Ciphrix

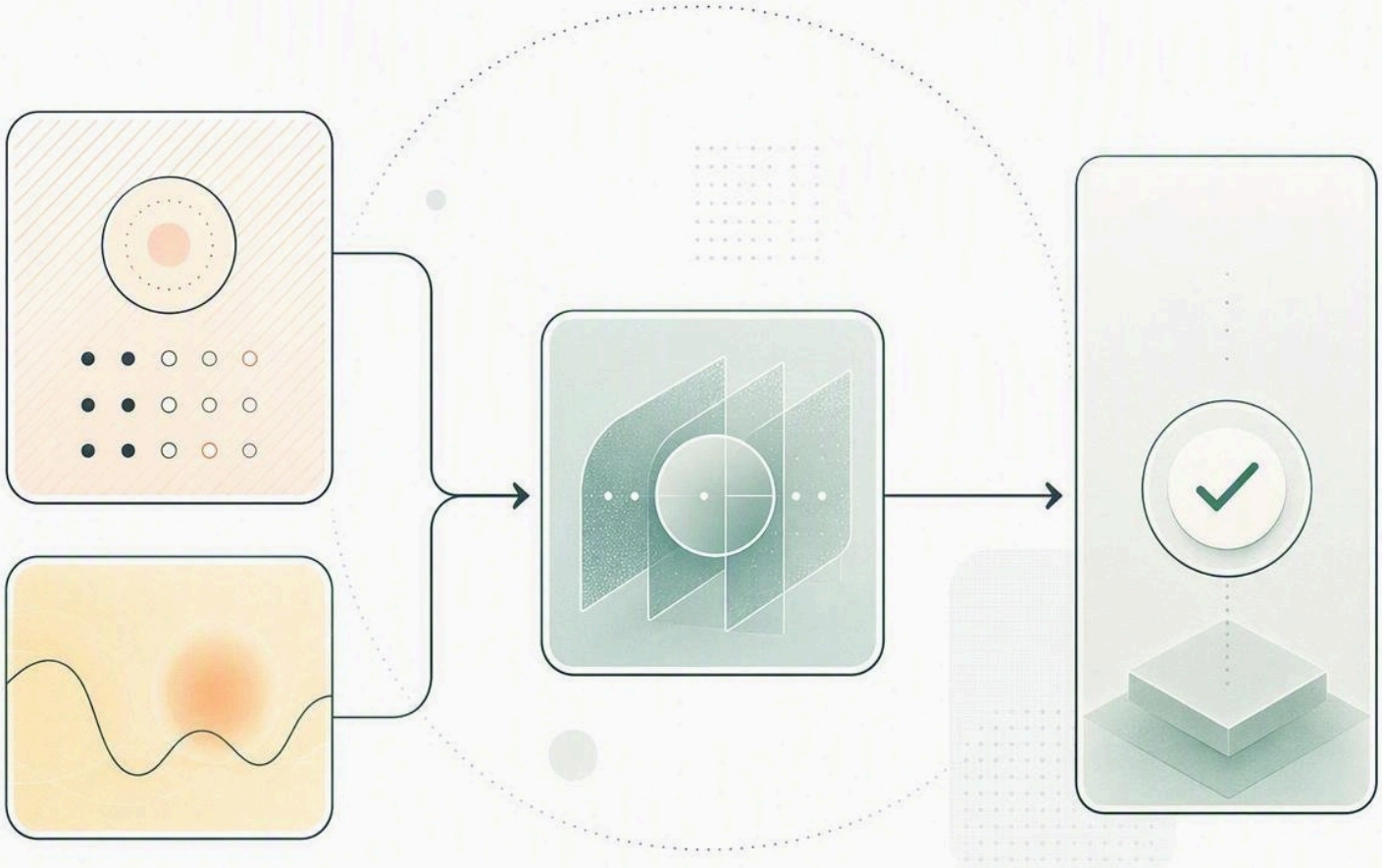
BUYER RESOURCE

PRACTICAL GUIDE

ISO 27001 Audit-Readiness Checklist

A practical control, evidence and decision tracker for moving from scope to a reviewable ISMS

