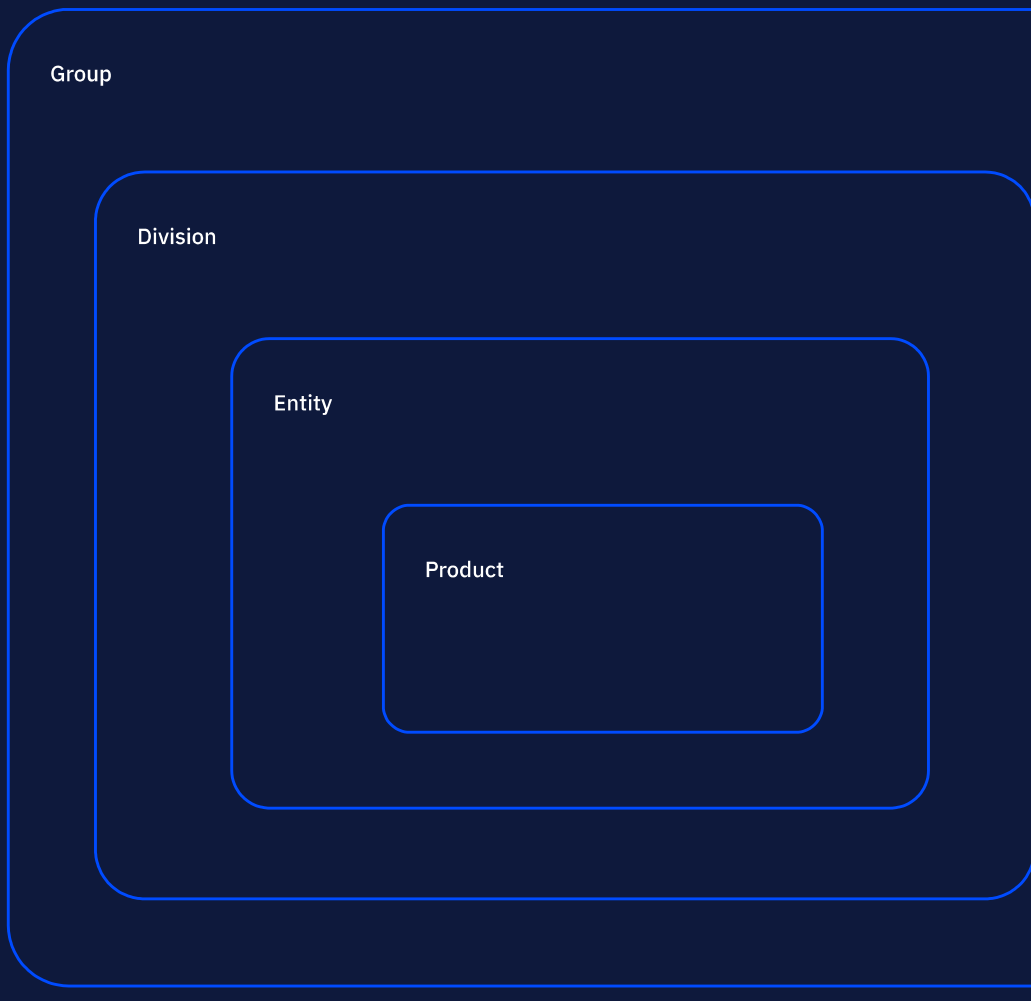
Free workbook

ISO 27001 Enterprise ISMS Design Workbook

Scope, ownership, integration and audit readiness for ISO/IEC 27001:2022 at scale

Companion to the ISO 27001 Enterprise ISMS Design Guide 2026



SURECLOUD®

Version 1.0 | October 2026

Before you start

Certification at enterprise scale is a governance programme, not a documentation project.

This workbook turns the guide into decisions. Work through it with your ISMS lead and control owners, then bring the five outputs to your next steering meeting.

Read the full guide →

Who it's for

CISOs and Heads of Information Security

ISMS managers and programme leads

Heads of GRC, Risk and Compliance

Section map

01	02	03	04	05	06	07
Readiness	**Scope**	**Ownership**	**Integration**	**Audit readiness**	**Tooling**	**Plan**
Clauses 4 to 10	4.3	5	6	9.3, 10.1		

Expert view

> "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

01 Readiness

Know what the standard asks of you at scale.

Profile your programme, then score the four clauses that create the most friction.

From the guide Clauses 4 to 10 are mandatory. Clauses 4, 5, 6 and 9 create the most friction in large organisations. Certification bodies sample evidence in proportion to your size.

