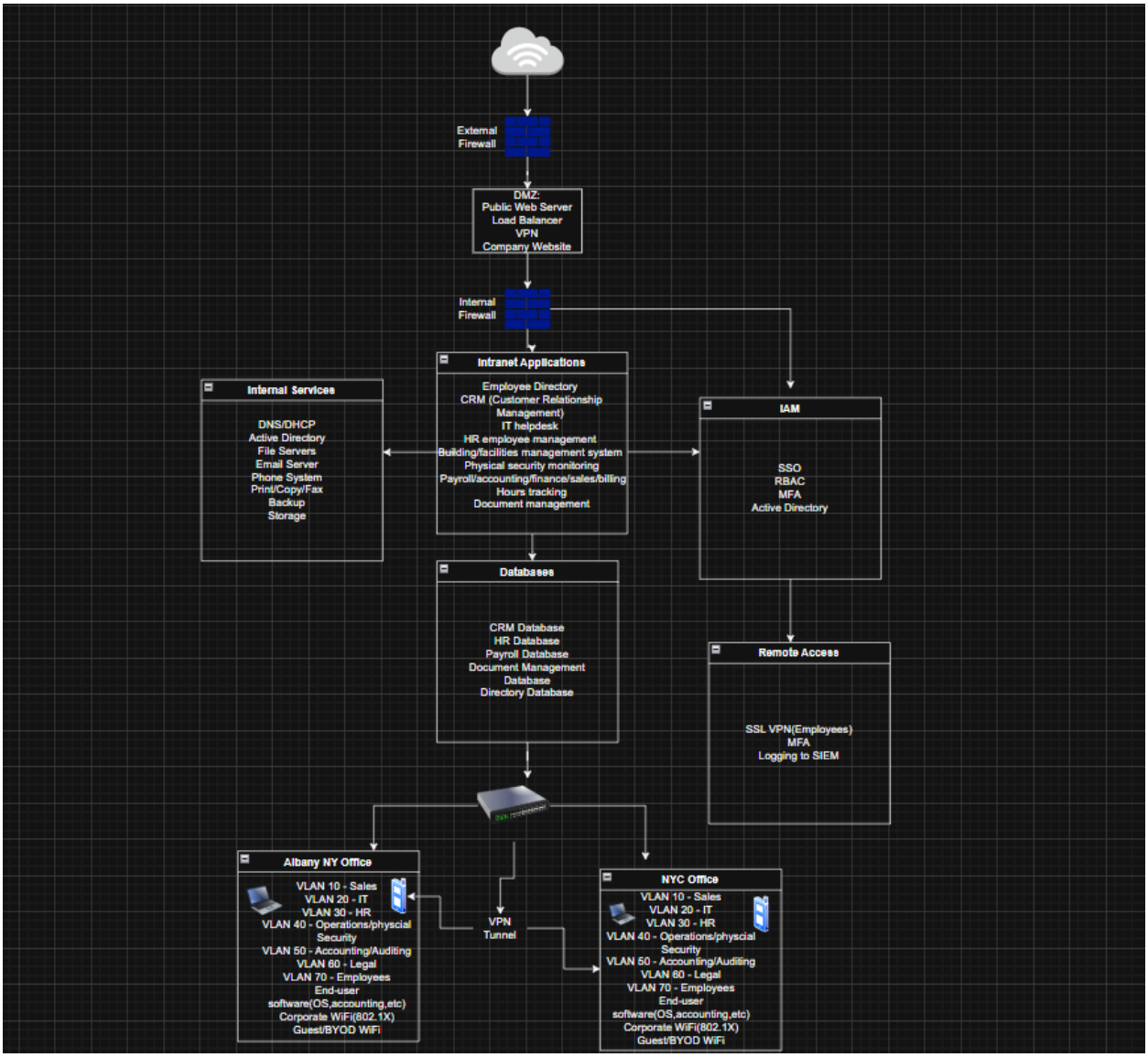
Information Security Compliance Auditing

Assignment 2

Iturralde, Lapointe, Patanjo and Rosenblum

Table of Contents

Part 1 – Design, Configure and Implement



The newly restructured company operates across Albany, NY and New York City (NYC) and has about 100-200 employees across both locations. To ensure business day-to-day operations after the split, a redesign of the company's information technology infrastructure was required. The design shown above provides a secure, segmented, and fully functional network capable of supporting business operations, internal services, employee access, and internet-facing systems. The architecture prioritizes security, scalability, and auditability to meet industry compliance requirements.