PUBLISHED 8 August 2026 FROM Ciphrix DOCUMENT ID CPX-BG-2608-5139



BUYER RESOURCE

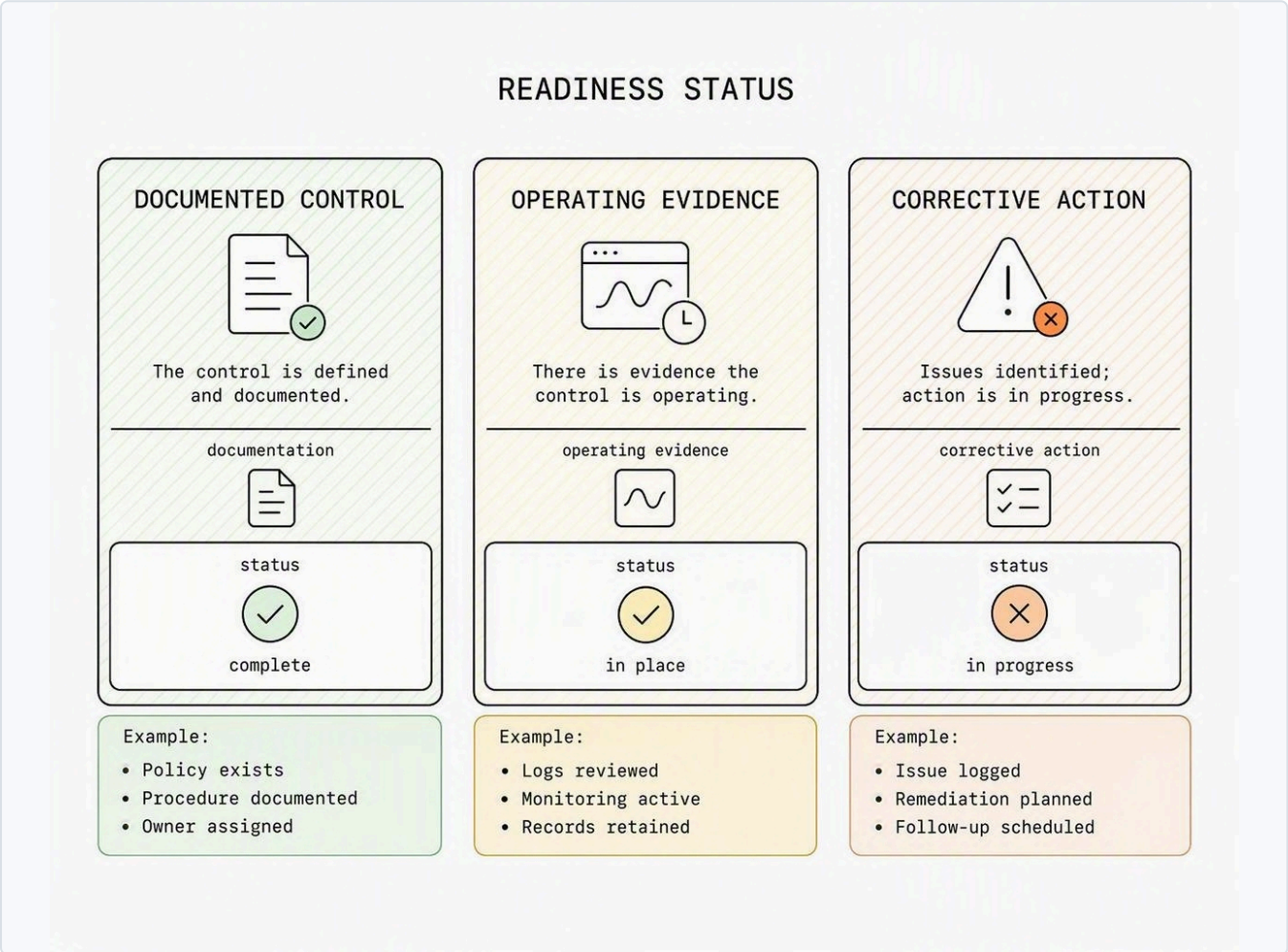
ISO 27001 Audit-Readiness Checklist

CIPHRIX
BUYER GUIDE

A practical control, evidence and decision tracker for moving from scope to a reviewable ISMS

A practical control, evidence and decision tracker for moving from scope to a reviewable ISMS

Use this as a working tracker—not an assertion that ISO 27001 requirements have been met. ISO 27001 readiness depends on your organisation's scope, risk treatment, Statement of Applicability (SoA), implemented controls, records and assessment context.



Readiness moves from documented control to operating evidence to corrective action.

