Arcline

November 6, 2026

SAMPLE DELIVERABLE

90-Day Remediation Plan

The owner-by-owner sequence: what to delete, what to build, and what to deliberately leave alone.

SAMPLE Fictional demonstration data · Prepared by Arcline

PREPARED FOR

Northwind Payments

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

Cloud spend, the Kubernetes platform, delivery pipeline, on-call practice, and the evidence behind SOC 2 and PCI DSS controls, across production and staging.

01 How to use this plan

This is the owner-by-owner sequence behind the findings report. It is ordered by what removes risk or cost fastest per day of effort, not by severity: two of the highest-value items are deletions that take a day, and the compliance work is scheduled so it lands before the audit window rather than during it.

Every item names an owner, an effort estimate, and its monthly effect. Nothing here requires a migration, a new platform, or a freeze on product work.

02 First 14 days

Delete the idle node pool

+$4,300/MO

Platform · 1 day

Zero pods for 61 days. Nothing depends on it; confirm with the workload team and delete.

Delete 42 unattached disks and 31 stale snapshots

+$4,000/MO

Platform · 1 day

Cross-check tags against the retention policy first, then delete. No application impact.

Agree the three SLIs and the SLOs

RISK

Platform + product · 2 days

Checkout success, checkout p95, webhook delivery. Three numbers, one owner each, agreed in writing.

Adopt an error-budget policy

RISK

Platform + product · 1 day

Above 50% budget: ship freely. Below 25%: reliability work takes priority. Exhausted: freeze and fix.

03 Days 15–30

Enable Kubernetes audit logging

COMPLIANCE

Platform · 3 days

Metadata level baseline, RequestResponse for secrets and RBAC. Ship to immutable storage.

Set 12-month retention on audit and application logs

+$1,500/MO

Platform · 2 days

30 days hot, 12 months archive. This is the CC7.2 evidence and it costs less than the current 90-day hot tier.

Rightsize the managed database

+$5,200/MO

Platform · 1 week

16 vCores from a 14-day baseline. Schedule a maintenance window and watch p95 during the cutover.

04 Days 31–60

Codify the drift and add a nightly check

RISK

Platform · 1 week

Import the 14 resources, apply from the pipeline only, and open a ticket when drift is detected.

Design a two-person on-call rotation

RISK

Platform · 1 week

Primary and secondary, a real escalation policy, and five runbooks for the alerts that actually fire.

Set resource requests and limits per namespace

+$2,000/MO

Platform · 1 week

Two-week usage baseline, then a LimitRange per namespace. Let the autoscaler shrink the pools.

Tier logs and drop debug ingestion

+$1,900/MO

Platform · 3 days

Debug goes to a 7-day tier, or nowhere. Production keeps what an incident actually needs.

05 Days 61–90

Enable point-in-time recovery and volume snapshots

COMPLIANCE

Platform · 3 days

35-day retention. This is the control, not the backup job — the evidence is the drill.

Run the first timed restore drill

COMPLIANCE

Platform · 1 day

Restore the database and one volume, record the duration, and file it as the A1.2 evidence.

Replace the shared cluster-admin credential

COMPLIANCE

Platform · 3 days

Per-person, time-bound access through the IdP, with session logging. Rotate and retire the shared key.

Commit the stable baseline to a savings plan

+$6,800/MO

Platform · 1 week

Only after the deletions, so the commitment covers what actually remains.

06 What we would not do yet

SCOPE DISCIPLINE

Three things are deliberately absent. A cluster upgrade, because it changes nothing in this report and would consume the first month. A service mesh, because the current ingress works and the operational cost is not yet justified. And a multi-region active-active deployment, because 99.9% does not require it — the SLO conversation should come before the architecture.

Saying no to those three is most of why this plan fits in 90 days.