# Plan of Action & Milestones

Every open deficiency with its control, owner, milestones and due date, exported from the workspace on September 26, 2026. Ten items tracked, nine open, one closed this quarter. The 90-day SLA runs from first observation; items past it are flagged for the board pack.

**TRACKED**
**10**
9 open · 1 closed in Q3

**AGING PAST 30 DAYS**
**5**
1 past the 90-day SLA

**CRITICAL / HIGH OPEN**
**0 / 4**
4 medium · 1 low

**SOURCES**
**3**
CloudSignals scan · pen test · internal audit

| ID | WEAKNESS | SEV. | SOURCE · CONTROL | OWNER | OPENED | DUE | MILESTONES | STATUS |
|---|---|---|---|---|---|---|---|---|
| POAM.2026.001 | **Privileged cloud credentials without rotation**<br>AWS Production · one access key 410 days old, two over 180 | CRIT. | CloudSignals<br>SOC 2 CC6.1 · ISO A.5.17 · NIST PR.AA | Platform eng. lead | Jun 23 | Sep 21 | **Done** inventory of keys (Jul 2)<br>**Done** rotation runbook (Jul 30)<br>**Blocked** legacy SFTP integration<br>**Due** rotate all, enforce 90-day policy (Dec 15, pending board) | PAST 90 DAYS |
| POAM.2026.002 | **Publicly reachable storage with sensitive data**<br>Azure Production · 3 blob containers | HIGH | CloudSignals<br>SOC 2 CC6.6 · ISO A.8.3 · PCI 1.3 | Platform eng. lead | Aug 4 | Nov 2 | **Done** access review (Aug 20)<br>**In progress** private endpoints (Oct 10)<br>**Due** public access disabled, evidence attached (Oct 31) | IN PROGRESS |
| POAM.2026.003 | **MFA not enforced for third-party contractor accounts**<br>Microsoft 365 · 2 contractor groups, 41 accounts | HIGH | Internal audit<br>SOC 2 CC6.1 · ISO A.5.16 · NIST PR.AA-03 | IT operations manager | Aug 11 | Nov 9 | **Done** conditional-access policy drafted (Sep 5)<br>**Due** enforce for group A (Oct 14), group B (Oct 28) | IN PROGRESS |
| POAM.2026.004 | **Public S3 bucket with build artifacts**<br>AWS Production · 1 bucket | HIGH | CloudSignals<br>SOC 2 CC6.6 · CIS AWS 2.1.5 | Platform eng. lead | May 12 | Aug 10 | **Done** bucket policy restricted, block public access (Jun 3)<br>**Done** verified by scan of Jun 4 | CLOSED JUN 4 |
| POAM.2026.005 | **CI/CD repositories without branch protection**<br>AWS Production · 14 repositories (6 archived) | HIGH | Pen test<br>SOC 2 CC8.1 · ISO A.8.25 · NIST PR.PS | Head of Technology | Aug 18 | Nov 16 | **Done** required reviews on 8 active repos (Sep 12)<br>**Decision due** archive or protect the 6 inactive repos (Oct 17) | DECISION DUE |

| ID | WEAKNESS | SEV. | SOURCE · CONTROL | OWNER | OPENED | DUE | MILESTONES | STATUS |
|---|---|---|---|---|---|---|---|---|
| POAM.2026.006 | **Management ports open to the internet**<br>Azure Production · 6 hosts, RDP and SSH | MED. | CloudSignals<br>SOC 2 CC6.6 · CIS Azure 7.1 · NIST PR.IR | Network lead | Aug 25 | Nov 23 | **Done** bastion deployed (Sep 19)<br>**Due** NSG rules closed on 6 hosts (Oct 24) | IN PROGRESS |
| POAM.2026.007 | **Incident-response contact tree outdated**<br>CIRP · 4 of 11 contacts changed roles | MED. | Internal audit<br>SOC 2 CC7.4 · ISO A.5.24 · NIST RS.CO | IR lead | Sep 2 | Dec 1 | **Due** contact tree refreshed and tested (Oct 31)<br>**Due** tabletop exercise (Nov 6) | SCHEDULED |
| POAM.2026.008 | **Audit logging disabled in secondary regions**<br>AWS Production · 2 regions, 14% of resources | MED. | CloudSignals<br>SOC 2 CC7.2 · ISO A.8.15 · PCI 10.2 | Platform eng. lead | Sep 8 | Dec 7 | **Due** CloudTrail enabled, centralized, 12-month retention (Nov 14) | SCHEDULED |
| POAM.2026.009 | **S3 buckets without default encryption in staging**<br>AWS Staging · 9 buckets | MED. | CloudSignals<br>SOC 2 CC6.7 · ISO A.8.24 · PCI 3.5 | Platform eng. lead | Sep 15 | Dec 14 | **Due** default SSE-KMS applied by policy (Oct 31) | SCHEDULED |
| POAM.2026.010 | **Endpoint backup agent missing on finance workstations**<br>Finance · 12 of 38 workstations | LOW | Internal audit<br>SOC 2 A1.2 · ISO A.8.13 · NIST PR.DS-11 | IT operations manager | Sep 19 | Dec 18 | **Due** agent deployed by policy, restore test (Nov 21) | SCHEDULED |

# How the POA&M is kept.

## Where items come from

Three sources feed the POA&M. CloudSignals raises an item when a scan finding is accepted into the register (findings are first triaged in the index; only risks that need a plan become POA&M entries). Penetration tests and internal audits add items from their reports, with the report attached as evidence. Every item carries the controls it affects across the frameworks in the control baseline, so one fix updates SOC 2, ISO 27001 and PCI DSS pass rates at the next scan.

## The SLA

Ninety days from first observation, regardless of severity; critical and high items are expected sooner and are reviewed weekly at the vCISO cadence. An item past 90 days is flagged in the board pack and needs a recorded decision: extend with compensating controls, accept the risk, or transfer it. The decision is written to the audit trail in both the workspace and CloudSignals.

## Closing an item

An item closes when the next scan no longer raises the finding, or when the auditor-facing evidence (configuration export, screenshot, ticket, policy) is attached and reviewed. Closed items stay in the export for the quarter so the board can see what was finished, then move to the archive.

### COLUMNS IN THE FULL EXPORT

ID · weakness · description · severity · source · affected controls (per framework) · asset or scope · owner · opened · due · milestones with dates and status · compensating controls · evidence links · risk register link · status · closed date · closure evidence. The CSV and JSON exports include every column; this PDF shows the ones a reviewer reads first.

### SEVERITY AND SCORE

| | |
|---|---|
| **Critical** | Exploitable now with high impact; weekly review, 30-day target |
| **High** | Likely and impactful; 60-day target |
| **Medium** | Within the 90-day SLA |
| **Low** | Within the SLA; may be batched into a release |

Register risks use likelihood × impact (1–5 each); POA&M severity follows the finding's CVSS band or the auditor's rating.

This sample reproduces the structure of a Client Vision POA&M export using the Big Venture Incorporated demo workspace. Names, figures and dates are illustrative. 3HUE Executive Consulting LLC · 3hue.net · (954) 738-4454