Ciphrix

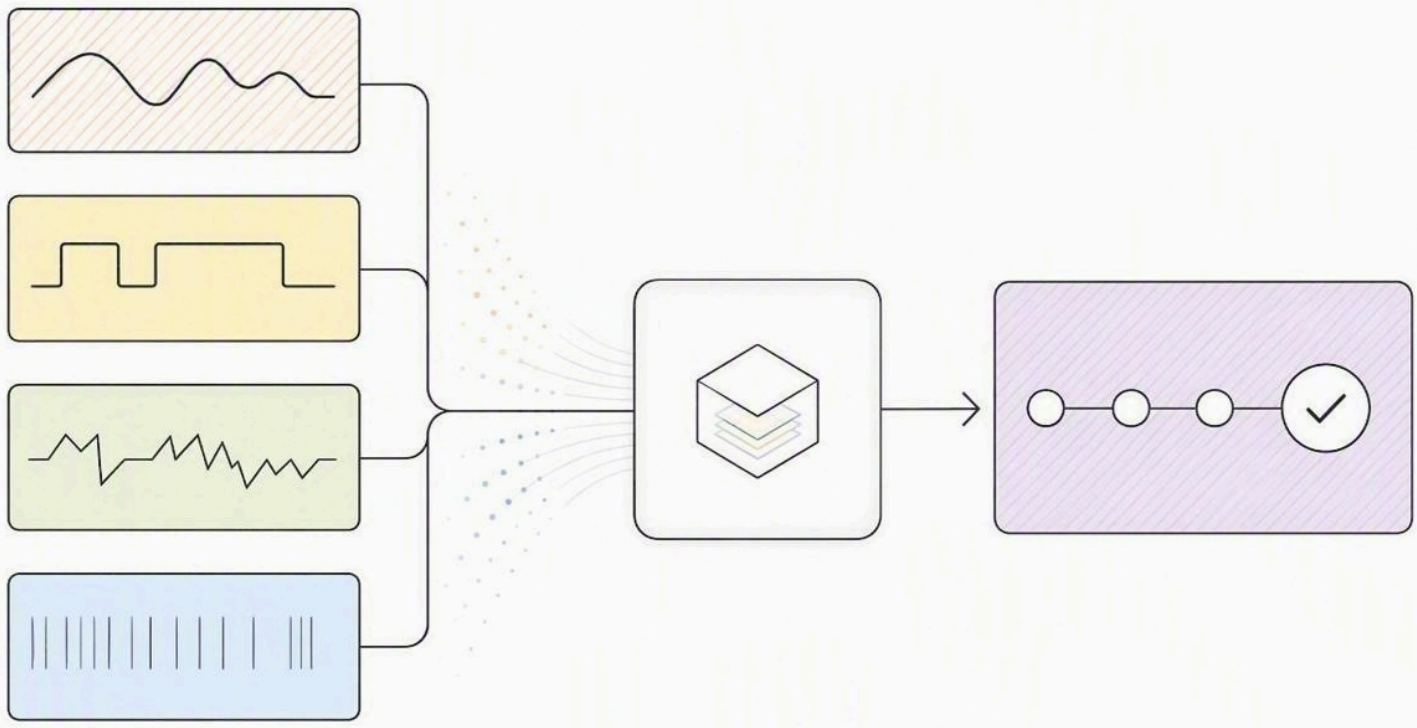
BUYER RESOURCE

PRACTICAL GUIDE

SOC 2 Evidence Collection Playbook

Define, collect, review and package evidence that can survive an auditor's questions

