Security remediation plan

An anonymized excerpt from a real 3PS assessment

The assessment connected endpoint inventory with a separate network discovery to identify patch, protection, lifecycle, and coverage gaps. The resulting plan sequenced the work around business risk, application owners, maintenance windows, and recovery readiness.

Source and scope

This excerpt is adapted from an assessment and remediation plan prepared by 3PS. Client names, system identifiers, estate counts, and sensitive findings have been removed; wording has been condensed. It shows recommended work and acceptance criteria, not evidence that remediation was completed.

Proposed remediation phases

These were the assessment's proposed planning windows. Timing, scope, owners, and maintenance access must be agreed for each engagement.

Days 0–2

Establish safety and scope

Confirm backups and restore checks, assign application owners, agree change windows, reconcile coverage, and define pilot groups.

Planned evidence Approved schedule, owner list, and rollback checklist.

Days 3–10

Address the highest risks

Validate priority vulnerabilities, address protection gaps, and test changes on low-impact systems before business-critical services.

Planned evidence First remediation wave with recorded evidence.

Days 11–30

Roll out controlled changes

Deploy approved updates in stages, coordinate restarts, validate applications, and close reporting gaps.

Planned evidence Reduced priority patch backlog, with recorded installation evidence and application checks.

Days 31–60

Harden the infrastructure

Validate virtualization updates and network-control changes; document vendor compatibility and exceptions.

Planned evidence Infrastructure remediation register.

Days 61–90

Resolve lifecycle decisions

Sequence migration, replacement, or isolation of legacy systems and establish recurring reporting.

Planned evidence Lifecycle roadmap and an operating review cadence.

Controlled rollout and acceptance

An anonymized excerpt from a real 3PS assessment

Rollout rings

01 Pilot

Validate installation, restart behavior, services, logs, and rollback on low-impact systems.

02 Representative systems

Have application owners verify essential workflows on a small group before broader rollout.

03 Production

Use agreed maintenance windows and post-change checks for standard systems.

04 Critical systems

Require a dedicated change plan, backup verification, owner sign-off, and a recovery path.

05 Exceptions

Document unsupported or vendor-blocked systems, compensating controls, an owner, and a replacement target.

Source and scope

This excerpt is adapted from an assessment and remediation plan prepared by 3PS. Client names, system identifiers, estate counts, and sensitive findings have been removed; wording has been condensed. It shows recommended work and acceptance criteria, not evidence that remediation was completed.

Acceptance criteria

- [ ] **Coverage is accounted for**

  In-scope systems appear in the inventory or have a documented exclusion; other platform types have assigned inventory sources.

- [ ] **Changes have evidence**

  Approved patches show as installed or have a documented vendor exception and compensating control.

- [ ] **The business workflow works**

  An assigned application owner confirms essential application and interface checks after maintenance.

- [ ] **Recovery is ready**

  The backup, restore point, and rollback procedure are validated before a high-risk change.

- [ ] **Protection is operating**

  Endpoint protection is active, updating, and reporting across supported systems, with the intended standard documented.

- [ ] **Lifecycle decisions are recorded**

  Unsupported or aging systems have a documented migration, replacement, isolation, extended-support, or risk-acceptance decision.

- [ ] **Leadership can see what remains**

  Reporting separates open, remediated, accepted, and overdue risks, with supporting evidence.