Enterprise Network Consolidation with Regulatory Compliance (HIPAA & PCI DSS)

Isabel Romero

Abstract

Company A has acquired Company B and wants to integrate both network systems. Using the provided vulnerability scans, topology diagrams and cybersecurity tools and capabilities I have created a detailed plan to merge the network systems of the companies.

Executive Summary

Following a corporate acquisition, a financial services organization and a healthcare services provider required secure integration of their network infrastructures while maintaining regulatory compliance and operational continuity.

A security assessment identified critical vulnerabilities including legacy operating systems, exposed services, weak authentication controls, and publicly accessible databases. These weaknesses posed significant risk to Protected Health Information (PHI) and payment card data.

A hybrid cloud architecture was designed to modernize application hosting, enforce zero trust access controls, eliminate high-risk exposures, and align infrastructure with regulatory standards under PCI DSS and HIPAA Security Rule guidance.

The proposed design reduces external attack surface, improves scalability, enhances resilience against ransomware threats, and establishes a foundation for long-term security maturity.

Initial Security Assessment

Company A - Financial Services Environment

Authentication and Access Control Weakness

Company A enforces a minimum password length of eight characters without complexity requirements or periodic review. This policy is not in alliance with the guidance of the National Institute of Standards and Technology SP 800-63B and increases susceptibility to credential stuffing, brute-force, and password spraying attacks.

Open ports (21-90 and 3389) were identified as externally accessible. Exposure of services like FTP and Remote Desk Protocol (RDP) increase the attack surface significantly and elevates the risk of unauthorized remote access.

Business Impact: The organization processes financial data subject to PCI Security Council PCI DSS requirements, therefore weak authorization controls and exposed remote services present a high likelihood of regulatory non-compliance and potential data breaches.

Infrastructure and Platform Risk

The environment contains a mix of Windows 10 Pro, Windows 7, and Windows 11 endpoints. With a lack of standardization centralized patch management and policy enforcement are complicated.

Additionally, Windows Server 2012 systems were identified as end-of-life (EOL). EOL platforms do not receive security updates, which increases vulnerability exposure and creates compliance risk under PCI DSS lifecycle management requirements.

Risk Severity: High - Legacy systems materially increase exploitability due to unpatched vulnerabilities and unsupported security controls.

Overall Risk Posture - Company A

The financial services environment presents elevated risk primarily driven by weak identity controls, exposed services, and legacy infrastructure. Immediate remediation should prioritize MFA enforcement, closure of unnecessary ports, and decommissioning of end-of-life systems.

Company B - Healthcare Services Environment

Identity and Access Management Gaps

Multi-Factor Authentication (MFA) is not enforced for user authentication. While U.S. The Department of Health and Human Services (HIPAA) does not explicitly require MFA, it requires all covered entities to implement any and all reasonable and appropriate safeguards to protect Protected Health Information (PHI). MFA is widely recognized as an industry best practice control to reduce unauthorized access risk.

Business Impact: Absence of MFA significantly increases the likelihood of credential compromise and unauthorized access to PHI.

Data Exposure Risks

A PostgreSQL database was identified as accessible from the public internet. Internet-exposed databases are high-risk configurations and are frequently targeted in automated scanning and ransomware attacks.

If exploited, unauthorized access could result in compromise of PHI and financial data.

Risk Severity: Critical - Externally exposed databases increase exploitability and attack surface.

Legacy Systems and Insecure Remote Services

Company B operates Windows XP and Windows 7 systems, both of which are end-of-life and unsupported. These systems cannot receive security patches, increasing vulnerability to exploitation.

Additionally, insecure remote services like Rexec and VNC were identified. These protocols lack modern encryption and authentication safeguards, making them susceptible to interception and unauthorized access.

Business Impact: The organization processes PHI, therefore control failures increase the likelihood of breaches and expose the organization to regulatory penalties under HIPAA Security Rule requirements.

Overall Risk Posture - Company B

Vulnerability Analysis

Risk Rating Methodology

Risk ratings were determined based on qualitative assessment of **Impact × Likelihood**, aligned with industry risk management practices and regulatory exposure considerations.

