InfoSecAI

A BRIEF FOR CISOS · BISOS · GRC LEADERSHIP

FIELD NOTE · 2026

The ISO 22301 Documentation That Decides Your BCMS Certification

A practitioner field note for CISOs, business continuity managers, operational resilience leads and lead implementers preparing for certification.

AUTHORED BY

Paul Jolliffe

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

01 · THE PLAN THAT WAS WRITTEN BUT NEVER TESTED

The plan that was written but never tested

The most common way an ISO 22301 audit goes wrong is not a missing document. It is a beautifully written set of plans that have never been exercised. A business continuity plan is a hypothesis until it is tested. Until then it is a statement of intent, and an auditor knows the difference on sight. The second most common failure is closely related: an organisation brings an IT disaster recovery plan to a business continuity audit and discovers, in the room, that continuity is a much wider thing than failing over a data centre.

ISO 22301:2019 certifies a Business Continuity Management System, the BCMS. It shares the harmonised structure of ISO 27001 and ISO 42001: the same Clauses 4 to 10, the same Plan-Do-Check-Act backbone. If you have certified one of those, the management-system scaffolding will be familiar.

Two things make 22301 different in practice. The first is the spine. Where ISO 27001 hangs from the risk assessment, the BCMS hangs from the Business Impact Analysis, the BIA. The BIA identifies the prioritised activities, their resource dependencies, and the recovery objectives that govern everything downstream: the Maximum Tolerable Period of Disruption, the Recovery Time Objective, and the Recovery Point Objective. If the BIA is thin or stale, every plan built on it inherits the weakness.

Figure 1. The BIA is the artefact the recovery objectives, strategies and plans hang from.

The second difference is structural, and it changes how the documentation works. Unlike ISO 27001, ISO 22301 has never carried an Annex A of discretionary controls, so there is no Statement of Applicability to map against. The requirements sit directly in the main clauses, and in Clause 8 in particular. The 2019 revision streamlined that clause and made it less prescriptive, but the effect on documentation is unchanged: more of the BCMS sits on the mandatory side than you might expect coming from 27001. The plans themselves are required, not optional.

02 · MANDATORY DOCUMENTED INFORMATION

Mandatory documented information

These are the documents and records ISO 22301 explicitly requires by clause. A certification body will ask for every one.

DOCUMENT	CLAUSE	WHAT THE AUDITOR IS CHECKING
BCMS scope statement	4.3	Boundaries of the BCMS: which activities, locations, products, and services are in scope, and the exclusions justified.
Business continuity policy	5.2	Approved by top management, communicated, and appropriate to the purpose of the organisation.
BC objectives	6.2	Measurable, consistent with the policy, with owners and plans to achieve them.
Evidence of competence	7.2	The people in continuity roles, including crisis leadership, can be shown to be competent for them.
Business impact analysis: process and results	8.2.2	A consistent method, and a completed BIA per prioritised activity with MTPD, RTO, RPO, and dependencies. This is the spine.
BC risk assessment results	8.2.3	Risks of disruption to prioritised activities identified, analysed, and evaluated.
Business continuity strategies and solutions	8.3	Strategies that address people, premises, technology, information, and suppliers, not technology alone.
Business continuity plans and procedures	8.4	Documented plans with a defined response structure, warning and communication procedures, and recovery steps.
Exercise programme and results	8.5	Plans are exercised on a defined cadence, and the results are recorded. An unexercised plan is the classic finding.
Evaluation of BC documentation and capabilities	8.6	Evidence the BCMS is reviewed after exercises, incidents, and material change, and kept current.
Monitoring and measurement results	9.1	Evidence the BCMS is measured, including whether recovery objectives are actually being met.
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.

Where 22301 audits break most often: a BIA not refreshed after material change, activities prioritised without a consistent methodology, an RTO never validated by exercise, a crisis management plan that exists but has never been run, and supplier dependencies absent from the contracts that should carry continuity clauses.

03 · SUPPORTING DOCUMENTATION

Supporting documentation

Because the requirements sit in Clause 8 rather than a discretionary annex, the supporting layer here is thinner than in ISO 27001. It is largely the methodology and the registers that make the mandatory artefacts credible. Each is shown against the clause it serves.

