# Mitigation Plan – Week 2

Project: ShopNimbus SecureCloud (Three-Tier GCP Architecture)

## 1. Introduction

This document outlines the Mitigation Plan for the ShopNimbus SecureCloud project. It builds upon the Week 2 Risk Register, which identified and scored risks across the three-tier Google Cloud Platform (GCP) architecture using the STRIDE framework.  
The purpose of this plan is to present prioritized mitigation strategies, using preventive, detective, and corrective controls, to reduce risks to acceptable levels while maintaining system confidentiality, integrity, and availability.

## 2. High-Priority Risks and Mitigation Strategies

## R-1: Compromise of Service Account Keys

Risk Level: High

Impact: Compromised service account keys could allow unauthorized access to backend services, bypassing authentication and enabling privilege escalation.

Mitigation Strategy:

• Preventive: Enforce Workload Identity Federation; disable the creation of long-lived service account keys.

• Detective: Configure Cloud Logging and Security Command Center (SCC) alerts to detect abnormal key usage.

• Corrective: Immediately revoke compromised keys, rotate credentials, and redeploy affected workloads.

Residual Risk: Medium

### R-5: Distributed Denial of Service (DDoS) Attack on Web Tier

Risk Level: High

Impact: A DDoS attack could overwhelm the web tier, causing outages and service degradation, resulting in financial loss and reputational damage.

Mitigation Strategy:

• Preventive: Apply Cloud Armor WAF rules, rate limiting, and adaptive protection to block malicious traffic.

• Detective: Implement Cloud Monitoring alerts for traffic spikes and Load Balancer health-check failures.

• Corrective: Scale the Managed Instance Group (MIG), block offending IP addresses, and activate auto-healing.

Residual Risk: Medium

### R-6: Over-Privileged IAM Role Escalation

Risk Level: High

Impact: Inappropriate IAM role assignments (e.g., broad Owner/Editor access) could result in unauthorized privilege escalation across the environment.

Mitigation Strategy:

• Preventive: Apply least-privilege IAM policies; use IAM Recommender to continuously optimize permissions.

• Detective: Enable SCC and Cloud Logging alerts for IAM policy and role changes.

• Corrective: Revoke unauthorized roles, roll back IAM changes, and implement approval workflows for elevated access.

Residual Risk: Medium

## 3. Medium-Priority Risks

The following risks were assessed as Medium but require mitigation to maintain layered security:  
  
• R-2 (SQL Injection): Use parameterized queries, WAF SQLi rules, audit logging, point-in-time recovery.  
• R-3 (Insufficient Logging Retention): Export logs to BigQuery/Storage, configure SCC alerts, extend log retention.  
• R-4 (Unencrypted App–DB Traffic): Enforce TLS, monitor with VPC Flow Logs, rotate DB credentials as needed.  
• R-7 (Public Cloud Storage Buckets): Apply organization policy blocking public access, detect with SCC, remove public ACLs.  
• R-8 (Cloud SQL Outages): Deploy HA Cloud SQL, enable monitoring, failover to replicas, restore from backups.

## 4. Governance and Monitoring

Sustainable mitigation requires ongoing governance and continuous monitoring:  
  
• Security Command Center (SCC): Enterprise-wide visibility of misconfigurations and threats.  
• Cloud Logging & Monitoring: Real-time detection and automated alerting for anomalies.  
• IAM Policy Reviews: Quarterly reviews to enforce least privilege across accounts and services.  
• Incident Response Protocol: Documented corrective steps (revocation, rollback, restore) ensure swift recovery.

## 5. Conclusion

The mitigation strategies outlined here directly address the most significant risks identified in Week 2. By implementing layered preventive, detective, and corrective controls—supported by native GCP security services—ShopNimbus will reduce risk exposure to a manageable level and strengthen resilience against both internal and external threats.  
  
This proactive risk management approach establishes a secure foundation for upcoming project phases, including Week 3 (IAM and firewall hardening) and Week 4 (monitoring and incident response).