Kyūdō

SOVEREIGNTY-GRADE AI · GRC

ISO 27001 Implementation Guide

Vigilance with Purpose. Security with Control.

PRESENTED BY

Kyūdō — a KMicro Technologies platform

3525-265 Hyland Avenue

Costa Mesa, CA 92626 · kyudo.ai

hello@kyudo.ai

kyudo.ai · April 2026

CLASSIFICATION: PUBLIC

00 · READ THIS FIRST

ISO 27001 is a management system, not a control checklist.

This is the single mistake that derails more ISO 27001 implementations than any other. Teams treat the standard as a list of 93 Annex A controls to implement and produce evidence for. The auditor arrives expecting an Information Security Management System — a living, governed, continuously improving capability with documented context, leadership commitment, planned objectives, operational discipline, performance evaluation, and demonstrable improvement — and what the team has assembled is a folder of policies and a spreadsheet of controls. The certification audit does not go well.

The standard itself is structured to prevent this confusion. Clauses 4 through 10 — Context, Leadership, Planning, Support, Operation, Performance Evaluation, and Improvement — define the management system that every ISO 27001-certified organization must build. Annex A is a reference catalog of 93 controls that an organization may select from, justify, and implement to treat the risks identified by the management system. Clauses are the ‘what.’ Annex A is one possible ‘how.’ The certification opinion is on the management system.

This guide is structured the same way. Section 1 establishes ISO 27001:2022 as it stands in 2026 — post-transition, post-October 2025 deadline, with the 93-control Annex A as the only valid version. Section 2 walks Clauses 4 through 10 with the documentation each clause requires and the auditor's actual expectations. Section 3 covers Annex A: the four themes, the eleven new controls introduced in 2022, and the Statement of Applicability. Section 4 maps Annex A to the Microsoft Security stack control by control. Section 5 is the Statement of Applicability mechanics in detail — the single most important document in the ISMS from an audit perspective. Section 6 is the certification cycle: Stage 1, Stage 2, surveillance, recertification. Section 7 is the twelve-month implementation timeline. Section 8 is the Kyūdō continuous-readiness model applied to the ISMS.

If you read nothing else, read Section 2 and Section 5. Most certification failures trace back to a weak management system or a Statement of Applicability that does not survive scrutiny.

> **This guide reflects ISO/IEC 27001:2022 in the post-transition reality**
>
> The October 31, 2025 transition deadline has passed. ISO/IEC 27001:2013 certificates issued before that date are no longer valid. All initial certifications and recertifications now occur against ISO/IEC 27001:2022, with Annex A organized as 93 controls in 4 themes (Organizational, People, Physical, Technological).
>
> Engage an accredited certification body to conduct your audit. This guide is a practitioner reference, not a substitute for the ISO standards.

01 · FOUNDATIONS

ISO 27001:2022, in the post-transition reality.

The standard, in one paragraph

ISO/IEC 27001 is the international standard for information security management systems, published by the International Organization for Standardization and the International Electrotechnical Commission. The current version, ISO/IEC 27001:2022, was published on October 25, 2022. It specifies requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. Certification is performed by accredited certification bodies and is valid for a three-year cycle, with annual surveillance audits and a full recertification audit at the end of the cycle.

ISO 27001 vs. ISO 27002 — keep them straight

ISO/IEC 27001:2022 is the certifiable standard. It contains the management-system requirements (Clauses 4–10) and Annex A, which lists the 93 reference controls. ISO/IEC 27002:2022 is the companion implementation guidance. It elaborates each Annex A control with purpose, attributes, and implementation guidance. Organizations are certified against ISO 27001; they consult ISO 27002 to understand how to implement the controls they selected. The two standards are released together but serve different purposes.

The 2022 revision in one table

The 2022 revision is best understood as a modernization, not a rewrite. The management-system clauses received minor clarifications. Annex A was substantially restructured — not because the security objectives changed, but because the 2013 organization had become unwieldy as cloud, remote work, and modern threat landscapes evolved.

Dimension	ISO 27001:2013 (no longer valid)	ISO 27001:2022 (current standard)
Annex A controls	114 controls	93 controls
Annex A structure	14 domains (A.5 through A.18)	4 themes (A.5 Organizational, A.6 People, A.7 Physical, A.8 Technological)
New controls	—	11 new controls; 24 merged from 57; 58 minor updates; no controls removed

Dimension	ISO 27001:2013 (no longer valid)	ISO 27001:2022 (current standard)
Control attributes	None	5 attributes per control: control type, information security properties, cybersecurity concepts, operational capabilities, security domains
Management clauses	Clauses 4–10	Clauses 4–10, with new Clause 6.3 (Planning of changes) and refined Clause 9.3 (Management review)
Validity	Certificates expired October 31, 2025	Three-year cycle from initial certification, renewed every three years

Sources — ISO/IEC 27001:2022; ISO/IEC 27002:2022; IAF Mandatory Document IAF MD 26.

Organizations that did not transition before October 31, 2025 lost their certification. Those organizations must now pursue full Stage 1 plus Stage 2 initial certification against ISO/IEC 27001:2022 — not a transition audit. This is more time, more cost, and more disruption than a transition would have been. If your organization is in this situation, the timeline in Section 7 of this guide applies.

The four themes of Annex A:2022

Annex A:2022 contains 93 controls organized into four themes. Each theme corresponds to a domain of accountability: organizational policies and processes, people behavior and capability, physical and environmental protections, and technical implementations.

Theme	Count	What it covers
A.5 Organizational	37	Information security policies, roles and responsibilities, segregation of duties, supplier relationships, threat intelligence, cloud services governance, ICT readiness, incident management, legal and regulatory requirements, intellectual property, and similar organization-level governance topics.
A.6 People	8	Screening, terms and conditions of employment, awareness and training, disciplinary process, responsibilities after termination or change of employment, confidentiality and non-disclosure agreements, remote working, information security event reporting.
A.7 Physical	14	Physical security perimeters, physical entry, securing offices and facilities, monitoring physical access, protecting against environmental threats, working in secure areas, clear desk and

Theme	Count	What it covers
		screen policy, equipment siting and protection, security of assets off-premises, storage media, supporting utilities, cabling, equipment maintenance, and secure disposal or re-use of equipment.
A.8 Technological	34	User endpoint devices, privileged access rights, information access restriction, identity management, authentication, capacity management, protection against malware, technical vulnerability management, configuration management, information deletion, data masking, data leakage prevention, monitoring, web filtering, secure development, secure coding, network controls, cryptography, backup, redundancy, logging, source code, and the rest of the technical control surface.

Source — ISO/IEC 27001:2022 Annex A; ISO/IEC 27002:2022 control descriptions.

The 11 new controls introduced in 2022

Eleven controls in Annex A:2022 had no direct equivalent in the 2013 version. Each addresses a gap that emerged as cloud, hybrid work, supply-chain attacks, and modern data protection regulations changed the threat landscape. Treat these as priority items in any new ISO 27001 implementation — they are the areas where the auditor will pay closest attention to your design choices.

