YourIT!
Your Logo Goes Here

PCI DSS - SAQ A

Policies and Procedures

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for:
Client Company
Prepared by:
YourIT Company

Table of Contents

Purpose

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance payment card account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. While specifically designed to focus on environments with payment card account data, PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem.

Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Account Data

Cardholder Data includes:

- Primary Account Number (PAN)
- Cardholder Name
- Expiration Date
- Service Code

Sensitive Authentication Data includes:

- Full track data (magnetic-stripe data or equivalent on a chip)
- Card verification code
- PINs/PIN blocks

Scope

SAQ A APPLICABILITY
Self-Assessment Questionnaire (SAQ) A includes only those PCI DSS requirements applicable to merchants with account data functions completely outsourced to PCI DSS validated and compliant third parties, where the merchant retains only paper reports or receipts with account data.

SAQ A merchants may be either e-commerce or mail/telephone-order merchants (card-not-present) and do not store, process, or transmit any account data in electronic format on their systems or premises.

This SAQ is not applicable to face-to-face channels.

This SAQ is not applicable to service providers.

SAQ A merchants confirm that, for this payment channel:

* The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions;

* All processing of account data is entirely outsourced to PCI DSS compliant third-party service provider (TPSP)/payment processor;

* The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions;

* The merchant has reviewed the PCI DSS Attestation of Compliance form(s) for its TPSP(s) and confirmed that TPSP(s) are PCI DSS compliant for the services being used by the merchant; and

* Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Additionally, for e-commerce channels:

* All elements of the payment page(s)/form(s) delivered to the customer's browser originate only and directly from a PCI DSS compliant TPSP/payment processor.

This SAQ includes only those requirements that apply to a specific type of merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to the cardholder data environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for the merchant's environment.

Note: For this SAQ, PCI DSS Requirements that address the protection of computer systems (for example, Requirements 2, 6, and 8) apply to e-commerce merchants that redirect customers from their website to a third party for payment processing, and specifically to the merchant web server upon which the redirection mechanism is located. Mail order/telephone order (MOTO) or e-commerce merchants that have completely outsourced all operations (where there is no redirection mechanism from the merchant to the third party) and therefore do not have any systems in scope for this SAQ, would consider these requirements to be "not applicable." Refer to guidance on the following pages for how to report requirements that are not applicable.

For SAQ A and e-commerce channels, PCI DSS requirements that refer to the "cardholder data environment" are applicable to the merchant website(s) that provides the address (the URL) of the TPSP's payment page/form to merchant customers. This is because the merchant website impacts how the account data is transmitted, even though the website itself does not receive account data.

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.

PCI DSS 2.2 - System components are configured and managed securely.

PCI DSS - SAQ A 2.2 System components are configured and managed securely.	Other Requirements N/A

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

Configure all system components securely and consistently and in accordance with industry- accepted hardening standards or vendor recommendations.

Guidance
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.

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

Related Internal Controls

- PCIDSS-3 - Configuration and Maintenance: Configuration standards for Network Security Controls rulesets are: • Defined. • Implemented. • Maintained. Customized Approach Objective The way that Network Security Controls are configured and operate are defined and consistently applied.

References

- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 2.2.2 - Vendor Default Accounts

PCI DSS - SAQ A 2.2.2 Vendor Default Accounts	**Other Requirements** N/A

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

Defined Approach Requirements

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.

Customized Approach Objective

System components cannot be accessed using default passwords.

Applicability Notes

This applies to ALL vendor default accounts and passwords, including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, and Simple Network Management Protocol (SNMP) defaults.

This requirement also applies where a system component is not installed within an entity's environment, for example, software and applications that are part of the CDE and are accessed via a cloud subscription service.

Guidance
Purpose

Malicious individuals often use vendor default account names and passwords to compromise operating systems, applications, and the systems on which they are installed. Because these default settings are often published and are well known, changing these settings will make systems less vulnerable to attack.

Good Practice

All vendor default accounts should be identified, and their purpose and use understood. It is important to establish controls for application and system accounts, including those used to deploy and maintain cloud services so that they do not use default passwords and are not usable by unauthorized individuals.

