the system	No	Nonconformity and improvement procedure	Management review minutes
10.2	Nonconformities reacted to and their causes evaluated, corrective action taken and reviewed, with the nature of each nonconformity and the results kept	Yes	Nonconformity and improvement procedure	Nonconformity and corrective action register

ISO/IEC 42001 — Annex A controls (38)

Annex B of ISO 42001 is normative — the implementation guidance is part of the standard itself.

Control	Title	Typical document	Where it's recorded
A.2 — Policies related to AI			
A.2.2	AI policy	AI policy	AI policy
A.2.3	Alignment with other organizational policies	AI policy	AI policy
A.2.4	Review of the AI policy	AI policy	Management review minutes
A.3 — Internal organization			
A.3.2	AI roles and responsibilities	AI management system manual and scope	AI management system manual and scope
A.3.3	Reporting of concerns	Concerns and AI incidents procedure	Concern and incident record
A.4 — Resources for AI systems			
A.4.2	Resource documentation	Competence and AI resources procedure	AI system inventory; AI resources register
A.4.3	Data resources	Competence and AI resources procedure	AI resources register
A.4.4	Tooling resources	Competence and AI resources procedure	AI resources register
A.4.5	System and computing resources	Competence and AI resources procedure	AI resources register
A.4.6	Human resources	Competence and AI resources procedure	AI resources register; Competence register
A.5 — Assessing impacts of AI systems			
A.5.2	AI system impact assessment process	AI system impact assessment procedure	AI system impact assessment procedure
A.5.3	Documentation of AI system impact assessments	AI system impact assessment procedure	AI system impact assessment record
A.5.4	Assessing AI system impact on individuals or groups of individuals	AI system impact assessment procedure	AI system impact assessment record
A.5.5	Assessing societal impacts of AI systems	AI system impact assessment procedure	AI system impact assessment record
A.6.1 — Management guidance for AI system development			
A.6.1.2	Objectives for responsible development of AI system	AI objectives and change-planning procedure	Objectives register
A.6.1.3	Processes for responsible AI system design and development	AI system life cycle procedure	AI system life cycle procedure
A.6.2 — AI system life cycle			
A.6.2.2	AI system requirements and specification	AI system life cycle procedure	AI system life cycle record

Control	Title	Typical document	Where it's recorded
A.6.2.3	Documentation of AI system design and development	AI system life cycle procedure	AI system life cycle record
A.6.2.4	AI system verification and validation	AI system life cycle procedure	AI system life cycle record
A.6.2.5	AI system deployment	AI system life cycle procedure	AI system life cycle record
A.6.2.6	AI system operation and monitoring	Operation, monitoring and logging procedure	Operation, monitoring and logging procedure
A.6.2.7	AI system technical documentation	Transparency and information procedure	AI system technical documentation
A.6.2.8	AI system recording of event logs	Operation, monitoring and logging procedure	Operation, monitoring and logging procedure
A.7 — Data for AI systems			
A.7.2	Data for development and enhancement of AI system	Data management procedure	Data management procedure
A.7.3	Acquisition of data	Data management procedure	AI resources register
A.7.4	Quality of data for AI systems	Data management procedure	Data provenance and quality record
A.7.5	Data provenance	Data management procedure	Data provenance and quality record
A.7.6	Data preparation	Data management procedure	Data provenance and quality record
A.8 — Information for interested parties of AI systems			
A.8.2	System documentation and information for users	Transparency and information procedure	Information for users
A.8.3	External reporting	Transparency and information procedure	Concern and incident record
A.8.4	Communication of incidents	Concerns and AI incidents procedure	Concerns and AI incidents procedure
A.8.5	Information for interested parties	Document and record control procedure	Document and record control procedure
A.9 — Use of AI systems			
A.9.2	Processes for responsible use of AI systems	Operation, monitoring and logging procedure	Operation, monitoring and logging procedure
A.9.3	Objectives for responsible use of AI system	AI objectives and change-planning procedure	Objectives register
A.9.4	Intended use of the AI system	Operation, monitoring and logging procedure	Operation, monitoring and logging procedure
A.10 — Third-party and customer relationships			
A.10.2	Allocating responsibilities	Third parties, suppliers and customers procedure	Supplier and responsibility register
A.10.3	Suppliers	Third parties, suppliers and customers procedure	Supplier and responsibility register
A.10.4	Customers	Third parties, suppliers and customers procedure	Third parties, suppliers and customers procedure