Control	Title	What it expects
A.5.7	Threat intelligence	Collect, analyze, and use information about information security threats. Practitioner test: can you produce the threat-intelligence inputs that informed your last risk assessment update?
A.5.23	Information security for use of cloud services	Establish processes for acquisition, use, management, and exit from cloud services. Test: do you have a documented cloud-services lifecycle that includes onboarding, security review, ongoing monitoring, and offboarding with data deletion evidence?
A.5.30	ICT readiness for business continuity	ICT readiness should be planned, implemented, maintained, and tested based on business continuity objectives. Test: does your BCP/DR program have ICT-specific recovery objectives and a tested recovery plan, not just a paper continuity plan?
A.7.4	Physical security	Monitor sensitive areas to allow only authorized

Control	Title	What it expects
	monitoring	people to access them. Test: do you have evidence of monitoring (CCTV, access logs, guard rounds) over the audit period?
A.8.9	Configuration management	Configurations of hardware, software, services, and networks should be established, documented, implemented, monitored, and reviewed. Test: do you have a configuration baseline, documented exceptions, and drift detection?
A.8.10	Information deletion	Information stored in systems, devices, or other storage media should be deleted when no longer required. Test: can you produce evidence of deletion against a documented retention schedule?
A.8.11	Data masking	Data masking should be used to protect sensitive data, in line with the organization's policy on access control and topic-specific policies. Test: where you handle sensitive data, do non-production environments use masked or synthetic data?
A.8.12	Data leakage prevention	Data leakage prevention measures should be applied to systems, networks, and devices that process, store, or transmit sensitive information. Test: do you have DLP coverage on the channels where sensitive data could exfiltrate — email, endpoint, cloud, web?
A.8.16	Monitoring activities	Networks, systems, and applications should be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents. Test: do you have a SIEM with tuned rules and documented alert handling?
A.8.23	Web filtering	Access to external websites should be managed to reduce exposure to malicious content. Test: do you have web filtering deployed with a documented allow/deny policy?
A.8.28	Secure coding	Secure coding principles should be applied to software development. Test: do you have secure-coding training, code-review checklists, and SAST/DAST scanning in your development

Control	Title	What it expects
		pipeline?

Sources — ISO/IEC 27001:2022 Annex A; ISO/IEC 27002:2022 implementation guidance.

Control attributes — useful, not mandatory

ISO/IEC 27002:2022 introduces five attributes for each Annex A control. The attributes are not required for ISO 27001 certification, but they are powerful for control selection, risk treatment planning, and cross-framework mapping.

Attribute	Values
Control type	Preventive, Detective, Corrective
Information security properties	Confidentiality, Integrity, Availability
Cybersecurity concepts	Identify, Protect, Detect, Respond, Recover (mirrors NIST CSF functions)
Operational capabilities	Governance, Asset management, Information protection, Human resource security, Physical security, System and network security, Application security, Secure configuration, Identity and access management, Threat and vulnerability management, Continuity, Supplier relationships security, Legal and compliance, Information security event management, Information security assurance
Security domains	Governance and ecosystem, Protection, Defence, Resilience

In practice, the cybersecurity-concepts attribute is the most useful for organizations that already operate against NIST CSF — the Identify/Protect/Detect/Respond/Recover language is identical. The operational-capabilities attribute is the most useful for control selection during the Statement of Applicability process.

Clauses 4 through 10 — the part the auditor actually certifies.

The certification opinion is on the management system. Annex A controls support the management system; they do not constitute it. This section walks each clause, the documented information it requires, and what the auditor will look for.

Clause 4 — Context of the organization

Establish what the organization is, what it does, and the internal and external issues that affect the ISMS. Identify interested parties — customers, regulators, employees, suppliers, partners — and document their requirements relevant to information security. Define the scope of the ISMS in terms that name what is in and what is out, with the rationale.

Required documented information

- Documented scope of the ISMS, including products, services, locations, and any boundaries with respect to other parts of the organization or third parties.
- Documented analysis of internal and external issues affecting information security.
- Documented analysis of interested parties and their requirements.

What the auditor checks

The auditor will read the scope statement first. If the scope is ambiguous, contradicts the marketing posture (‘we are ISO 27001 certified’ with a scope that excludes the product the customer is buying), or excludes obviously material parts of the business, that is a Stage 1 finding. The scope must be precise, defensible, and consistent with how the organization presents itself externally.

Clause 5 — Leadership

Top management must demonstrate leadership and commitment to the ISMS. Establish an information security policy. Assign roles, responsibilities, and authorities. Ensure resources are available.

Required documented information

- Information security policy, approved by top management.
- Documented assignment of information-security roles and responsibilities.

What the auditor checks

The auditor will interview top management. The interview is not a formality. The auditor is testing whether leadership commitment is real or pro-forma. Top management is expected to know the scope of the ISMS, the principal information-security risks the organization faces, the

policy, and the broad outline of how the ISMS is operating. ‘My CISO handles all that’ is not a passing answer. The auditor will also confirm that resources — budget, staffing, tools — are actually committed and not aspirational.

Clause 6 — Planning

This is the most consequential clause. Plan how the organization will identify, assess, and treat information security risks, and how it will set and pursue information security objectives. Clause 6 is also where the new Clause 6.3 — Planning of changes — lives, requiring controlled-change management for the ISMS itself.

Required documented information

- Information security risk assessment process.
- Information security risk treatment process and the resulting risk treatment plan.
- Statement of Applicability (SoA) — see Section 5 of this guide for detailed treatment.
- Information security objectives and plans to achieve them.
- Documented information related to changes that affect the ISMS (Clause 6.3).

What the auditor checks

The auditor will inspect the risk assessment methodology and apply it to a sampled risk to confirm the methodology is followed in practice, not just documented. Risks must connect to controls in the SoA, and controls in the SoA must produce evidence of operation in Clause 8 (Operation). Information security objectives must be measurable, time-bound, and connected to actual measurement evidence in Clause 9 (Performance evaluation). Changes to the ISMS — new products, new locations, new subservice organizations, new processing activities — must trigger documented change-management activity in the ISMS itself.

> **Where Clause 6 most often fails**
>
> Risk register that is a snapshot in time, not a live document. Auditors expect to see updates over the period: new risks added, risks treated and closed, residual risk reassessed.
>
> Risk treatment plan that does not connect risks to specific controls. Each risk must trace to one or more controls in the SoA, and the SoA must justify whether the control is included or excluded.
>
> Information security objectives that are vague or unmeasurable. ‘Improve our security posture’ is not an objective. ‘Reduce mean-time-to-detect for high-severity incidents from 4 hours to 1 hour by Q4’ is.
>
> Changes to the ISMS that happen without documented planning under Clause 6.3 — a new region added without a risk reassessment, a new processor onboarded without an SoA update, a new product line shipped without an updated risk treatment plan.

Clause 7 — Support

Resources, competence, awareness, communication, and documented information. The infrastructure that the management system runs on.

Required documented information

- Evidence of competence (training records, certifications, qualifications) for personnel performing work that affects information security performance.
- Documented information determined necessary for the effectiveness of the ISMS, with version control, review, and retention.
- Records of awareness activities.

What the auditor checks

Document control is a recurring finding source. Documents must be versioned, dated, approved by named owners, reviewed on a defined cadence, and protected from unintended changes. The auditor will sample a policy and ask: who approved it, when, what is the next review date, where is the previous version, and what changed. Awareness training must be evidenced — a training record per individual, with completion dates — not a slide deck on SharePoint.

Clause 8 — Operation

Plan, implement, and control the processes needed to meet the ISMS requirements. Implement the actions determined in Clause 6.1, including the risk treatment plan. Control planned changes and review the consequences of unintended changes. Address externally provided processes, products, or services that are relevant to the ISMS.

Required documented information

- Evidence that the planned processes have been performed as planned.
- Records of risk assessments performed.
- Records of risk treatment activities performed.

What the auditor checks

Clause 8 is where the management system meets reality. The auditor verifies that the things planned in Clause 6 are actually happening: risk assessments are being performed on the documented cadence, risk treatments are being executed, controls in the SoA are operating, and changes are being managed. Sampling here resembles SOC 2 Type II practice — the auditor will test operating effectiveness over the audit period for a sampled set of processes and controls.

Clause 9 — Performance evaluation

Monitor, measure, analyze, and evaluate the performance and effectiveness of the ISMS. Conduct internal audits at planned intervals. Conduct management reviews.

Required documented information

- Evidence of monitoring and measurement results.

- Internal audit program and internal audit results.
- Management review minutes, including inputs and outputs.