PUBLISHED 23 August 2026 **FROM** Ciphrix **DOCUMENT ID** CPX-BG-2608-9294



BUYER RESOURCE

SOC 2 Evidence Collection Playbook

CIPHRIX
BUYER GUIDE

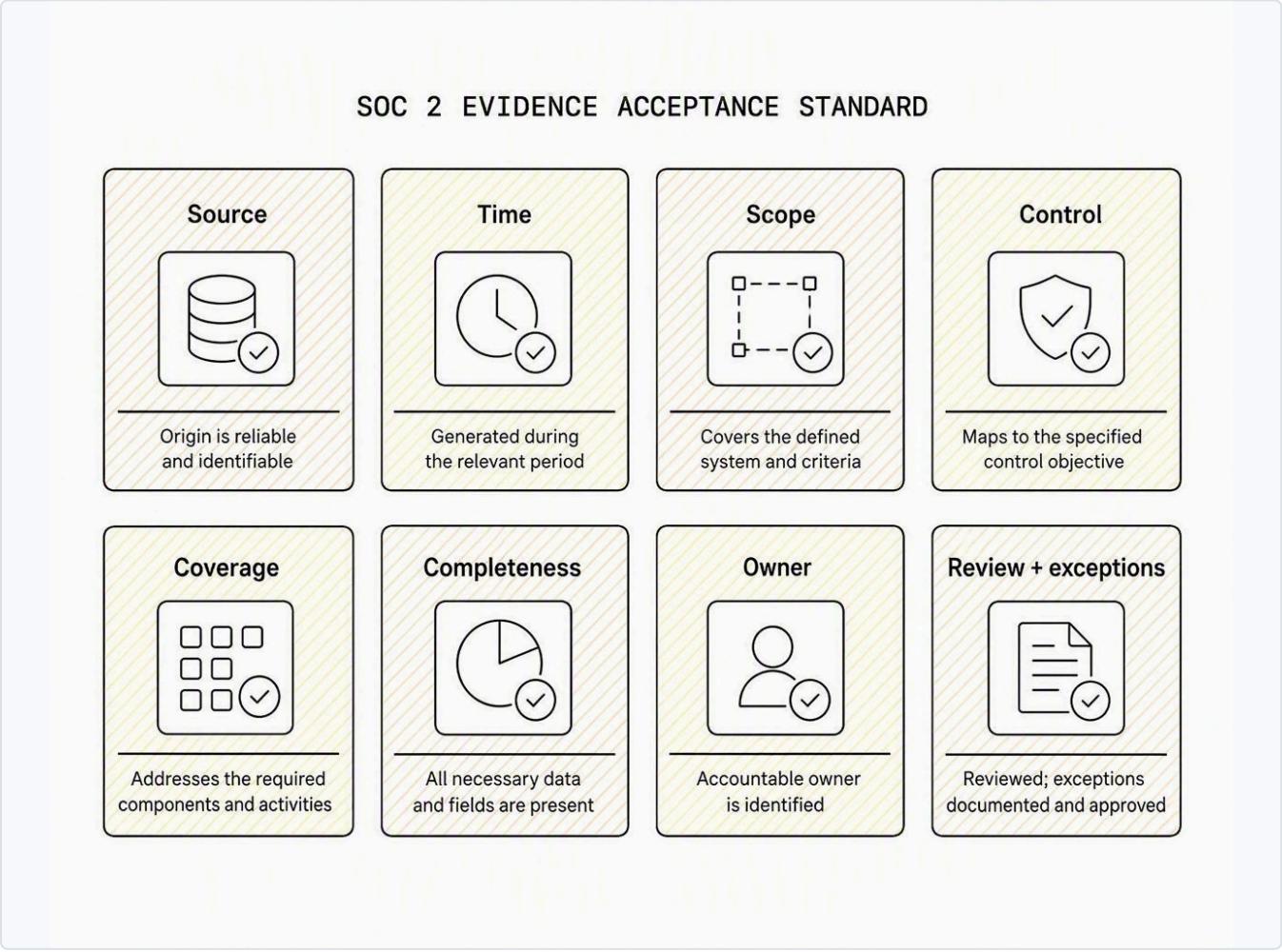
Define, collect, review and package evidence that can survive an auditor's questions

Define, collect, review and package evidence that can survive an auditor's questions

SOC 2 evidence is not a folder of screenshots. It is the traceable proof that a particular control was designed—and, for a Type II examination, operated during the relevant period. The difference matters because a policy can describe a control while an export, review record, ticket or log demonstrates what actually happened.

This pack gives teams a practical method for making evidence reviewable before the auditor requests it. It is an editorial planning tool, not an auditor-prescribed evidence list. A SOC 2 engagement is an independent attestation examination performed by a licensed CPA; the auditor evaluates evidence sufficiency and reaches the conclusion.

1. The evidence acceptance standard



Eight essential checks for clear, reviewable SOC 2 evidence.

