InfoSecAI

A BRIEF FOR CISOS · BISOS · GRC LEADERSHIP

FIELD NOTE · 2026

The ISO 27001 Documentation That Decides Your Stage 2 Audit

A practitioner field note for CISOs, ISMS managers and lead implementers preparing for a Stage 2 certification audit.

AUTHORED BY

Paul Jolliffe

Paul Jolliffe, Founder, InfoSecAI · MBA · CISSP · ISO 27001:2022 LA / LI / IA · PRINCE2 Practitioner

01 · DOCUMENTATION, NOT CONTROLS, DECIDES THE AUDIT

Documentation, not controls, decides the audit

Almost every failed Stage 2 audit I have sat in on failed on documentation, not on controls. The firewalls were configured. The access reviews were happening. The backups restored. What was missing was the evidence that any of it was governed: a Statement of Applicability (SoA) with controls marked applicable but never implemented, a risk treatment plan no risk owner had signed, a management review that skipped half its required inputs.

ISO/IEC 27001:2022 does not certify your security. It certifies your management system. And a management system is, in the auditor's hands, a documentation system. Get the documentation right and Stage 2 is a confirmation exercise. Get it wrong and no amount of strong technical control will save the certificate.

The single most useful distinction to hold in your head is mandatory versus supporting. Confusing the two is what produces both of the common failure modes: teams that under-document because they did not realise a record was required, and teams that over-document because they treated every Annex A control as demanding its own policy.

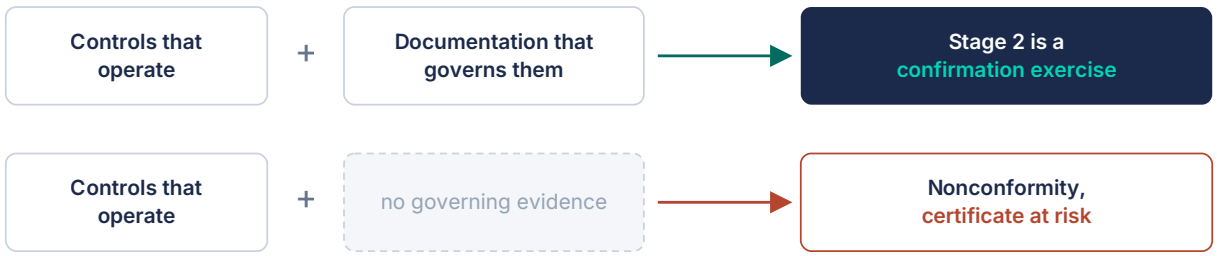

Figure 1. The same controls, two outcomes. Documentation is what separates them.

02 · MANDATORY DOCUMENTED INFORMATION

Mandatory documented information

These are the documents and records the standard explicitly requires by clause. A certification body will ask for every one of them. There is no negotiating this list.

DOCUMENT	CLAUSE	WHAT THE AUDITOR IS CHECKING
ISMS scope statement	4.3	Boundaries are defined and consistent with the SoA and the certificate scope. Interfaces and dependencies are stated, not assumed.
Information security policy	5.2	Approved by top management, communicated, version-controlled, and it sets or frames the objectives.

DOCUMENT	CLAUSE	WHAT THE AUDITOR IS CHECKING
Risk assessment process	6.1.2	A repeatable method with defined risk-acceptance criteria. Run twice, it should give consistent results.
Risk treatment process	6.1.3	Treatment options and the logic for selecting controls, linked back to Annex A.
Statement of Applicability	6.1.3 d)	All 93 Annex A controls accounted for: applicable or not, with justification, and implementation status.
Information security objectives	6.2	Measurable, with owners, timelines, and the resources to achieve them.
Evidence of competence	7.2	The people doing security-relevant work can be shown to be competent for it.
Risk assessment results	8.2	The actual output: a completed, scored risk register.
Risk treatment plan and results	8.3	Actions, owners, dates, residual risk, and risk-owner sign-off. The sign-off is the part most often missing.
Monitoring and measurement results	9.1	Evidence the ISMS is measured, not just operated. Metrics with analysis.
Internal audit programme and results	9.2	A schedule, reports, and evidence the auditor was independent of what they audited.
Management review results	9.3	Minutes covering every required input and output, with decisions and actions.
Nonconformities and corrective actions	10.2	A log with root cause analysis, corrective action, and an effectiveness check.

If you want a shortlist of where Stage 2 audits actually break: the Statement of Applicability, the risk treatment sign-off, internal audit coverage and independence, and management review inputs. Those four account for the majority of nonconformities I see raised.

Figure 2. Where the majority of nonconformities are raised.

