YourIT!
Your Logo Goes Here

PCI DSS - SAQ A-EP

Policies and Procedures

Prepared for:
Client Company
Prepared by:
YourIT Company

Table of Contents

Purpose

The intended audience for this SAQ includes e-commerce merchants that partially outsource their payment processing to PCI DSS-compliant TPSPs. This SAQ should be utilized when the merchant's website does not directly receive cardholder data but impacts the security of the payment transaction. It outlines unique compliance requirements, including the necessity for merchants to confirm TPSP compliance and to maintain secure configurations for their web servers. This SAQ is distinct from others as it specifically addresses the security implications of e-commerce environments without direct cardholder data handling.

Scope

This Self-Assessment Questionnaire (SAQ) A-EP applies to e-commerce merchants that do not store, process, or transmit cardholder data but affect the security of payment transactions through their websites. It encompasses all system components, personnel, and processes involved in the e-commerce payment channel, specifically focusing on the merchant's website and its interaction with third-party service providers (TPSPs). The SAQ requires merchants to confirm that their TPSPs are PCI DSS compliant and that the merchant's website does not directly handle cardholder data. Segmentation considerations must be in place to ensure compliance with applicable PCI DSS requirements.

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

Requirement 1 - Install and Maintain Network Security Controls

PCI DSS - SAQ A-EP Requirement 1 Install and Maintain Network Security Controls	Other Requirements N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.
1.2 Network security controls (NSCs) are configured and maintained.
1.3 Network access to and from the cardholder data environment is restricted.
1.4 Network connections between trusted and untrusted networks are controlled.
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

Guidance
Overview
Network security controls (NSCs), such as firewalls and other network security technologies, are network policy enforcement points that typically control network traffic between two or more logical or physical network segments (or subnets) based on pre-defined policies or rules.

NSCs examine all network traffic entering (ingress) and leaving (egress) a segment and decide, based on the policies defined, whether the network traffic is allowed to pass or whether it should be rejected. Typically, NSCs are placed between environments with different security needs or levels of trust, however in some environments NSCs control the traffic to individual devices irrespective of trust boundaries. Policy enforcement generally occurs at layer 3 of the OSI model, but data present in higher layers is also frequently used to determine policy decisions.

Traditionally this function has been provided by physical firewalls; however, now this functionality may be provided by virtual devices, cloud access controls, virtualization/container systems, and other software-defined networking technology.

NSCs are used to control traffic within an entity's own networks for example, between highly sensitive and less sensitive areas and also to protect the entity's resources from exposure to untrusted networks. The cardholder data environment (CDE) is an example of a more sensitive area within an entity's network. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into sensitive systems. NSCs provide a key protection mechanism for any computer network.

Common examples of untrusted networks include the Internet, dedicated connections such as business-to-business communication channels, wireless networks, carrier networks (such as cellular), third-party networks, and other sources outside the entity's ability to control. Furthermore, untrusted networks also include corporate networks that are considered out-of-scope for PCI DSS, because they are not assessed, and therefore must be treated as untrusted because the existence of security controls has not been verified. While an entity may consider an internal network to be trusted from an infrastructure perspective, if a network is out of scope for PCI DSS, that network must be considered untrusted for PCI DSS.

Refer to Appendix G for definitions of PCI DSS terms.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- PCI-1.1.1 - Requirement 1.1.1:
  Processes and mechanisms for installing and maintaining network security controls are defined and understood.

  1.1.1 All security policies and operational procedures that are identified in Requirement 1 are:
  • Documented.
  • Kept up to date.
  • In use.
  • Known to all affected parties.

  Procedure
  - Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 1 are managed in accordance with all elements specified in this requirement.

- PCI-1.2.1 - Requirement 1.2.1:
  Network security controls (NSCs) are configured and maintained.

  1.2.1 Configuration standards for NSC rulesets are:
  • Defined.
  • Implemented.
  • Maintained.

  Procedure
  - Examine the configuration standards for NSC rulesets to verify the standards are in accordance with all elements specified in this requirement.
  - Examine configuration settings for NSC rulesets to verify that rulesets are implemented according to the configuration standards.

- PCI-1.2.2-v4.0.1 - Requirement 1.2.2:
  Network security controls (NSCs) are configured and maintained.

