www.surecloud.com

ENTERPRISE COMPLIANCE TOOLKIT · 2026

ISO 27001 at enterprise scale. The ISMS Design Workbook.

A practical, fill-in planning tool for the four design decisions that determine whether your ISMS delivers ongoing assurance — or becomes a compliance liability: scope, control ownership, GRC integration and surveillance readiness.

ISO 27001

FOR COMPLIANCE LEADS, CISOS & GRC PRACTITIONERS

SURECLOUD®

Companion to: ISO 27001 at Enterprise Scale — ISMS Design Guide
Authored by SureCloud GRC experts

START HERE

How to use this workbook.

Enterprise ISO 27001:2022 certification is a governance programme, not a documentation project. The decisions made before a single control is mapped shape cost, audit complexity, and what your certificate actually covers.

This workbook turns those decisions into structured, recordable outputs you can take into a planning session and hand to stakeholders. Work through it in order — each worksheet builds on the one before it.

> **"The organisations that struggle at Stage 2 audit almost always made the same mistake: they defined scope too late and ownership too vaguely. A control register with no named owner three months before certification day is a non-conformance waiting to happen."**
>
> — Matt Davies · Chief Product Officer, SureCloud

The four design decisions, in order

1 **Scope architecture** — WORKSHEET 1

The single most consequential early decision. Choose the model that satisfies your buyers and regulators without overreaching your governance capacity.

2 **Control ownership at scale** — WORKSHEET 2

Distribute the 93 Annex A controls across the functions best placed to operate them, while the ISMS team retains the framework.

3 **Wider GRC integration** — WORKSHEET 3

Map controls once and apply them across DORA, NIS2 and GDPR rather than running parallel workstreams.

4 **Surveillance readiness** — WORKSHEETS 4 & 5

Pre-empt the four failure points that account for most enterprise non-conformances.

A NOTE ON TOOLING

- This workbook is deliberately a static document — the same way most enterprise ISMS programmes still begin life in a spreadsheet.
- As you complete it, note where version control, evidence linkage and audit-ready reporting start to strain. Those friction points are exactly where a GRC platform earns its place. There is more on that at the end.

WORKSHEET 1

Scope decision matrix.

Clause 4.3 requires you to determine which departments, sites, systems, processes and products or services are in scope. Score each model against your organisation, then record your decision. Resolve scope **before** you draft the Statement of Applicability, not after.

SCOPE MODEL	BEST SUITED TO	KEY TRADE-OFF	FIT (1–5)
Single legal entity	Holding groups where one entity is client-facing; initial certification ahead of phased expansion.	Clean, lower-cost audit, but excludes subsidiaries and may not satisfy group-wide buyer requirements.	
Group-wide	Groups with an integrated IT environment; regulated groups where buyers require group-level assurance.	Full-scope assurance, but complex governance and higher audit cost across all entities.	
Divisional	Large groups pursuing staged certification; divisions with distinct IT environments and risk profiles.	Resource-manageable stages, but risk of control gaps between in-scope and out-of-scope divisions.	
Product or service perimeter	Technology companies certifying a platform; service providers certifying a defined managed service.	Focused and lower-complexity, but may not satisfy buyers needing broader organisational coverage.	

Decision factors to weigh: legal structure · maturity of governance · expectations of key customers and regulators · resources available to sustain the ISMS.

CHOSEN SCOPE MODEL AND RATIONALE

PHYSICAL BOUNDARIES

Sites and facilities

LOGICAL BOUNDARIES

Systems, networks, data flows, cloud and shared services

WATCH — SCOPE CREEP

- Scope creep is the leading cause of enterprise ISMS cost overrun. Agree a formal scope change procedure now, embedded in your governance framework, so scope cannot expand by default.

SCOPE CHANGE PROCEDURE — OWNER AND TRIGGER POINTS

WORKSHEET 2

Control ownership register.

Assigning all 93 Annex A controls to a central team is unsustainable at scale; distributing them without accountability produces inconsistency. The hybrid model is what surveillance audits expect: the ISMS team owns the framework, business units own their domains. Assign a named owner and evidence obligation for each theme.

THEME	RECOMMENDED OWNER	EXAMPLE CONTROLS	NAMED OWNER	EVIDENCE CADENCE
Organisational 37	ISMS team / Legal / Risk	Security policies (A.5.1); supplier relationships (A.5.19–A.5.22); access control policy (A.5.15); threat intelligence (A.5.7)		
People 8	HR / ISMS team	Screening (A.6.1); terms and conditions (A.6.2); awareness training (A.6.3); disciplinary process (A.6.4); remote working (A.6.7)		
Physical 14	Facilities / IT / ISMS team	Security perimeters (A.7.1); entry controls (A.7.2); clear desk and screen (A.7.7); equipment disposal (A.7.14)		
Technological 34	IT / Security engineering	Endpoint devices (A.8.1); privileged access (A.8.2); authentication (A.8.5); encryption (A.8.24); logging (A.8.15); vulnerability management (A.8.8)		

IT security engineering carries the heaviest lift: the technological theme is 34 of the 93 controls and includes the most operationally demanding obligations. Resource ownership here accordingly.