Where a default account is not intended to be used, changing the default password to a unique password that meets PCI DSS Requirement 8.3.6, removing any access to the default account, and then disabling the account, will prevent a malicious individual from re-enabling the account and gaining access with the default password.

Using an isolated staging network to install and configure new systems is recommended and can also be used to confirm that default credentials have not been introduced into production environments.

Examples

Defaults to be considered include user IDs, passwords, and other authentication credentials commonly used by vendors in their products.

Defined Approach Testing Procedures

2.2.2.a Examine system configuration standards to verify they include managing vendor default accounts in accordance with all elements specified in this requirement.

2.2.2.b 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.

2.2.2.c Examine configuration files and interview personnel to verify that all vendor default accounts that will not be used are removed or disabled.

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

Related Internal Controls

- PCIDSS-22 - Vendor Default Accounts: Manage vendor default accounts as follows: • If the vendor default account(as) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(as) will not be used, the account is removed or disabled. This applies to ALL vendor default accounts and passwords, including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, and Simple Network Management Protocol (SNMP) defaults. This requirement also applies where and system component is not installed within and entity's environment, for example, software and applications that are part of the Cardholder Data Environment and are accessed via and cloud subscription service.

References

- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 3.1 - Protecting Stored Account Data

PCI DSS - SAQ A	**Other Requirements**
3.1 Protecting Stored Account Data	N/A

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

Processes and mechanisms for protecting stored account data are defined and understood.

Guidance
Protection methods such as encryption, truncation, masking, and hashing are critical components of account data protection. If an intruder circumvents other security controls and gains access to encrypted account data, the data is unreadable without the proper cryptographic keys and is unusable to that intruder. Other effective methods of protecting stored data should also be considered as potential risk-mitigation opportunities. For example, methods for minimizing risk include not storing account data unless necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies such as e-mail and instant messaging.

If account data is present in non-persistent memory (for example, RAM, volatile memory), encryption of account data is not required. However, proper controls must be in place to ensure that memory maintains a non-persistent state. Data should be removed from volatile memory once the business purpose (for example, the associated transaction) is complete. In the case that data storage becomes persistent, all applicable PCI DSS Requirements will apply including encryption of stored data.

Requirement 3 applies to protection of stored account data unless specifically called out in an individual requirement.

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

Related Internal Controls

- PCIDSS-30 - Protect Stored Account Data:

References

- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 3.1.1 - Data Protection Policies and Procedures

PCI DSS - SAQ A	**Other Requirements**
3.1.1 Data Protection Policies and Procedures	N/A

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

Defined Approach Requirements

All security policies and operational procedures that are identified in Requirement 3 are:
- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

Customized Approach Objective

Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management’s intent.

Guidance
Purpose Requirement 3.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 3. While it is important to define the specific policies or procedures called out in Requirement 3, it is equally important to ensure they are properly documented, maintained, and disseminated.

Good Practice

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle.

Definitions

Security policies define the entity’s security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

Defined Approach Testing Procedures

3.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 3 are managed in accordance with all elements specified in this requirement.

SAQ Completion Guidance:

Selection of any of the In Place responses for Requirement 3.1.1 means that, if the merchant has paper storage of account data, the merchant has policies and procedures in place that govern merchant activities for Requirement 3. This helps to ensure personnel are aware of and following security policies and documented operational procedures for managing the secure storage of any paper records with account data.

If merchant does not store paper records with account data, mark this requirement as Not Applicable and complete Appendix D: Explanation of Requirements Noted as Not Applicable.

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

Related Internal Controls

- PCIDSS-1 - Policies and procedures: All security policies and operational procedures that are identified in each PCI-DSS Requirement are: • Documented. • Kept up to date. • In use. • Known to all affected parties. Customized Approach Objective Expectations, controls, and oversight for meeting activities within each Requirement are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.

References

- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 3.2 - Minimum Data Storage

PCI DSS - SAQ A	Other Requirements
3.2 Minimum Data Storage	N/A

Policy

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

Storage of account data is kept to a minimum.

