Arcline

November 6, 2026

SAMPLE DELIVERABLE

Audit Evidence Pack: SOC 2 Technical Controls

Ten controls, the evidence behind each one, and the two gaps that would fail an audit today.

SAMPLE Fictional demonstration data · Prepared by Arcline

PREPARED FOR

Northwind Payments

Fintech / payments (PCI DSS scope) · 28 engineers · 3 Kubernetes clusters · Azure and AWS

Framework: SOC 2 Type II (technical controls) · Evidence assembled from the platform

01 Control status

5	3	2
CONTROLS MET	PARTIAL	GAPS

This is the evidence pack for one framework's technical controls, assembled from the platform rather than from a policy document. Each row names the control, the evidence that satisfies it, and the owner. The point is that an auditor can be handed this table and the exports behind it, without a reconstruction project.

Five controls are met and evidenced automatically. Three are partial, which in practice means the control exists but the evidence is manual or incomplete. Two are genuine gaps, and both are the same finding an auditor reaches first: privileged actions are not logged, and recovery has never been tested.

02 Control evidence

CONTROL	REF	STATUS	EVIDENCE	OWNER
Access is provisioned from the identity provider	CC6.1	MET	SCIM group to RBAC mapping exported nightly; join table retained 12 months	Platform
Access is removed within one business day of departure	CC6.1 / CC6.6	PARTIAL	Offboarding script runs on a schedule; 90-day average is 2.7 days	IT + Platform
Production changes are reviewed before they merge	CC7.1 / PCI 6.5	MET	Branch protection requires one approval; 100% of merges in the last 90 days have one	Platform
Every production change is traceable to a deploy	CC7.1	MET	Argo CD application history joined to commit SHA; retained with the cluster	Platform
Privileged actions are logged	CC7.2	GAP	Kubernetes audit policy is unset; control-plane logs expire in 3 days	Platform
Logs are retained for 12 months	CC7.2	PARTIAL	Application logs 90 days; audit logs not collected at all	Platform
Data is encrypted in transit	CC6.7	MET	TLS 1.2+ enforced at ingress and between services; cipher policy in the ingress config	Platform
Data is encrypted at rest, with managed keys	CC6.7	MET	Provider-managed keys on Postgres and disks; key rotation record exported quarterly	Platform
The platform restores within the documented RTO	A1.2	GAP	No restore has ever been performed; retention is 7 days and no RTO is documented	Platform

CONTROL	REF	STATUS	EVIDENCE	OWNER
Incidents are reviewed and actions tracked	CC7.3 / CC7.4	PARTIAL	Postmortems exist for 6 of 11 incidents this year; actions are not tracked to closure	Platform

03 The two gaps that would fail an audit

Privileged actions are not logged. Without a Kubernetes audit policy, the platform cannot show who ran a command in production, who changed a role binding, or who read a secret. Every other access control depends on this record, so a single missing audit log undermines the four controls above it that currently pass.

Recovery has never been tested. A backup policy is not evidence that the platform can restore. Auditors increasingly ask for the date, duration, and result of the last drill, and “we have backups” is not an answer. Both gaps close in under a week of engineering, which is why they are first in the remediation plan.

04 What good evidence looks like

The five passing controls have one thing in common: the evidence is produced by the platform, on a schedule, without anyone assembling it. The group-to-role mapping is exported nightly. The merge approval count comes from the Git host. The deploy history comes from Argo CD.

That is the difference between an audit that takes an afternoon and one that takes six weeks. It is also why the work is worth doing beyond the certificate: a platform that can produce this table on demand is a platform where access is reviewed, changes are traceable, and recovery has been proven.