Quinton Green

Secure Network Design- D482

DHN1 Task 1: Network Merger and Implementation Plan

Western Governors University

# Table of Contents

[Table of Contents 2](#_Toc206766834)

[A. BUSINESS REQUIREMENTS 3](#_Toc206766835)

[B1- VULNERABILITIES 4](#_Toc206766836)

[B2. -IMPACT, RISK, LIKELIHOOD 4](#_Toc206766837)

[C.  TOPOLOGY DIAGRAM 6](#_Toc206766838)

[D.  TOPOLOGY COMPONENTS 7](#_Toc206766839)

[E.  RATIONALE 8](#_Toc206766840)

[F.  SECURE NETWORK DESIGN PRINCIPLES 13](#_Toc206766841)

[G.  REGULATORY COMPLIANCE 14](#_Toc206766842)

[H.  EMERGING THREATS 16](#_Toc206766843)

[I.  SUMMARY RECOMMENDATIONS 19](#_Toc206766844)

[J. SOURCES 22](#_Toc206766845)

# BUSINESS REQUIREMENTS

Two current network security problems and two current infrastructure problems for *each* company, based on business requirements given in the scenario are:

**COMPANY A:**

**Network Security Problem 1:** Open ports (21–90, 3389) which are easy targets for exploitation and attack. Port 3389 (RDP) exposes the network to remote access attacks, brute force, and ransomware attacks.

**Network Security Problem 2:** Weak password policies where all users use 8- characters and periodic password changes are not enforced.

**Infrastructure Problem 1:** Wireless Infrastructure – Only 2 Meraki MR28 access points for the entire network.

**Infrastructure Problem 2:** End-of-life equipment still in use ex: Windows 7 laptops, Windows Server 2012, 2012 R2 all currently being used.

**COMPANY B-**  
**Network Security Problem 1:** Critical Remote Code Execution Vulnerabilities – Services such as Distributed Ruby (dRuby/DRb), Java RMI Server Insecure default configuration, and Apache Tomcat AJP(Ghostcat)

**Network Security Problem 2:** Multifactor authentication (MFA) is not enforced for all users.

**Infrastructure Problem 1:** Mixed operating system environment with outdated workstations and no patching updates available due to End-of-life being reached (Windows 7, XP, mixed with MacOS versions, Ubuntu, Windows 10, Windows 11)

**Infrastructure Problem 2:** Cybersecurity policies and documentation are incomplete. The environment is operating with minimal documentation.

# B1- VULNERABILITIES

Two existing vulnerabilities for *each* company are as follows:

**COMPANY A-**

1. **Vulnerability 1:** Weak Password Policy
2. **Vulnerability 2:** Open Ports 21–90, 3389

**COMPANY B-**

1. **Vulnerability 1:** Multifactor Authentication (MFA) not enforced.
2. **Vulnerability 2:** Critical Remote Code Execution vulnerabilities

# B2. -IMPACT, RISK, LIKELIHOOD

Here are the impact, risk, and likelihood associated with *each* described vulnerability from part B1 as it relates to *each* company.

**COMPANY A-**

**Vulnerability 1: Weak Password Policy**

* **IMPACT-** High**.** Weak password policies leave the company open to data breaches. Attackers can gain access to sensitive systems, customer data, financial information, escalate privileges, install malware, exfiltrate data, disable security controls. It also violates regulatory compliance.
* **RISK-** High due to the ability to crack weak passwords.
* **LIKELIHOOD-** High due to the weak simple passwords. Password cracking tools can brute force passwords. Since passwords aren’t changed information can be leaked to the dark web and phishing attacks can take place.

**Vulnerability 2: Open Ports 21–90, 3389**

* **IMPACT -**High. Open ports expose HTTP on port 80, FTP on port 21, Telnet, SSH, RDP port 3389 which is common for ransomware, brute force attacks and other services open to exploit. Attackers can move through the company’s system easily through open ports.
* **RISK-** High. These are common ports used in enumeration scans and directly expose the company to attack.
* **LIKELIHOOD-** High. Attackers are always scanning open ports to gain access and entry.