Guidance

To define appropriate retention requirements, an entity first needs to understand its own business needs as well as any legal or regulatory obligations that apply to its industry or to the type of data being retained. Implementing an automated process to ensure data is automatically and securely deleted upon its defined retention limit can help ensure that account data is not retained beyond what is necessary for business, legal, or regulatory purposes.

Responsibilities

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

Related Internal Controls

- PCIDSS-31 - Account Data Storage: Account data storage is kept to and minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for and sensitive authentication data stored prior to completion of authorization. • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes and documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.

References

- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 3.2.1 - Account Data Storage

PCI DSS - SAQ A 3.2.1 Account Data Storage	Other Requirements N/A

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

Defined Approach Requirements

Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following:
• Coverage for all locations of stored account data.
• Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization.

This bullet is a best practice until its effective date; refer to Applicability Notes below for details.

• Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements.
• Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.
• Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.
• A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.

Customized Approach Objective

Account data is retained only where necessary and for the least amount of time needed and is securely deleted or rendered unrecoverable when no longer needed.

Applicability Notes

Where account data is stored by a TPSP (for example, in a cloud environment), entities are responsible for working with their service providers to understand how the TPSP meets this requirement for the entity. Considerations include ensuring that all geographic instances of a data element are securely deleted.

The bullet above (for coverage of SAD stored prior to completion of authorization) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.

Guidance
Purpose

A formal data retention policy identifies what data needs to be retained, for how long, and where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed. The only account data that may be stored after authorization is the primary account number or PAN (rendered unreadable), expiration date, cardholder name, and service code.

The storage of SAD data prior to the completion of the authorization process is also included in the data retention and disposal policy so that storage of this sensitive data is kept to minimum, and only retained for the defined amount of time.

Good Practice

When identifying locations of stored account data, consider all processes and personnel with access to the data, as data could have been moved and stored in different locations than originally defined. Storage locations that are often overlooked include backup and archive systems, removable data storage devices, paper-based media, and audio recordings.

To define appropriate retention requirements, an entity first needs to understand its own business needs as well as any legal or regulatory obligations that apply to its industry or to the type of data being retained. Implementing an automated process to ensure data is automatically and securely deleted upon its defined retention limit can help ensure that account data is not retained beyond what is necessary for business, legal, or regulatory purposes.

Methods of eliminating data when it exceeds the retention period include secure deletion to complete removal of the data or rendering it unrecoverable and unable to be reconstructed. Identifying and securely eliminating stored data that has exceeded its specified retention period prevents unnecessary retention of data that is no longer needed. This process may be automated, manual, or a combination of both.

The deletion function in most operating systems is not “secure deletion” as it allows deleted data to be recovered, so instead, a dedicated secure deletion function or application must be used to make data unrecoverable.

Remember, if you don't need it, don't store it!

Examples

An automated, programmatic procedure could be run to locate and remove data, or a manual review of data storage areas could be performed. Whichever method is used, it is a good idea to monitor the process to ensure it is completed successfully, and that the results are recorded and validated as being complete. Implementing secure deletion methods ensures that the data cannot be retrieved when it is no longer needed.

Further Information
See NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization.

Defined Approach Testing Procedures

3.2.1.a Examine the data retention and disposal policies, procedures, and processes and interview personnel to verify processes are defined to include all elements specified in this requirement.

3.2.1.b Examine files and system records on system components where account data is stored to verify that the data storage amount and retention time does not exceed the requirements defined in the data retention policy.

3.2.1.c Observe the mechanisms used to render account data unrecoverable to verify data cannot be recovered.

SAQ Completion Guidance:

Selection of any of the In Place responses for Requirement 3.2.1 means that if a merchant stores any paper (for example, receipts or paper reports) that contain account data, the merchant only stores the paper as long as it is needed for business, legal, and/or regulatory reasons and destroys the paper once it is no longer needed.

If a merchant never prints or stores any paper containing account data, mark this requirement as Not Applicable and complete Appendix D: Explanation of Requirements Noted as Not Applicable.

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

Related Internal Controls

- PCIDSS-31 - Account Data Storage: Account data storage is kept to and minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for and sensitive authentication data stored prior to completion of authorization. • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes and documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.