  1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.

  Procedure
  - Examine documented procedures to verify that changes to network connections and configurations of NSCs are included in the formal change control process in accordance with Requirement 6.5.1.
  - Examine network configuration settings to identify changes made to network connections. Interview responsible personnel and examine change control records to verify that identified changes to network connections were approved and managed in accordance with Requirement 6.5.1.
  - Examine network configuration settings to identify changes made to configurations of NSCs. Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1.

- PCI-1.2.3 - Requirement 1.2.3:
  Network security controls (NSCs) are configured and maintained.

  1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.

  Procedure
  - Examine diagram(s) and network configurations to verify that an accurate network diagram(s) exists in accordance with all elements specified in this requirement.
  - Examine documentation and interview responsible personnel to verify that the network diagram(s) is accurate and updated when there are changes to the environment.

- PCI-1.2.4 - Requirement 1.2.4:
  Network security controls (NSCs) are configured and maintained.

  1.2.4 An accurate data-flow diagram(s) is maintained that meets the following:
  • Shows all account data flows across systems and networks.
  • Updated as needed upon changes to the environment.

  Procedure
  - Examine data-flow diagram(s) and interview personnel to verify the diagram(s) show all account data flows in accordance with all elements specified in this requirement.
  - Examine documentation and interview responsible personnel to verify that the data-flow diagram(s) is accurate and updated when there are changes to the environment.

- PCI-1.2.5 - Requirement 1.2.5:
  Network security controls (NSCs) are configured and maintained.

  1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need.

  Procedure
  - Examine documentation to verify that a list exists of all allowed services, protocols, and ports, including business justification and approval for each.
  - Examine configuration settings for NSCs to verify that only approved services, protocols, and ports are in use.

- PCI-1.2.6 - Requirement 1.2.6:
  Network security controls (NSCs) are configured and maintained.

  1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.

  Procedure
  - Examine documentation that identifies all insecure services, protocols, and ports in use to verify that for each, security features are defined to mitigate the risk.
  - Examine configuration settings for NSCs to verify that the defined security features are implemented for each identified insecure service, protocol, and port.

- PCI-1.2.7 - Requirement 1.2.7:
  Network security controls (NSCs) are configured and maintained.

  1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.

Procedure
- Examine documentation to verify procedures are defined for reviewing configurations of NSCs at least once every six months.
- Examine documentation of reviews of configurations for NSCs and interview responsible personnel to verify that reviews occur at least once every six months.
- Examine configurations for NSCs to verify that configurations identified as no longer being supported by a business justification are removed or updated.

- PCI-1.2.8 - Requirement 1.2.8:
  Network security controls (NSCs) are configured and maintained.

  1.2.8 Configuration files for NSCs are:
  • Secured from unauthorized access.
  • Kept consistent with active network configurations.

  Procedure
  - Examine configuration files for NSCs to verify they are in accordance with all elements specified in this requirement.

- PCI-1.3.1 - Requirement 1.3.1:
  Network access to and from the cardholder data environment is restricted.

  1.3.1 Inbound traffic to the CDE is restricted as follows:
  • To only traffic that is necessary.
  • All other traffic is specifically denied.

  Procedure
  - Examine configuration standards for NSCs to verify that they define restricting inbound traffic to the CDE is in accordance with all elements specified in this requirement.
  - Examine configurations of NSCs to verify that inbound traffic to the CDE is restricted in accordance with all elements specified in this requirement.

- PCI-1.3.2 - Requirement 1.3.2:
  Network access to and from the cardholder data environment is restricted.

  1.3.2 Outbound traffic from the CDE is restricted as follows:
  • To only traffic that is necessary.
  • All other traffic is specifically denied.

  Procedure
  - Examine configuration standards for NSCs to verify that they define restricting outbound traffic from the CDE in accordance with all elements specified in this requirement.
  - Examine configurations of NSCs to verify that outbound traffic from the CDE is restricted in accordance with all elements specified in this requirement.

- PCI-1.3.3 - Requirement 1.3.3:
  Network access to and from the cardholder data environment is restricted.

