# Week 3 Mitigation Plan Update (Summary Table)

Project: IAM & Network Security Hardening

Covers: Week 2 → Week 3 Updates for All Risks (R1–R15)

Linked Back To: Week 2 Mitigation Plan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk ID | Week 2 Status (Summary) | Week 3 Change / Progress | Responsible | Next Step |
| R1 | IAM roles manually reviewed; draft least-privilege policy created. | Automated IAM scanner tested with Cloud Asset Inventory. | Security Lead | Complete automation and validation by Week 4. |
| R2 | Multiple SAs had broad permissions (Editor roles). | Reduced SA scope; added key rotation and workload identity federation planning. | Cloud Admin | Roll out federation to all service accounts. |
| R3 | Default VPCs active with broad ingress rules. | Created custom firewall tiers and verified segmentation. | Network Engineer | Add subnet-based staging and production isolation. |
| R4 | Audit logs enabled for 50% of projects. | Centralized 80% coverage in Cloud Logging with export setup. | Security Team | Add SCC-based alert metrics and dashboard. |
| R5 | Some public endpoints lacked HTTPS enforcement. | Enabled HTTPS load balancers and WAF (Cloud Armor). | DevOps Engineer | Implement automated SSL certificate renewal alerts. |
| R6 | Legacy projects using default VPC configuration. | Deleted 25% of default VPCs and developed Terraform template. | Network Engineer | Remove remaining defaults and apply template organization-wide. |
| R7 | No CSPM process existed for misconfiguration scans. | Began SCC deployment for continuous monitoring. | Security Analyst | Enable daily scheduled CSPM scans across all projects. |
| R8 | Inconsistent IAM naming across resources. | Drafted standard naming convention under review. | IAM Manager | Apply across org-level IAM templates. |
| R9 | Manual patch updates conducted quarterly. | Automation framework introduced; 60% completion achieved. | System Administrator | Finalize automation and verify dashboard accuracy. |
| R10 | MFA optional; applied inconsistently across admin accounts. | MFA enforcement approved; rollout 40% complete. | Security Lead | Complete remaining MFA enforcement and verify compliance. |
| R11 | Firewall rules permitted open ingress (0.0.0.0/0). | Restricted rules; created review schedule for quarterly audits. | Network Engineer | Audit compliance and block remaining open rules. |
| R12 | Cloud Storage lacked retention policies and versioning. | Enabled object versioning and lifecycle management rules. | Cloud Admin | Audit configurations and adjust lifecycle retention. |
| R13 | Inactive service accounts not disabled automatically. | Introduced lifecycle disablement policy (>90 days). | IAM Manager | Deploy org-wide automation and review logs monthly. |
| R14 | CIS baseline compliance incomplete (Level 1 partial). | Deployed SCC compliance scanner for monthly remediation. | Security Team | Track and close all Level 1 findings by next audit. |
| R15 | Backups not validated for recovery testing. | Instituted monthly restoration testing for all instances. | System Administrator | Maintain restoration verification reports monthly. |