Company A - Financial Services Environment:

- **Weak Password Policy:**

  - **Description:** Minimum password length of 8 characters without enforced complexity controls or MFA.
  - **Threat Scenario:** An external attacker performs credential stuffing or brute-force attacks against exposed authentication services.
  - **Business Impact:** Compromise of financial records, customer PII, or internal intellectual property. There are also potential violations of PCI DSS authentication control requirements.
  - **Likelihood:** Very high, because password-based attacks remain one of the most common initial access vectors.
  - **Risk Rating:** High
  - **Recommendation Controls:**
    - Enforce MFA
    - Align password policy with NIST SP 800-63B guidance
    - Implement account lockout and monitoring controls
- **Open Ports (21-90, 3389)**:
  - **Description:** Multiple externally accessible ports increase the attack surface, including FTP and RDP exposure.
  - **Threat Scenario:** Threat actors identify exposed services via automated scanning and exploit misconfigurations or weak credentials.
  - **Business Impact:** Unauthorized remote access, data exfiltration, ransomware deployment, operational disruption.
  - **Likelihood:** High, because RDP and legacy service exploitation remain common attack vectors.
  - **Risk Rating:** High
  - **Recommended Controls:**
    - Close unnecessary ports
    - Restrict RDP via VPN

        - Implement firewall rules and network segmentation
        - Enable logging and intrusion detection

Company B - Healthcare Services Environment:

- **Absence of Multi-Factor Authentication**:
    - **Description:** User authentication relies solely on single-factor credentials.
    - **Threat Scenario:** Phishing campaign leads to credential compromise and unauthorized access to PHI systems.
    - **Business Impact:** Exposure of Protected Health Information (PHI), regulatory investigation, reputational damage. Increased scrutiny under U.S. Department of Health and Human Services HIPAA Security Rule safeguards.
    - **Likelihood:** High, because credential compromise via phishing remains a leading breach cause in healthcare.
    - **Risk Rating:** High
    - **Recommended Controls:**
        - Enforce MFA for all privileged and remote access accounts
        - Implement phishing-resistant authentication where feasible
        - Deploy login anomaly detection
- **Publicly Accessible PostgreSQL Database**:
    - **Description:** Database server is directly accessible from the public internet.
    - **Threat Scenario:** Automated scanning identifies exposed databases; attacker exploits weak authentication or configuration errors.
    - **Business Impact:** Unauthorized disclosure or modification of PHI and payment data. Potential non-compliance with both HIPAA and PCI DSS requirements under the PCI Security Standards Council framework.
    - **Likelihood:** High, because internet-exposed databases are frequently targeted in opportunistic attacks.

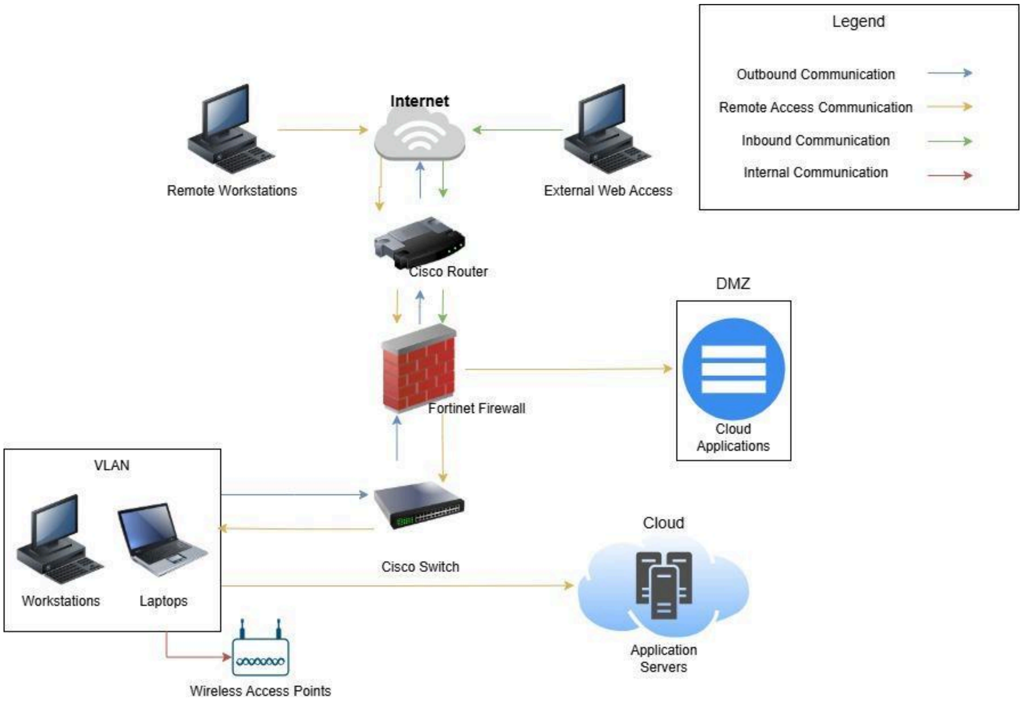
- **Risk Rating:** Critical
- **Recommended Controls:**
    - Remove public internet exposure
    - Restrict database access via private network/VPN
    - Implement encryption at rest and in transit
    - Enable database activity monitoring