**COMPANY B-**

**Vulnerability 1: Multifactor Authentication (MFA) not enforced.**

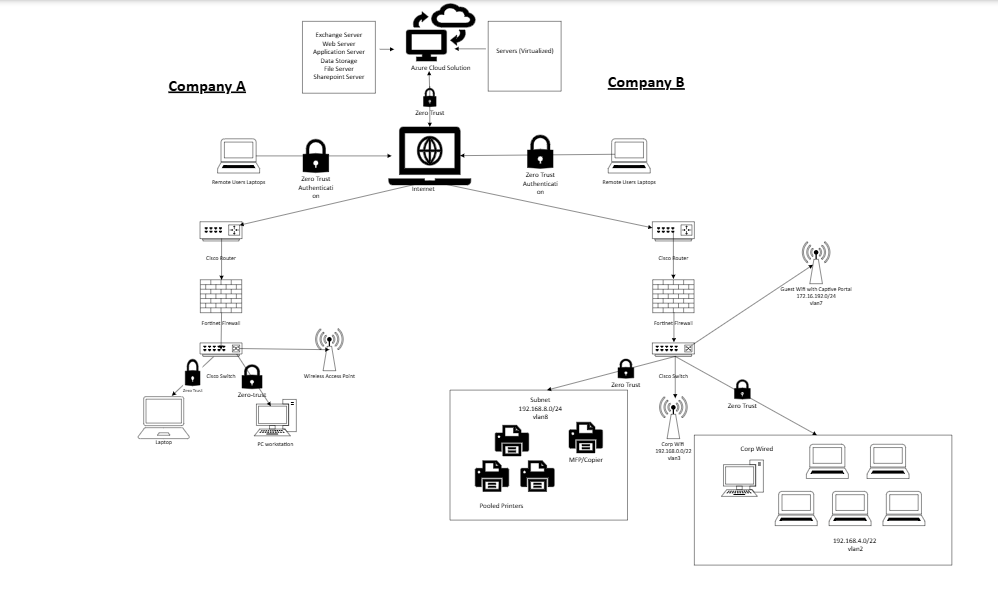
* **IMPACT-** High. MFA not being enforced means that credentials can be stolen and grant full access to the company network and phishing campaigns could be performed.
* **RISK-** High. It leaves risk for remote access infiltration and security breach.
* **LIKELIHOOD-** High. Usernames and passwords are targeted highly by attackers and are one of the most common sources of security breaches.

**Vulnerability 2: Critical Remote Code Execution vulnerabilities**

* **IMPACT-** Critical. Remote Code Execution allows attackers to execute arbitrary code, perform lateral movement and network pivoting, data theft, and install malware leading to full compromise of the system. Service disruption and data exfiltration can occur.
* **RISK-** Critical**.** Remote Code Executions are highly severe and are extreme threats on internet-facing systems.
* **LIKELIHOOD-** Critical. These vulnerabilities have public exploits. Exploitation is sure with this vulnerability unpatched

# C.  TOPOLOGY DIAGRAM

Here is the network topology diagram with details of the proposed merged network requirements. Visio link: [Network Topology 1.vsdx](https://westerngovernorsuniversity-my.sharepoint.com/:u:/r/personal/qgree11_wgu_edu/Documents/Network%20Topology%201.vsdx?d=w8313ffc2f68543bda189bd555ed7c035&csf=1&web=1&e=6j2be3)



# D.  TOPOLOGY COMPONENTS

Identify the layer for *all*components in the topology diagram referencing the layers of the OSI model and TCP/IP protocol stack.