What the auditor checks

Internal audit is the most-frequently-cited Clause 9 finding source. The internal audit program must cover the entire ISMS over a defined cycle (typically annual), be performed by competent and independent auditors (‘independent’ means the auditor does not audit their own work, not that the auditor must be external), and produce documented findings that are tracked to closure. Management review must be performed at planned intervals — typically at least annually — with documented inputs (audit results, performance metrics, risk register status, status of objectives, changes in interested parties' requirements) and documented outputs (decisions, resource allocations, opportunities for improvement).

Clause 9.3.2 (revised in 2022) added ‘changes in needs and expectations of interested parties relevant to the information security management system’ as a mandatory management review input. Auditors check for it explicitly.

Clause 10 — Improvement

Continually improve the suitability, adequacy, and effectiveness of the ISMS. When a nonconformity occurs, react to it, evaluate it, take action to eliminate the cause, implement the action, review effectiveness, and update the ISMS as needed.

Required documented information

- Records of nature of nonconformities and any subsequent actions taken.
- Records of the results of any corrective action.

What the auditor checks

Nonconformities can come from internal audits, customer complaints, security incidents, supplier issues, or external audits (including the certification audit itself). Each must be logged, investigated for root cause, corrected, and verified to confirm the correction was effective. The corrective-action register is one of the artifacts the auditor will sample most heavily — it tells the story of whether the ISMS is genuinely improving or whether issues are being closed without addressing root cause.

The 93 controls, the four themes, and how to think about selection.

Annex A is a reference catalog. The organization is not required to implement all 93 controls. The organization is required to select controls based on the risk treatment plan, document its selections in the Statement of Applicability with justification, and implement the selected controls. This is the structural difference between ISO 27001 and frameworks that prescribe a fixed control set.

This section walks each theme with the specific controls that are most consequential for organizations on the Microsoft Security stack — not because the others can be ignored, but because these are the ones where the auditor's questions will be most pointed and where Microsoft-stack organizations have the strongest native evidence to produce.

A.5 Organizational controls (37)

The largest theme. Organizational controls cover the policy and process layer that shapes information security across the enterprise.

Most consequential A.5 controls

Control	Title	What auditors look for
A.5.1	Policies for information security	Approved, communicated information security policies, reviewed at planned intervals; topic-specific policies (acceptable use, access control, cryptography, supplier security, etc.).
A.5.7	Threat intelligence (NEW 2022)	Documented threat-intelligence inputs feeding the risk assessment process; sources include vendor advisories, ISAC/ISAO feeds, government alerts, internal incident learnings.
A.5.9	Inventory of information and other associated assets	A maintained inventory of assets in scope; asset owners assigned; classification applied.
A.5.15	Access control	Topic-specific access control policy, approved and applied. Role-based access, least privilege, and segregation of duties.
A.5.19–5.22	Supplier relationships (4 controls)	Information security in supplier agreements; addressing security in supplier contracts; managing supplier services; managing changes to supplier services. Live, monitored

Control	Title	What auditors look for
		vendor program — not a one-time questionnaire.
A.5.23	Information security for use of cloud services (NEW 2022)	Documented cloud-services lifecycle: acquisition, use, management, exit. Evidence of security review at onboarding and exit including data deletion.
A.5.24–5.28	Information security incident management (5 controls)	Documented incident response, classification, evidence handling, learning from incidents. Tested incident response procedure with evidence of execution within the audit period.
A.5.30	ICT readiness for business continuity (NEW 2022)	ICT continuity requirements derived from BIA; documented ICT continuity plans; tested within the audit period.
A.5.36	Compliance with policies, rules, and standards for information security	Periodic review of compliance with policies; nonconformities raised and tracked to closure.
A.5.37	Documented operating procedures	Operating procedures for information processing facilities, available to those who need them and reviewed for accuracy.

A.6 People controls (8)

The smallest theme by count, the one most likely to surface findings during interviews. People controls are tested by talking to people — not by reading documents.

Most consequential A.6 controls

Control	Title	What auditors look for
A.6.1	Screening	Background verification appropriate to the role, business requirements, and the classification of information accessed.
A.6.3	Information security awareness, education, and training	Awareness program reaching all personnel and relevant interested parties, with completion records and refresher training.
A.6.5	Responsibilities after termination or change of employment	Documented procedure ensuring rights, equipment, and information are recovered or transferred when personnel leave or change roles.

Control	Title	What auditors look for
A.6.6	Confidentiality or non-disclosure agreements	Signed NDAs in place; periodic review for currency; replacement when terms change.
A.6.7	Remote working	Topic-specific remote-working policy addressing endpoints, network, physical environment, and incident reporting.
A.6.8	Information security event reporting	Channels for reporting events; awareness that channels exist; evidence of reports being received and triaged.

A.7 Physical controls (14)

Physical controls apply to the organization's own facilities. For cloud-native organizations, most physical controls are inherited from the cloud provider — Azure, in the case of Microsoft-stack organizations — and the inheritance is documented through the Azure ISO 27001 certificate, the Service Trust Portal, and shared-responsibility documentation. Physical controls for the organization's corporate offices and any on-premises infrastructure remain in scope.

Most consequential A.7 controls

Control	Title	What auditors look for
A.7.2	Physical entry	Controlled physical entry to areas containing information assets. For corporate offices, badged access and visitor management; for cloud, inherited from the provider's certified controls.
A.7.4	Physical security monitoring (NEW 2022)	CCTV, access logs, or guard rounds for sensitive areas; evidence over the audit period.
A.7.7	Clear desk and clear screen	Policy and observed practice. Auditors do walk the floor.
A.7.10	Storage media	Inventory and lifecycle management of removable media; secure disposal procedures.
A.7.14	Secure disposal or re-use of equipment	Documented procedures for disposing of equipment containing storage media, with evidence of disposal certificates.

A.8 Technological controls (34)

The largest theme by control density. This is where most of the Microsoft-native evidence sources concentrate, and where the cross-mapping to other frameworks (SOC 2 CC6–CC8, NIST CSF Protect/Detect, CMMC L2 technical controls) is densest.

Most consequential A.8 controls

Control	Title	What auditors look for
A.8.1	User endpoint devices	Inventory, configuration baselines, encryption, and management of endpoints; topic-specific policy.
A.8.2	Privileged access rights	Management of privileged access; just-in-time elevation preferred; periodic review of privileged accounts.
A.8.3	Information access restriction	Access to information restricted in line with topic-specific access-control policy; logical and physical controls aligned.
A.8.5	Secure authentication	MFA, strong authentication for privileged and remote access, password policies aligned to current best practice.
A.8.7	Protection against malware	Endpoint protection, EDR/XDR, mail gateway protection, and user awareness.
A.8.8	Management of technical vulnerabilities	Vulnerability identification, prioritization, and remediation with documented SLAs by severity.
A.8.9	Configuration management (NEW 2022)	Documented baselines for hardware, software, services, and networks; drift detection; change-managed exceptions.
A.8.10	Information deletion (NEW 2022)	Retention schedule; evidence of deletion against the schedule, including from cloud services and backups.
A.8.11	Data masking (NEW 2022)	Masking, anonymization, or pseudonymization for sensitive data in non-production or analytics contexts.
A.8.12	Data leakage prevention (NEW 2022)	DLP policies and controls covering email, endpoint, cloud, and web channels.
A.8.15	Logging	Logs covering activities, exceptions, and information security events; protection from

Control	Title	What auditors look for
		tampering; retention aligned to legal and contractual requirements.
A.8.16	Monitoring activities (NEW 2022)	Monitoring of networks, systems, and applications for anomalous behavior; SIEM with documented analytic rules; alert handling and escalation.
A.8.20–8.22	Network controls (3 controls)	Network security; segregation; restrictions on network connections.
A.8.23	Web filtering (NEW 2022)	Web filtering deployed; documented allow/deny policy; bypass procedures controlled.
A.8.24	Use of cryptography	Topic-specific cryptography policy; key management; encryption at rest and in transit.
A.8.25–8.32	Secure development (8 controls including 8.28 Secure coding NEW 2022)	Secure development lifecycle; environment separation; code review; SAST/DAST; secure coding training; controlled changes; outsourced development oversight.
A.8.33–8.34	Test information; protection of information systems during audit testing	Test data protection; controls for audit-testing activities to avoid disrupting production.