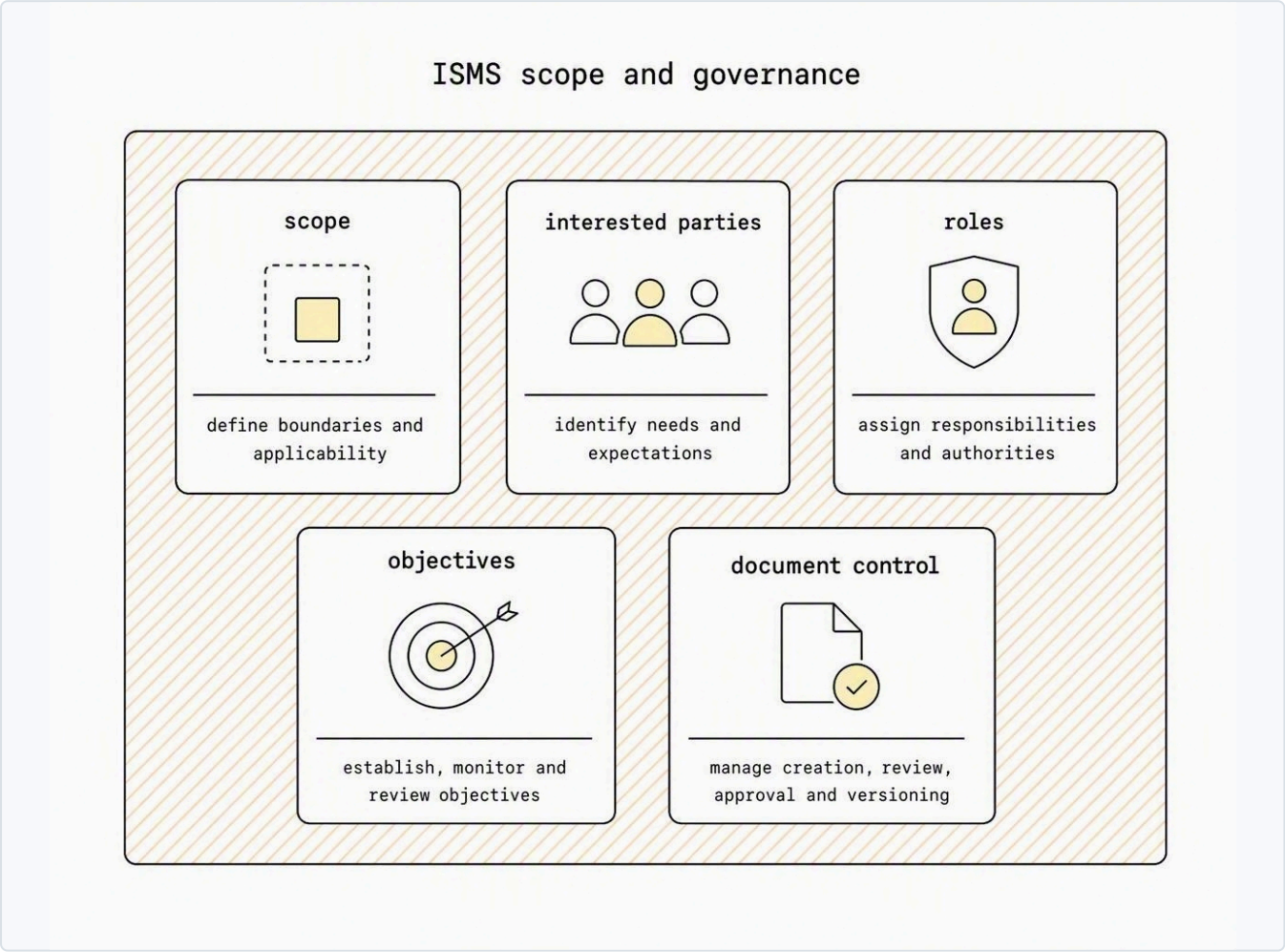
The tracker follows this sequence: first establish that a control is documented, then show that it operates, then record and close the gaps that remain. Do not mark an item complete merely because a policy exists.

How to use this tracker

1. Confirm the ISMS scope before adding tasks.

2. Turn each material gap into an owner-backed action with a verification method.
3. Record operating evidence as work happens; do not create an evidence folder at the end.
4. Use the “decision / exception” field whenever scope, risk treatment or timing requires management judgement.