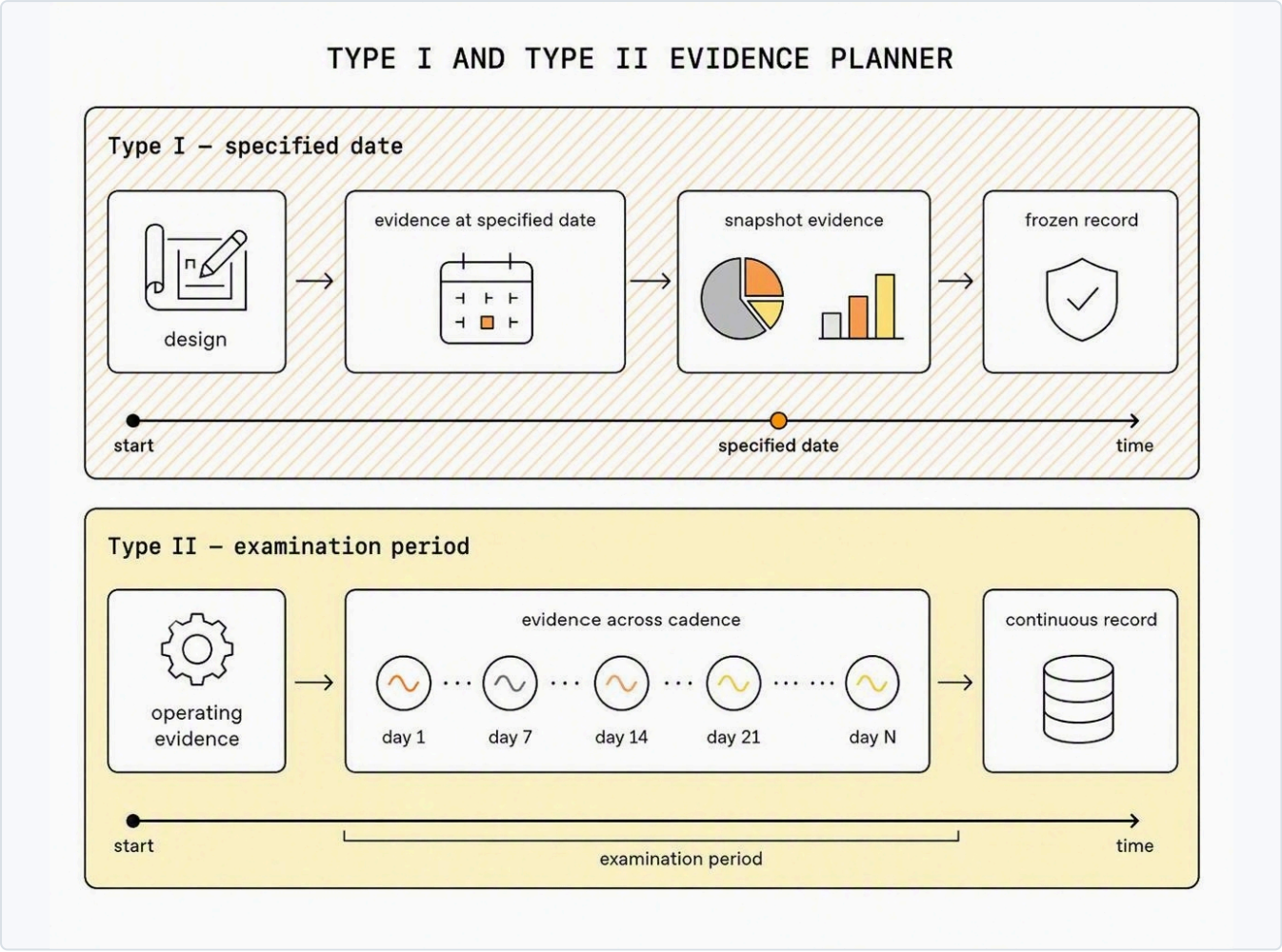
Before submitting an artifact, answer eight questions:

1. **Source:** Did it come from the system of record?
2. **Time:** Does it show when it was generated or the period it covers?
3. **Scope:** Does it relate to the in-scope service, system, environment and population?
4. **Control:** Is the control it supports explicit?
5. **Coverage:** Does it cover the requested report date or examination period?
6. **Completeness:** Are filters, fields, populations and exclusions clear?
7. **Ownership:** Is the control owner or responsible team known?
8. **Review and exceptions:** Where review is required, can a reviewer and any exception/remediation trail be seen?

Quick quality test

WEAK EVIDENCE	STRONGER EVIDENCE
Cropped configuration screenshot with no visible system/date/context.	Source-system export or screenshot with system context, time, relevant configuration and mapping.
Access review list with no reviewer, date or exception decision.	Complete population, review date, reviewer, exceptions and closure/remediation links.
Change ticket with no production linkage.	Approval, testing, deployment timestamp, production linkage and any exception route.
Policy PDF only.	Version, owner, approval, effective date and operating/acknowledgement evidence where relevant.