Annex A: 93 controls across four themes



Your programme at a glance

Legal entities

Sites

Headcount

Business units involved

Target audit date

Certification body

Audit type (tick one)

☐ Initial certification ☐ Surveillance ☐ Recertification

Other frameworks in scope (tick all that apply)

☐ DORA ☐ NIS2 ☐ GDPR ☐ ISO 22301 ☐ SOC 2

☐ Other

Self-check: clause pressure points

Tick one score per clause

Clause 4 Context and scope	☐ 0 Not in place	☐ 1 Partial	☐ 2 In place
Clause 5 Leadership	☐ 0 Not in place	☐ 1 Partial	☐ 2 In place
Clause 6 Planning and risk treatment	☐ 0 Not in place	☐ 1 Partial	☐ 2 In place
Clause 9 Performance evaluation	☐ 0 Not in place	☐ 1 Partial	☐ 2 In place

02 Scope

Scope is the most consequential early decision you'll make.

Compare the four models, then tick the one that fits.

From the guide Settle scope before your risk assessment and before you draft the Statement of Applicability.

Model	Best when	Watch out for	Tick
Single legal entity	One client-facing entity drives the need, or you want a phased start	Shared group systems must still be assessed and any exclusion justified in writing	☐
Group-wide	Environments are integrated, or buyers need group-level assurance	The largest evidence burden and the deepest audit sampling	☐
Divisional	You're running a staged programme	Controls and evidence can drift between divisions	☐
Product or service perimeter	Customers want assurance over a specific product or service	Interfaces and dependencies need precise definition	☐

Decision questions

Do customers or regulators ask for group-level assurance?	☐ Yes	☐ No
Are core systems shared across entities?	☐ Yes	☐ No
Does one entity drive most of the commercial demand?	☐ Yes	☐ No
Do you have owners and budget for every site now?	☐ Yes	☐ No

Why this model

What would trigger a move to a different model?

02 Scope Clause 4.3 Output 1 of 5

Write a scope statement an auditor can test.

Fill in each boundary, then combine them into one statement.

From the guide Define physical boundaries (sites and facilities) and logical boundaries (systems, networks and data flows, including cloud and shared services).

Boundary	Your answer
Legal entities in scope	
Sites and locations	
Business units and functions	
Systems, services and data	
Interfaces and dependencies Shared services, group IT, key suppliers	
Exclusions and written justification	

Your scope statement

The ISMS of [organisation] covers [products or services] delivered by [entities] from [sites], including [systems], supported by [functions]. It excludes [exclusion] because [justification].

Approved by | **Role** | **Date**

02 Scope

Scope creep is the leading cause of enterprise ISMS cost overruns.

Name an owner for each step, then log every scope change against it.

From the guide Creep comes from imprecise scope statements, systems added without a formal change process, and control owners reading their obligations too broadly.

Scope change procedure		Owner
1	**Trigger.** Tick the change that started the process. ☐ New entity or acquisition ☐ New site ☐ New system or service ☐ Organisational change ☐ Other	
2	**Assess** the impact on risks, controls, Statement of Applicability, evidence and cost	
3	**Approve**, with a named approver and role	
4	**Update** the scope statement, Statement of Applicability and risk register	
5	**Notify** your certification body where required	
6	**Brief** affected control owners	

Change log

Date	Change	Impact	Approved by	Certification body notified
				☐ Y ☐ N
				☐ Y ☐ N
				☐ Y ☐ N
				☐ Y ☐ N
				☐ Y ☐ N

03 Ownership Clause 5

Leadership commitment has to be demonstrable, not delegated.

Score each requirement, then record where the evidence lives and who owns it.

From the guide Clause 5 needs named accountability at board or C-suite level. Auditors look for it in management review outputs, risk decisions and resource allocation.

Requirement	Score	Evidence location	Owner
Information security policy approved by top management	☐ 0 ☐ 1 ☐ 2		
ISMS objectives set and aligned to business strategy	☐ 0 ☐ 1 ☐ 2		
Roles, responsibilities and authorities assigned and communicated	☐ 0 ☐ 1 ☐ 2		
Resources allocated to the ISMS	☐ 0 ☐ 1 ☐ 2		
Management review scheduled with agenda and attendees	☐ 0 ☐ 1 ☐ 2		
Board or executive reporting cadence agreed	☐ 0 ☐ 1 ☐ 2		

Score: 0 Not in place, 1 Partial, 2 In place

Building board reporting? See the ISO 27001 board reporting framework.

