Governance, Risk, and Compliance Assessment of ABC Corporation's Systems

Isabel Romero

Abstract

This report evaluates the security posture of ABC Corporation’s enterprise IT environment, identifying critical gaps in access control, authentication, endpoint protection, risk management, and PCI DSS compliance. Controls were assessed against NIST SP 800-53, NIST SP 800-30, and industry best practices. A prioritized remediation roadmap was developed, including role-based access control, continuous monitoring, formal risk assessment, and PCI DSS-aligned POS security. The report demonstrates both technical and governance improvements to reduce organizational risk and ensure regulatory compliance.

Security Control Gap Analysis

A comprehensive review of ABC Corporation’s security framework identified multiple control deficiencies impacting confidentiality, integrity, and availability of sensitive data, including Protected Health Information (PHI) and payment card data.

1. **Access Control Weaknesses (NIST AC Family)**
   ABC Corporation lacks documented access control policies and does not enforce least privilege principles. User permissions are not aligned with job responsibilities, increasing the likelihood of unauthorized access to sensitive systems and data. Without structured account management there is an increased risk of insider threats and lateral movement.

2. **Legacy and End-of-Life Infrastructure**
   Critical network components, including the primary firewall, are operating on unsupported or end-of-life software. This increases exposure to known vulnerabilities and limits the organization’s ability to defend against threat actors.

3. **Inadequate Authentication Controls**
   Multifactor authentication (MFA) has not been implemented for system access, including environments handling sensitive patient data. The absence of MFA increases the risk of credential compromise and unauthorized system access.

4. **Insufficient Endpoint Protection**
   Several workstations lack updated antivirus and endpoint protection solutions. Without centralized management and monitoring, malware infections and ransomware threats may go undetected, posing operational and compliance risks.

5. **PCI DSS Non-Compliance in POS Environment**
   The point-of-sale (POS) system does not meet PCI DSS v4.0 requirements. Identified deficiencies include lack of network segmentation, absence of a properly configured

firewall, and inadequate endpoint protection. These gaps increase the risk of cardholder data compromise.

6. **Governance and Risk Management Deficiencies**
   ABC Corporation does not maintain a current risk assessment, formal risk response strategy, or comprehensive asset inventory. Also, the absence of a documented Information Security Program Plan (ISPP) limits visibility into organizational risk posture and compliance alignment.

Collectively, these deficiencies indicate a security posture lacking formal governance structure and continuous risk oversight. Immediate remediation is required to reduce regulatory exposure and operational risk.

Control Risk Analysis and Remediation Justification

The following controls were evaluated against organizational requirements and industry standards, including NIST Special Publication 800-53, NIST Special Publication 800-30, and Office of Management and Budget Circular A-130.

AC-6 — Least Privilege

Risk Rating: High

Risk Analysis:
The absence of enforced least privilege significantly increases the likelihood of unauthorized access to sensitive systems and Protected Health Information (PHI). Excessive permissions create opportunities for insider threats, credential abuse, and lateral movement.

Business Impact:
Compromise of sensitive data could result in regulatory penalties, reputational damage, and operational disruption.

Remediation Justification:
Implementation of least privilege is a foundational requirement under NIST access control standards. Enforcing role-based access controls reduces attack surface, limits scope in the event of compromise, and strengthens regulatory alignment.

CA-5 — Plans of Action and Milestones (POA&M)

Risk Rating: Moderate

Risk Analysis:
Without a formal POA&M process, identified vulnerabilities may remain untracked or unresolved, increasing exposure duration. This governance gap weakens accountability.

Business Impact:
Delayed remediation increases audit findings and regulatory scrutiny, especially in regulated environments handling healthcare and financial data.

Remediation Justification:
OMB Circular A-130 emphasizes structured risk remediation tracking. Establishing a formal POA&M process improves transparency, accountability, and executive oversight of security risks.

CA-7 — Continuous Monitoring

Risk Rating: High

Risk Analysis:
Lack of centralized logging and continuous monitoring reduces visibility into malicious activity. Threat actors may persist undetected, increasing potential impact.

Business Impact:
Failure to detect and respond to incidents in a timely manner increases breach impact, regulatory exposure, and recovery costs.

Remediation Justification:
Continuous monitoring is a core requirement within NIST control families and supports proactive risk management. Implementing SIEM-based monitoring improves detection capability and the incident response effectiveness.

RA-3 — Risk Assessment

Risk Rating: High

Risk Analysis:
The absence of recurring risk assessments prevents the organization from formally identifying, scoring, and prioritizing threats. This impedes strategic decision-making and resource allocation.

Business Impact:
Without structured risk identification, leadership lacks visibility into exposure levels, which increases the likelihood of regulatory and operational risk.

Remediation Justification:
NIST risk management guidance requires periodic risk assessments to develop mitigation strategies and compliance alignment. Formal assessments support evidence-based security investment decisions.

RA-7 — Risk Response

Risk Rating: Moderate

Risk Analysis:
ABC Corporation does not maintain a documented risk response framework that defines mitigation, transfer, acceptance, or avoidance strategies. This may cause inconsistent risk treatment decisions.