2. Plan Type I and Type II evidence differently

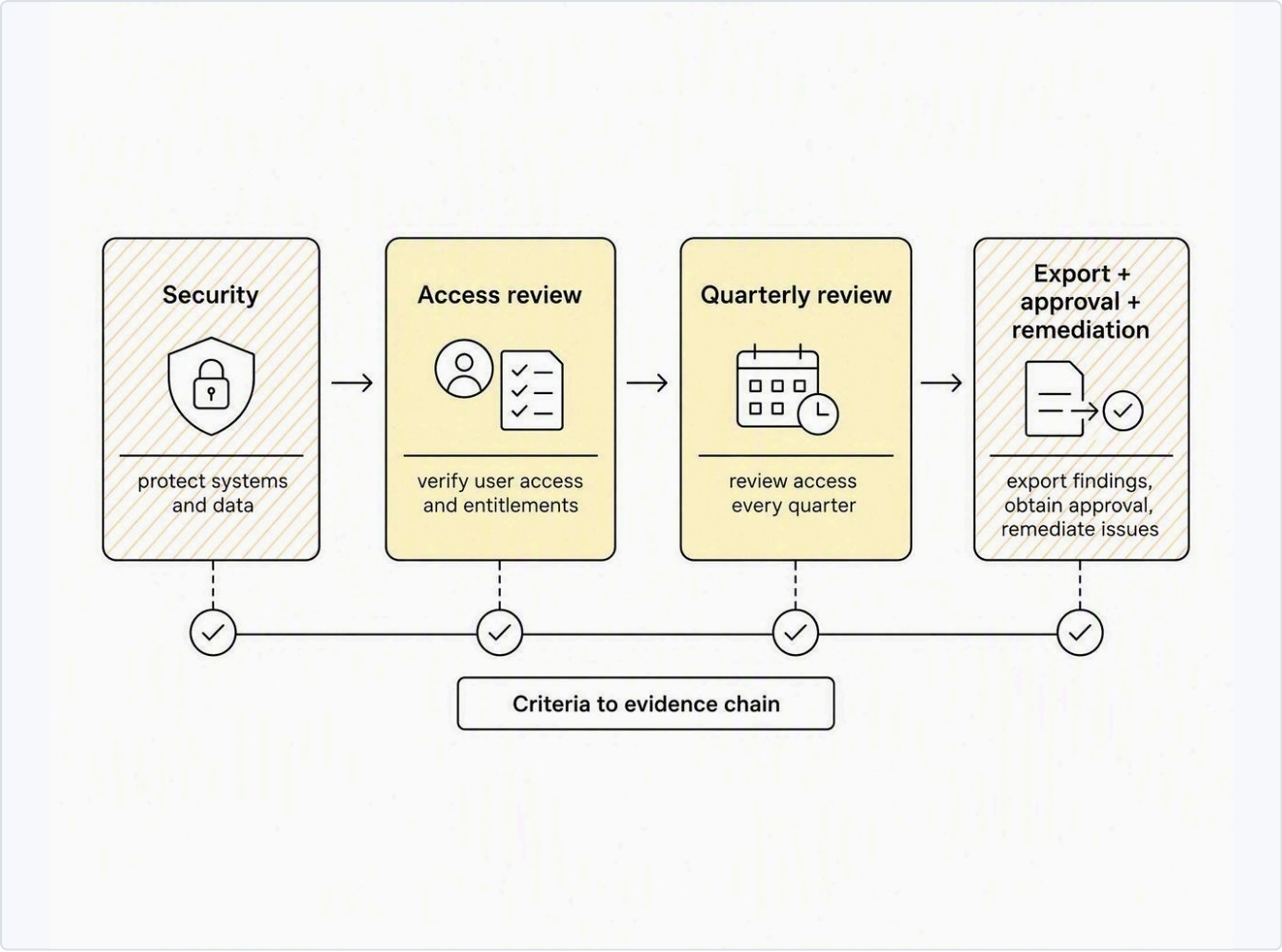


Type I evidence at a specified date versus Type II evidence across an examination period.

QUESTION	TYPE I	TYPE II
What is examined?	Control design as of a specified date.	Control design and operating effectiveness over a defined period.
Evidence pattern	Point-in-time configuration, approval or completed activity may support the relevant design question.	Evidence needs to show that recurring controls operated at their defined cadence throughout the period.
Common failure mode	Treating a current screenshot as proof that the control design is understood.	Collecting one current example and missing earlier periods, exceptions or remediation.
Operator focus	Clear scope, design, owner and source evidence.	Cadence, population, evidence continuity, exceptions and closure history.

For Type II, do not decide evidence needs only at fieldwork. If access reviews, vulnerability scans, backup checks or training cycles were not retained across the period, an end-of-period scramble cannot recreate the missing operation.

3. Start from the criterion, then control, then evidence



A traceable chain from Security to a quarterly access review and its evidence.