From Annex A control to native Microsoft signal.

This section maps the highest-frequency Annex A controls to the specific Microsoft service that produces the evidence. It is not exhaustive — it covers the controls where Microsoft-native evidence is the most defensible and direct path. Where your environment includes additional sources, those become supplementary evidence for the same controls.

Identity, access, and authentication (A.5.15, A.8.2, A.8.3, A.8.5)

Annex A control	Microsoft signal source
A.5.15 Access control	Microsoft Entra ID role assignments, group membership policies, Conditional Access policy export, access-package definitions in Entra ID Governance.
A.8.2 Privileged access rights	Microsoft Entra Privileged Identity Management activation logs, role assignment audit logs, JIT activation records, privileged access reviews.
A.8.3 Information access restriction	Microsoft Purview sensitivity labels enforced via Conditional Access, SharePoint sensitivity-label policies, restricted-access policies in M365 apps.
A.8.5 Secure authentication	Entra Conditional Access policies enforcing MFA, Entra ID sign-in logs filtered by authentication method, FIDO2 / passwordless adoption metrics.

Threat detection, monitoring, and incident management (A.5.7, A.5.24–5.28, A.8.7, A.8.15, A.8.16)

Annex A control	Microsoft signal source
A.5.7 Threat intelligence (NEW)	Microsoft Defender Threat Intelligence; Sentinel threat-intelligence connectors; Defender XDR threat analytics; documented use of these inputs in risk assessment.
A.5.24–5.28 Incident management (5 controls)	Microsoft Sentinel incidents (status, ownership, evidence, RCA), Defender XDR investigations, automated playbook executions, after-action reports linked to specific incidents.

Annex A control	Microsoft signal source
A.8.7 Protection against malware	Microsoft Defender for Endpoint (EDR posture, alert handling, automated investigation outcomes), Defender for Office 365 (mail-based threat protection), Defender Antivirus configuration baselines.
A.8.15 Logging	Microsoft Sentinel ingestion (sources connected, retention period, immutability via Azure Storage immutable blobs), Entra ID audit and sign-in logs, Microsoft 365 Unified Audit Log.
A.8.16 Monitoring activities (NEW)	Microsoft Sentinel analytic rules (rule definitions, MTTR, hunting query history), Defender XDR detection coverage by MITRE ATT&CK technique.

Configuration, vulnerability, and change management (A.8.8, A.8.9)

Annex A control	Microsoft signal source
A.8.8 Management of technical vulnerabilities	Microsoft Defender Vulnerability Management findings and remediation history, Defender for Cloud recommendations and resolved status, third-party scanner findings exported to Sentinel.
A.8.9 Configuration management (NEW)	Azure Policy compliance state over time, Azure Resource Graph baseline queries, Defender for Cloud regulatory compliance dashboard, Microsoft Intune compliance and configuration policies for endpoints.

Data protection (A.8.10, A.8.11, A.8.12, A.8.24)

Annex A control	Microsoft signal source
A.8.10 Information deletion (NEW)	Microsoft Purview retention labels and policies, Microsoft 365 retention policy execution evidence, Azure data lifecycle management policies on storage accounts.
A.8.11 Data masking (NEW)	Microsoft Purview data classification, Azure SQL dynamic data masking, Microsoft Fabric data masking for analytics, sensitivity labels driving downstream masking behavior.
A.8.12 Data leakage prevention (NEW)	Microsoft Purview Data Loss Prevention policies (endpoint, email, Teams, SharePoint, OneDrive, third-party apps), Defender for Cloud Apps DLP, Insider Risk Management signals.
A.8.24 Use of cryptography	Azure Storage encryption configuration, Azure SQL TDE status, Azure Key Vault key inventory and rotation, customer-managed keys, certificate inventory and expiry monitoring.

Network and web (A.8.20–8.22, A.8.23)

Annex A control	Microsoft signal source
A.8.20 Network security	Azure Firewall logs, NSG flow logs, Defender for Cloud network recommendations, private endpoint adoption metrics.
A.8.21 Network services security	Azure Front Door / Application Gateway WAF policies and logs, DDoS Protection metrics, ExpressRoute / VPN configuration evidence.
A.8.22 Network segregation	VNet topology evidence, NSG rule exports, private endpoint topology, Azure Resource Graph queries showing segregation enforcement.
A.8.23 Web filtering (NEW)	Microsoft Defender for Endpoint web content filtering, Microsoft Edge for Business policies, Defender for Cloud Apps URL filtering, Entra Internet Access (where deployed).

Secure development (A.8.25–8.32 including A.8.28 NEW)

Annex A control	Microsoft signal source
A.8.25 Secure development life cycle	Documented SDLC; Azure DevOps / GitHub workflows enforcing the lifecycle stages.
A.8.27 Secure system architecture and engineering	Architecture review records, threat modeling artifacts, design-review approvals.
A.8.28 Secure coding (NEW)	Secure-coding training records, code-review enforcement via branch protection, GitHub Advanced Security (or equivalent) findings, SAST/DAST integrated into pipelines.
A.8.31 Separation of development, test, and production environments	Subscription / management group topology evidence, RBAC scoping per environment, Azure Policy enforcing environment-specific rules.
A.8.32 Change management	Azure DevOps Boards / GitHub Issues change records, pipeline run history with stage approvals, configuration-as-code commit history with reviewer evidence.

Continuity and resilience (A.5.30, A.8.13, A.8.14)

Annex A control	Microsoft signal source
A.5.30 ICT readiness for business	Azure Site Recovery test failover reports, multi-region deployment

Annex A control	Microsoft signal source
continuity (NEW)	topology, documented RTO/RPO commitments and tests.
A.8.13 Information backup	Azure Backup recovery point success metrics, restore-test reports, retention schedule alignment with policy.
A.8.14 Redundancy of information processing facilities	Azure availability zone deployment evidence, paired-region replication status, load-balancer health probe history.

Cloud services and supplier relationships (A.5.19–5.22, A.5.23)

Annex A control	Microsoft signal source
A.5.19–5.22 Supplier relationships (4 controls)	Vendor inventory in GRC platform of record, vendor security evidence on file (SOC 2, ISO 27001, security questionnaires), Microsoft 365 third-party app governance, Entra ID third-party application consent monitoring.
A.5.23 Information security for use of cloud services (NEW)	Azure subscription inventory, Defender for Cloud Apps cloud-app inventory, documented cloud onboarding / offboarding procedures, Microsoft Service Trust Portal evidence files for inherited Azure controls.

The single most important document in the ISMS.

The Statement of Applicability (SoA) is the document the auditor reads first in Stage 1, returns to throughout Stage 2, and references in every surveillance audit for the next three years. It is the central reference point where the management system, the risk treatment plan, and the Annex A controls intersect.

A weak SoA produces a weak audit. A clear, complete, justified SoA tells the auditor that the organization understands its risks, has selected controls deliberately, and can defend its decisions. The remainder of the audit then becomes a verification exercise. With a weak SoA, the auditor is doing the organization's work in the audit room — and that produces findings.

What the SoA must contain

ISO/IEC 27001:2022 Clause 6.1.3 d) requires a Statement of Applicability that contains, for each Annex A control:

Element	What it states
The control reference	Annex A clause and number (e.g., A.8.5 Secure authentication).
Whether the control is applicable	Included or excluded.
The justification	Why the control is included (which risks it treats, which interested-party requirements it addresses) or why it is excluded (the rationale for why the control does not apply to the organization in scope).
The implementation status	How the control is implemented in the organization — a brief summary, with reference to the policy, procedure, or technical control that operationalizes it.