**Company A**

|  |  |  |
| --- | --- | --- |
| **Device** | **OSI Layer** | **TCP/IP Layer** |
| Azure Cloud Solution | Layer 7- Application | Application |
| Cisco Router | Layer 3- Network | Internet |
| Fortinet Firewall | Layer 7- Application | Application |
| Cisco Switch | Layer 3- Network | Internet |
| Wireless Access Points | Layer 2- Data Link | Network Access |
| Laptops and workstations | Layer 7- Application | Application |
| Cabling | Layer 1-Physical | Network Access |

**Company B**

|  |  |  |
| --- | --- | --- |
| **Device** | **OSI Layer** | **TCP/IP Layer** |
| Azure Cloud Solution | Layer 7- Application | Application |
| Cisco Router | Layer 3- Network | Internet |
| Fortinet Firewall | Layer 7- Application | Application |
| Cisco Switch | Layer 3- Network | Internet |
| Wireless Access Points | Layer 2- Data Link | Network Access |
| Laptops and workstations | Layer 7- Application | Application |
| Cabling | Layer 1-Physical | Network Access |

# E.  RATIONALE

Here is the rationale for adding, deleting, or repurposing network components in the newly merged network topology diagram, including details of how *each* component addresses budgetary constraints. Discussed are the components purchased, retained or repurposed and the reasons why the prices for the devices are listed in a cost summary table and the purpose for the purchase.

**Additions:**

**Azure Cloud Solution**

* **Total Price:** **$24,000/year** ($2,000/month)
* **Deployment Model:** **Hybrid Cloud** (Azure + on-premises equipment).
* **Service Models Used:** **SaaS** (Microsoft 365) and **PaaS** (Azure App Services, Databases, Security).
* **Rationale:**
  + Consolidates email, collaboration, security monitoring, application hosting, and databases into one predictable subscription cost.
  + Provides scalability (you only pay for what you use), security (Zero Trust, Defender, Sentinel), and regulatory compliance (PCI DSS, HIPAA, SOX).
  + Makes budgeting simple for executives — one line item for “Azure Cloud Solution.”

**Components Purchased**

1. **Cisco Catalyst 9200 24-port PoE+ Switches (2 units)**

**Price**: Approximately $2,947 each from CDW [CDW](https://www.cdw.com/product/cisco-catalyst-9200-network-advantage-switch-24-ports-smart-rack/5423319?utm_source=chatgpt.com)

**Rationale**:

* Upgraded from end-of-life hardware to modern, stackable switches offering PoE capability for new Wi-Fi 7 APs and support for network segmentation.
* The CDW price reflects current enterprise rates under licensing bundles, offering performance and support at a reasonable cost.
* PoE features of new Catalyst and APs can support any remaining physical endpoints before full cloud migration.
* Pricier than older gear but valuable for support and future growth; still under budget when replacing previous units.

1. **Fortinet FortiGate 100F Firewalls (2 units)**

**Price**: $2,069.99 each from CDW [CDW](https://www.cdw.com/product/fortinet-fortigate-100f-security-appliance/5615104?utm_source=chatgpt.com)

**Rationale**:

* Core NGFWs providing deep packet inspection, Zero Trust enforcement, and SD-WAN.
* They replace older, less capable firewalls while balancing performance and cost effectively.
* Handles Zero-Trust workloads, SSL decryption, and advanced IPS at scale.
* Supports dual 10G uplinks for data centers or cloud interconnect.
* Consistency across Company A & B simplifies policies.
* Longer lifecycle and future firmware support

1. **Cisco Catalyst 8200 (C8200-1N-4T) Routers (2 units)**

**Price**: $1,707.99 each from CDW (current discounted price) [CDW](https://www.cdw.com/product/cisco-catalyst-8200-1n-4t-router-rack-mountable/7364597?utm_source=chatgpt.com)

**Rationale**:

* Enterprise-grade routers with SD-WAN capabilities and SASE readiness, replacing legacy or consumer-grade routers.
* The CDW price provides good value for the performance and flexibility needed. It’s cost-effective given the longevity, fewer support issues, and compatibility with Azure VPN.
* For Company B, the Verizon Fios CR1000A were great for home/SMB, but not an enterprise edge. It has no advanced routing/SD-WAN/segmentation.
* For Company A, the Cisco 7600 reached end-of-life, was power-hungry, had no modern SD-WAN, and was a weak fit for small/medium branch.