The network's perimeter is secured by an external firewall that is the main interface between the internal environment and the public internet. This firewall protects the demilitarized zone (DMZ), which holds all systems facing the external internet such as the public web server and

load balancer that gives access to the company's website. The DMZ has the company's VPN gateway, which authenticates remote workers before granting access to the internal network. Placing the VPN gateway in the DMZ reduces the risk of exposing sensitive information while still allowing public accessibility, making it adherent to industry's best practices for internet-facing systems.

Behind the internal firewall is the core internal network, which is segmented into serval functional zones to support business operations and security. The Intranet Applications Zone holds the internal software services used daily by employees, including the Employee Directory, Customer Relationship Management system, HR management tools, IT Helpdesk, facilities management system, physical security monitoring systems, payroll and finance systems, hours tracking tools, and documentation management tools. These applications are used within the company and are logically separated from databases and authentication systems for security.

The Database Zone provides a centralized storage space for CRM data, HR data, Finance records, documentation metadata, and directory information. Separating application servers from the databases makes access control management easier.

The core IT infrastructure is located in the Albany office. This includes services such as DNS, DHCP, Active Directory, email servers, BYOD mobile devices, file servers, print/copy/fax services, and SIEM centralized logging. Identity Access Management systems are also hosted in Albany and support SSO, RBAC, MFA, and active directory authentication. These systems enforce the least privilege and keep access consistent across both office locations.

The company's workforce is divided between the Albany and New York City offices. Due to the geographical separation, a Site-to-Site VPN tunnel connects both locations, providing encrypted communications between both sites' networks. Albany hosts the IT infrastructure and internal applications, while the NYC office functions as an employee's workspace. The VPN tunnel makes sure that employees in NYC can securely access systems hosted in Albany including intranet applications, file servers, email and identity management services. This approach is more efficient and easier to manage.

Both offices use VLAN segmentation to ensure separation of roles, departments, and security zones. Each department, such as sales, IT, HR, operations, accounting/auditing, legal and employees, has its own VLAN. This segmentation reduces the risk of lateral network movement, enhances compliance, and supports department-specific access controls. The same VLAN number scheme is used in both offices for simplicity.

Each office has two wireless networks: Corporate Wi-Fi, which uses 802.1X authentication with Active Directory and Guest/BYOD Wi-Fi, which is isolated from the internal network and only

has internet access, keeping personal devices away from internal systems. This design ensures that personal devices and visitors cannot interact with internal systems or sensitive data.

The remote access zone supports SSL-based VPN connections with multifactor authentication. Employee VPN traffic enters through the DMZ, goes through identity verification through Active Directory, and IAM controls, and is then routed to internal network resources. This architecture provides secure and auditable remote access for employees. The backup server ensures system resilience and data integrity. Regular backups support disaster recovery and provide the basis for retention policies to ensure industry compliance.

The network infrastructure provides a secure and well-segmented environment capable of supporting business operations across both offices. It includes all required business services, security zones, departmental segmentation, DMZ structure, wireless networks, VPN connectivity, and identity management components. The design is auditable due to centralized logging, access control, and network segmentation. This architecture is the baseline of which the company can operate and be evaluated against compliance frameworks.

To design the network architecture, a requirements-driven methodology was followed. First, the company's needs were gathered based on strict specifications such as departmental separation, required business services, wireless access, remote activity, backup servers, and public-facing applications. These requirements were aligned with security principles such as defense-in-depth, least privilege, and network segmentation to ensure that the architecture meets both operational and compliance expectations.

Next, the design process involved breaking the network into layers: the perimeter, DMZ, internal services, internal applications, databases, identity management, and branch off environments. Each layer was crafted using industry best practices, such as placing public web servers in a DMZ, separating application servers from databases, isolating admin services, and implementing VLANs to enforce departmental segmentation. Consideration was given to the company's post-split structure, where Albany kept most of the infrastructure, and NYC retained most of the staff. This was important when thinking about the placement of servers, wireless systems, and the VPN link that connects both offices.