1. Scope and governance tracker

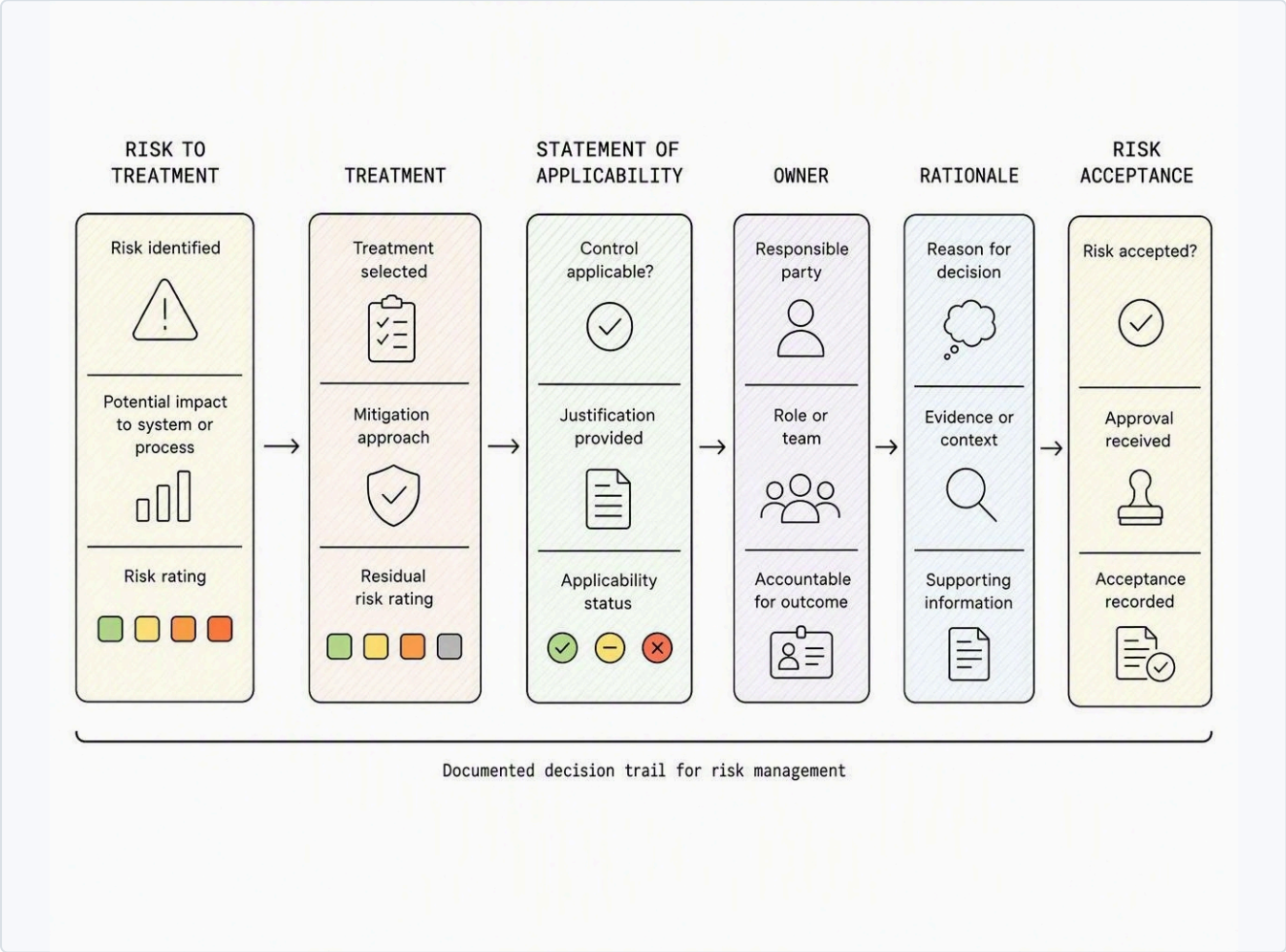


ISMS scope and governance connect boundaries, interested parties, roles, objectives and document control.

ITEM	OWNER	EVIDENCE / OUTPUT	STATUS	DECISION / EXCEPTION
Define ISMS scope: service, sites, people, systems, data, interfaces and exclusions	ISMS owner + leadership	Approved scope statement		
Identify interested parties and relevant requirements	Compliance / legal	Requirement register		
Assign ISMS roles, authorities and reporting path	Leadership	Role map / charter		
Establish information-security objectives and measures	Security leadership	Objectives, metrics and review cadence		

ITEM	OWNER	EVIDENCE / OUTPUT	STATUS	DECISION / EXCEPTION
Establish document-control and approval process	ISMS owner	Versioned document register		