Many organizations also add columns for: control owner, attribute mappings (control type, IS properties, cybersecurity concepts, operational capabilities), reference to the risk treatment plan, and reference to the evidence source. These are optional enhancements that materially improve the audit experience — they are not required by the standard.

Justifying inclusion

Inclusion is the easier case. The justification typically references one or more risks in the risk treatment plan, an interested-party requirement (a customer contract, a regulation), or an organizational policy that mandates the control. Strong inclusion justifications are specific.

Weak inclusion justification	Strong inclusion justification
A.8.5 Secure authentication: Included — industry best practice.	A.8.5 Secure authentication: Included — treats Risk R-014 (unauthorized access to customer data via credential compromise) and addresses the MFA requirement in MSA Section 7.2 with [Customer X]. Implemented via Microsoft Entra Conditional Access policy 'Require MFA for all users' (effective 2024-03-15).
A.5.7 Threat intelligence: Included — required by 2022 revision.	A.5.7 Threat intelligence: Included — supports risk treatment for Risks R-007 and R-022 (advanced persistent threats targeting customer environment). Implemented via Microsoft Defender Threat Intelligence and ISAC feed integration; threat-intelligence inputs reviewed quarterly in the Risk Committee per RACI in policy SEC-POL-003.

Justifying exclusion

Exclusion is where SoAs most often go wrong. Auditors are skeptical of exclusions — not because exclusions are inappropriate, but because they are easy to assert and hard to defend. Every excluded control needs a rationale that the auditor can accept on its face. The rationale must connect to the scope of the ISMS or to the absence of the asset, activity, or risk that the control addresses.

Weak exclusion justification	Strong exclusion justification
A.7.10 Storage media: Excluded — not applicable.	A.7.10 Storage media: Excluded — the organization does not use removable storage media in any in-scope environment. All endpoints are configured via Microsoft Intune to block USB mass-storage devices (verified by configuration policy 'Endpoint-Block-USB-Storage'); production data resides exclusively in Azure-hosted services. The control therefore has no in-scope assets to protect.
A.6.7 Remote working: Excluded — we do not have remote workers.	A.6.7 Remote working: Excluded for the in-scope ISMS — the in-scope service is operated entirely from the [Location X] data center and corporate office. All personnel performing in-scope work do so on-site. Remote-work activity by other personnel is

Weak exclusion justification	Strong exclusion justification
	out of scope of the ISMS.

The exclusion test

If the exclusion can be invalidated by a single counter-example the auditor finds during fieldwork, the exclusion is weak. ‘We do not use cloud services’ collapses the moment the auditor sees Microsoft 365 in use. ‘We do not have remote workers’ collapses when the auditor sees a laptop on a home network. The exclusion must be true within the scope of the ISMS, defensible by evidence, and consistent with how the organization operates.

Exclusions of new-in-2022 controls (A.5.7, A.5.23, A.5.30, A.7.4, A.8.9 through A.8.12, A.8.16, A.8.23, A.8.28) require particularly strong justification. These controls were added because they reflect modern operational realities — an exclusion suggests either that the organization is genuinely outside those realities or that the SoA is not current.

Maintaining the SoA over the certification cycle

The SoA is not a set-and-forget document. Changes in the organization, the threat landscape, or the regulatory environment trigger SoA updates. The new Clause 6.3 (Planning of changes) explicitly requires controlled change management for the ISMS, and the SoA is the document where many of those changes land.

Trigger	SoA action
New product, service, or business unit added to scope	Re-run the risk assessment; identify additional controls required; update SoA with new inclusions; update risk treatment plan.
Material change to a subservice organization (new cloud provider, new processor)	Update A.5.19–5.22 and A.5.23 implementations; reassess inherited controls; re-execute supplier security review.
New regulatory or contractual requirement	Map requirement to applicable Annex A controls; update justifications to reference the new requirement; update related risks.
Annual ISMS review or management review identifying changes	Update SoA in conjunction with the management review outputs; document changes in the change log on the SoA itself.
Internal audit finding affecting control applicability	Update SoA implementation column to reflect remediated control; cross-reference the corrective-action record.

Maintain a version history on the SoA itself — a changelog table at the front or back of the document. Auditors will ask for the prior version and compare. A clear changelog establishes that the SoA is a living document, not a recreation produced before each audit.

Stage 1, Stage 2, surveillance, recertification.

ISO 27001 certification is performed by accredited certification bodies on a three-year cycle. The cycle has a defined cadence that organizations should plan around. This section walks each stage with the auditor's focus and the artifacts the organization should expect to produce.

Stage 1 — Documentation review and readiness

Stage 1 is the auditor's first formal engagement with the ISMS. It is sometimes called the readiness review. The auditor evaluates whether the ISMS is documented to the standard's requirements and whether the organization is ready for Stage 2. Stage 1 typically takes one to three days depending on the size and complexity of the scope.

What the auditor reviews

- Scope statement (Clause 4.3).
- Information security policy (Clause 5.2).
- Risk assessment methodology and the most recent risk assessment results (Clause 6.1.2).
- Risk treatment plan (Clause 6.1.3).
- Statement of Applicability (Clause 6.1.3 d)).
- Information security objectives (Clause 6.2).
- Documented operating procedures (selected sample).
- Internal audit program and most recent internal audit results (Clause 9.2).
- Most recent management review minutes (Clause 9.3).

Stage 1 outcome

The auditor produces a Stage 1 report identifying any areas of concern that must be addressed before Stage 2 can proceed. Findings at this stage are typically classified as Areas of Concern, Opportunities for Improvement, or Major / Minor Nonconformities. Major nonconformities will block Stage 2 until they are corrected. Minor nonconformities will not block Stage 2 but must be corrected before certification can be granted.

The most common Stage 1 finding is a Statement of Applicability that does not justify exclusions adequately. The second most common is an internal audit program that has not yet completed a full cycle of the ISMS scope.

Stage 2 — Implementation and operating effectiveness

Stage 2 is the substantive audit. The auditor verifies that the documented ISMS is actually implemented, that controls are operating, and that the management system is effective. Stage 2

typically takes three to ten days for mid-market organizations, longer for larger or more complex scopes.

What the auditor does

- Interviews top management to test leadership commitment (Clause 5).
- Interviews control owners and operators to test understanding and execution.
- Inspects evidence for sampled controls in the SoA — typically a representative sample across all four Annex A themes.
- Tests the operation of key processes: risk assessment, change management, incident management, internal audit, management review.
- Walks the floor: physical security, clear desk, asset handling.
- Sampling — the auditor selects evidence across the audit period (typically the past 3–12 months for first-time certification, depending on operational history) to confirm controls are operating, not just designed.

Stage 2 outcome

The auditor presents findings at a closing meeting and produces a written audit report. Major nonconformities must be corrected within a defined window (typically 90 days) before certification can be granted. Minor nonconformities can be addressed through a documented corrective-action plan that the certification body monitors. With no major nonconformities, certification is recommended; the certification body's review committee makes the final decision and issues the certificate.

Surveillance audits — years 2 and 3

After initial certification, the certification body conducts surveillance audits at least annually for the next two years. Surveillance audits are smaller in scope than Stage 2 — typically two to five days for mid-market organizations — but they are not a formality. The auditor samples a subset of the ISMS each year, with a focus on:

- Continued operation of controls.
- Closure of nonconformities from prior audits.
- Internal audit program and findings.
- Management review.
- Significant changes to the ISMS, scope, or context.
- New or modified Annex A controls (particularly the 11 introduced in 2022).

Surveillance findings can result in suspension or withdrawal of the certificate if the issues are severe enough or are not corrected. Certification is not a static state; it is a continuously demonstrated condition.

Recertification — year 3

At the end of the three-year cycle, the certification body conducts a recertification audit. Recertification is similar in scope to Stage 2 — the auditor reviews the entire ISMS, not just a sample — and is the basis for issuing a new three-year certificate. Plan recertification at least three months before the current certificate expires; certification bodies have limited audit capacity and late-cycle organizations risk a gap in their certification.