The diagram was then built using logical groupings that mirror real-world architectures. This included separating offices, zones, VLANs, and security boundaries. All services listed were found in the requirements of the network architecture, such as CRM, HR tools, email, phone services, file servers, and a backup system were incorporated into the internal services and intranet application zones. Remote access, BYOD, and Wi-Fi segmentation were added to enhance security. This network design is auditable against industry compliance frameworks and supports the company's operations going forward.

Part 2 – Compliance Audit (PCI DSS) for Dick's Sporting Goods

Executive Summary

In this case, we are implementing and redesigning the infrastructure of a network to be able to allow a keener focus on security and the functionality of compliance for Albany NY, and New York City offices. Assessing the architecture of the network like segmentations, site-to-site VPN connectivity, identity and access management, and recovery mechanisms. This redesign and audit were conducted under the PCI DSS framework to evaluate the organization's compliance posture and technical readiness.

This study's scope is to use VLAN segmentation, remote access controls, and backup systems. The assessment covered both internal and perimeter systems that handle or could impact cardholder data environments. Having potential issues when coming to security due to a restriction in visibility when using third party systems or companies that could potentially change the way the network configurations are configured. These third-party visibility gaps with limited historical documentation represent key limitations in this audit.

Some key findings that were demonstrated are how in the redesigned network there was a better environment to have scalability, audibility, and security. Having perimeter firewall defense, VLAN segmentation to limit the amount of lateral movement, using Wi-Fi with the authentication method of 802.1X, guest networks becoming more isolated, VPN multifactor authentication, and adding backup measures in case of any kind of disaster ready for whatever recovery method they need. However, the audit revealed several procedural deficiencies like outdated password policies, inactive multifactor authentication enforcement, lack of periodic penetration testing, and incomplete patch management documentation. The network overall has its way to be able to maintain up to security standards and support compliance requirements.

Preamble

The focus of this study is network security and IT infrastructure compliance. To prioritize the security of the networks of data, design, and access control. From a company standpoint it is crucial for them to be able to have a reliable IT service across multiple locations due to how many organizations rely on it.

Continuing the organizational split, the company implemented a redesigned IT infrastructure to be able to still be efficient while still trying to maintain the requirements of compliance. Examining VLAN segmentations into separate roles and zones of the department, securing wireless networks while keeping proper authentication, SSL-based VPN for remote access, and having more robust backup systems. These are ways that were all implemented to have the purpose of mitigating risks. Some of which are like unauthorized access, lateral movement across the network, and data loss. They are making sure that the system is going to be kept up to regulatory standards. By being able to align compliance frameworks with the network architecture, the security of sensitive data, and maintainability of the audit, the company can be able to fully support it.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

PCI DSS Quick Reference Guide

Surveys/Instruments

Question	Response
Section 1-	--
Requirement 1	--
Is there a documented network diagram showing all cardholder data flow?	Maintains a documented network diagram; developed 25 years ago and no update since; not accurate
Are firewall/router rules reviewed and approved before implementation, and how often are they reviewed?	Goes through Capacity Management process; all changes are well documented
Are inbound/outbound connections limited to only what's required for business?	Only inbound connection; perimeter where any outbound connection is not connected to the network; separate outside network
How are default "allow any" or "permit all" rules prevented or controlled?	Don't use default on any devices; stringent access policy on the network
Requirement 2	--
Are all default passwords and SNMP strings changed before deployment?	Yes; all changed
How is compliance with secure configuration standards (e.g., CIS Benchmarks) verified?	No way of verifying if the business is in compliance
How are unused default accounts/services removed or disabled?	Have a process; once approved the account will be removed
Is there a configuration hardening checklist for new systems?	No checklist
Section 2-	--
Requirement 3	--
Where and how is cardholder data stored (e.g., databases, logs, backups), and is it separate from membership data?	All data is on one server
Is data stored on-premises, in the cloud, or elsewhere?	All data stored on-prem
What encryption algorithms and key lengths are used for storage? How are they stored, rotated, and destroyed?	Default Windows Encryption solution; using standard BitLocker on Windows 7
How are data retention and disposal handled per policy?	Data Retention Policy; no implementation even though there is an existing policy
Requirement 4	--
What kind of encryption protocols are being used to transmit the cardholder's data?	Uses IPSec
Are wireless networks transmitting cardholder data secured with WPA2 or stronger encryption?	Doesn't use wireless