1. **Ubiquiti U7-Pro Wi-Fi 7 Access Points (3 units)**

**Price**: $189 each from Ubiquiti Store [Ubiquiti Store](https://store.ui.com/us/en/products/u7-pro?utm_source=chatgpt.com)[streakwave.com](https://www.streakwave.com/ubiquiti-networks-u7-pro-us-unifi-ap-7-pro-us?utm_source=chatgpt.com)

**Rationale**: High-performance Wi-Fi 7 APs providing modern wireless coverage with high device concurrency. Chosen for affordability and future readiness.

**Components Retained or Repurposed**

* **User Workstations and Laptops** (Windows 10, 11, MacOS, Ubuntu)
  + **Rationale**: Still functional for end-users; no immediate replacement needed. This avoids unnecessary expenses.
* **Cable Plant (Cat5e at Company A)**
  + **Rationale**: Upgrading to Cat6 is deferred to next year due to budget constraints. The cost is about $10,000. It retains operational infrastructure while cash flow is conserved.
* **Cables (Cat6a at Company B)** – no changes were needed since they were already up to date with cabling standards.
* **Remaining Endpoints / Devices**
  + **Rationale**: Devices that meet baseline security and operational needs continue to function post-merger, reducing immediate replacement costs.

**Repurposed Components**

* None of the core network hardware was repurposed beyond the Hyper-V hosts—every switch, router, firewall, and AP was upgraded to meet zero-trust, PoE+, and multi-gig requirements.

**Deleted System Components (Post-Merger)**

Because all servers are migrated to Azure Cloud, the following on-premises system components were deleted/retired:

* **Company A Deleted Components**
  + Windows Server 2019 (SharePoint, Exchange)
  + Windows Server 2012 (Application server)
  + Windows Server 2012R2 (File server)
  + Windows Server 2012 (FTP + External Web Server in DMZ)
* **Company B Deleted Components**
  + Hyper-V Virtualized Farm (2 hosts)
  + 20 Virtualized Servers (including FTP, Domain Controllers, File Server, Ruby, Elasticsearch cluster, Web servers, PostgreSQL, MariaDB, Tomcat/PHP, Remote Desktop Servers, Legacy Exchange Servers)

**Rationale:**

Migrating to Azure eliminates redundant, legacy, and unsupported servers, reducing patching burden, EOL risks, and on-prem infrastructure costs.

**Security:** Migrating to Azure ensures all workloads run on supported platforms with built-in patching and monitoring.

**Compliance:** Cloud services like M365, Azure Database, and Defender for Cloud are already PCI DSS, HIPAA, and SOX compliant, meeting Company A’s financial requirements and Company B’s healthcare requirements.

**Scalability:** Workloads like ElasticSearch, web apps, and SQL scale up/down with demand.

**Cost Control:** Legacy, power-hungry servers are retired, lowering expenses.

**Cost Summary Table**

| **Category** | **Item(s)** | **Units** | **Unit Price** | **Total** |
| --- | --- | --- | --- | --- |
| **Azure Cloud Solution** | SaaS (M365), PaaS (App Service, DB, Logic Apps, Defender, Sentinel, AVD) | N/A | $2,000/month | **$24,000 / year** |
| **Switches** | Cisco Catalyst 9200 24-port PoE+ | 2 | $2,946.99 | **$5,893.98**[CDW](https://www.cdw.com/product/cisco-catalyst-9200-network-advantage-switch-24-ports-smart-rack/5423319?utm_source=chatgpt.com) |
| **Firewalls** | Fortinet FortiGate 100F | 2 | $2,069.99 | **$4,139.98**[CDW](https://www.cdw.com/product/fortinet-fortigate-100f-security-appliance/5615104?utm_source=chatgpt.com) |
| **Routers** | Cisco Catalyst 8200 (C8200-1N-4T) | 2 | $1,707.99 | **$3,415.98**[CDW](https://www.cdw.com/product/cisco-catalyst-8200-1n-4t-router-rack-mountable/7364597?utm_source=chatgpt.com) |
| **Wireless APs** | Ubiquiti U7-Pro | 3 | $189.00 | **$567.00**[Ubiquiti Store](https://store.ui.com/us/en/products/u7-pro?utm_source=chatgpt.com) |
| **TOTAL (Year 1)** |  |  |  | **$37,996.94** |