Maintaining certification — the operational rhythm

The mature ISO 27001 program has an operational rhythm that aligns to the certification cycle. The rhythm is what makes audits routine rather than disruptive.

Cadence	Activity
Continuous	Risk register updates, incident logging, control operation evidence capture, vendor monitoring, change management.
Monthly	Security operations metrics review, vulnerability remediation tracking, KRI/KPI dashboards.
Quarterly	Privileged access review, vendor portfolio review, threat-intelligence input review feeding the risk register, ISMS objectives status review.
Semi-annually	Internal audit covering at least half the ISMS scope (so the full scope is covered annually).
Annually	Full risk reassessment, management review, BCP/DR exercise (A.5.30), policy review, comprehensive internal audit, awareness training refresh, SoA review.
Three-year	Recertification audit; revisit fundamental program design choices.

Twelve months from kickoff to certificate.

This timeline assumes initial certification against ISO/IEC 27001:2022 for an organization of 100–500 personnel with the Microsoft Security stack already operating at a baseline level. Organizations with no prior security program need 18–24 months. Organizations with a mature SOC 2 Type II program need 6–9 months. The phases do not change — the duration of each does.

Phase 1 — Foundation (months 1–2)

Goal

Establish the management system foundation: scope, leadership commitment, governance structure, and the documentation framework that everything else will populate.

Activities

1. Define the ISMS scope. Document what is in and out, with the rationale. Get scope approved by top management. The scope decision determines everything that follows; revising the scope mid-implementation costs months.
2. Establish ISMS governance. Identify the ISMS owner (commonly the CISO or Head of Information Security). Form the Information Security Steering Committee or equivalent. Define RACI for ISMS operation.
3. Conduct context analysis (Clause 4.1, 4.2). Document internal and external issues, identify interested parties and their information security requirements.
4. Draft and approve the information security policy (Clause 5.2). Communicate it across the organization.
5. Establish documentation control. Decide where ISMS documents will live (typically a controlled SharePoint site or a GRC platform), how they will be versioned, who approves changes, and what the review cadence is.
6. Engage a certification body. Submit a request for proposal; review accreditation status (UKAS, ANAB, or equivalent); negotiate the engagement with planned dates for Stage 1 and Stage 2.

Exit criteria

- Approved scope statement.
- Approved information security policy.
- ISMS governance documented and operating.
- Engagement letter signed with accredited certification body.

Phase 2 — Risk and design (months 2–4)

Goal

Conduct the first formal risk assessment, develop the risk treatment plan, and produce the first draft of the Statement of Applicability.

Activities

1. Document the risk assessment methodology (Clause 6.1.2). Decide whether to use a likelihood/impact matrix, a quantitative method, a qualitative method, or a hybrid. Document the risk acceptance criteria.
2. Conduct the asset inventory (A.5.9). Identify information assets, owners, and classifications. The inventory feeds the risk assessment.
3. Perform the first risk assessment. Document each identified risk with description, threat, vulnerability, likelihood, impact, and current control state.
4. Develop the risk treatment plan (Clause 6.1.3). For each risk above the acceptance threshold, decide on treatment: modify (apply controls), accept, avoid, or share. Document the treatment decision and the responsible owner.
5. Draft the Statement of Applicability. For each of the 93 Annex A controls, decide inclusion or exclusion, write the justification, and reference the implementation. See Section 5 of this guide for detail.
6. Define information security objectives (Clause 6.2). Make them measurable and time-bound. Identify how progress will be measured and reported.

Exit criteria

- Documented risk assessment methodology.
- Completed first risk assessment with risk register populated.
- Approved risk treatment plan.
- First draft of the SoA covering all 93 Annex A controls.
- Approved information security objectives with measurement plan.

Phase 3 — Build and remediate (months 4–8)

Goal

Implement the controls in the SoA that are not already in operation. Stand up the operational processes the management system requires. Close every gap before the operational evidence period begins.

Activities

1. Implement missing controls. The 11 new-in-2022 controls (A.5.7, A.5.23, A.5.30, A.7.4, A.8.9 through A.8.12, A.8.16, A.8.23, A.8.28) often require new design, not just documentation.

2. Develop topic-specific policies as required by Annex A: access control (A.5.15), supplier security (A.5.19), classification (A.5.12), cryptography (A.8.24), backup (A.8.13), incident management (A.5.24), and others. Each policy must be approved, communicated, and have a defined review cadence.
3. Stand up evidence collection at source. Configure log forwarding, ticketing-system tagging, access-review automation, and SIEM analytics so that controls produce evidence as a byproduct of operating.
4. Establish the internal audit program (Clause 9.2). Identify auditors, plan the audit schedule covering the entire ISMS scope, document the audit methodology.
5. Schedule and conduct the first management review (Clause 9.3). Document inputs and outputs. The first management review can occur before all activities are mature — the auditor will check that it occurred and that the inputs and outputs were appropriate.
6. Roll out awareness training (A.6.3) to all personnel. Track completion. Refresher training for personnel who joined before the program existed.

Exit criteria

- All controls in the SoA are implemented.
- Topic-specific policies approved and communicated.
- Internal audit program operating; at least one internal audit completed.
- First management review completed with documented minutes.
- Awareness training delivered to all in-scope personnel.

Phase 4 — Operational evidence and Stage 1 (months 8–10)

Goal

Operate the ISMS continuously to build the evidence base for Stage 2. Complete Stage 1 successfully.

Activities

7. Operate every control on its frequency. Capture evidence at execution time. Maintain the deviation log.
8. Complete a full cycle of the internal audit program. Track findings to closure.
9. Conduct an internal mock audit. Have someone outside the program test sampled controls. Track time-to-find evidence and quality of evidence.
10. Conduct Stage 1 with the certification body. Address any Stage 1 findings before Stage 2.
11. Conduct a second management review with at least one full cycle of operating evidence as input.

Exit criteria

- Stage 1 completed; any major nonconformities corrected.
- Internal audit cycle completed with findings tracked.
- At least 3–6 months of continuous operating evidence captured.

Phase 5 — Stage 2 and certification (months 10–12)

Goal

Pass Stage 2 with no major nonconformities. Receive the certificate. Establish the operational rhythm for the three-year cycle.

Activities

7. Designate a single audit liaison who triages all auditor requests and routes them to control owners.
8. Stand up a structured evidence channel: a SharePoint site, a Teams channel, or a GRC platform module that gives auditors organized access without ad-hoc emails.
9. Conduct Stage 2. Resolve findings within the certification body's required windows.
10. Receive the certificate. Distribute to customers, post on the trust center, update sales collateral.
11. Schedule the surveillance audit calendar. Year 1 surveillance is typically scheduled 9–12 months after certification.
12. Run a post-certification retrospective. What controls produced evidence cleanly? Which ones required heroic effort? What automation needs to be in place before the next audit cycle?

Exit criteria

- Certificate received.
- Surveillance audit schedule confirmed.
- Retrospective findings logged into the program backlog.

08 · COMMON FINDINGS

Eight findings that show up in nearly every initial certification.

Initial certification audits routinely surface a similar set of findings. Each is preventable. Recognizing the patterns before the auditor does turns potential nonconformities into design improvements that strengthen the ISMS.

1. Scope statement that is too broad or too narrow

The pattern: the scope is defined to make the certificate look impressive (‘the entire enterprise’) but the ISMS only governs one product line. Or the scope is defined narrowly to make certification easier, but the marketing posture implies broader coverage. Auditors test the scope statement against operational reality, customer commitments, and external posture.

Prevent it by defining a scope that is honest, specific, and defensible. Name the in-scope products, services, locations, and supporting functions. Name the out-of-scope items where ambiguity could exist. Confirm that the scope statement matches what customers see when they receive the certificate.

