

# Infrastructure Modernization Plan

This document outlines the comprehensive infrastructure modernization plan for fiscal year 2026. The initiative covers cloud migration, network redesign, and security hardening across all data centers.

The total estimated budget is \$4.7 million with a projected ROI of 340% over three years. Implementation will proceed in four phases starting January 2026.

Phase	Timeline	Budget	Owner
Cloud Migration	Q1 2026	\$1.8M	VP Engineering
Network Redesign	Q2 2026	\$1.2M	Dir. Infrastructure
Security Hardening	Q3 2026	\$0.9M	CISO
Testing & Rollout	Q4 2026	\$0.8M	VP Engineering
Contingency	Ongoing	\$0.5M	CFO

# Cloud Migration Details

The cloud migration phase involves transferring all on-premises workloads to a hybrid cloud architecture. This includes database servers, application servers, file storage, and disaster recovery systems. The migration will use a lift-and-shift approach for legacy applications and a re-architecture approach for cloud-native services. Each workload will be assessed individually using a five-point readiness framework covering dependencies, data sensitivity, performance requirements, compliance obligations, and team readiness.

Workload	Current Host	Target	Risk Level	Migration Window	Status
ERP System	DC-East-01	AWS us-east-1	High	72 hours	Planning
CRM Platform	DC-West-02	Azure West US	Medium	48 hours	Ready
Data Warehouse	DC-East-01	GCP us-central1	High	96 hours	Assessment
Email Server	DC-West-01	M365 Cloud	Low	24 hours	In Progress
File Storage	DC-East-02	AWS S3	Low	120 hours	Planning
CI/CD Pipeline	On-prem	GitHub Actions	Medium	8 hours	Ready
Monitoring	DC-East-01	Datadog SaaS	Low	4 hours	Complete

## Network Architecture Requirements

The network redesign must satisfy the following requirements to maintain service level agreements during and after the migration:

- Minimum 99.99% uptime for production workloads during migration windows
- Maximum 50ms latency between cloud regions for inter-service communication
- Zero-trust security model with mutual TLS for all service-to-service traffic
- Automated failover with less than 30 second recovery time objective
- Full network segmentation between development, staging, and production
- DDoS protection with 10Tbps mitigation capacity at the edge
- Centralized logging with 90-day retention for compliance audit trail

# Security Hardening Procedures

The security hardening phase encompasses a comprehensive set of procedures designed to reduce the attack surface across all infrastructure components. This includes implementing CIS benchmarks for all operating systems, applying NIST 800-53 controls for federal compliance requirements, configuring Web Application Firewalls with custom rulesets tailored to our application portfolio, deploying endpoint detection and response agents on all server instances, establishing a vulnerability management program with weekly scanning cadence and a 72-hour critical patch SLA, implementing privileged access management with just-in-time elevation and session recording, and conducting quarterly penetration testing by an independent third-party assessor. The security hardening phase encompasses a comprehensive set of procedures designed to reduce the attack surface across all infrastructure components. This includes implementing CIS benchmarks for all operating systems, applying NIST 800-53 controls for federal compliance requirements, configuring Web Application Firewalls with custom rulesets tailored to our application portfolio, deploying endpoint detection and response agents on all server instances, establishing a vulnerability management program with weekly scanning cadence and a 72-hour critical patch SLA, implementing privileged access management with just-in-time elevation and session recording, and conducting quarterly penetration testing by an independent third-party assessor. The security hardening phase encompasses a comprehensive set of procedures designed to reduce the attack surface across all infrastructure components. This includes implementing CIS benchmarks for all operating systems, applying NIST 800-53 controls for federal compliance requirements, configuring Web Application Firewalls with custom rulesets tailored to our application portfolio, deploying endpoint detection and response agents on all server instances, establishing a vulnerability management program with weekly scanning cadence and a 72-hour critical patch SLA, implementing privileged access management with just-in-time elevation and session recording, and conducting quarterly penetration testing by an independent third-party assessor.

# Final Recommendations

## Immediate Actions (Next 30 Days)

Begin workload assessment for the first batch of applications identified in the cloud migration readiness matrix above.

## Medium-Term Goals (60-90 Days)

Complete network architecture design review and obtain sign-off from the architecture review board. Initiate procurement for new security tools.

## Long-Term Vision

Achieve a fully automated, self-healing infrastructure with predictive scaling, zero-touch deployment, and continuous compliance monitoring. Target completion: December 2026.