03 Ownership

At scale, ownership has to be shared and still accountable.

Compare the three models, then record where you are today.

Centralised

The ISMS team owns and evidences all 93 controls.

Where it breaks

A single point of failure. Only workable in smaller or well-resourced organisations.

Distributed

Each control sits with the function best placed to operate it.

Where it breaks

Coherence is lost across the organisation.

Hybrid Recommended

The ISMS team owns the framework. Domain leads own operational controls with documented accountability. A GRC platform gives visibility across both.

How the hybrid model splits ownership

ISMS team owns	Domain leads own
Policy	Operational Annex A controls
Risk treatment	Evidence of operation
Statement of Applicability	Documented accountability
Management review	
Internal audit	

Our model today (tick one)

☐ Centralised ☐ Distributed ☐ Hybrid

What needs to change

03 Ownership

Output 2 of 5

Every control needs a named owner before Stage 2.

Name an owner for each theme, then list every control that still needs one.

From the guide A control register with no named owner close to certification is a likely non-conformance.

Theme (controls)	Suggested owner	Example control	Accountable owner	Deputy	Review frequency
Organisational (37)	ISMS team, Legal or Risk	**A.5.1** Policies for information security			
People (8)	HR, with the ISMS team setting requirements and auditing evidence	**A.6.1** Screening			
Physical (14)	Facilities, IT and the ISMS team	**A.7.1** Physical security perimeters			
Technological (34)	IT and security engineering, with the ISMS team owning policy and audit	**A.8.2** Privileged access rights			

Unowned controls to resolve

Control ID	Control name	Owner to assign	By date

04 Integration

Your ISMS can't run as an island.

Record each connection, score whether the link works today and set the next action.

From the guide The ISMS risk register should feed, and draw from, enterprise risk. Third-party risk and business continuity connect to specific Annex A controls.



Connection	Owner	Where it lives today	Link in place	Next action
Enterprise risk register			☐ 0 ☐ 1 ☐ 2	
Third-party risk management			☐ 0 ☐ 1 ☐ 2	
Business continuity, ISO 22301			☐ 0 ☐ 1 ☐ 2	
			☐ 0 ☐ 1 ☐ 2	

Score: 0 Not in place, 1 Partial, 2 In place

04 Integration

Output 3 of 5

Map each control once. Apply it everywhere.

Start from the worked examples, then add the controls your programme relies on most.

From the guide ISO 27001:2022 overlaps with DORA, NIS2 and GDPR Article 32. One control, evidenced once, can satisfy several frameworks.

ISO/IEC 27001:2022 control	DORA	NIS2	GDPR	Owner	Evidence location
Example *A.5.19 to A.5.22 Supplier relationships*	*Art. 28 to 30, ICT third-party risk*	*Art. 21(2)(d), supply chain security*	*Art. 28, processors*		
Example *A.5.24 to A.5.26 Incident management*	*Art. 17 and 19, incident management and reporting*	*Art. 23, reporting obligations*	*Art. 33, breach notification*		
Example *A.5.29 and A.5.30 Continuity and ICT readiness*	*Art. 11, response and recovery*	*Art. 21(2)(c), business continuity*	*Art. 32(1)(c), restoring availability*		
Example *A.8.24 Use of cryptography*	*Art. 9, protection and prevention*	*Art. 21(2)(h), cryptography and encryption*	*Art. 32(1)(a), encryption*		

Worked examples are a starting point. Confirm applicability with your legal and compliance teams.

05 Audit readiness Clause 9.3

Surveillance audits test consistency, not completeness.

Date each milestone in your cycle, then record your last management review.

From the guide

Stage 1 reviews your documentation and readiness. Stage 2 tests whether the ISMS operates as documented, sampling evidence across your scope. Certification from a UKAS-accredited body lasts three years, with surveillance audits in between.

Your certification cycle

Stage 1	Stage 2	Certificate issued	Surveillance year 1	Surveillance year 2	Recertification year 3
Date	Date	Date	Date	Date	Date

Management review record

Date of last review	Next review date	Attendees

Inputs covered (tick all that apply)

- [ ] Status of previous actions
- [ ] Changes in internal and external issues
- [ ] Changes in interested parties' needs
- [ ] Information security performance (nonconformities, monitoring, audit results, objectives)
- [ ] Feedback from interested parties
- [ ] Risk assessment results and treatment plan status
- [ ] Opportunities for continual improvement

Decisions documented? ☐ Yes ☐ No

05 Audit readiness Clause 9.3 Clause 10.1 Output 4 of 5

Four common failure points. Score yourself honestly.