2. Risk assessment that is a one-time exercise, not a process

The pattern: the risk assessment was conducted once, twelve months ago, by a consultant. There is no evidence of updates as new risks emerged, new threats appeared, new technologies were adopted, or new business changes occurred. The risk register is static.

Prevent it by treating the risk assessment as a continuous process. Schedule a full reassessment annually. Trigger updates whenever Clause 6.3 changes occur (new products, processors, regions). Document threat-intelligence inputs (A.5.7) feeding the register. Maintain a risk-register changelog the auditor can review.

3. Statement of Applicability with weak exclusion justifications

The pattern: ten or twenty controls are excluded with one-line justifications like ‘not applicable’ or ‘not part of our environment.’ The auditor probes one or two and finds them invalid. The auditor then doubts the rest.

Prevent it by writing exclusion justifications that the auditor can verify on inspection. Connect each exclusion to the scope statement, the asset inventory, or operational reality. Be especially rigorous on the 11 new-in-2022 controls — weak exclusions of these are a red flag.

4. Internal audit program that has not completed a full cycle

The pattern: internal audits started recently and have only covered a portion of the ISMS scope. The certification body cannot confirm that the entire ISMS has been audited internally before being audited externally.

Prevent it by starting the internal audit program at least six months before Stage 1. Plan the audit cycle to cover the full scope. If the scope is large, plan rolling audits across the cycle but ensure no part of the scope goes longer than the documented cycle without being audited.

5. Management review that is pro-forma

The pattern: management review minutes exist, but they read like meeting notes from a status update, not a strategic review. There is no evidence that decisions were made, resources were reallocated, or improvements were identified.

Prevent it by treating management review as a strategic forum. Pre-circulate inputs (audit results, performance metrics, risk register summary, status of objectives). Capture decisions in the minutes. Track follow-up actions to closure.

6. Documentation control without operational discipline

The pattern: policies exist but lack version control, dated approval signatures, or scheduled reviews. The auditor finds two versions of the same policy on different SharePoint sites with conflicting requirements.

Prevent it by establishing a single source of truth for ISMS documentation. Use SharePoint with versioning enabled and a documented approval workflow. Enforce a review cadence (typically annual) per document. Retire old versions promptly.

7. Awareness training without records

The pattern: training materials exist; the program is described in policy; but the records of who completed training and when are incomplete. Auditors will sample employees and ask them about the training they received.

Prevent it by tracking awareness training in an LMS, HRIS, or dedicated training tool that produces auditable completion records. Issue training automatically on hire and annually for renewal. Track non-completers and escalate.

8. New-in-2022 control gaps

The pattern: the 11 controls introduced in 2022 receive less attention than the legacy controls. Auditors specifically test these because they were the focus of the revision and reflect modern operational realities.

Prevent it by treating the 11 new controls as priority items. Each should have a documented implementation, a control owner, and observable evidence:

- A.5.7 — documented threat-intelligence inputs feeding the risk assessment.
- A.5.23 — cloud-services lifecycle with onboarding, monitoring, and exit evidence.
- A.5.30 — ICT continuity tested within the audit period.
- A.7.4 — monitoring evidence for sensitive areas.
- A.8.9 — configuration baselines and drift detection.
- A.8.10 — retention schedule with deletion evidence.
- A.8.11 — masking or pseudonymization for sensitive data outside production.
- A.8.12 — DLP coverage on email, endpoint, cloud, and web channels.
- A.8.16 — SIEM with tuned analytic rules and alert handling records.
- A.8.23 — web filtering with documented allow/deny policy.
- A.8.28 — secure-coding training, code-review enforcement, SAST/DAST in pipelines.

Continuous readiness as the architecture of the ISMS.

ISO 27001 is a management system standard. It is designed to produce continuous improvement, not periodic certification. The organizations that maintain certification across multiple three-year cycles without scrambling are the organizations whose ISMS operates as architecture, not as a project that resumes before each audit. The patterns that follow describe how that architecture works at a structural level. They are useful whether or not you ever evaluate Kyūdō specifically.

Pattern 1 — The SoA as a live document, not a deliverable

In most ISO 27001 implementations, the Statement of Applicability is a Word or Excel file that is rebuilt before each audit. The audit-cycle scramble described in the introduction to this guide is largely about reconstructing what the SoA should already represent.

The continuous-readiness pattern treats the SoA as a queryable view over a graph: every Annex A control is a node, every risk is a node, every implementation is a node, and the relationships between them are first-class data. When a control's implementation changes — a new Conditional Access policy, a new DLP policy, a new key rotation — the SoA reflects that change automatically. The auditor's view of the SoA is always current. The change log is the graph's history, not a manual list.

Kyūdō's Knowledge Graph operationalizes this pattern. The SoA is one of many views over the graph; the Risk Register, the Control Matrix, the Evidence Index, and the Statement of Applicability are different traversals of the same underlying data.

Pattern 2 — Annex A controls mapped to live Microsoft signal

The conventional ISMS captures Annex A control evidence through periodic exports: a screenshot of the Conditional Access policy, a quarterly access review report, a backup-success summary. The evidence is point-in-time and re-collected before each audit.

The continuous-readiness pattern reads Microsoft signal continuously — Microsoft Entra ID for identity and access, Microsoft Defender for endpoint and identity threats, Microsoft Sentinel for monitoring and incident records, Microsoft Purview for data protection and DLP, Azure Policy for configuration baselines — and recalculates control state on every signal. The evidence for A.8.5 (secure authentication) is not a screenshot of the Conditional Access policy. It is the live policy plus the running record of every authentication event evaluated against it. The auditor's question ‘is MFA enforced?’ has a continuous, queryable answer.

One control set, every framework

The SCF meta-framework anchors 1,470+ controls across 80+ frameworks. Annex A controls in ISO 27001:2022 map to SCF, and SCF maps to SOC 2 Common Criteria, NIST CSF v2.0, CMMC v2, HIPAA Security Rule, PCI DSS v4.0.1, EU GDPR, EU AI Act, ISO 42001, and the rest. A single piece of evidence — a Microsoft Defender for Cloud configuration baseline, a Microsoft Sentinel detection record, a Microsoft Purview DLP policy execution — attests against every framework where the SCF crosswalk holds. ISO 27001 certification, SOC 2 Type II report, and CMMC assessment become views of the same underlying control state.

Pattern 3 — Sovereignty as architecture

The conventional GRC architecture deploys a SaaS governance platform that ingests evidence from the customer's environment, processes it externally, and presents posture in the vendor's cloud. This requires data egress: control-state telemetry, risk register contents, and sometimes raw logs leave the customer's environment to be governed.

The continuous-readiness pattern inverts this. The governance layer deploys inside the customer's own security boundary — in regulated organizations on the Microsoft stack, this means inside the customer's Azure tenant. Microservices run in customer-owned AKS clusters with private endpoints, system-assigned managed identities, and customer-managed encryption keys. No governance data crosses the tenant boundary. The deployment model is the moat — no SaaS-first competitor can replicate it without re-architecting their platform.

For ISO 27001 specifically, this matters because Annex A.5.23 (Information security for use of cloud services) and A.5.19–5.22 (supplier relationships) become substantially easier to satisfy when the governance platform itself is not a third-party processor of in-scope data. The exclusion of governance data from the supplier-risk calculus is an architectural property, not a contractual claim.

Pattern 4 — Auditor-defensible AI

AI in GRC is now a category-saturated claim. Most platforms position AI as a chat layer over documents. The continuous-readiness pattern requires AI that survives the auditor's next question: every AI-produced explanation, mapping, or recommendation must have a source, a confidence level, and a re-performable result.

In Kyūdō, AI is layered. Deterministic functions handle scoring, state transitions, and Statement of Applicability rendering. AI functions handle explanation, draft policy generation, control-mapping suggestions, and natural-language traversal of the Knowledge Graph. The two layers never share a trust contract: the deterministic engine produces the answer, AI produces the prose. Where an auditor asks ‘how was this control determined to be applicable?’ the answer traces to the risk, the asset, the threat, and the policy — not to a model output.