References

- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 6.3 - Security Vulnerabilities

PCI DSS - SAQ A 6.3 Security Vulnerabilities	**Other Requirements** N/A

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

Security vulnerabilities are identified and addressed.

Guidance
Actors with bad intentions can use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which must be installed by the entities that manage the systems. All system components must have all appropriate software patches to protect against the exploitation and compromise of account data by malicious individuals and malicious software.

Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For bespoke and custom software, numerous vulnerabilities can be avoided by applying software lifecycle (SLC) processes and secure coding techniques.

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

Related Internal Controls

- PCIDSS-77 - Security Vulnerability Management: Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned and risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at and minimum, all vulnerabilities considered to be and high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

References

- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 6.3.1 - Security Vulnerability Management

PCI DSS - SAQ A 6.3.1 Security Vulnerability Management	**Other Requirements** N/A

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

Defined Approach Requirements

Security vulnerabilities are identified and managed as follows:
• New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
• Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
• Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
• Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

Customized Approach Objective

New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.

Applicability Notes

This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.

Guidance
Purpose

Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.

Good Practice

Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk-assessment strategy.

When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution.

An organization’s processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.

Examples

Some organizations that issue alerts to advise entities about urgent vulnerabilities requiring immediate patches/updates are national Computer Emergency Readiness/Response Teams (CERTs) and vendors.

Criteria for ranking vulnerabilities may include criticality of a vulnerability identified in an alert from Forum of Incident Response and Security Teams (FIRST) or a CERT, consideration of the CVSS score, the classification by the vendor, and/or type of systems affected.

Further Information

Trustworthy sources for vulnerability information include vendor websites, industry newsgroups, mailing lists, etc. If software is developed in- house, the internal development team should also consider sources of information about new vulnerabilities that may affect internally developed applications. Other methods to ensure new vulnerabilities are identified include solutions that automatically recognize and alert upon detection of unusual behavior. Processes should account for widely published exploits as well as “zero-day” attacks, which target previously unknown vulnerabilities.

For bespoke and custom software, the organization may obtain information about libraries, frameworks, compilers, programming languages, etc. from public trusted sources (for example, special resources and resources from component developers). The organization may also independently analyze third-party components and identify vulnerabilities.

For control over in-house developed software, the organization may receive such information from external sources. The organization can consider using a “bug bounty” program where it posts information (for example, on its website) so third parties can contact the organization with vulnerability information. External sources may include independent investigators or companies that report to the organization about identified vulnerabilities and may include sources such as the Common Vulnerability Scoring System (CVSS) or the OWASP Risk Rating Methodology.

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

Related Internal Controls

- PCIDSS-77 - Security Vulnerability Management: Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned and risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at and minimum, all vulnerabilities considered to be and high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

References

- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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 6.3.3 - Security Patches and Updates

PCI DSS - SAQ A 6.3.3 Security Patches and Updates	**Other Requirements** N/A

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

Defined Approach Requirements

All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

• Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.

• All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).

Customized Approach Objective

System components cannot be compromised via the exploitation of a known vulnerability.

Guidance
Purpose

New exploits are constantly being discovered, and these can permit attacks against systems that have previously been considered secure. If the most recent security patches/updates are not implemented on critical systems as soon as possible, a malicious actor can use these exploits to attack or disable a system or gain access to sensitive data.

Good Practice

Prioritizing security patches/updates for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released.

An entity's patching cadence should factor in any re-evaluation of vulnerabilities and subsequent changes in the criticality of a vulnerability per Requirement 6.3.1. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities individually considered to be low or medium risk could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.

Defined Approach Testing Procedures

6.3.3.a Examine policies and procedures to verify processes are defined for addressing vulnerabilities by installing applicable security patches/updates in accordance with all elements specified in this requirement.

6.3.3.b Examine system components and related software and compare the list of installed security patches/updates to the most recent security patch/update information to verify vulnerabilities are addressed in accordance with all elements specified in this requirement.

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

Related Internal Controls

- PCIDSS-79 - Security Patches and Updates: All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within and appropriate time frame as determined by the entity (for example, within three months of release).

References

- PCI DSS Requirements & Testing Procedure - https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1655305034600
- 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

Truncated Sample Report