**Rationale**

* **Azure Cloud Solution ($24K/year):** Consolidates all cloud services into a single predictable subscription that covers email, collaboration, web apps, databases, remote desktop, and security. This makes budgeting simple for executives while ensuring compliance and scalability.
* **Hardware ($14K one-time expense):** Modernized switches, firewalls, routers, and APs provide secure, future-proof infrastructure at both sites while staying below budget.
* **Total Project Spend = $38K,** leaving $12K in budget left for contingencies (support contracts, licenses, or future upgrades).
* By purchasing only, the essential switches, firewalls, routers, and APs—while retaining virtualization hosts and deferring cabling, we align our $50K budget to deliver a secure, zero-trust hybrid network without unnecessary capital spending.

# F.  SECURE NETWORK DESIGN PRINCIPLES

Here are two secure network design principles that are used in the proposed network topology diagram.

**Network design principle 1: Redundancy**

Redundancy: This principle involves implementing backup systems and protocols to ensure the availability of resources in the event of a failure or attack. This can include backup servers, redundant communication paths, and disaster recovery plans. (Landoll,2021). The Azure Cloud Solution was added as a redundant platform for critical services (Exchange, SharePoint, Application Hosting, Data Storage). If on-premises servers or networking hardware fail at either Company A or Company B, employees can still access the cloud-hosted resources. The topology diagram shows separate firewalls, routers, and switches for Company A and Company B. This segmentation creates redundancy between sites. If one company’s site has a localized outage, the other can still function independently while remaining securely connected. This redundancy increases network availability and resilience, meeting the executives’ requirements for scalability and continuity of operations.

**Network design principle 2: Least Privilege**

Least privilege: This principle involves granting users and devices the minimum level of access needed to perform their job duties. (Landoll,2021).  This helps to reduce the risk of unauthorized access to sensitive resources. Least privilege is implemented through Zero Trust principles installed into the new merged network topology. For both companies on the topology, every entry point (remote laptops, wired workstations, wireless access, and subnets) is gated by Zero Trust controls. In Company A and Company B, all laptops and PCs connect through Zero Trust gateways before reaching the internet or Azure Cloud Solution. This ensures employees cannot bypass authentication, and their permissions are limited to only the services they need. This network design principle reduces risks from insider threats, compromised accounts, or malware spreading laterally across the merged network and is a benefit to the business.

Zero Trust promotes the principle of least privilege by requiring users to request access for things like downloading apps, programs, and games to their laptops or workstations. These applications requests will be compared to allow rules based on the user’s job position and functional department. This will keep unnecessary downloading and keep the attack surface of the company to a minimum. If the application is not essential to the user performing their job functions, it will be denied. This network design principle also promotes productivity and efficiency in workplace activities.

# G.  REGULATORY COMPLIANCE

Here is an explanation of how the proposed merged network topology diagram addresses two regulatory compliance requirements that are relevant to the newly merged company.

**Regulatory compliance #1: PCI-DSS (Payment Card Industry Data Security Standard).**

•   PCI-DSS (Payment Card Industry Data Security Standard). The PCI DSS (Payment Card Industry Data Security Standard) has been devised to increase security around card transactions. The Standard is acknowledged the world over, and compliance is mandatory for card-accepting organizations. It requires merchants to demonstrate a secure IT network that protects cardholder data, maintain a vulnerability management program, implement access control measures, and regularly test their networks (GRC International Group. (n/d)).

•   This standard is relevant to both Company B and Company A. Company B processes credit card payments, and Company A (financial services) also deals with payment card data. PCI-DSS compliance ensures protection of cardholder data.

•   How Implemented in the Merged Topology:

* Segmentation**:** Payment processing servers are isolated in their own VLAN behind firewalls.
* Azure Key Vault secures encryption keys used in transactions.
* Zero Trust MFA: ensures only payment system administrators can manage card processing applications.

**Example:** A transaction from a medical provider using Company B’s platform is encrypted end-to-end, tokenized in Azure Payment Gateway, and stored in a PCI-DSS compliant environment.