Where this leaves you

If you are pursuing initial ISO 27001 certification for the first time, you do not need a continuous-readiness platform. You need scope, leadership commitment, a real risk assessment, a defensible Statement of Applicability, and the operational discipline to run the management system as specified for at least three to six months before Stage 2. This guide gives you the playbook for that.

If you are maintaining ISO 27001 across multiple cycles, adding new frameworks (SOC 2, CMMC, HIPAA, EU AI Act) on top, or scaling the program to multiple business units or geographies, the architecture this section describes is the direction the practice is moving. The marginal cost of adding one more framework, one more region, or one more product line should approach zero. If it does not, the bottleneck is the architecture.

Kyūdō is the platform that makes that architecture available to regulated organizations running Microsoft 365 and Azure. The next step, if useful, is a deployment workshop in your tenant. The architecture brief is one click. The conversation is one email.

—

If this is useful, the next step is concrete

Architecture briefing — a 30-minute walkthrough of the Kyūdō deployment in your Azure tenant: ISMS structure, Annex A control coverage, evidence flow, and the sovereignty model. → hello@kyudo.ai

Controls workshop — 90 minutes mapping your current ISMS to the continuous-evidence model, with side-by-side ISO 27001:2022, SOC 2, NIST CSF, and CMMC views. → kyudo.ai/workshop

Trust packet — our SOC 2 posture, ISO 27001 architecture commitments, data-residency statement, and the Microsoft estate dependency map. Available on request.

APPENDIX A · DOCUMENTED INFORMATION AT A GLANCE

Every document the standard requires.

ISO 27001:2022 calls out specific documented information that the ISMS must maintain. This list is the minimum. Most certifying organizations exceed it, particularly in the area of topic-specific policies. Documents below marked Required are explicitly required by the standard; documents marked Practical are not explicitly required but are widely expected by auditors and used in practice.

Document	Clause / Annex	Required or practical	Notes
ISMS scope	4.3	Required	First document the auditor reads.
Information security policy	5.2	Required	Approved by top management; communicated.
Risk assessment process	6.1.2	Required	Methodology and acceptance criteria.
Risk treatment process	6.1.3	Required	Treatment plan and decisions.
Statement of Applicability	6.1.3 d)	Required	All 93 Annex A controls with inclusion/exclusion and justification.
Information security objectives	6.2	Required	Measurable; assigned; tracked.
Evidence of competence	7.2	Required	Training records, qualifications.
Documented information for ISMS effectiveness	7.5	Required	Versioned, approved, retained.
Operational planning and control records	8.1	Required	Evidence the planned processes were performed.
Risk assessment results	8.2	Required	Outputs of each risk assessment.
Risk treatment results	8.3	Required	Outputs of each treatment activity.
Monitoring and	9.1	Required	Evidence the ISMS is being

Document	Clause / Annex	Required or practical	Notes
measurement results			measured.
Internal audit program and results	9.2	Required	Plans, findings, actions.
Management review minutes	9.3	Required	Inputs and outputs.
Nonconformity and corrective action records	10.1	Required	Investigation, action, verification.
Asset inventory	A.5.9	Required (control)	Reference for risk assessment.
Topic-specific access control policy	A.5.15	Practical	Auditors expect a documented policy.
Acceptable use policy	A.5.10	Practical	Personnel acknowledgment.
Cryptography policy	A.8.24	Practical	Algorithms, key management.
Backup policy	A.8.13	Practical	RPO/RTO, retention, testing.
Incident management procedure	A.5.24	Practical	Tested at least annually.
BCP / DR plan and test results	A.5.30	Practical	Tested within the audit period.
Supplier security policy	A.5.19	Practical	Supplier review and monitoring.
Cloud services policy	A.5.23	Practical	Lifecycle: onboarding to exit.
Secure development policy	A.8.25	Practical	SDLC; code review; testing.
Change management procedure	A.8.32	Practical	Approval, testing, deployment.

APPENDIX B · AUTHORITATIVE SOURCES

Where to verify and go deeper.

ISO standards are copyrighted and must be purchased from ISO, ANSI, BSI, or a national standards body. The references below identify the primary standards; secondary sources are useful for practitioner perspective.

Primary — ISO and IEC

- ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. The certifiable standard.
- ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls. The implementation guidance for Annex A controls.
- ISO/IEC 27003 — Information security management system implementation guidance.
- ISO/IEC 27004 — Information security management — Monitoring, measurement, analysis and evaluation.
- ISO/IEC 27005:2022 — Guidance on managing information security risks.
- ISO/IEC 27007 — Guidelines for information security management systems auditing.

Accreditation and certification

- IAF Mandatory Document IAF MD 26 — Transition Requirements for ISO/IEC 27001:2022.
- ISO/IEC 17021-1 — Conformity assessment — Requirements for bodies providing audit and certification of management systems. The standard your certification body operates under.
- UKAS, ANAB, JAS-ANZ, and equivalent national accreditation bodies — register of accredited certification bodies.

Microsoft documentation

- Microsoft Service Trust Portal — Microsoft's own ISO/IEC 27001:2022 certificate and audit reports for Azure, Microsoft 365, and Dynamics 365. Establishes the inherited subservice controls.
- Microsoft Purview Compliance Manager — ISO/IEC 27001:2022 assessment template with improvement actions mapped to Microsoft 365 and Azure.
- Microsoft Defender for Cloud — ISO/IEC 27001:2022 regulatory compliance dashboard.
- Microsoft Cloud Adoption Framework — Security baseline guidance aligned to ISO 27001 controls.

Practitioner perspectives

- Selected articles from A-LIGN, Drata, Secureframe, Advisera, Protiviti, Hicomply, Citation ISO, Insight Assurance, BALTUM, and Glocert International were consulted for current 2025–2026 transition and certification practice.

APPENDIX C · PRE-ENGAGEMENT CHECKLIST

Twenty-five items. Run them before Stage 1.

If you can answer ‘yes, with evidence’ to every item below, your initial certification audit is positioned to succeed. If you cannot answer ‘yes’ to ten or more, postpone Stage 1 and do additional work first.

Management system foundations

- Scope statement is documented, approved by top management, and consistent with external posture.
- Information security policy is approved, communicated, and accessible to personnel.
- Top management can articulate the ISMS scope, principal risks, and information security objectives.
- ISMS roles and responsibilities are documented and assigned.
- Context analysis (internal/external issues, interested parties) is documented.

Risk and SoA

- Risk assessment methodology is documented; the most recent risk assessment was performed within the last 12 months.
- Risk register is current and reviewed at a documented cadence.
- Risk treatment plan is current; each above-threshold risk has a treatment decision and an owner.
- Statement of Applicability covers all 93 Annex A controls with inclusion/exclusion and justification.
- Exclusion justifications are specific and defensible.
- The 11 new-in-2022 controls are addressed (each has either an implementation or a strong exclusion).

Operations

- Topic-specific policies are in place and approved (access control, supplier security, cryptography, backup, incident management, etc.).
- Awareness training has been delivered to all in-scope personnel within the last 12 months.
- Asset inventory is maintained and aligned with the risk assessment.
- Change management procedure exists, distinguishes change types, and produces evidence.
- Incident response procedure has been exercised within the last 12 months with documented after-action.
- Backup and recovery testing has been performed within the audit period.
- BCP/DR with ICT continuity (A.5.30) tested within the audit period.

Performance and improvement

- Internal audit program has completed at least one cycle covering the entire ISMS scope.
- Internal audit findings are tracked to closure.
- Management review has occurred with documented inputs and outputs.
- Information security objectives are tracked with measurement evidence.
- Nonconformity and corrective action register is operating with evidence of closures.

Documentation control

- ISMS documents are versioned, dated, approved by named owners, with documented review cadences.
- Document repository has access controls; old versions are retired and not accessible to introduce confusion.