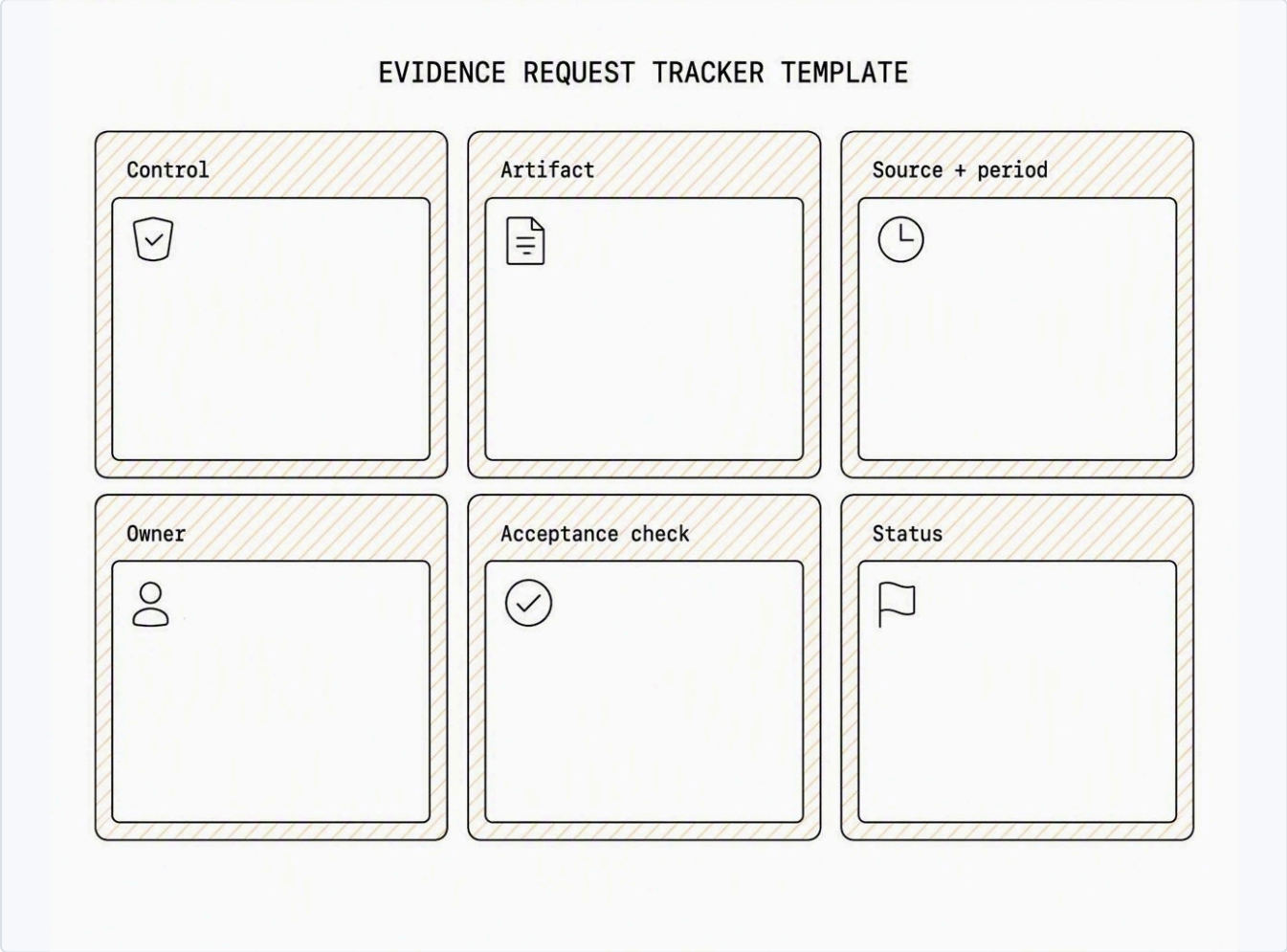
Security is the required SOC 2 baseline. Availability, Processing Integrity, Confidentiality and Privacy should be added only when they are relevant to the in-scope service, commitments, data and stakeholder needs. Do not collect evidence for a generic imagined SOC 2 programme; collect it for the scope and controls your organisation has actually selected.

Evidence request tracker template

FIELD	WHAT TO RECORD
Auditor request / control ID	The request identifier and the specific control it supports.
Control objective	What the control is meant to achieve.
Artifact required	The record/report/export/ticket needed and why.
Source system	System of record and report/query/configuration path.
Scope and period	In-scope population/environment and date range.
Cadence	Event-driven, monthly, quarterly or other control rhythm.

FIELD	WHAT TO RECORD
Owner / reviewer	Who collects, confirms and approves it.
Acceptance checks	What must be visible for the artifact to be reviewable.
Status / exception	Ready, pending, needs clarification, exception or remediated—with link to action.