**Regulatory compliance #2: HIPAA (Health Insurance Portability and Accountability Act**

HIPAA (Health Insurance Portability and Accountability Act). HIPAA is a United States federal regulation, passed in 1996, that regulates how patient data can be used by covered entities and business associates who work with personally identifiable information (PII) and protected health information (PHI) (Hiter,2021).

•   Relevance to the newly merged company? Company B provides software to medical providers and accepts credit card payments. Any handling of Protected Health Information (PHI) by their software requires HIPAA compliance.

•   How Implemented in the Merged Topology:

* Azure Compliance Features**:** Company B’s software hosted in Azure App Services leverages HIPAA-certified infrastructure.
* Encrypted Databases (PostgreSQL/MariaDB in Azure) protect PHI both at rest and in transit (TLS 1.2/1.3).
* Zero Trust + Entra ID (Azure AD**)** ensures role-based access to PHI. Doctors logging into Company B’s platform only get access to the patient records necessary for their work.

**Example:** When a medical provider logs in to Company B’s platform, traffic is routed through the FortiGate firewall, authenticated with Azure AD MFA, and stored in HIPAA-compliant encrypted Azure databases, preventing unauthorized disclosure of PHI.

# H.  EMERGING THREATS

Here are possible threats that could occur during or after the merger.

**Emerging Threat #1: Ransomware Attack**.

Ransomware attacks are popular methods among cybercriminals to infiltrate organizations and to extract payments. This malware may enter the organization’s system through social engineering, insecure websites, trojan horse downloads, or weak account credentials. When a ransomware attack has successfully deployed it typically encrypts critical systems files disabling all systems (Landoll, 2021)

**Potential network security risks of implementing the topology:**

* Company A previously had open ports (3389 RDP, 21 FTP)
* Company B had brute-force risks on FTP/VNC.
* Even after migration, attackers could target remote access paths (VPN, RDP, remote desktops).
* Company A has other issues that could allow attackers to take over the system:
  + All users use eight-character passwords.
  + User accounts no longer required are not removed.
  + All users have local administrative privileges.
  + Regular password changes are not enforced.
* Privilege Escalation: Since all users have local admin rights, ransomware executes system-wide changes without restriction.
* Weak 8-character admin-level passwords allow brute-force entry.

•   **Potential performance impacts on the merged network after implementation of the proposed design**:

* Mass encryption across hybrid environments (cloud + on-prem endpoints) could interrupt financial transactions and medical software access. High computing usage from ransomware could slow Azure workloads and network bandwidth.
* Attackers could utilize the inactive user accounts and with the local administrative privileges.
* Increased Network Traffic from Exploitation Attempts
* System Resource Drain from Malware & Ransomware

•   **How to manage the identified potential security risks**:

* Enable endpoint security to block unauthorized encryption processes.
* Use FortiGate 100F firewalls with intrusion prevention (IPS) to block ransomware command-and-control traffic.
* Conduct user training against phishing, the #1 ransomware entry point.
* Deploy Azure Backup & Site Recovery + Immutable Blob Storage for untampered backups.

**Emerging Threat #2: Legacy Device Exploitation (On-Prem Workstations & Laptops)**

•   **Potential network security risks of implementing the topology:**

* Company A still has Windows 7 laptops, and Company B had Windows XP and Windows 7 workstations. Even if servers move to Azure, these endpoints could be exploited as entry points into the merged network.
* Unpatched devices could be leveraged for lateral movement into the cloud.
* Dormant accounts that were never deleted may be leveraged to spread ransomware further and gain persistence.
* Ransomware uses SMB/NTLM flaws to propagate across hybrid networks (on-prem and into cloud-connected devices).

•   **Potential performance impacts on the merged network after implementation of the proposed design:**

* Compromised endpoints could inject malware into the network and slow traffic.
* Ransomware can encrypt files on mapped drives, including Azure-synced cloud storage.
* Compatibility and Integration Issues: XP/7 systems may not fully support modern encryption, VPN, or Zero Trust tools.
* Hybrid connections between on-prem XP/7 machines and Azure services may cause latency due to encryption downgrades.
* Downtime if legacy devices are compromised.