DOCUMENT	CLAUSE REFERENCE
Roles, responsibilities and authorities for the BCMS	5.3
Competence and training procedure	7.2
BCMS communication plan	7.4
Documented information procedure	7.5
BIA methodology	8.2.2
BIA register	8.2.2
BC risk treatment plan	8.2.3
Resource requirements document	8.3
Supplier dependency register	8.3
ICT continuity strategy, the ISO 27031 subset	8.3
Activity-level recovery plans	8.4
Crisis management plan	8.4
Crisis communications plan	8.4
Disaster recovery plan	8.4
Exercise plan and exercise report templates	8.5
Lessons-learned procedure	8.5

A note on the supplier dependency register specifically. Supplier continuity is the single most frequent audit finding I see on 22301. A prioritised activity often depends on a third party whose own continuity arrangements were never assessed and whose contract carries no continuity obligation. The register is what surfaces that gap before the auditor does.

04 · THE POINT THAT CATCHES PEOPLE: DOCUMENTED IS NOT THE SAME AS DEMONSTRATED

The point that catches people: documented is not the same as demonstrated

This is the distinction that does the most damage. ISO 22301 does not reward a well-written plan. It rewards a plan that has been exercised, evaluated, and corrected. Clause 8.5 requires an exercise programme. Clause 8.6 requires evaluation of the documentation and the capability. Clause 9 requires the results to feed monitoring and management review. The standard is built so that an untested plan cannot quietly pass.

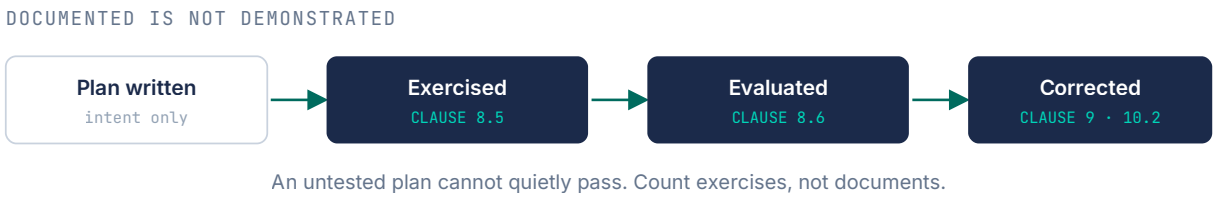

Figure 2. The standard is built so that an untested plan cannot quietly pass.

So when you assess readiness, do not count documents. Count exercises. For every prioritised activity, ask: has the recovery plan been run, when, what failed, and was the lesson closed before the next cycle. A plan with no exercise history behind it is not evidence of continuity capability. It is evidence of good intentions, and intentions are not certifiable.

05 · WHAT GOOD LOOKS LIKE BEFORE THE AUDIT

What good looks like before the audit

Run the mandatory list as a hard gate: every item exists, is approved, is current, and an owner can speak to it. Then take the BIA register and pick one prioritised activity. Walk it from the BIA entry, to its recovery objectives, to the strategy selected, to the recovery plan that implements it, to the exercise report that tested it, to any lesson logged and closed. If you can do that walk cleanly, you are close to ready. If the trail ends at a plan with no exercise behind it, you have found the gap before the auditor did.

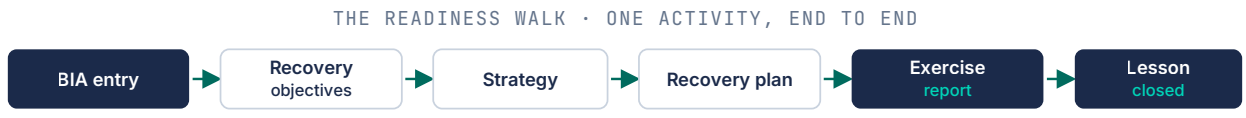

Figure 3. If the trail ends at a plan with no exercise behind it, you have found the gap.

The standard is not asking you to have written about resilience. It is asking you to be able to show that you have 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