Cloud Environment Security Gap Analysis Sample

1. Introduction

This document provides a sample template for conducting a security gap analysis in a cloud environment. It outlines key security controls, current state, target state, and associated gaps for review and remediation planning.

2. Gap Analysis Summary Table

Security Domain	Control	Current State	Target State	Gap	Recommendation
Identity & Access Management	Multi-Factor Authentication (MFA) for Admins	MFA enabled for some admin accounts	MFA enabled for all admin accounts	Partial coverage	Enable MFA for all privileged accounts
Data Protection	Data Encryption At Rest	Data is stored unencrypted	All sensitive data is encrypted at rest	No encryption present	Implement encryption for storage services
Network Security	Restrict Inbound Traffic	All IPs allowed	Only whitelisted IPs allowed	Open access	Update security group rules to restrict traffic
Monitoring & Logging	Centralized Log Collection	Logs stored locally only	All logs centralized & retained 90 days	Non-centralized	Implement centralized logging solution

3. Key Findings

- Multi-factor authentication is not enforced for all privileged users.
- Sensitive data is present without encryption at rest.
- Network security controls are weak due to overly permissive rules.
- Log collection is not centralized, risking gaps in incident detection.

4. Recommendations

- Mandate and enforce MFA for all users with admin access.
- Encrypt all sensitive data at rest using managed keys.
- Review and restrict inbound/outbound security group and firewall rules.
- Deploy centralized log aggregation and retain logs as per policy.

5. Next Steps

- Assign remediation actions to responsible teams.
- Set timelines for implementation and review progress.
- Schedule follow-up gap analysis to verify closure of findings.