Secure Azure Infrastructure Implementation Report

Author: Isabel Romero

Project Type: Cloud Security Implementation & Remediation

Environment: Microsoft Azure (IaaS)

Standards Referenced: NIST SP 800-53, PCI DSS, FISMA

Executive Summary

An internal security review of a Microsoft Azure Infrastructure-as-a-Service (IaaS) environment identified multiple misconfigurations that increased the organization's exposure to privilege escalation, data leakage, and regulatory noncompliance.

The organization operates in a regulated environment subject to FISMA and PCI DSS requirements. The assessment revealed excessive role-based access permissions, weak encryption boundary segmentation, inadequate backup enforcement, and insufficient governance controls.

This remediation initiative focused on enforcing least privilege access controls, segmenting encryption boundaries, implementing automated backup policies, and strengthening governance through tagging and policy enforcement. The implemented controls align with NIST SP 800-53 control families including Access Control (AC), System & Communications Protection (SC), and Contingency Planning (CP).

Environment Overview

The Azure environment consisted of:

- Multiple departmental resource groups (Marketing, Accounting, IT)
- Azure Virtual Machines hosted under IaaS
- Shared Azure Key Vault resources
- Inconsistent backup configurations
- Broad RBAC assignments spanning departments

The shared resource structure and inherited permissions introduced unnecessary risk across business units.

Identified Security Risks

The following critical risks were identified:

Excessive RBAC Permissions

Users were granted permissions outside their departmental scope, violating the principle of least privilege. This increased the risk of lateral movement and privilege escalation.

Shared Key Vault Access

Encryption keys and secrets were accessible across departments, weakening isolation boundaries and increasing potential impact of credential compromise.

Inconsistent Backup Enforcement

Backup policies were not uniformly applied across virtual machines. Certain disk configurations prevented backup policy enforcement.

Insufficient Governance Controls

Lack of standardized tagging limited audit visibility and policy enforcement capabilities.

Remediation & Security Control Implementation

Role-Based Access Control (RBAC) Hardening

RBAC assignments were restructured to enforce least privilege:

- Contributor roles were scoped at the resource group level.
- Cross-department access was removed.
- Role inheritance was reviewed and cleaned.

- Access aligned strictly with departmental responsibilities.

Security Outcome:
Reduced attack surface and minimized risk of unauthorized resource access or privilege escalation.

Azure Key Vault Segmentation

To strengthen encryption boundary isolation:

- Dedicated Key Vaults were created for each department.
- Access policies were restricted to department-specific users.
- Cross-department secret access was removed.
- Key Vault-managed encryption was enforced for applicable resources.

Encryption at rest and certificate management for encrypted communications were validated to support PCI DSS requirements.

Security Outcome:
Improved compartmentalization of cryptographic materials and reduced blast radius in the event of credential compromise.

Backup & Disaster Recovery Controls

A standardized backup policy was implemented with the following configuration:

- Daily backups at 7:00 PM EST
- Recovery Point Objective (RPO): 24 hours
- Retention period: 45 days
- Instant restore snapshot retention: 3 days

Virtual machines were validated to ensure compatibility with backup enforcement requirements. Disk configuration issues preventing policy application were resolved.

Security Outcome:

Strengthened disaster recovery posture and improved compliance alignment with NIST Contingency Planning (CP) controls.

Governance & Policy Enforcement

Governance controls were strengthened through:

- Department-based resource tagging standards
- Azure Policy enforcement for compliance validation
- Improved resource visibility for audit and reporting

Security Outcome:

Enhanced long-term cloud security posture management and reduced risk of configuration drift.

Compliance Alignment

The implemented controls align with:

- **NIST SP 800-53**
    - AC (Access Control)
    - SC (System and Communications Protection)
    - CP (Contingency Planning)
- **PCI DSS**
    - Access control enforcement
    - Encryption of sensitive data
    - Backup and recovery validation
- **FISMA**
    - Risk management and control implementation requirements

Security Improvements Summary

Control Area	Pre-Remediation State	Post-Remediation State
RBAC	Cross-department access	Scoped by Resource Group
Key Vault	Shared access	Segmented per department
Encryption	Unverified	Key Vault-managed controls
Backup	Inconsistent	Automated daily enforcement
Governance	No tagging standards	Standardized tagging + policy enforcement

Lessons Learned

- RBAC scoping must be carefully managed to prevent privilege creep.
- Encryption boundaries should mirror organizational segmentation.
- Backup enforcement depends on correct disk configuration.
- Governance controls are critical for scalable cloud environments.
- Post-consultant security validation is essential to reduce residual risk.

Conclusion

This remediation effort significantly reduced the Azure environment's exposure to privilege escalation, data leakage, and regulatory noncompliance. Enforcing least privilege, segmenting encryption controls, standardizing backup policies, and strengthening governance mechanisms, improved the organization's overall cloud security posture and regulatory alignment.