4. Use this working evidence matrix



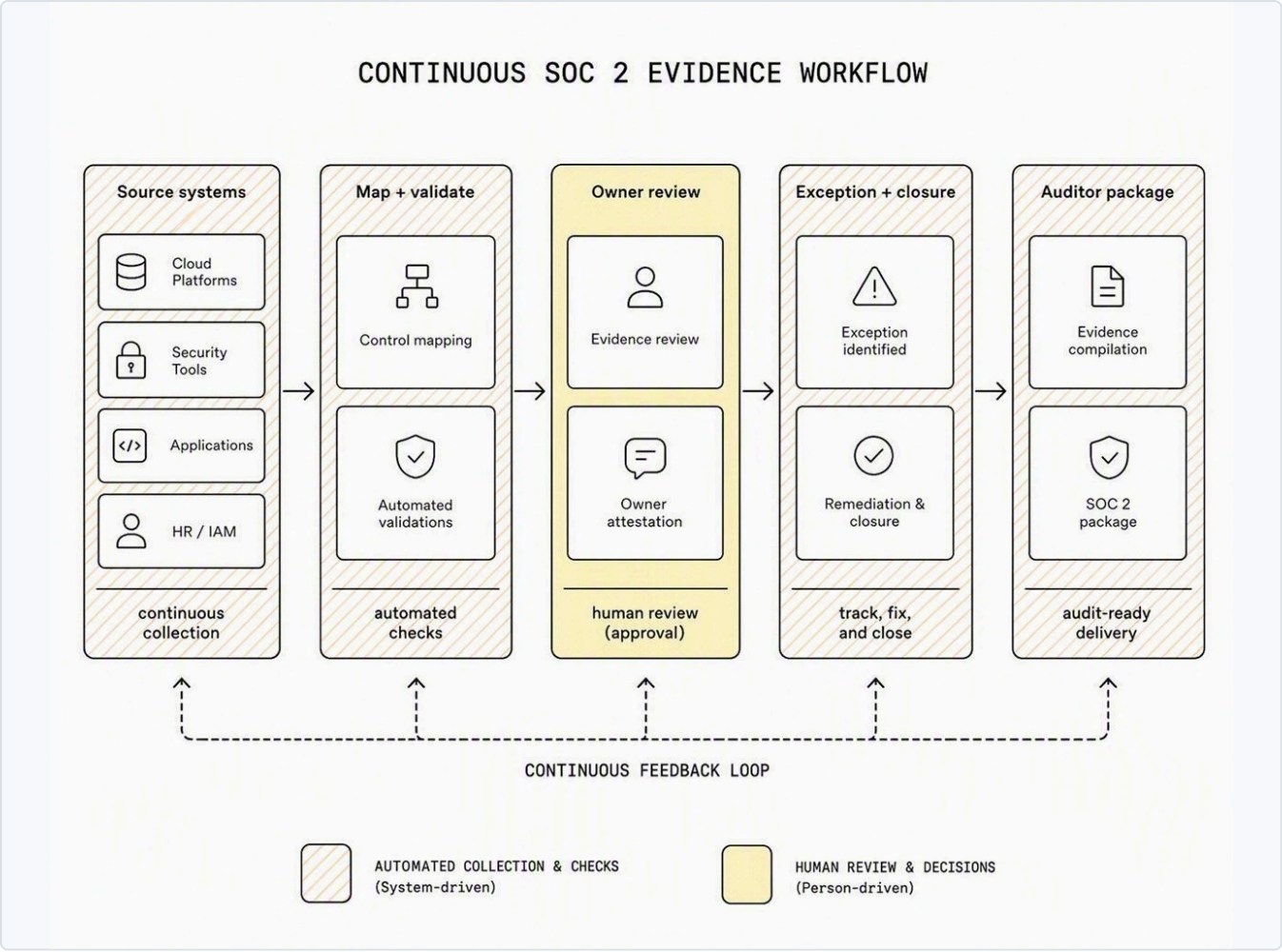
A practical evidence-request tracker with control, artifact, source and period, owner, acceptance check and status.

CONTROL AREA	EXAMPLE ARTIFACT	SOURCE / CADENCE	ACCEPTANCE CHECKS
Access management	Access review export, reviewer approval and exception/remediation record.	Identity provider, HRIS and ticketing; control-defined cadence.	Complete population, roles, reviewer/date, exception disposition.
Change management	Change ticket, approval, test evidence and deployment linkage.	Ticketing, CI/CD, repository; per change.	Clear approver, timestamps, production linkage and any emergency-change follow-up.
Vulnerability management	Scan report plus remediation tickets.	Scanner and ticketing; scan cadence.	In-scope assets, scan date, severity, finding status and resolution evidence.