Score each failure point, add up your total, then log the corrective actions.

From the guide Four failure patterns account for most surveillance non-conformances at enterprise scale. Auditors sample sites and interview owners who had no part in audit prep.

Failure point	What auditors find	Evidence you'd show	Score
1 **Inconsistent evidence across sites**	Operational sites lack the evidence processes the central team uses		☐ 0 ☐ 1 ☐ 2
2 **Control owners unaware of obligations**	Owners notified once by email and never engaged again can't describe or evidence their duties		☐ 0 ☐ 1 ☐ 2
3 **No management review evidence**	Reviews held as a formality, with no documented outputs or decisions		☐ 0 ☐ 1 ☐ 2
4 **Corrective actions not closed**	Actions confirmed by email, with no cause analysis or effectiveness check		☐ 0 ☐ 1 ☐ 2

Score: 0 Not in place, 1 Partial, 2 In place

Total score

☐ / 8

0 to 3
Likely findings. Act now.

4 to 6
Gaps to close before your next audit.

7 to 8
Ready. Keep it consistent.

Corrective action log

Finding	Root cause	Action	Owner	Due	Effective
					☐ Y ☐ N
					☐ Y ☐ N
					☐ Y ☐ N

06 Tooling

Spreadsheets don't fail on day one. They fail at scale.

Tick what's true today, then score what your current tooling provides.

Part A. Where it breaks

Tick any that are true today

- [ ] Versions drift across business units
- [ ] Evidence isn't linked to the controls it proves
- [ ] Nobody is reminded when evidence needs refreshing
- [ ] Audit packs take days to assemble
- [ ] Every new entity or framework adds manual effort

Part B. What enterprise ISMS tooling should provide

0 Not in place, 1 Partial, 2 In place

Central control register and Statement of Applicability with version history	☐ 0	☐ 1	☐ 2
Automated evidence workflows with owner notifications	☐ 0	☐ 1	☐ 2
Role-based access for distributed owners	☐ 0	☐ 1	☐ 2
Scheduled management reviews with documented outputs	☐ 0	☐ 1	☐ 2
Audit-ready reporting without manual consolidation	☐ 0	☐ 1	☐ 2
Multi-entity scope support	☐ 0	☐ 1	☐ 2
Integration with IT service management	☐ 0	☐ 1	☐ 2
Automated mapping to DORA, NIS2 and GDPR	☐ 0	☐ 1	☐ 2

SURECLOUD

One platform for your control register, evidence workflows and cross-framework mapping. 80% less audit prep for ISO 27001, SOC 2 and NIST CSF 2.0.

See how it works →

07 Your 90-day plan

Output 5 of 5

Turn your answers into a 90-day plan.

Pull the actions from each section. Give every one an owner and a date.

Action	Source page	Owner	Due	Window (days)
Approve scoping model and scope statement (p5)				☐ 30 ☐ 60 ☐ 90
Name an owner for every Annex A control (p9)				☐ 30 ☐ 60 ☐ 90
Schedule the next management review (p12)				☐ 30 ☐ 60 ☐ 90
				☐ 30 ☐ 60 ☐ 90
				☐ 30 ☐ 60 ☐ 90
				☐ 30 ☐ 60 ☐ 90
				☐ 30 ☐ 60 ☐ 90
				☐ 30 ☐ 60 ☐ 90
				☐ 30 ☐ 60 ☐ 90
				☐ 30 ☐ 60 ☐ 90

Decisions needed from the steering group

Run your ISMS as a programme, not a spreadsheet.

SureCloud gives enterprise ISMS teams one place for scope, controls, evidence and cross-framework mapping. Gracie AI Agents with Personas and Skills perform the activities that slow your team down, so your people spend their time on judgement, not admin.

Book an ISO 27001 demo

Further reading

ISO 27001 resource hub

Statement of Applicability guide

Annex A at enterprise scale

Automating ISO 27001 evidence collection

Sources

ISO/IEC 27001:2022

UKAS

Regulation (EU) 2022/2554 (DORA)

Directive (EU) 2022/2555 (NIS2)

Regulation (EU) 2016/679 (GDPR), Article 32

This workbook supports planning. It doesn't replace the standard, legal advice or your certification body's guidance. © SureCloud 2026.

Your Business Assured.

SURECLOUD®

surecloud.com