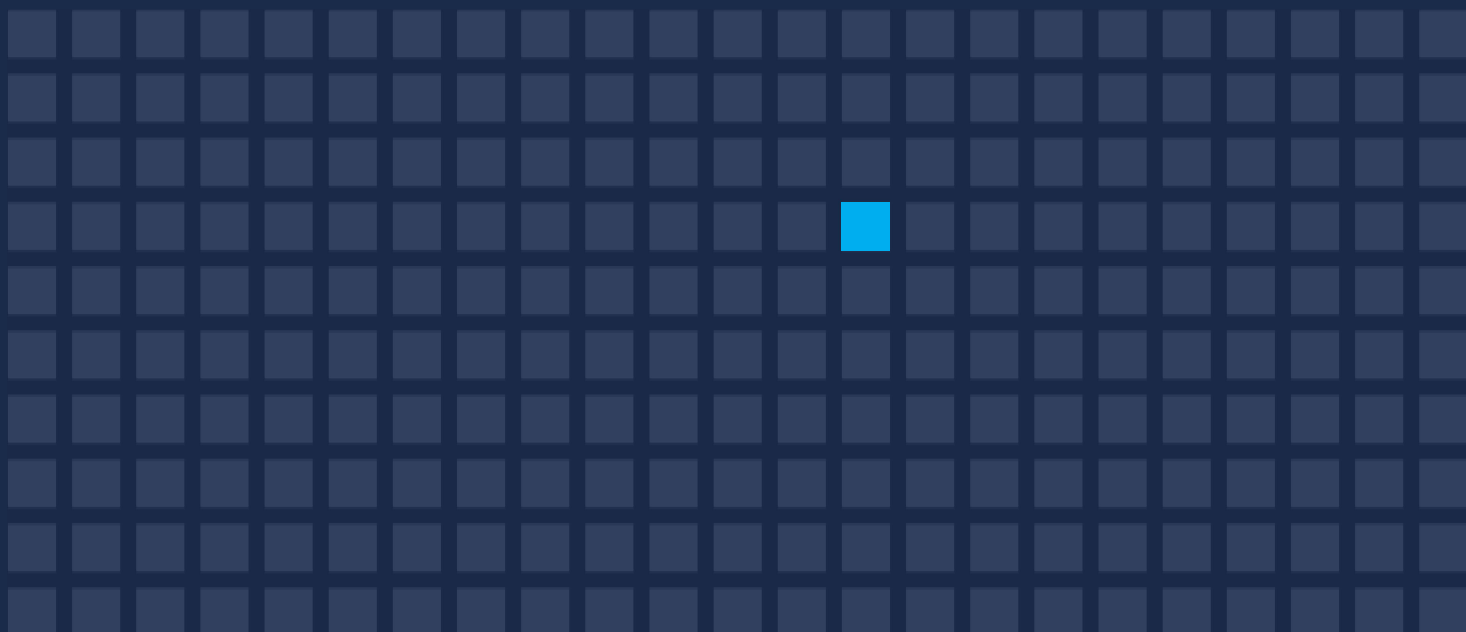


The control ownership toolkit

Four templates and a health check to give every control one named owner.



"IT owns this" is not an owner.

A control register can look tidy and still fail. The reason is usually simple. A team was written down. A person never was.

When nobody is named, nobody attests, nobody escalates and nobody hands over. The control keeps its place on the register. It stops doing its job.