Business Impact:
Uncoordinated risk handling can lead to unmanaged exposure and governance breakdowns.

Remediation Justification:
A structured risk response strategy ensures executive awareness and formal acceptance of residual risk. This aligns security operations with organizational risk tolerance.

Risk-Based Remediation Roadmap

Remediation efforts were prioritized based on risk severity, regulatory exposure, and operational impact.

Phase 1: Immediate Remediation (0–30 Days)

AC-6 — Least Privilege

Objective: Reduce unauthorized access risk through structured access control.

Actions:

- Implement Role-Based Access Control (RBAC) aligned to job functions.
- Review and remove excessive permissions.
- Enforce periodic access recertification.

Ownership: Identity & Access Management (IAM) Team
Expected Outcome: Reduction in excessive privilege assignments and minimized insider threat exposure.

CA-7 — Continuous Monitoring

Objective: Improve threat detection capability and reduce incident dwell time.

Actions:

- Deploy a centralized SIEM solution (e.g., Splunk or Microsoft Sentinel).
- Aggregate authentication, endpoint, and firewall logs.
- Establish alert thresholds for anomalous behavior.

Ownership: Security Operations
Expected Outcome: Improved detection visibility and faster incident response.

Phase 2: Governance Strengthening (30–90 Days)

RA-3 — Risk Assessment

Objective: Establish recurring enterprise risk evaluation process.

Actions:

- Conduct formal risk assessment aligned with NIST Special Publication 800-30.
- Document assets, threats, vulnerabilities, likelihood, and impact.
- Present findings to executive leadership.

Ownership: GRC Team
Expected Outcome: Improved strategic visibility into enterprise risk posture.

RA-7 — Risk Response

Objective: Formalize risk treatment decision-making process.

Actions:

- Develop a risk response matrix (mitigate, transfer, accept, avoid).
- Define risk tolerance thresholds.
- Require executive sign-off for risk acceptance.

Ownership: CISO / Risk Committee
Expected Outcome: Consistent and documented risk treatment decisions.

CA-5 — POA&M Implementation

Objective: Improve remediation tracking and accountability.

Actions:

- Implement centralized POA&M tracking system (e.g., RSA Archer).
- Assign remediation owners and deadlines.
- Conduct monthly status reviews.

Ownership: GRC Team
Expected Outcome: Increased accountability and reduced vulnerability exposure duration.

PCI DSS–Aligned Point-of-Sale (POS) Security Policy

1. Purpose

This policy establishes security requirements for ABC Corporation's Point-of-Sale (POS) systems to ensure compliance with PCI Security Standards Council requirements under PCI DSS v4.0 and to protect cardholder data from unauthorized access, disclosure, or compromise.

2. Scope

This policy applies to all POS systems, supporting infrastructure, and personnel responsible for administering or accessing payment processing systems.

3. Policy Requirements

3.1 Network Security Controls (PCI DSS Requirement 1)

- All POS systems must be protected by a currently supported next-generation firewall.
- The POS network must be segmented from internal corporate networks and public-facing systems.
- Firewall rules must follow a deny-by-default posture, allowing only explicitly approved traffic.
- Firewall configurations must be reviewed at least every six months.

Control Owner: Network Administrator

3.2 Anti-Malware Protection (PCI DSS Requirement 5)

- All POS systems must run centrally managed anti-malware software.
- Automatic signature updates must be enabled.
- Weekly system scans must be scheduled and logged.
- Anti-malware alerts must integrate with centralized monitoring systems.

Control Owner: IT Security Officer

3.3 Secure Configuration and Credential Management (PCI DSS Requirement 2)

- All vendor-supplied default credentials must be removed prior to deployment.
- Default services, accounts, and ports must be disabled unless explicitly required.
- Administrative access must require unique credentials and strong authentication mechanisms.
- Password policies must enforce complexity and rotation requirements consistent with organizational standards.

Control Owner: System Administrator

4. Monitoring and Compliance

- POS systems must be included in centralized logging and continuous monitoring processes.
- Quarterly internal vulnerability scans must be performed.
- Annual PCI DSS compliance validation must be conducted and documented.

5. Enforcement

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment, and may expose the organization to regulatory penalties.

Implementation of these controls reduces the risk of cardholder data compromise and supports regulatory compliance obligations. Proper segmentation, endpoint protection, and credential management significantly decrease the likelihood of payment system breach scenarios.

E. References

- National Institute of Standards and Technology. (2020). *NIST special publication 800-53 rev. 5: Security and privacy controls for information systems and organizations*. U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

- National Institute of Standards and Technology. (2012). *NIST SP 800-30: Guide for conducting risk assessments*. U.S. Department of Commerce.

- Office of Management and Budget. (2016). *Circular A-130: Managing information as a strategic resource*.

- PCI Security Standards Council. (2022). *PCI DSS v4.0: Payment Card Industry Data Security Standard*. https://www.pcisecuritystandards.org

- National Institute of Standards and Technology. (2004). *FIPS 199: Standards for security categorization of federal information and information systems*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf