Cloud Security Review

Representative Engagement

Executive Summary

This cloud security review evaluates exposure within a cloud-native environment by analyzing access paths, blast radius, and detection capability, rather than enumerating individual services or configurations.

The objective is to identify where compromise would most likely occur and where its impact would be greatest, then prioritize controls that meaningfully reduce that exposure.

Overall Cloud Risk Posture

Moderate

Primary Risk Concentration

Identity access paths, logging coverage, third-party integrations

Key Constraint

Balancing security improvements with operational velocity

Review Scope

The review focused on cloud components that materially affect security posture:

In Scope

- Identity and access management
- Production and staging account separation
- Storage access controls
- Logging and monitoring coverage
- Third-party access to cloud resources

Explicitly Out of Scope

- Application code security
- Infrastructure-as-code pipeline review
- End-user endpoint security

These exclusions were intentional to maintain focus on structural cloud risk drivers.

Architectural Context

The environment reviewed reflects a typical modern SaaS architecture:

Cloud Provider: AWS

Multi-account structure with production and non-production separation

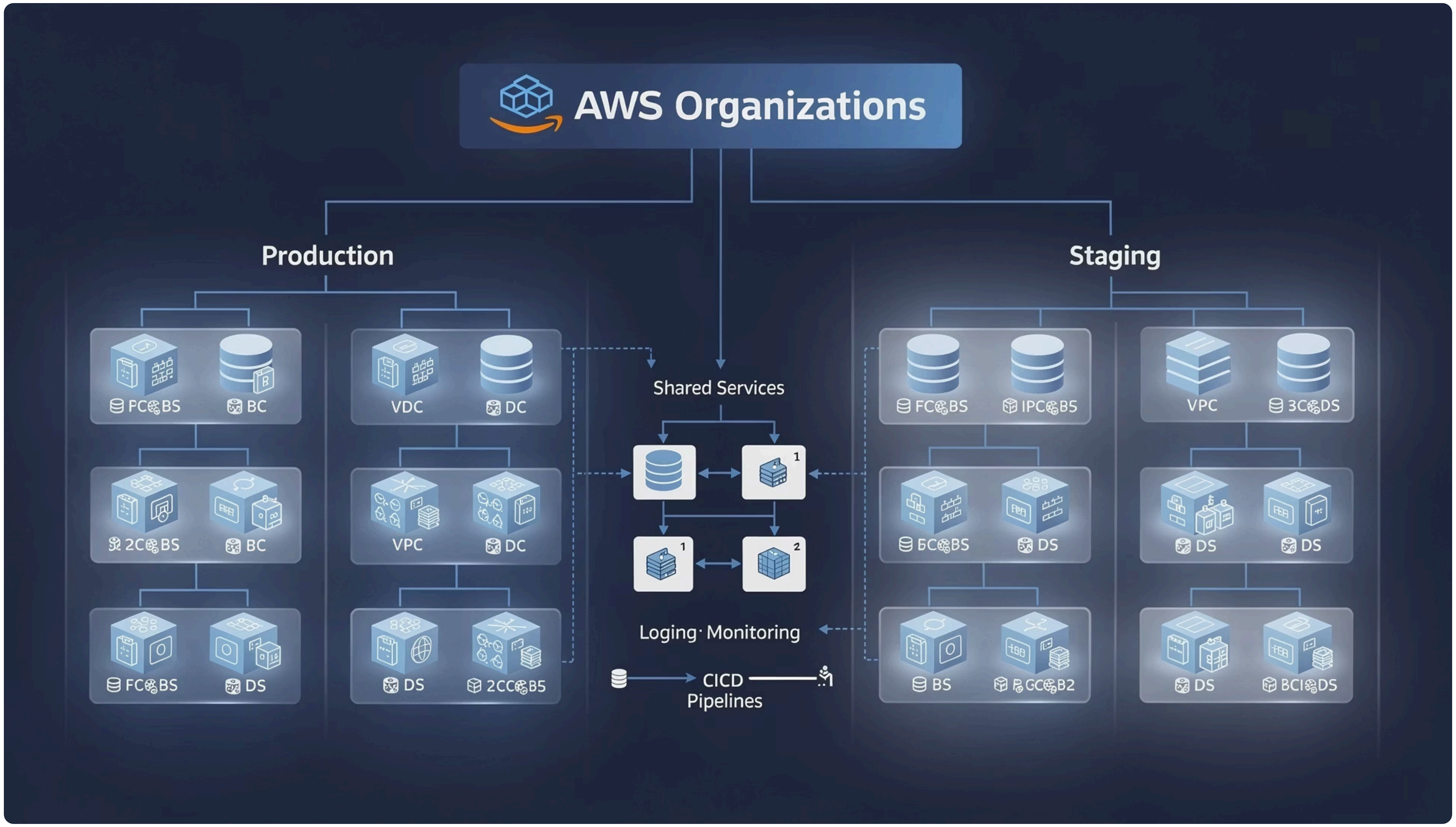
CI/CD Integration

CI/CD pipeline integrated with cloud services

Third-Party Tooling

Reliance on third-party monitoring and operational tooling

Security posture is therefore highly dependent on identity discipline and visibility.



Operating Assumptions

This review is based on the following assumptions:

Developer Access

Developers require elevated access for operational efficiency

Automation Priority

Automation is favored over manual processes

Cost Sensitivity

Cost sensitivity influences logging and monitoring depth

Shared Ownership

Security ownership is shared across teams rather than centralized

Recommendations are calibrated to these realities.

Access Path Analysis

Risk evaluation centered on how access flows through the environment, not individual permissions in isolation.

Developer Account → Admin Role	High
CI/CD Token → Production Resources	Medium
Support Tool → Customer Data	Medium
Third-Party Vendor → Cloud APIs	Medium

Access paths with broad blast radius were prioritized over narrow misconfigurations.

Key Findings

1

Broad Administrative Access

Risk Level: High

Multiple users and services retain standing administrative privileges, increasing the impact of credential compromise.

2

Partial Logging Coverage

Risk Level: Medium

Logging exists but is inconsistently centralized, reducing the ability to detect and investigate incidents quickly.

3

Third-Party Access Visibility Gaps

Risk Level: Medium

Vendor access is not consistently documented or reviewed, increasing exposure through external dependencies.

Finding 1: Broad Administrative Access

High Risk

Multiple users and services retain standing administrative privileges, increasing the impact of credential compromise.

Impact: A single compromised credential could provide an attacker with full control over production resources, customer data, and critical infrastructure.

Finding 2: Partial Logging Coverage

Logging exists but is inconsistently centralized, reducing the ability to detect and investigate incidents quickly.

Medium Risk

Impact: Without comprehensive logging, security teams cannot reliably detect unauthorized access, trace attacker movements, or conduct effective incident response.

Finding 3: Third-Party Access Visibility Gaps

Medium Risk

Vendor access is not consistently documented or reviewed, increasing exposure through external dependencies.

Impact: Unmonitored third-party access creates blind spots where compromised vendor credentials or malicious insiders could access sensitive resources without detection.

Why Certain Controls Were Deprioritized

The following controls were identified but intentionally deferred:

Advanced SIEM Correlation and Tuning

Provides diminishing returns until basic logging consistency improves

Continuous Configuration Scanning

Less impactful than addressing identity hygiene first

Zero Trust Segmentation

Beyond identity controls, requires foundational improvements first

These controls provide diminishing returns until identity hygiene and logging consistency improve.

Recommended Remediation Strategy

01

Phase 1: Access Hardening (0–30 Days)

- Reduce standing admin privileges
- Enforce strong authentication on privileged roles
- Audit and document third-party access

02

Phase 2: Visibility Improvements (30–60 Days)

- Centralize audit logs
- Define alerting for high-risk access events
- Establish ownership for cloud security monitoring

03

Phase 3: Maturity Enhancements (60–90 Days)

- Expand log retention
- Conduct access path reviews quarterly
- Align cloud security documentation with operations

Expected Impact

Implementing the Phase 1 and Phase 2 recommendations is expected to significantly reduce the likelihood and impact of cloud account compromise without materially slowing development workflows.

Risk Reduction Approach

Risk reduction is achieved through access discipline and visibility, not increased tooling complexity.

Operational Balance

Security improvements are designed to integrate with existing workflows without creating friction for development teams.

Strategic Takeaway for Leadership

> Cloud security failures rarely originate from infrastructure scale. They originate from unmanaged access and delayed detection.

Effective cloud security investment prioritizes **who can do what**, **how quickly issues are detected**, and **how confidently teams can respond**.

Footer

This document represents a sample engagement created to demonstrate methodology and deliverables. It does not reference a specific organization.