PCI Audit Program

Janco Associates, Inc.

2023

PCI Audit Program

Table of Contents

PCI Compliance Security Audit Program

Introduction

The PCI Security Audit Procedures[1] are designed for use by assessors conducting onsite reviews for merchants and service providers required to validate compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) requirements. The requirements and audit procedures presented in this document are based on the PCI DSS and the most recent set of privacy mandates – including GDPR.

This document contains the following:

- Introduction
- Policy – Sensitive Information
- Policy – Record Management, Retention, and Disposition
- PCI DSS Applicability Information
- The scope of Assessment for Compliance with PCI DSS Requirements
- Instructions and Content for *Report On Compliance*
- Revalidation of Open Items
- Security Audit Procedures
- Appendices
    - Appendix A: PCI DSS Applicability for Hosting Providers (with Testing Procedures)
    - Appendix B: Compensating Controls
    - Appendix C: Compensating Controls Worksheet/Completed Example

Wit d regulatory agencies, there are often
com this reason, we have provided "draft"
poli n Policy" and a "Record Management,
Rete

[1] Portions of this test program were extracted from the published PCI requirements and have been enhanced by Janco Associates, Inc. Note we are not attorneys and do not express any legal nor PCI standards opinion in this document. The use of this audit program should consult with their own legal and PCI compliance staff.

PCI DSS Applicability Information

The following table illustrates commonly used elements of the cardholder and sensitive authentication data; whether the storage of each data element is permitted or prohibited; and if each data element must be protected. This table is not exhaustive but is presented to illustrate the different types of requirements that apply to each data element. At the same time, compliance with Record Retention and Disposition standards (see https://e-janco.com/recordmanagementpolicy.html) needs to be coordinated with the PCI DSS requirements. A Sensitive Information policy (see https://e-janco.com/sensitive.htm) for the enterprise should be implemented.

	Data Element	***Storage Permitted***	***Protection Required***	***PCI DSS Requirement 3.4***
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	C			
	Se			
	Ex			
Sensitive Authentication Data**	Fu			
	CVC2/CVV2/CID	No	N/A	N/A
	Pin / Pin Block	No	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN (Primary Account Number). This protection must be consistent with PCI DSS requirements for the general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data or proper disclosure of a company's practices if consumer-related personal data is being collected during business operations. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored after authorization (even if encrypted).

The scope of Assessment for Compliance with PCI DSS Requirements

The PCI DSS security requirements apply to all “system components.” A system component is defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (internet) applications.

Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from the rest of the network, may reduce the scope of the cardholder data environment. The assessor must verify that the segmentation is adequate to reduce the scope of the audit.

anage components such as routers, firewalls, impact on the security of the cardholder data be scrutinized either in the:

compliance validation must be performed on all system components where cardholder data is stored, processed, or transmitted unless otherwise specified.

For merchants required to undergo an annual onsite review, the scope of compliance validation is focused on any system(s) or system component(s) related to authorization and settlement where cardholder data is stored, processed, or transmitted, including the following:

- All external connections into the merchant network (for example; employee remote access, payment card company, and third-party access for processing, and maintenance)
- All connections to and from the authorization and settlement environment (for example, connections for employee access or devices such as firewalls and routers)
- Any data repositories outside of the authorization and settlement environment where more than 500 thousand account numbers are stored. Note: Even if some data repositories or systems are excluded from the audit, the merchant is still responsible for ensuring that all systems that store, process, or transmit cardholder data are compliant with the PCI DSS
- A point-of-sale (POS) environment – the place where a transaction is accepted at a merchant location (that is, retail store, restaurant, hotel property, gas station, supermarket, or other POS location)
- If there is no external access to the merchant location (by the Internet, Wi-Fi, Bluetooth, a virtual private network (VPN), dial-in, broadband, or publicly accessible machines such as kiosks), the POS environment may be excluded.

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.1 Establish firewall configuration standards that include the following:	**1.1** Obtain and inspect the firewall configuration standards and other documentation specified below to verify that standards are complete.			
1.1.1 A formal process for approving and testing all exter network connections and char to the firewall configuration	formal ment approval on			
	ges to the firewall.			
	1.1.1c Verify logs are in place and are actively being monitored			
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify that a current network diagram exists and verify that it documents all connections to cardholder data, including any wireless networks			
	1.1.2.b. Verify that the diagram is kept current			

What's New

2023 Edition

- Update to meet the latest requirements
- Updated graphics
- Corrected errata

2022 Edition

- Update to meet the latest requirements
- Updated graphics

Version 3.1

- Updated to meet the latest privacy and security requirements

Version 3.0

- Update to meet the latest requirements
- Updated graphics