03 · SUPPORTING DOCUMENTATION

Supporting documentation

These documents are not named by the clauses. They are how you demonstrate that the Annex A controls you marked applicable in the SoA genuinely operate. An auditor will ask to see them as evidence. Their absence rarely produces a clause nonconformity directly, but it leaves you unable to prove a control, which produces one indirectly.

DOCUMENT	ANNEX A REFERENCE	THEME
Asset inventory	A.5.9	Organisational
Acceptable use policy	A.5.10	Organisational
Threat intelligence procedure	A.5.7	Organisational
Access control policy	A.5.15 to A.5.18	Organisational
Information classification and handling	A.5.12, A.5.13	Organisational
Supplier security policy	A.5.19 to A.5.22	Organisational
Incident management procedure	A.5.24 to A.5.28	Organisational
Business continuity and ICT continuity	A.5.29, A.5.30	Organisational
Human resources security: screening, terms, disciplinary	A.6.1 to A.6.6	People
Remote working policy	A.6.7	People
Physical security procedures	A.7.1 to A.7.14	Physical
Logging and monitoring standard	A.8.15, A.8.16	Technological
Backup policy	A.8.13	Technological
Cryptography and key management policy	A.8.24	Technological
Vulnerability management procedure	A.8.8	Technological
Change management procedure	A.8.32	Technological
Secure development policy	A.8.25 to A.8.28	Technological

04 · ONE DOCUMENT, SEVERAL CONTROLS

One document, several controls

The over-documentation failure mode is worth naming directly. There is no requirement for 93 separate policies. One access control policy can satisfy A.5.15 through A.5.18. One incident management procedure can span A.5.24 through A.5.28. Auditors accept consolidated documents without complaint, provided every control referenced inside them is genuinely addressed and not merely listed.

The discipline is the reverse of what teams expect. The risk is not too few documents. It is too many documents, each thinner than the control it claims to cover, written to populate a folder rather than to govern anything. A practitioner can tell the difference in about ninety seconds. So can an auditor.

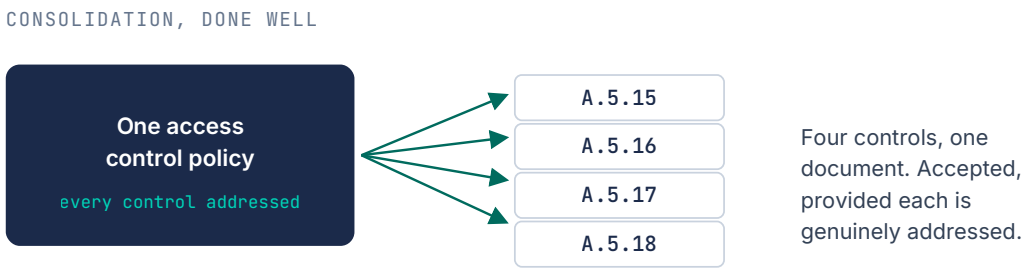

Figure 3. Consolidation is accepted when every referenced control is genuinely addressed.

05 · WHAT GOOD LOOKS LIKE BEFORE STAGE 2

What good looks like before Stage 2

Run the mandatory list as a hard gate. Every item exists, is approved, is current, and an owner can speak to it. Then walk the SoA control by control and ask one question of each applicable control: where is the evidence, and does a supporting document point to it. Where it does not, you have found your gap before the auditor did.

That is the whole exercise. The standard is not asking you to be impressive. It is asking you to be governed, and to be able to show it.

InfoSecAI

About InfoSecAI

InfoSecAI is an independent UK consultancy helping organisations turn security, regulatory, resilience and AI governance requirements into practical operating models, stronger controls and robust delivery.

We work across strategy, governance, risk, compliance, AI security, assurance, operations and engineering. Our services help leadership teams assess their current position, align to standards and regulation, define the target operating model, and deliver the governance, controls, artefacts and ways of working needed to move from intent to implementation.

Our toolkit capability accelerates structured work across ISO 27001, ISO 22301, ISO 42001, NIST CSF, NIST AI RMF, CIS Controls, Cyber Essentials, DORA, NIS 2, the EU AI Act, GDPR, UK GDPR, SOC 1 and SOC 2. The approach combines AI-enabled workflow support with senior practitioner judgement, so outputs remain proportionate, usable and connected to the way the organisation actually operates.

InfoSecAI was founded in **2025** by **Paul Jolliffe**. The company is built for organisations that need clarity, senior leadership and hands-on delivery across information security and AI governance, without adding unnecessary complexity or treating compliance as a paperwork exercise.

infosecai.net · paul.jolliffe@infosecai.net