  1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that:
  • All wireless traffic from wireless networks into the CDE is denied by default.
  • Only wireless traffic with an authorized business purpose is allowed into the CDE.

  Procedure

- Examine configuration settings and network diagrams to verify that NSCs are implemented between all wireless networks and the CDE, in accordance with all elements specified in this requirement.

- PCI-1.4.1 - Requirement 1.4.1:
  Network connections between trusted and untrusted networks are controlled.

  1.4.1 NSCs are implemented between trusted and untrusted networks.

  Procedure
  - Examine configuration standards and network diagrams to verify that NSCs are defined between trusted and untrusted networks.
  - Examine network configurations to verify that NSCs are in place between trusted and untrusted networks, in accordance with the documented configuration standards and network diagrams.

- PCI-1.4.2 - Requirement 1.4.2:
  Network connections between trusted and untrusted networks are controlled.

  1.4.2 Examine vendor documentation and configurations of NSCs to verify that inbound traffic from untrusted networks to trusted networks is restricted in accordance with all elements specified in this requirement.

  Procedure
  - Examine vendor documentation and configurations of NSCs to verify that inbound traffic from untrusted networks to trusted networks is restricted in accordance with all elements specified in this requirement.

- PCI-1.4.3 - Requirement 1.4.3:
  Network connections between trusted and untrusted networks are controlled.

  1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.

  Procedure
  - Examine vendor documentation and configurations for NSCs to verify that anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.

- PCI-1.4.4 - Requirement 1.4.4:
  Network connections between trusted and untrusted networks are controlled.

  1.4.4 System components that store cardholder data are not directly accessible from untrusted networks.

  Procedure
  - Examine the data-flow diagram and network diagram to verify that it is documented that system components storing cardholder data are not directly accessible from the untrusted networks.
  - Examine configurations of NSCs to verify that controls are implemented such that system components storing cardholder data are not directly accessible from untrusted networks.

- PCI-1.4.5 - Requirement 1.4.5:
  Network connections between trusted and untrusted networks are controlled.

1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties.

Procedure
- Examine configurations of NSCs to verify that the disclosure of internal IP addresses and routing information is limited to only authorized parties.
- Interview personnel and examine documentation to verify that controls are implemented such that any disclosure of internal IP addresses and routing information is limited to only authorized parties.

- PCI-1.5.1 - Requirement 1.5.1:
  Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

  1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows:
  • Specific configuration settings are defined to prevent threats being introduced into the entity's network.
  • Security controls are actively running.
  • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.

  Procedure
  - Examine policies and configuration standards and interview personnel to verify security controls for computing devices that connect to both untrusted networks, and the CDE, are implemented in accordance with all elements specified in this requirement.
  - Examine configuration settings on computing devices that connect to both untrusted networks and the CDE to verify settings are implemented in accordance with all elements specified in this requirement.

References
- PCI Security Standards Council Document Library - https://www.pcisecuritystandards.org/document_library/
- PCI Security Standards Council - https://www.pcisecuritystandards.org/
- PCI DSS v4.0 At a Glance - https://www.pcisecuritystandards.org/document_library?category=pcidss&document=dss4aag
- PCI DSS Requirements & Testing Procedure - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

Requirement 2 - Apply Secure Configurations to All System Components

PCI DSS - SAQ A-EP	Other Requirements
Requirement 2 Apply Secure Configurations to All System Components	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.
2.2 System components are configured and managed securely.

Guidance
Overview
Malicious individuals, both external and internal to an entity, often use default passwords and other vendor default settings to compromise systems. These passwords and settings are well known and are easily determined via public information.

Applying secure configurations to system components reduces the means available to an attacker to compromise the system. Changing default passwords, removing unnecessary software, functions, and accounts, and disabling or removing unnecessary services all help to reduce the potential attack surface.

Refer to Appendix G for definitions of PCI DSS terms.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- PCI-2.1.1 - Requirement 2.1.1:
  Processes and mechanisms for applying secure configurations to all system components are defined and understood.

  2.1.1 All security policies and operational procedures that are identified in Requirement 2 are:
  • Documented.
  • Kept up to date.
  • In use.
  • Known to all affected parties.

  Procedure
  - Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 2 are managed in accordance with all elements specified in this requirement.

