# Compliance Lifecycle & Evidence Plan (v2) – PCI DSS & GDPR Integrated

Project: IAM & Network Security Hardening

Coverage: Weeks 1–2 — Risk, Compliance, and Evidence Management (with PCI DSS & GDPR Integration)

## 1. Compliance Lifecycle Overview

The compliance lifecycle follows a continuous improvement model aligned with NIST CSF, CIS GCP, PCI DSS v4.0, and GDPR Articles 5 and 32. Each phase ensures security controls are documented, tested, and maintained across the organization’s cloud environment.

|  |  |  |
| --- | --- | --- |
| Phase | Description | Responsible |
| Scope & Identify | Define applicable compliance frameworks (NIST CSF, CIS GCP, PCI DSS, GDPR). Identify regulated data (payment, PII) and affected systems. | Security Lead, Data Governance |
| Assess & Implement | Perform gap analysis against PCI DSS and GDPR; implement policies for encryption, retention, and logging; enforce GCP Org Policies. | Security Lead, IAM Engineer |
| Monitor & Detect | Enable continuous monitoring via SCC, Cloud Logging, and alerting to detect non-compliance and potential data breaches. | Security Analyst |
| Report & Review | Prepare compliance reports covering NIST, CIS, PCI DSS, and GDPR mappings. Export SCC findings for evidence. | Security Lead |
| Improve & Remediate | Address audit findings, close compliance gaps, update controls based on new standards or regulation updates. | All Team Leads |

## 2. Framework Integration Overview

This project integrates key compliance frameworks to ensure both internal and regulatory obligations are met:  
• \*\*NIST CSF\*\* – Provides the overarching Identify → Protect → Detect → Respond → Recover structure.  
• \*\*CIS GCP Benchmarks\*\* – Define implementation-level guidance for GCP resources.  
• \*\*PCI DSS v4.0\*\* – Focuses on cardholder data protection, access control, and logging requirements.  
• \*\*GDPR (Articles 5 & 32)\*\* – Emphasizes data minimization, lawful processing, and protection of personal data.

|  |  |  |
| --- | --- | --- |
| Framework Control | Control Focus | Mapped Implementation |
| PCI DSS 8.3 | MFA enforcement for all administrative access | MFA 100% rollout via Google Identity |
| PCI DSS 10.2 | Track and monitor all access to network resources | Cloud Logging with BigQuery Export |
| PCI DSS 3.2 | Encryption of stored cardholder data | CMEK enforced in Cloud SQL and Storage |
| GDPR Art. 5(1)(e) | Data minimization and retention limits | Lifecycle rules in Cloud Storage |
| GDPR Art. 32(1) | Security of processing (encryption, pseudonymization) | IAM least privilege + CMEK + SCC monitoring |

## 3. Evidence Collection & Retention

Evidence collection incorporates cross-framework validation across NIST, CIS, PCI DSS, and GDPR. Each artifact supports multiple control objectives where applicable.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Evidence Type | Source / Tool | Framework Reference | Storage Location | Retention Policy |
| Audit Logs | Cloud Logging | PCI DSS 10.2, GDPR Art. 32 | BigQuery Central Dataset | 180 days (auto archived) |
| Compliance Reports | Security Command Center | NIST DE.CM-7, PCI DSS 12.11 | Shared Drive (Compliance Folder) | 1 year |
| Access Control Records | IAM Analyzer | PCI DSS 7.1, GDPR Art. 25 | Google Drive (IAM Audit Folder) | 1 year |
| Data Retention Reports | DLP + Lifecycle Rules | GDPR Art. 5(1)(e) | Data Governance Drive | 1 year |
| Backup Validation Reports | Cloud SQL | PCI DSS 9.5, NIST RC.RP-1 | Secure Folder | 90 days |
| Configuration Snapshots | Terraform + Config Validator | CIS 3.4, NIST PR.IP-1 | Source Repository | Permanent (version-controlled) |

## 4. Audit & Escalation Workflow

• Monthly compliance reviews include PCI DSS and GDPR checkpoints.  
• High-severity findings are escalated within 48 hours to the Project Sponsor.  
• Annual compliance audit performed by internal or external teams covering all frameworks.  
• Evidence tagged by framework (NIST, CIS, PCI DSS, GDPR) in BigQuery and shared drives for traceability.

## 5. Continuous Improvement & Cross-Framework Tracking

Each framework integration is reviewed quarterly to account for updated regulations, new GCP services, and audit findings. Lessons learned are used to refine policies, tighten access, and enhance automation for compliance monitoring.