2. Risk and treatment tracker



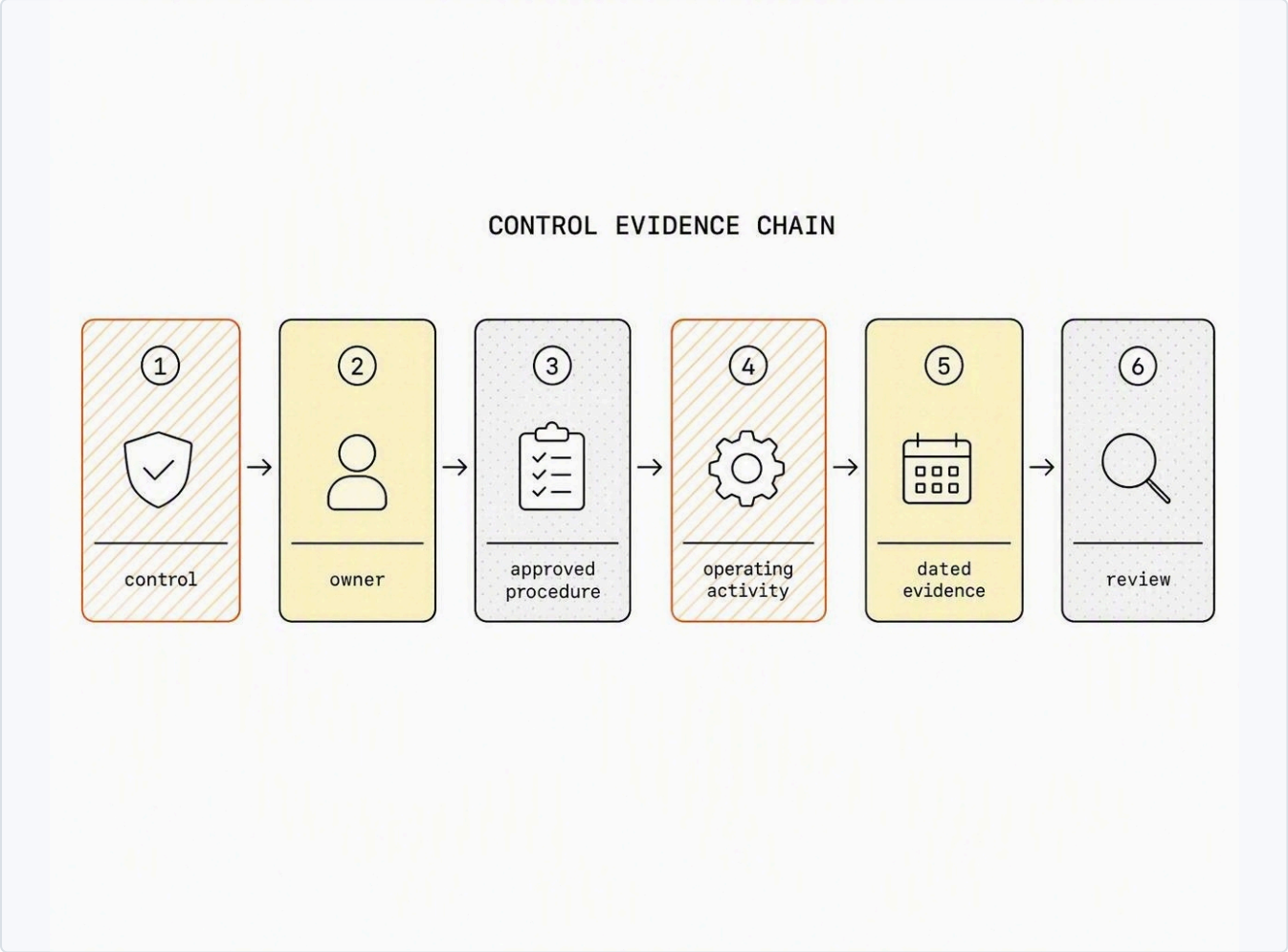
Risk assessment, treatment and Statement of Applicability connect to ownership, rationale and acceptance.

ITEM	OWNER	EVIDENCE / OUTPUT	STATUS	DECISION / EXCEPTION
Define risk assessment methodology and acceptance criteria	Risk owner	Approved method		
Identify information-security risks in scope	Control / risk owners	Risk register		
Assess and prioritise risks	Risk owner + relevant SMEs	Ratings and rationale		
Select treatment and relevant controls	ISMS owner	Treatment plan		

ITEM	OWNER	EVIDENCE / OUTPUT	STATUS	DECISION / EXCEPTION
Create and maintain the Statement of Applicability	ISMS owner	SoA with inclusion/exclusion rationale		
Record residual-risk acceptance	Authorised risk owner	Approval and expiry/review date		