- PCI-2.2.1 - Requirement 2.2.1:
  System components are configured and managed securely.

  2.2.1 Configuration standards are developed, implemented, and maintained to:

• Cover all system components.
• Address all known security vulnerabilities.
• Be consistent with industry-accepted system hardening standards or vendor hardening recommendations.
• Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1.
• Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.

Procedure

- Examine system configuration standards to verify they define processes that include all elements specified in this requirement.
- Examine policies and procedures and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.3.1
- Examine configuration settings and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before or immediately after a system component is connected to a production environment.

- PCI-2.2.2 - Requirement 2.2.2:
  System components are configured and managed securely.

  2.2.2 Vendor default accounts are managed as follows:
  • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6.
  • If the vendor default account(s) will not be used, the account is removed or disabled.

  Procedure
  - Examine system configuration standards to verify they include managing vendor default accounts in accordance with all elements specified in this requirement.
  - Examine vendor documentation and observe a system administrator logging on using vendor default accounts to verify accounts are implemented in accordance with all elements specified in this requirement.
  - Examine configuration files and interview personnel to verify that all vendor default accounts that will not be used are removed or disabled.

- PCI-2.2.3 - Requirement 2.2.3:
  System components are configured and managed securely.

  2.2.3 Primary functions requiring different security levels are managed as follows:
  • Only one primary function exists on a system component,
  OR
  • Primary functions with differing security levels that exist on the same system component are isolated from each other,
  OR
  • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.

  Procedure
  - Examine system configuration standards to verify they include managing primary functions requiring different security levels as specified in this requirement.
  - Examine system configurations to verify that primary functions requiring different security levels are managed per one of the ways specified in this requirement.
  - Where virtualization technologies are used, examine the system configurations to verify that system functions requiring different security levels are managed in one of the

following ways: • Functions with differing security needs do not co-exist on the same system component. • Functions with differing security needs that exist on the same system component are isolated from each other. • Functions with differing security needs on the same system component are all secured to the level required by the function with the highest security need.

- PCI-2.2.4 - Requirement 2.2.4:
  System components are configured and managed securely.

  2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.

  Procedure
  - Examine system configuration standards to verify necessary system services, protocols, and daemons are identified and documented.
  - Examine system configurations to verify the following: • All unnecessary functionality is removed or disabled. • Only required functionality, as documented in the configuration standards, is enabled

- PCI-2.2.5 - Requirement 2.2.5:
  System components are configured and managed securely.

  2.2.5 If any insecure services, protocols, or daemons are present:
  • Business justification is documented.
  • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.

  Procedure
  - If any insecure services, protocols, or daemons are present, examine system configuration standards and interview personnel to verify they are managed and implemented in accordance with all elements specified in this requirement.
  - If any insecure services, protocols, or daemons, are present, examine configuration settings to verify that additional security features are implemented to reduce the risk of using insecure services, daemons, and protocols.

- PCI-2.2.6 - Requirement 2.2.6:
  System components are configured and managed securely.

  2.2.6 System security parameters are configured to prevent misuse.

  Procedure
  - Examine system configuration standards to verify they include configuring system security parameters to prevent misuse.
  - Interview system administrators and/or security managers to verify they have knowledge of common security parameter settings for system components.
  - Examine system configurations to verify that common security parameters are set appropriately and in accordance with the system configuration standards.

- PCI-2.2.7 - Requirement 2.2.7:
  System components are configured and managed securely.

  2.2.7 All non-console administrative access is encrypted using strong cryptography.

  Procedure

- Examine system configuration standards to verify they include encrypting all non-console administrative access using strong cryptography.
- Observe an administrator log on to system components and examine system configurations to verify that non-console administrative access is managed in accordance with this requirement.
- Examine settings for system components and authentication services to verify that insecure remote login services are not available for non-console administrative access.

References

- PCI Security Standards Council Document Library - https://www.pcisecuritystandards.org/document_library/
- PCI Security Standards Council - https://www.pcisecuritystandards.org/
- PCI DSS v4.0 At a Glance - https://www.pcisecuritystandards.org/document_library?category=pcidss&document=dss4aag
- PCI DSS Requirements & Testing Procedure - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

Truncated Sample Document