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

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.

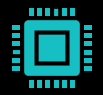
Patch Management: Regularly update operating systems and applications.

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).

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.

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*.