3. Control and evidence tracker

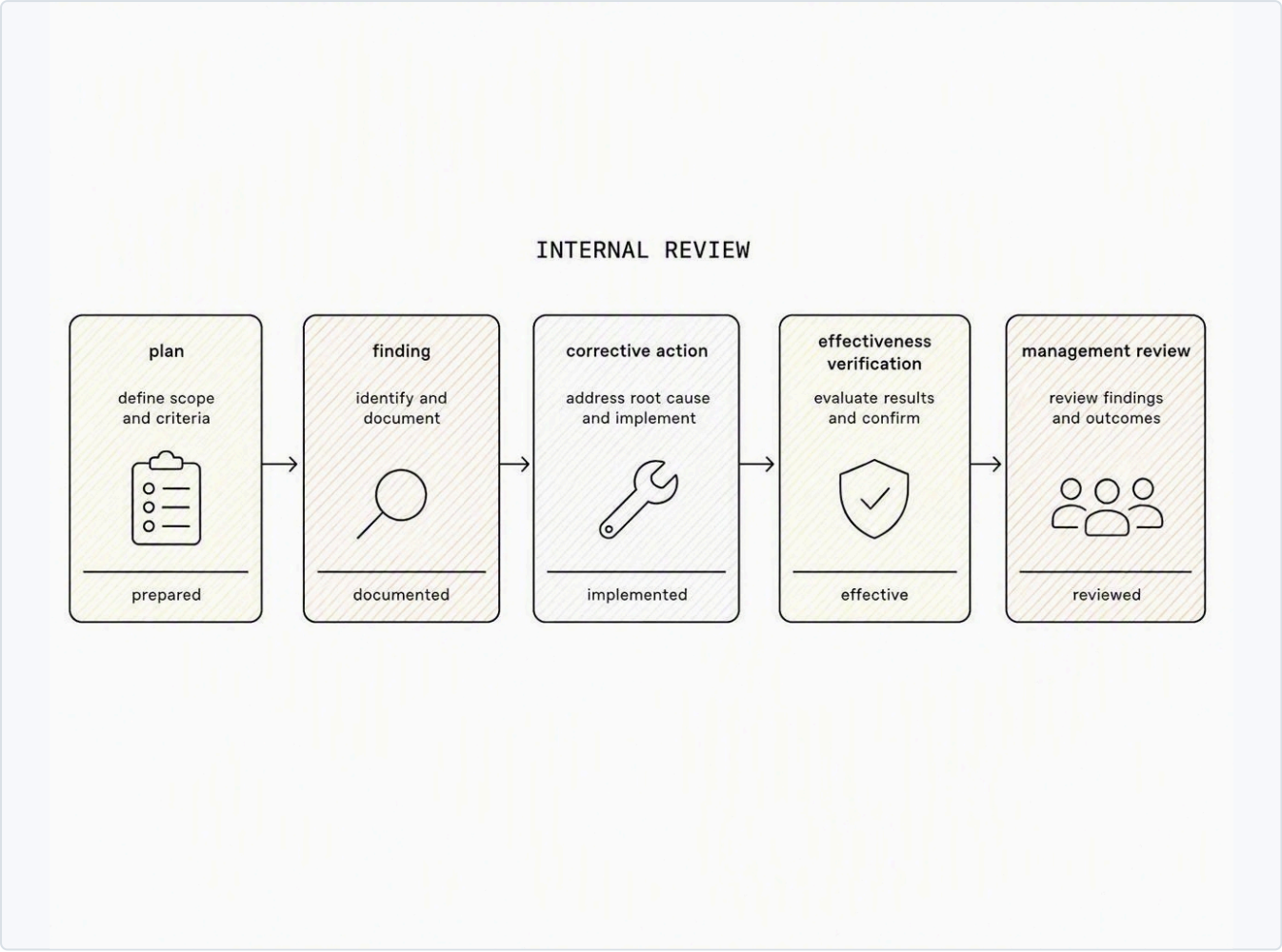
CONTROL AREA	WHAT TO PROVE	TYPICAL SOURCE / EVIDENCE	OWNER	CADENCE	STATUS
Access management	Access is authorised, reviewed and adjusted appropriately.	IAM exports, approvals, access reviews and remediation tickets.	IT / security	Defined control cadence	
Asset / information management	Relevant assets and information are identified and handled appropriately.	Asset inventory, classification records and owner assignments.	IT / data owners	Ongoing / periodic	
Supplier security	Suppliers are assessed, approved and reviewed according to risk.	Vendor register, due diligence, contracts and reassessments.	Procurement / security	Onboarding + periodic	
Secure change / development	Changes are controlled and traceable.	Tickets, code-review records, testing and deployment links.	Engineering	Per change	
Vulnerability management	Issues are identified, prioritised and handled.	Scan results, tickets, exception and closure records.	Security / infrastructure	Defined cadence	
Incident management	Incidents are detected, handled and learned from.	Incident records, decisions, post-incident actions and closure evidence.	Security	Event-driven	
Business continuity	Relevant continuity and recovery arrangements are maintained/tested.	Plans, test/exercise records and follow-ups.	Operations / leadership	Defined cadence	
Awareness and policy management	People receive relevant guidance and policies remain approved/current.	Policy register, approvals, acknowledgement/training records.	HR / security	Defined cycle	



A control evidence chain connects owner, procedure, operating activity, dated evidence and review.

What good looks like: for each priority control, a reviewer can move from the control to its accountable owner, approved procedure, operating activity and dated record without relying on a verbal explanation.