CONTROL AREA	EXAMPLE ARTIFACT	SOURCE / CADENCE	ACCEPTANCE CHECKS
Incident response	Incident record, timeline, owner, actions and closure.	Incident/ticket system; per incident.	Relevant scope, decision trail, closure and corrective action where applicable.
Vendor management	Vendor inventory and assessment/approval record.	Vendor/procurement system; onboarding and periodic review.	Complete in-scope vendor population, reviewer/date, decision and supporting documentation.
Backup/availability	Configuration, job-monitoring output, failure and resolution record.	Backup/monitoring system; defined cadence.	In-scope systems, time range, job status and response to failures.
Training/policy acknowledgement	Completion report and current policy version/approval.	LMS, HRIS, policy system; defined cycle/new-hire flow.	Assigned population, completion status, policy version/effective date and exceptions.
Risk management	Risk record, treatment decision and review history.	Risk register; review cadence.	Owner, rating, treatment, due date and current review status.

Treat the table as a tracker starter, not as a promise that every row is needed. Actual evidence depends on the selected criteria, control design, scope and audit plan.

5. Run the evidence workflow continuously



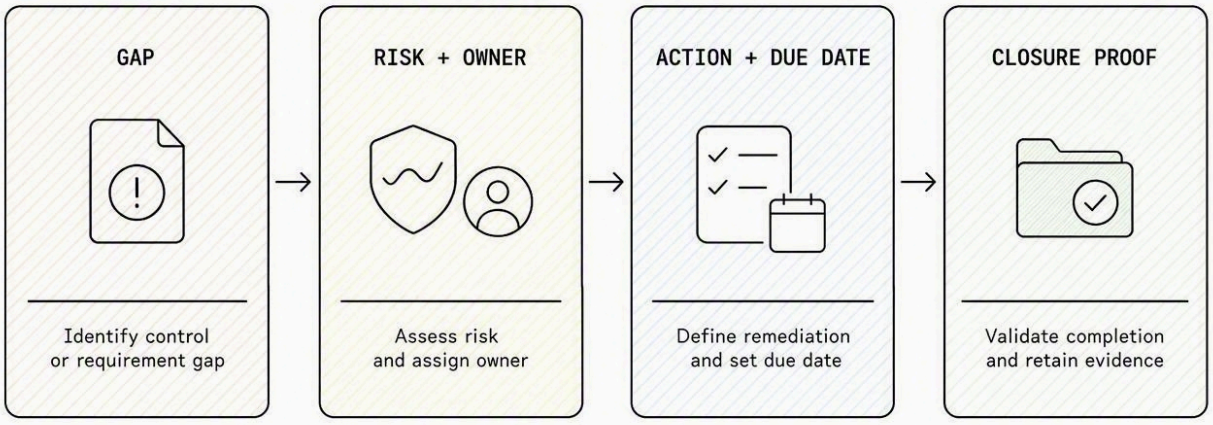
A continuous evidence route from source systems to validated, owner-reviewed auditor packaging.

1. **Collect from the source.** Retrieve exports, logs, approvals and records from the systems that operate the control.
2. **Map it.** Link the artifact to the control, scope, owner and requested period.
3. **Validate deterministically.** Flag missing dates, empty exports, incomplete fields, unclear filters, stale items and period gaps.
4. **Review.** The control owner confirms that the artifact accurately reflects reality and explains any exception.
5. **Track exceptions.** Assign owner, action, due date, decision and closure evidence.
6. **Package.** Give the auditor a clear route from request to evidence, context and follow-up.

Automation is valuable for collection, mapping, checks, reminders and packaging. It should not independently decide that a control was effective, that a risk is acceptable or that an auditor will accept the evidence.

