

Compliance Within User, Workstation, and LAN Domains

Joshua Farias

March 30th, 2024



Introduction

Focus: Critical IT Domains

Goals: Enhance security, ensure compliance with COBIT and PCI-DSS, and prepare for audits confidently.

Outcome: A secure, compliant, and efficient IT infrastructure to support S&H Aquariums.

User

- UAM
- Awareness Training

Workstation

- Antivirus Software
- Patch Management

LAN

- Network Segmentation
- Firewalls and IDPS

LAN-to-WAN

- Virtual Private Networks (VPN)
- Encryption Protocols

WAN

- Encryption
- Firewalls and IDPS

Remote Access

- Encryption
- Multifactor Authentication
- Firewalls and IDPS

System/Application

- Version Control & Patch Management
- Antivirus Software
- Security Auditing

Compliance Frameworks

- COBIT
- PCI-DSS

User Domain

The User Domain encompasses all the users (employees, contractors, and customers) who access the organization's information system.

User Access Management: Implement strong authentication methods and periodic access reviews.

Awareness Training: Regular security awareness training for all users to mitigate security risks.

Compliance Implications: These controls help in establishing a security-aware culture, reducing the risk of data breaches, and meeting PCI-DSS Requirement 12.6 which mandates security awareness training and aligns with COBIT's DSS05 (Management Security Services).

Workstation Domain



The Workstation Domain includes all endpoints (desktops, laptops) used within the organization.



Antivirus Software: Ensure all workstations are protected by updated antivirus software.



Patch Management: Regularly update operating systems and applications.



Compliance Implications: Protects against malware and vulnerabilities, essential for PCI-DSS Requirement 5 (Protect all systems against malware) as well as COBIT's APO11 (Management Quality).

LAN Domain



The LAN Domain focuses on the organization's local area network, including switches, routers, and other networking equipment.



Network Segmentation: Separating sensitive system networks from the general network.




Firewalls and Intrusion Detection Systems (IDS): Implementing firewalls and IDS to monitor and control inbound and outbound traffic.




Compliance Implications: Essential for securing cardholder data environment, aligns with PCI-DSS Requirement 1 (Install and maintain a firewall configuration) as well as COBIT's DSS01 (Management Operations).

LAN-to-WAN Domain


The LAN-to-WAN Domain focuses on the organization's local area network, including switches, routers, and other networking equipment and the connectivity and security between our internal network (LAN) and external (WAN) networks.



Network Segmentation: Separating sensitive system networks from the general network.



Firewalls and Intrusion Detection Systems (IDS): Implementing firewalls and IDS to monitor and control inbound and outbound traffic.

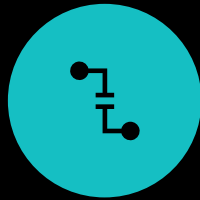


Compliance Implications: Essential for securing cardholder data environment, aligns with PCI-DSS Requirement 1 (Install and maintain a firewall configuration) as well as COBIT's DSS05 (Management Security Services).

WAN Domain



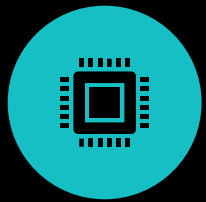
The WAN Domain focuses on networks that span a broad area, ensuring the secure transmission of data across different locations



Network Segmentation: Separating sensitive system networks from WAN connected networks is essential.



Encryption: Use encrypted protocols such as HTTPS on web servers that handle cardholder data. Encrypt stored cardholder data at rest.



Firewalls and Intrusion Detection Systems (IDS): Implementing firewalls and IDS to monitor and control inbound and outbound traffic.



Compliance Implications: Essential for securing cardholder data environment, aligns with PCI-DSS Requirement 4 (Encryption of cardholder data across open, public networks) as well as COBIT's MEA03 (Monitor, Evaluate, and Assess Compliance with External Requirements).

Remote Access Domain

The Remote Access Domain deals with policies and technologies that manage access to the network by users and devices outside of the physical and logical perimeters of the organization.