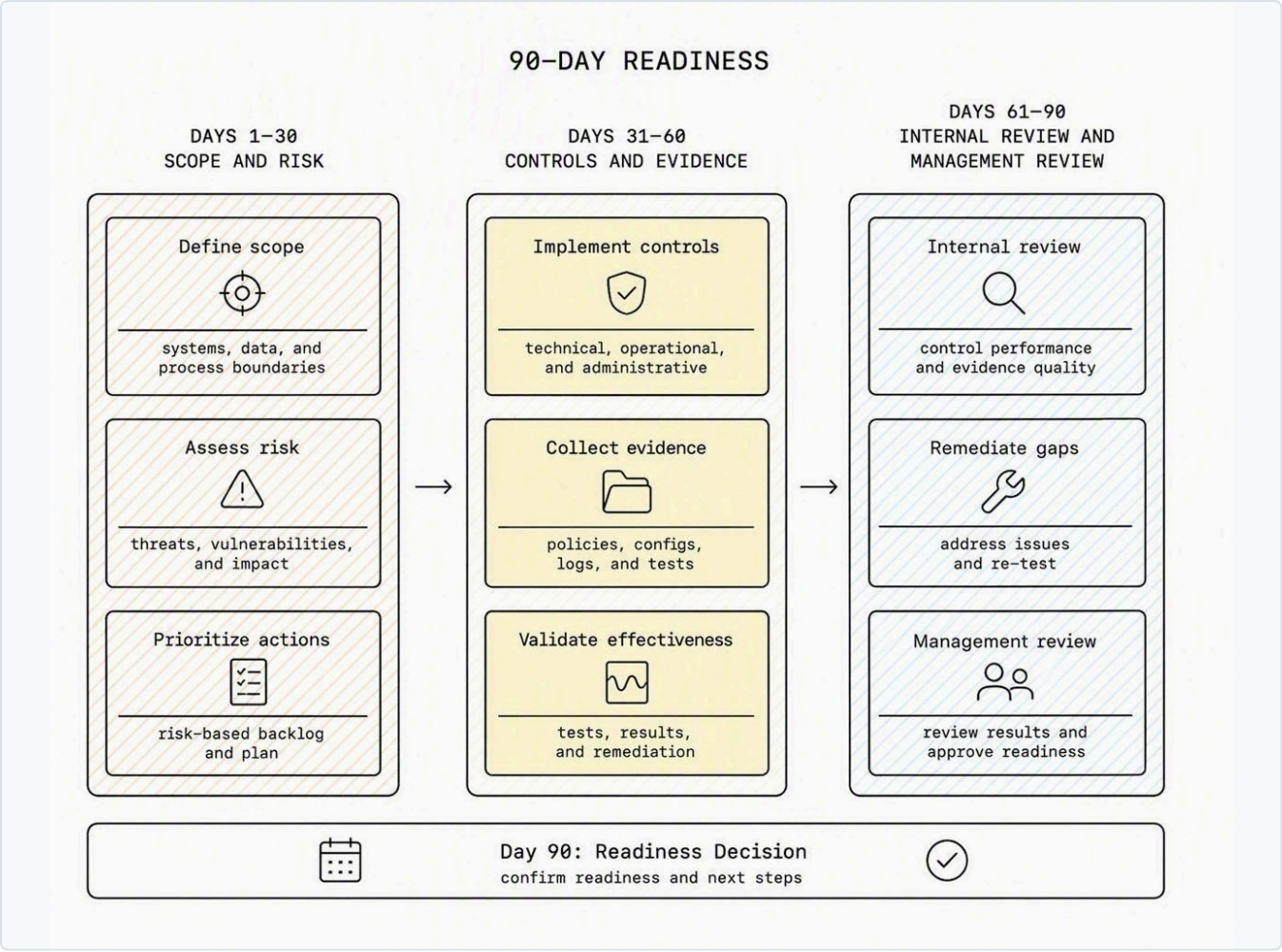
4. Internal review and corrective-action tracker



Internal review moves from plan and finding to corrective action, effectiveness verification and management review.

ITEM	OWNER	EVIDENCE / OUTPUT	STATUS	FOLLOW-UP
Plan internal audit/review	Internal audit / ISMS owner	Audit plan and scope		
Conduct review and record findings	Independent reviewer	Findings, evidence and conclusions		
Assign corrective actions	Accountable control owners	Action plan, due dates and owners		
Verify corrective-action effectiveness	Reviewer / ISMS owner	Closure evidence		
Hold management review	Leadership	Inputs, decisions, resources and actions		