•   **How to manage the identified potential security risks:**

* Immediate retirement of Windows XP/7 systems.
* Replace with Windows 11 Enterprise laptops.
* Segment legacy endpoints in isolated VLANs until fully replaced.
* Apply network-level firewall rules to block SMB/RDP from these endpoints.
* Enforce privilege reduction to remove local admin rights.
* Require longer passwords (at least 12–16 characters with complexity).
* Require MFA for all accounts.
* Remove inactive/dormant accounts.
* Implement Privileged Access Workstations (PAWs) to reduce admin abuse.

# I.  SUMMARY RECOMMENDATIONS

My recommendation is to migrate all servers to Azure Cloud while maintaining upgraded on-premises network equipment at both company sites. This hybrid model delivers the scalability, redundancy, and regulatory compliance both companies require, while staying within the $50,000 budget.

By consolidating in Azure and implementing Zero Trust security, the merged company gains:

* Stronger security (defense against ransomware, insider threats, and cloud misconfigurations).
* Lower costs (Operation Expenses model avoids expensive server refreshes).
* Regulatory compliance built into the infrastructure.
* Future scalability to grow without additional capital expenditures.

**Cost-Benefit Analysis**

* **On-Premises**: High control, lower long-term cost, but high upfront hardware refresh expenses ($30k).
* **Cloud**: Scalable, resilient, pay-as-you-go; reduces physical maintenance; better disaster recovery ($20k/year).

**1. Cost–Benefit Analysis: On-Premises vs. Cloud Infrastructure**

| **Category** | **On-Premises Infrastructure** | **Cloud (Azure) Infrastructure** |
| --- | --- | --- |
| **Upfront Costs (CapEx)** | High: Hardware, servers, storage, licensing, power/cooling, data center space. | Low: Subscription model (OpEx), pay-as-you-go services. |
| **Ongoing Costs** | Hardware refresh every 3–5 years; high maintenance/support. | Predictable monthly/annual costs; scales up/down with demand. |
| **Scalability** | Limited: Scaling requires new physical equipment purchases. | High: Instant scalability via Azure services. |
| **Redundancy/Resilience** | Expensive to achieve; requires duplicate hardware and sites. | Built-in redundancy through Azure’s global data centers and availability zones. |
| **Security Capabilities** | Manual patching, on-premises firewalls only. | Cloud-native Zero Trust, Defender for Cloud, Sentinel SIEM, and MFA. |
| **Compliance** | Requires additional tools and audit resources. | Azure provides HIPAA, PCI DSS, GLBA, and SOC compliance certifications. |
| **Performance Risk** | Hardware aging leads to downtime and bottlenecks. | Microsoft ensures uptime SLAs (99.95%+). |

**2. Recommendations & Justification**

* **Migrate All Servers to Azure Cloud:**  
  Both Company A and Company B’s servers are consolidated into Azure SaaS and PaaS. This eliminates aging hardware, removes legacy operating system vulnerabilities, and provides built-in redundancy that an on-premises solution would not achieve under the $50,000 budget.
* **Adopt a Hybrid Deployment Model:**  
  Maintain on-premises network equipment (switches, firewalls, routers, wireless APs) for each company’s site to ensure local connectivity, while connecting securely to Azure for critical workloads. This balances security, cost, and performance.
* **Implement Zero Trust Security (Least Privilege + MFA):**  
  Azure AD, conditional access, and FortiGate firewalls provide strong identity and access controls. This is essential given Company B’s previous lack of a dedicated cybersecurity role and the risks from legacy devices.
* **Leverage Azure Services for Compliance:**  
  Azure provides regulatory compliance support for financial services (Company A – GLBA, PCI DSS) and healthcare (Company B – HIPAA, PCI DSS). This reduces compliance overhead and avoids costly fines.
* **Cost Alignment with Budget:**
  + **Azure Cloud Services (PaaS/SaaS hybrid):** = $24,000 annually (includes VMs, backup, security, compliance tools).
  + **Networking Equipment (switches, routers, firewalls, APs):** = $14,000 upfront.
  + **Total Project Spend =** $38K, leaving $12K in budget left for contingencies (support contracts, licenses, or future upgrades).
  + **Total < $50,000 (within budget).**