Risk Prioritization Summary

Finding	Company	Likelihood	Impact	Risk Rating
Public Database Exposure	B	High	Critical	Critical
No MFA	B	High	High	High
Weak Password Policy	A	Very High	High	High
Exposed RDP	A	High	High	High

Post-Integration Secure Network Architecture

The post-integration architecture was designed to reduce attack surface, enforce zero trust access principles, and centralize security controls across hybrid environments.



Security Control Placement

Control	Location	Purpose
MFA	Identity Layer	Prevent credential compromise
Firewall	Network Perimeter	Traffic inspection & segmentation
VPN	Remote Access Boundary	Encrypted remote connectivity
VLAN Segmentation	Internal Network	Limit lateral movement

Database Access Control	Cloud Private Network	Prevent public exposure

Architectural Decisions and Rationale

1. Migration to Hybrid Cloud Application Rationale

Application servers were migrated to a cloud-hosted environment to improve scalability, availability, and disaster recovery posture. This migration reduces capital expenditure associated with hardware lifecycle management, while shifting costs to predictable operational expenses.

While cloud adoption increases recurring operational costs, the improved resilience, elasticity, and reduced infrastructure risk justify the investment within projected budget constraints.

2. Consolidation of Perimeter Security Controls

The existing Fortinet firewall was retained as the primary perimeter control to:

- Centralize traffic inspection
- Terminate VPN connections
- Enforce network segmentation between internal, DMZ, and cloud-connected resources

This avoided unnecessary hardware acquisition while preserving enterprise-grade inspection capability.

3. Elimination of Legacy Infrastructure

The following components were decommissioned:

- On-premises application servers (replaced by cloud infrastructure)
- Sophos firewalls (consolidated into Fortinet platform)
- ISP router (replaced with enterprise-grade Cisco router)

This reduced complexity, improved throughput performance, and strengthened security standardization.

Secure Network Design Principles Applied

1. Least Privilege

Access controls were implemented to restrict user and system permissions strictly to operational requirements. VLAN segmentation and firewall rule sets enforce role-based access boundaries, reducing lateral movement risk.

2. Defense in Depth

The architecture integrates layered security controls including:

- Perimeter firewall inspection
- VPN-based encrypted remote access
- Cloud-native security controls
- MFA enforcement

This layered model reduces single-point-of-failure exposure and increases attack resistance.

Regulatory Alignment

HIPAA (Health Insurance Portability and Accountability Act):

Because Company B processes PHI, the architecture incorporates:

- Encrypted transmission channels (VPN/TLS)
- Segmented cloud workloads
- Centralized logging and monitoring
- Role-based access controls

These measures align with administrative, technical, and physical safeguard requirements under HIPAA.

PCI DSS (Payment Card Industry Data Security Standard):

As both entities process payment card data, the design addresses PCI DSS requirements through:

- Network segmentation to isolate cardholder data environments
- Strong authentication controls (MFA)
- Firewall configuration management
- Monitoring and logging of cloud-hosted workloads

Residual Risk and Emerging Threat Considerations

Ransomware:

Hybrid environments remain vulnerable to ransomware targeting exposed credentials and misconfigured services. Mitigation strategies include:

- Immutable backups
- MFA enforcement
- Endpoint detection and response (EDR)
- Network segmentation to reduce blast radius

Cloud Misconfigurations:

Improper IAM policies and excessive privileges represent ongoing cloud security risks. Mitigation includes:

- Configuration management tooling
- Continuous compliance monitoring
- Least-privilege enforcement
- Periodic access reviews

Financial Analysis and Recommendation

Financial Analysis

Model	Estimated Year-One Cost	Key Benefits	Key Risks
On-Premises	$20k-$25k	Lower recurring costs, direct hardware control	Limited scalability, disaster recovery complexity
Hybrid Cloud	$40k-$45k	High availability, scalability, improved resilience	Increased operational expense

Recommendation:

A hybrid cloud model is recommended due to:

- Improved scalability
- Reduced infrastructure lifecycle risk
- Enhanced disaster recovery capabilities
- Stronger alignment with regulatory controls

Although operational costs increase, the reduction in breach risk and infrastructure obsolescence exposure provides long-term strategic value.