5. 90-day readiness sequence

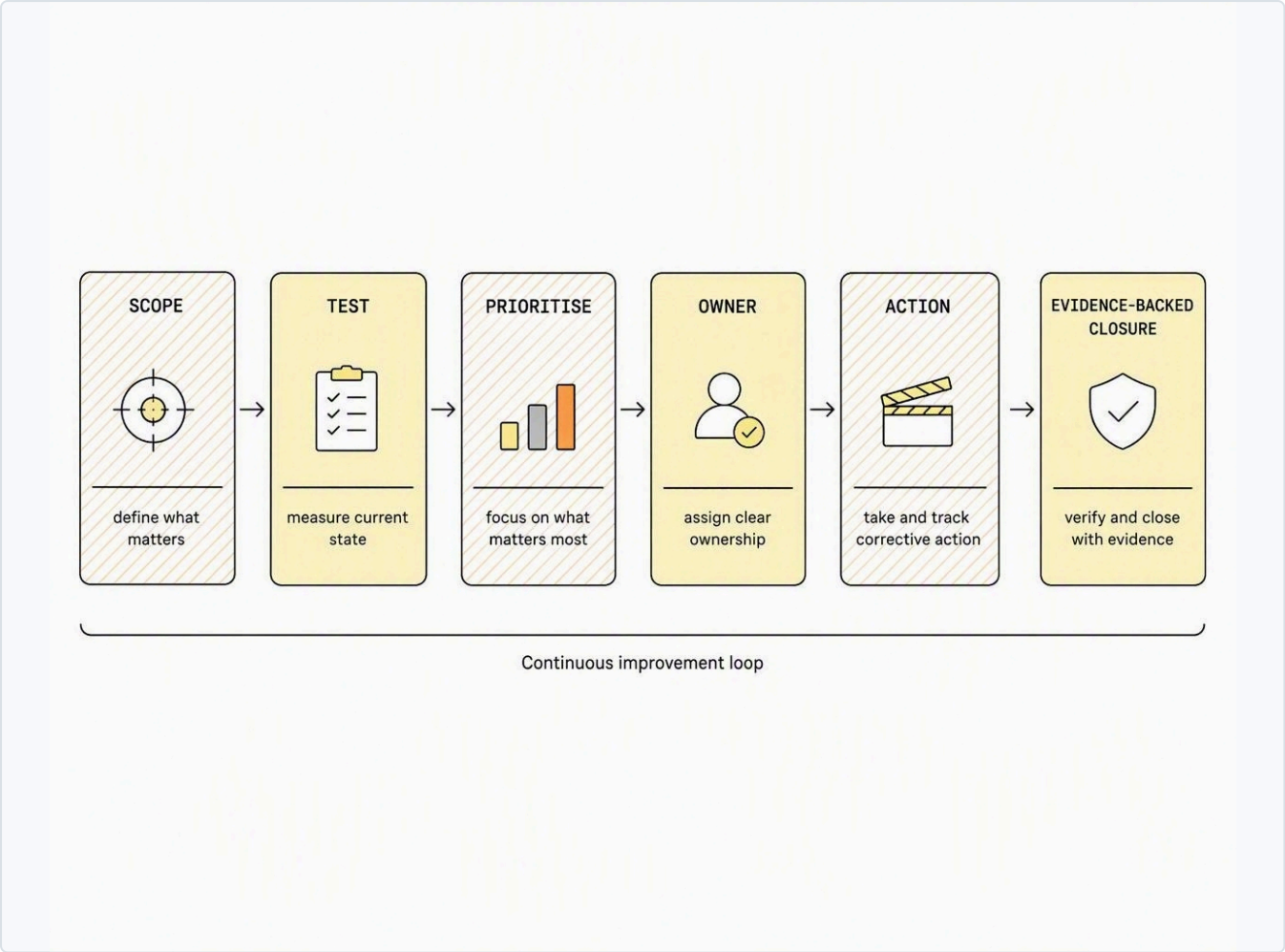


A 90-day readiness sequence covers scope and risk, controls and evidence, then internal and management review.

Days 1–30: lock scope, governance, risk method, initial risk register and SoA approach.

Days 31–60: operate priority controls, collect evidence from source systems and close critical design gaps.

Days 61–90: run an internal review, validate evidence, record corrective actions and prepare management review.



Evidence-backed gap analysis routes scope, testing, ownership and action to verified closure.

Use the final 30 days to prove closure, not to rewrite documents. A closed gap has a named owner, a completed action, supporting evidence and a reviewer's decision that the result is effective.

Final readiness check

- Scope and exclusions are explicit and approved.
- Risk treatment and SoA decisions are traceable.
- Priority controls have owners, operating evidence and exception paths.
- Policies match actual practice and have version/approval records.
- Internal review and management-review evidence are present.
- Open gaps have owners, dates, risk decisions and verification plans.

See it in your own environment

Ciphrix helps teams build a connected ISO 27001 workspace across scope, risks, controls, evidence and corrective actions—while human experts guide implementation and remain accountable for decisions. Book a demo to see the approach applied to your actual systems and programme.

Source notes

This tracker synthesises Ciphrix's published ISO 27001 audit checklist, certification process guide, gap analysis guide, Statement of Applicability guide, risk assessment guide, certification timeline guide and scope definition guide. Use the licensed ISO/IEC 27001 standard, your organisation's scope and your auditor or certification body to determine actual requirements and evidence expectations.