If a cardholder's data is being sent without an encryption then what kind of steps would you take to be able to prevent the data from being sent out.	There is only inbound traffic, nothing going out so only receiving data is feasible.
Section 3-	--
Requirement 5	--
What anti-malware solutions are deployed across systems in scope?	Standard Windows Malware Solution that came default on the machine
Are there other kinds of non-traditional systems that would be monitored (servers, Linux devices, POS) for malware threats?	Vulnerability management software that scans the servers; GFI Lionguard
When malware is detected, what kind of methods do you use to handle alerts?	IPS/IDS that is externally managed; alerts if there is a potential incident in the network
Requirement 6	
How are security patches evaluated, tested, and applied across systems?	Patches are not tested before being pushed out
What is the average timeframe between when a patch is released and the deployment of it out to the public?	No timeframe
Are your web applications tested for vulnerabilities and if so, what ways would you be testing them?	Vulnerability management software; go on and install the vendor patches
Section 4	--
Requirement 7	--
Is the principle of least privilege implemented, if so, how?	All users and staff have the same level of access
Who reviews and approves access to cardholder data systems?	One systems employee reviews the data
How frequently are access rights reviewed or recertified?	Never reviewed because everyone has the same access
Are access control lists (ACLs) documented and maintained?	Have a document of access but since everyone has the same access this does not totally apply
Requirement 8	
What multifactor authentication methods are used for administrative access?	Have MFA in place but it is not operationalized
How are password requirements configured (length, complexity, expiration)?	Last update to the password policy is 10+ years ago; not accurate
Requirement 9	
Where are cardholder data systems physically located?	On-site
Section 5-	--
Requirement 10	--

What logging mechanisms are in place for systems that store or process cardholder data?	Username and password for all users
Are logs centrally collected and reviewed regularly (e.g., via SIEM)?	Logs are centrally collected; only reviewed if there is an incident
How are failed login attempts and privileged activities monitored?	3 failed attempts notify someone which is considered as an incident, and it will be investigated
How long are logs retained?	Forever; have the space for the logs
Requirement 11	--
Does your organization run internal and external vulnerability scans? If so, how often?	Only internal vulnerability scan once a year
Are quarterly Approved Scanning Vendor (ASV) scans performed and documented?	No ASV scan performed
How often are penetration tests performed (internal/external)?	No penetration tests performed
Are intrusion detection/prevention systems (IDS/IPS) in place and monitored?	Yes
How are detected vulnerabilities tracked to remediation? Is this documented?	Log vulns in risk register; high impact, medium impact, low impact; remediation is addressed on impact to the business
Section 6-	--
Requirement 12	--
Do you maintain an information security policy? If so, is it reviewed and updated at least annually?	There is an information security policy; not reviewed or updated annually; hasn't been reviewed for 10 years
Is PCI DSS awareness training provided to all employees annually?	General training and awareness training upon onboarding; no continuous training
How is third-party/vendor compliance with PCI DSS monitored?	Sign a SLA and that third parties have to be compliant; no third-party risk assessments
How are incident response procedures tested and updated? Does your organization maintain an IRP? Is it tested at least annually?	Have contingency plans; never tested and haven't been reviewed for at least 5 years

Analysis

According to the results of the investigation, there is a high level of compliance used in the company when it comes to standard information security and IT governance practices. The infrastructure being redesigned has allowed adding multiple layers of security to be truly effective. These meet the core principles of the C.I.A triad.

The company has an infrastructure that is newly designed but was to make a strong foundation by being able to maintain the standard. The segmentation of the VLANs in the network allowed it for a mitigation in lateral movement risks and would enhance the data segregation. The firewall and system configurations being set up can help ensure that inbound and outbound

traffic is properly filtered and monitored to prevent unauthorized access or data exfiltration. Even with these improvements, compliance gaps still exist. MFA is in place but not fully working, which weakens identity management. Password policies and access rights are outdated and haven't been reviewed in over ten years. The company also doesn't perform regular penetration testing, which makes it harder to fix and find new threats. Patch management system hardening is not done consistently, which increases the chance of security issues.
From a policy standpoint, employees do not receive any regular security awareness training, and many company policies have not been updated in years. Although the technical design is strong, administrative and training areas will have to improve to maintain ongoing PCI DSS compliance.