FRAMEWORK OWNERSHIP HELD BY THE CENTRAL ISMS TEAM

ISMS policy · risk treatment process · Annex A Statement of Applicability · management review process · internal audit programme

LEADERSHIP ACCOUNTABILITY (CLAUSE 5)

Named board / C-suite owner with documented authority — a nominal owner who signs off policies annually but has no substantive involvement will not satisfy an experienced auditor.

CONTROL OWNER ENGAGEMENT PLAN

A one-time email is the single most common reason owners cannot describe their obligations at audit. Record how owners will be briefed and re-engaged on a schedule.

WORKSHEET 3

Cross-framework mapping starter.

Many ISO 27001:2022 controls map directly to other obligations. A well-designed ISMS maps a control **once** and applies it across frameworks — so a single logging policy can satisfy ISO 27001 and DORA simultaneously. Record where you can consolidate effort.

ISO 27001:2022 AREA	MAPS TO	INTERNAL OWNER	SINGLE CONTROL REFERENCE
ICT risk management, incident reporting, resilience testing, ICT third-party risk	DORA (Reg. (EU) 2022/2554)		
Security measures and incident reporting (Clauses 6 and 8; several Annex A controls)	NIS2		
Security of processing (Organisational and Technological themes)	GDPR Article 32		
Information continuity controls (Annex A)	ISO 22301 business continuity		

ISMS-to-enterprise integration points

Shade one circle per row — red (not connected) · amber (partial) · green (integrated and evidenced).

ISMS risk register feeds into and draws from the enterprise risk register. ○ ○ ○

Third-party risk management connects to Annex A supplier relationship controls. ○ ○ ○

Business continuity (ISO 22301) managed through a single control framework, not a separate set. ○ ○ ○

ISMS risk reporting reaches board-level risk reporting rather than sitting as a silo. ○ ○ ○

NOTES ON CONSOLIDATION OPPORTUNITIES AND CURRENT DUPLICATION

WORKSHEET 4

Surveillance audit readiness check.

Surveillance auditors sample proportionally across business units and sites, and interview control owners who had no part in audit prep. Four failure patterns account for the majority of enterprise non-conformances. Rate your current readiness for each, then note the action required.

FAILURE POINT	WHAT GOOD LOOKS LIKE	STATUS	ACTION / OWNER
Inconsistent evidence across sites	Every site and regional office has an equivalent evidence collection process, not just the locations the ISMS team controls directly.	○ ○ ○	
Owners unaware of obligations	Every control owner can describe their controls and produce evidence, supported by a structured engagement programme.	○ ○ ○	
Absent management review evidence	Clause 9.3 reviews held at planned intervals with documented inputs and outputs and genuine governance decisions.	○ ○ ○	
Corrective actions not tracked to closure	Clause 10.1 actions tracked in a workflow with owners, timelines and closure evidence — not an email thread.	○ ○ ○	

Shade one circle per row: red (not in place) · amber (partial) · green (in place and evidenced).

THE THREE-YEAR CYCLE

- Initial certification has two stages; the cycle then includes annual surveillance audits and recertification in year three. Surveillance audits assume the ISMS is running and test whether it does so **consistently**. Programmes that treat ISO 27001 as a project fail here.

HIGHEST-PRIORITY GAP TO CLOSE BEFORE THE NEXT SURVEILLANCE VISIT

WORKSHEET 5

Management review agenda.

Clause 9.3

Auditors ask for management review records and test whether the outputs demonstrate genuine governance engagement, not a brief agenda item. Use this structure to evidence inputs, decisions and outputs at each review.

REVIEW DATE	CHAIR	ATTENDEES

REQUIRED INPUT	SUMMARY / EVIDENCE REFERENCE
Status of actions from previous reviews	
Changes in internal and external issues relevant to the ISMS	
Feedback on ISMS performance (non-conformities, monitoring, audit results)	
Feedback from interested parties	
Results of risk assessment and status of the risk treatment plan	
Opportunities for continual improvement	

DOCUMENTED OUTPUTS AND DECISIONS

Include decisions on improvement opportunities and any changes to the ISMS, with owners and dates.

WHERE THIS GETS HARD

When the spreadsheet starts to strain.

If completing these worksheets surfaced friction, that is the point. Spreadsheet-based ISMS management works at small scale; at enterprise scale the failure modes are predictable. Version control breaks, evidence cannot be reliably linked to controls, and producing an audit-ready pack takes days of manual consolidation before every surveillance visit.

WHAT ENTERPRISE ISMS TOOLING SHOULD PROVIDE

- Centralised control register and Annex A SoA with version history.
- Automated evidence collection workflows that notify owners at defined intervals.
- Role-based access so distributed owners update their sections independently.
- Management review scheduling with structured inputs and documented outputs.
- Audit-ready reporting that produces a full evidence pack without manual consolidation.
- Automated mapping between ISO 27001:2022 and DORA, NIS2 and GDPR.