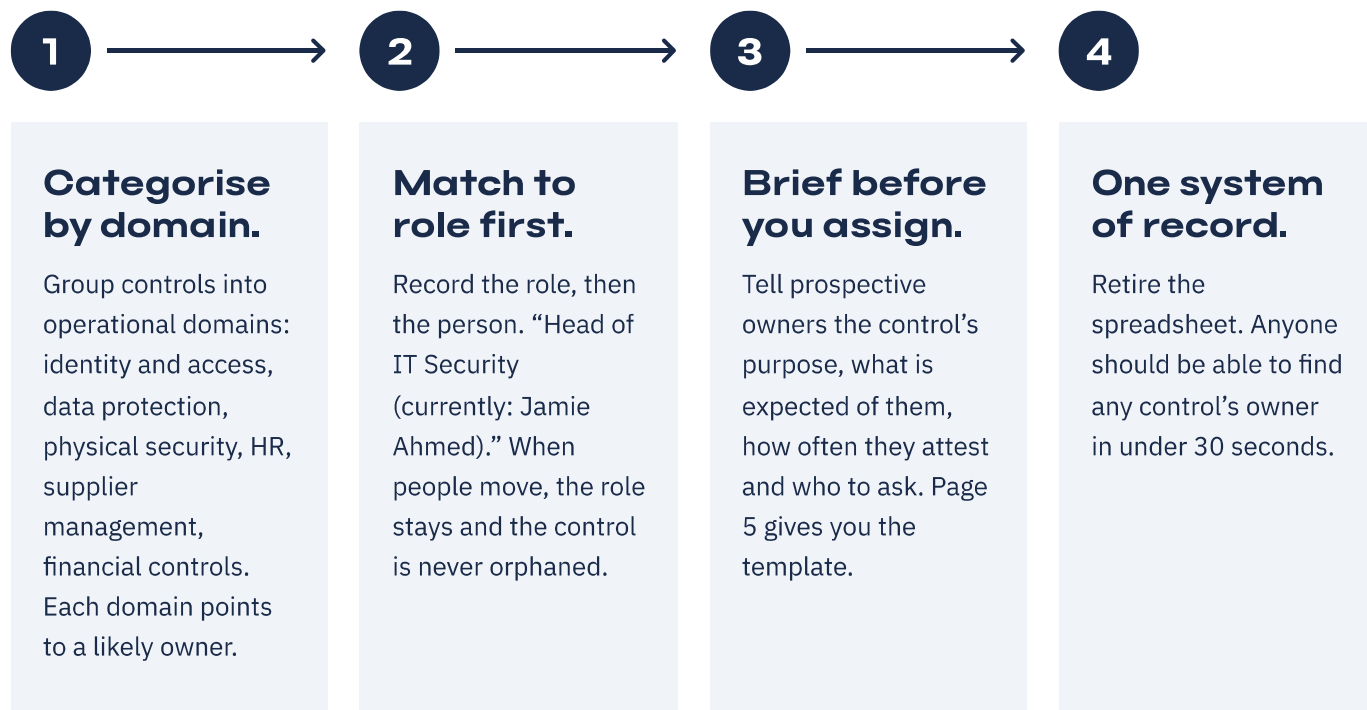
Fixing it starts with separating three roles that most teams blur together.

			
What they do	Accountable for the control operating as designed. Escalates problems. Provides evidence.	Carries out the control activity day to day.	Tests or monitors whether the control is effective.
Typical holder	Head of function, by role and by name	Analyst, engineer, administrator	Compliance, internal audit

Every control needs one named owner, by role and by name, who can be held accountable when it fails.

Aligns with ISO 27001 Annex A 5.2, information security roles and responsibilities.

Four steps. One owner per control.



What an owner commits to

-  **Operating confirmation.** Attest on schedule that the control works.
-  **Evidence.** Supply what auditors and assessors need.
-  **Escalation.** Say so early when the control cannot be maintained.
-  **Handover.** Formally transfer ownership when leaving the role.

Template 1. Control ownership register

One row per control. If a cell says “team”, rewrite it.

Grey row is an example.

Control ID	Control name	Domain	Owner (role)	Owner (name)	Performer(s)	Assurer	Contributing teams	Risk rating (H/M/L)	Attestation cadence	Last attested
A.5.15	Access control policy	Identity and access	Head of IT Security	Jamie Ahmed	IT Operations	Internal Audit	HR, Facilities	High	Quarterly	14 Sep
								H M L		
								H M L		
								H M L		
								H M L		
								H M L		
								H M L		

1

One owner per control. Other teams are listed as contributors.