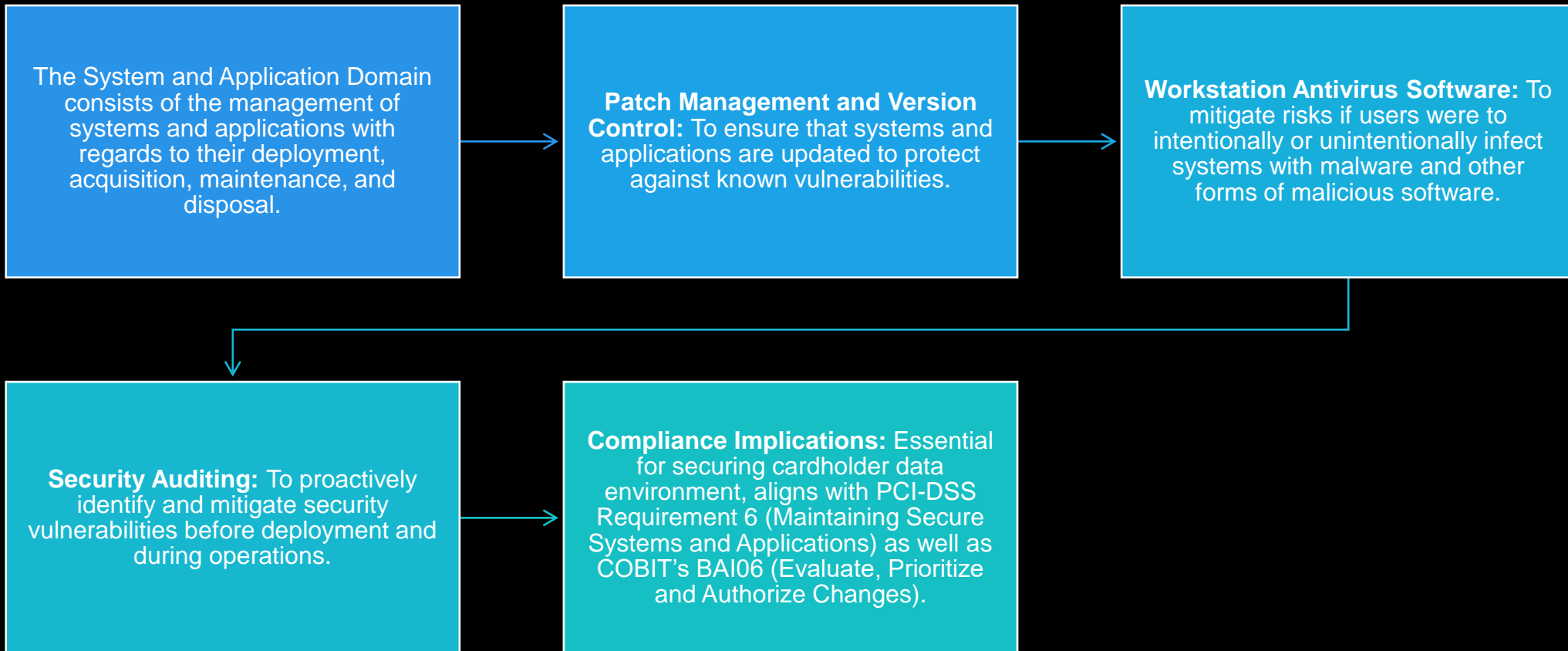
Virtual Private Network (VPN): Provide secure remote access to network resources via encrypted connections.

Multi-factor Authentication (MFA): To enhance security by requiring multiple forms of verification before granting access.

Firewalls and Intrusion Detection Systems (IDS): Implementing firewall rules to limit remote users only allowing access to what is needed for their daily work needs (principle of least privilege.) Implement an IDS to monitor VPN traffic.

Compliance Implications: Essential for securing cardholder data environment, aligns with PCI-DSS Requirement 8 (Implementing Identification and Authentication Mechanisms) as well as COBIT's DSS01 (Management Operations).

System/Application Domain



Implications for Compliance

- **User Domain Controls** strengthen our defense against unauthorized access and information leakage, directly supporting compliance with PCI-DSS Requirement 12 for information security policies.
- **Workstation Domain Controls** ensure the integrity and confidentiality of our data, crucial for meeting PCI-DSS Requirement 5 on protecting against malware.
- **LAN Domain Controls** secure our network infrastructure, addressing PCI-DSS Requirement 1 on installing and maintaining network security controls.
- **LAN-to-WAN Controls** secure our internal network infrastructure when connecting to external networks, addressing PCI-DSS Requirement 1 on maintaining network security controls and COBIT's DSS05 regarding the management of security services

Implications for Compliance Cont.

- **WAN Domain Controls** ensures the security of data transmitted over networks in various geographical locations aligning with PCI-DSS Requirement 4, which mandates encryption of cardholder data across open, public networks along with COBIT's MEA03 regarding the monitor, evaluate and assess compliance with external requirements.
- **Remote Access Domain Controls** ensures the security and authentication of users accessing company resources from external devices aligning with PCI-DSS Requirement 8, which mandates strong authentication methods along with COBIT's DSS01 (Manage Operations) for secure and reliable remote access solutions.

Implications for Compliance Cont.

- **System/Application Domain Controls** ensure the security of systems and applications from development through deployment and maintenance fulfilling PCI-DSS Requirement 6 regarding the development and maintenance of secure systems and applications.
- Each of these controls not only aims to safeguard our IT environment but also ensures our alignment with COBIT's framework for managing and governing enterprise IT and PCI DSS standards for securing credit card data.

References

- ISACA. (2019). *COBIT 2019 Framework: Introduction and Methodology*.
- Johnson , R., Weiss, M., & Solomon, M. G. (2022). Auditing IT infrastructures for Compliance. Jones & Bartlett Learning.
- PCI Security Standards Council. (n.d.). *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1*.