HackIoT Lab is currently partially compliant with PCI DSS standards. The redesigned infrastructure shows good progress in network security, access control, and data protection, but the organization needs stronger governance, updated policies, and continuous monitoring to reach full compliance.

Recommendations

To achieve compliance, HackIoT Lab should adopt to these recommendations:

1. Implementation of a Constant Monitoring System:

Having a constant monitor over the systems to make sure that all the configurations are correct. Also being able to access the permissions to make sure that everything is staying up to the current standard.

2. Enhancement of Security Awareness:

Making sure that employees are continuously getting trained in order to mitigate the amount of human error that can occur. Either it's some sort of compliance training or just cybersecurity training in general.

3. Conduct Penetration and Security Audit Tests:

By either doing annual or semi-annual checks to see if there are any new types of vulnerabilities or risks, then being able to identify them. Also, to make sure that security controls are still effective through tabletop exercises.

4. Strengthen Incident Responses and Recovery with Backups:

Being able to find a way to practice drills in case of a cyber-attack and making sure that all data is backed up, there is no chance of data loss. The more practice we get in a situation, the better it would be with the response time and recovery rate of the data.

5. Updating Access Control Priorities:

Making sure that all the roles in a department are accounted for. Make sure they are being looked over and that all the privileges are assorted for each role like employees and the public.
By addressing these security gaps, HackIoT Lab will greatly reduce its risk exposure, strengthen its security posture, and become more compliant with PCI DSS requirements.

Conclusion

The redesigned information system architecture and the PCI-DSS compliance audit provide a view of the organization's current security posture and its readiness to protect sensitive data across the two office locations. Part 1 formed a scalable, segmented, and security-focus network design that aligns with industry's best practices. This architecture includes separate DMZ applications, services, and databases zones, role-based VLAN across both Albany and New York City offices, secure wireless networks, and a site-to-site VPN that provides an encrypted connection between both offices. By building multi-tier applications, identity management, centralized logging, and backup capabilities. The design supports both operational efficiency and foundational security.

Part 2 evaluated the environment against the PCI-DSS framework and showed that, despite the improved network infrastructure, the organization still faces gaps in policy enforcement, configuration patches, encryption, and vulnerability management. The audit found several security gaps between the company's IT design and how things operate day to day. Issues such as no penetration tests being performed, weak data retention policies, outdated incident response polices, and no third-party risk assessments. These findings demonstrate the need for stronger admin controls and continuous compliance monitoring.

Together, the network design and audit show that meeting compliance is not solely a matter of implementing technical controls, but it also requires continuous policy management, documentation, and monitoring. The recommendations provided in this report give HackIoT Lab practical steps to take to close its current compliance gaps and maintain a secure, auditable environment. By following these steps and aligning future operations with the security principles built into the network design, the organization can strengthen its defenses, reduce the risk of credit card information being exposed and move towards being compliant with PCI-DSS.

Reference List

IBM Security. (2025). Cost of a data breach report 2025. https://www.ibm.com/reports/data-breach

PCI Security Standards Council. (2024, October). *Self-assessment questionnaire D for merchants: PCI DSS version 4.0.1* [PDF]. https://docs-prv.pcisecuritystandards.org/SAQ%20(Assessment)/SAQ/PCI-DSS-v4-0-1-SAQ-D-Merchant.pdf

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

SANS Institute. (2021). *Critical security controls for effective cyber defense v8.* SANS Institute. https://www.sans.org/critical-security-controls/

National Institute of Standards and Technology (NIST). (2020). *Special Publication 800-53 Rev. 5: Security and privacy controls for information systems and organizations.* U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

Center for Internet Security. (n.d.). *The 18 CIS Critical Security Controls*. Retrieved November 7, 2025, from https://www.cisecurity.org/controls/cis-controls-list

Cybersecurity & Infrastructure Security Agency. (2022, January 24). *Layering network security through segmentation: Infographic* [Infographic]. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2023-01/layering-network-security-segmentation_infographic_508_0.pdf