2

Role first, then name.

3

Watch concentration. Around 15 to 20 controls per owner is reasonable. Beyond that, the owner is a risk in themselves.

Template 2.

Owner briefing

Send this before you assign. People accept ownership faster when they know what they are accepting.

Control: _____ ID: _____

Proposed owner (role / name): _____ Date: _____

Briefed by: _____

Why this control exists 2 to 3 lines: the risk it reduces and the framework or requirement it supports

What you are accountable for

- Confirming the control is operating as designed
- Providing evidence when asked
- Escalating when it cannot be maintained
- Handing over formally if you change role

How often you will be asked to attest:

☐ Monthly ☐ Quarterly ☐ Bi-annually ☐ Annually

Who performs the control day to day: _____

Who tests it independently: _____

Where to ask questions: _____

Owner acknowledgement

☐ I understand and accept ownership

Signature / date: _____

Template 3.

Attestation cadence

Annual attestation misses failures. Weekly attestation gets ignored. Match the cadence to the risk.

Risk profile	Typical controls	Attest	Review ownership
High	Critical systems, regulatory obligations	Monthly or quarterly	Quarterly
Medium	Operational processes	Quarterly or bi-annually	Bi-annually
Low	Physical, administrative	Annually	Annually

Trigger an ownership review immediately when:

- ☐ A restructure or reorganisation is announced
- ☐ A system migration or major change goes live
- ☐ An audit finding points to unclear accountability
- ☐ An owner resigns, is promoted or changes role
- ☐ A new supplier takes over part of a control
- ☐ A new framework or regulatory obligation is adopted

■

Continuous Controls Monitoring checks technical controls in real time, so a failure surfaces when it happens, not when the next review comes round.

Template 4. How healthy is your control ownership?

Score one point per “yes”. Be honest. The gaps are the point.

	Yes	No
Naming		
1 Every control on the register has a named individual owner.	☐	☐
2 Every owner is recorded by role and by name.	☐	☐
3 No control is assigned to a team or department.	☐	☐
4 Contributing teams are listed separately from the owner.	☐	☐
Briefing		
5 New owners are briefed before they accept ownership.	☐	☐
6 Each owner knows their attestation frequency.	☐	☐
7 Owners know who to contact with questions.	☐	☐
Cadence and tracking		
8 Attestation frequency reflects each control’s risk, not a blanket schedule.	☐	☐
9 Attestation requests, reminders and escalations do not rely on email.	☐	☐
10 Anyone can find a control’s owner in under 30 seconds.	☐	☐
Change		
11 Ownership is reviewed whenever there is a restructure, migration or role change.	☐	☐
12 Departed or role-changed owners are flagged automatically.	☐	☐

Your score: _____ / 12

0

1

2

3

4

5

6

7

8

9

10

11

12

0 to 4. **Exposed.** Ownership exists on paper only. Start with Template 1 and Template 2 this week.

5 to 8. **Partly built.** The foundations are there. Fix cadence and change triggers next.

9 to 12. **Mature.** Keep ownership live. Automate attestation and flag changes as they happen.

When an owner leaves, the control should not.

HANDOVER CHECKLIST

☐ Outgoing owner lists every control they hold

☐ Successor briefed using Template 2

☐ Register updated and previous owner removed

☐ Successor named by role and by name

☐ Evidence locations and open items handed over

☐ Next attestation date confirmed

Stop chasing attestations. Start getting them.

SureCloud Compliance Management gives every control one owner, one record and one place to see what is overdue. Gracie AI Agents with Personas and Skills send structured attestation requests, chase non-responses and escalate, so your team stops running the process by hand.

Book a demo →

surecloud.com/book-a-demo