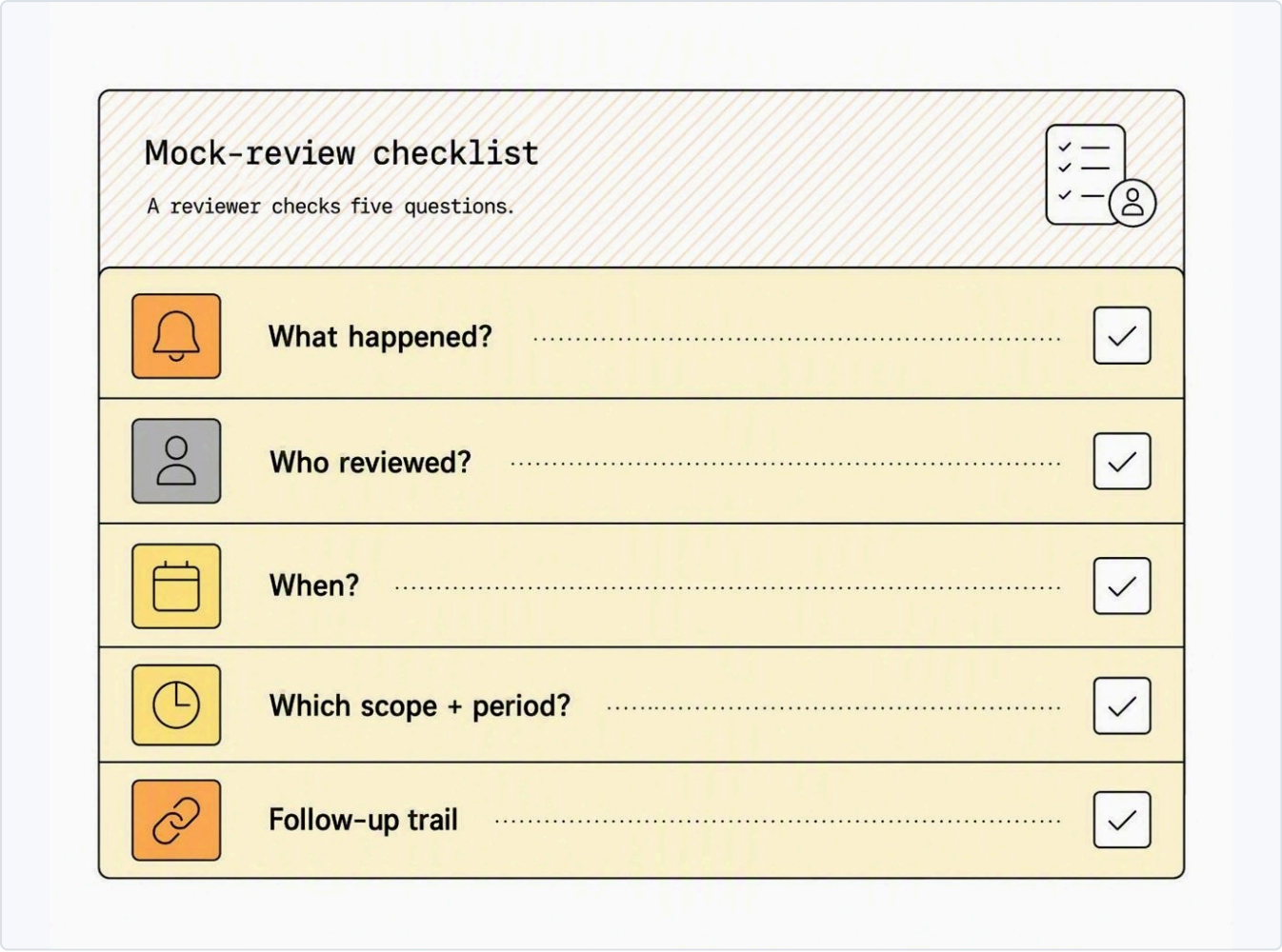
Exception and remediation record

FIELD	EXAMPLE
Control / artifact	Quarterly production-access review / Q2 export
Gap	Review completed late; two exceptions still open at review time
Scope and risk	Named production roles; risk and affected period recorded
Owner	IAM owner
Response	Remove inappropriate access; document time-bound approved exception where needed
Due date / escalation	Date, approver and escalation route
Closure proof	Retest/export, ticket updates and approval record



A concise exception record from identified gap through accountable closure proof.

6. Pre-submission and mock-review checklist



Five questions an independent reviewer should answer before an evidence package is submitted.

Before submission, ask a reviewer who did not collect the artifact:

- Can they identify the source system and control without an explanation call?
- Can they tell what happened, who performed/reviewed it, when and for which population?
- Can they see the relevant criteria, scope and period?
- Can they understand report filters, parameters, exceptions and exclusions?
- Can they trace a failed item or exception to a decision and closure record?
- For Type II, can they see that the control operated at the intended cadence across the period?

If the answer relies on “ask the person who made it,” the package needs more context.

Make SOC 2 evidence a maintained operating asset

Ciphrix helps teams collect evidence from source systems, map it to controls, surface gaps and route work to accountable owners—while expert humans retain review, scope and risk decisions.
Book a demo to see continuous SOC 2 evidence collection applied to your actual systems and controls.

Source notes

This pack synthesises Ciphrix's published SOC 2 evidence collection guide, SOC 2 audit guide, Trust Services Criteria guide, continuous evidence collection guide and audit readiness guide. Confirm report scope, controls and evidence expectations with your service auditor.