**3. Business Value for Executives**

* **Reduced Risk Exposure:** Eliminates unsupported systems (XP/7, Server 2012) that are highly exploitable.
* **Improved Security Posture:** Zero Trust + cloud monitoring reduces the likelihood of ransomware and insider threats.
* **Operational Efficiency:** Azure provides scalability, disaster recovery, and monitoring without requiring a dedicated on-premises data center.
* **Regulatory Compliance:** Meets PCI DSS and HIPAA/GLBA obligations seamlessly via Azure compliance frameworks.
* **Financial Justification:** Staying entirely on-premises would require over $150,000+ in CapEx (servers, redundant data centers, compliance tools), whereas the Azure hybrid delivers better security and redundancy within the $50,000 budget.

# J. [SOURCES](https://lrps.wgu.edu/provision/71484321)

* Landoll, D. J. (2021). *The Security Risk Assessment Handbook*. CRC Press. https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2759769&site=eds-live&scope=site&authtype=sso&custid=ns017578&ebv=EB&ppid=pp\_61 pg. 392
* Hiter, S. (2021, Sept 8). *Five Tips for Managing Compliance on Enterprise Networks.* <https://www.enterprisenetworkingplanet.com/standards-protocols/compliance-management-enterprise-networks/>
* GRC International Group. (n/d). *Governance and Regulatory Compliance.* <https://www.itgovernanceusa.com/compliance>

**Azure Cloud Services**

* Microsoft. (n.d.). *Compare all Microsoft 365 business products*. Microsoft. Retrieved August 17, 2025, from <https://www.microsoft.com/en-us/microsoft-365/business/compare-all-microsoft-365-business-products>
* Microsoft Azure. (n.d.). *App Service pricing*. Microsoft. Retrieved August 17, 2025, from <https://azure.microsoft.com/en-us/pricing/details/app-service/linux/>
* Microsoft Azure. (n.d.). *Azure Database for PostgreSQL flexible server pricing*. Microsoft. Retrieved August 17, 2025, from <https://azure.microsoft.com/en-us/pricing/details/postgresql/flexible-server/>
* Microsoft Azure. (n.d.). *Logic Apps pricing*. Microsoft. Retrieved August 17, 2025, from <https://azure.microsoft.com/en-us/pricing/details/logic-apps/>
* Microsoft Azure. (n.d.). *Virtual Desktop pricing*. Microsoft. Retrieved August 17, 2025, from <https://azure.microsoft.com/en-us/pricing/details/virtual-desktop/>
* Microsoft Azure. (n.d.). *Microsoft Sentinel pricing*. Microsoft. Retrieved August 17, 2025, from <https://azure.microsoft.com/en-us/pricing/details/microsoft-sentinel/>
* Microsoft Azure. (n.d.). *Microsoft Defender for Cloud pricing*. Microsoft. Retrieved August 17, 2025, from <https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/>

**Hardware Purchased**

* CDW. (n.d.). *Cisco Catalyst 9200 switches*. CDW. Retrieved August 17, 2025, from <https://www.cdw.com/search/?key=cisco+catalyst+9200>
* CDW. (n.d.). *Cisco Catalyst 9300 switches*. CDW. Retrieved August 17, 2025, from <https://www.cdw.com/search/?key=cisco+catalyst+9300>
* CDW. (n.d.). *Cisco Catalyst 8200 routers*. CDW. Retrieved August 17, 2025, from <https://www.cdw.com/search/?key=cisco+8200>
* CDW. (n.d.). *Fortinet FortiGate 100F firewall*. CDW. Retrieved August 17, 2025, from <https://www.cdw.com/search/?key=fortigate+100f>
* Ubiquiti Inc. (n.d.). *U7-Pro access point*. Ubiquiti Store. Retrieved August 17, 2025, from <https://store.ui.com/us/en/pro/category/all-unifi-access-points/products/u7-pro>