

PCI SSC — Complete FAQ Collection

All 284 frequently asked questions from the PCI Security Standards Council.

Source: <https://www.pcisecuritystandards.org/faqs/all/>

Compiled 23 June 2026

Where is the PCI Security Standards Council Located

Article 1003 | April 2012

The address for the PCI Security Standards Council is:

PCI Security Standards Council, LLC

401 Edgewater Place, Suite 600

Wakefield, MA 01880

Does the PCI Security Standards Council enforce compliance?

Article 1004 | April 2012

No, the PCI Security Standards Council will not be replacing the individual brands' compliance programs. The individual participating payment brands will separately determine what entities must be compliant, including any brand-specific enforcement programs.

In case of a suspected breach, should the PCI Security Standards Council be contacted directly?

Article 1009 | April 2012

No. In the event of a suspected account security breach, the business entity should follow existing, brand-specific processes and procedures for notifying the affected payment brand(s) and law enforcement officials.

Once my business has been determined to be compliant by a QSA, would I or the QSA need to communicate this fact to the PCI Security Standards Council?

Article 1011 | April 2012

No. The PCI Security Standards Council is not a compliance organization. Each brand maintains its own compliance programs.

Do QSAs and ASVs need to send reports of compliance (ROCs) or scanning results to the PCI Security Standards Council directly?

Article 1014 | April 2012

No. QSAs and ASVs do not send reports of compliance or scanning results to the PCI Security Standards Council, and they should continue to follow the payment brand specific procedures.

What are the consequences to my business if I do not comply with the PCI DSS?

Article 1015 | April 2012

The PCI Security Standards Council encourages all businesses that store payment account data to comply with the PCI DSS to help lower their brand and financial risks associated with account payment data compromises. The PCI Security Standards Council does not manage compliance programs and does not impose any consequences for non-compliance. Individual payment brands, however, may have their own compliance initiatives, including financial or operational consequences to certain businesses that are not compliant.

How can my organization find assistance in completing the Self-Assessment Questionnaire?

Article 1017 | December 2022

The Council encourages organizations to seek professional guidance in achieving compliance and completing the Self-Assessment Questionnaire. Entities can use any security professional they choose; however, PCI SSC recommends engaging a Qualified Security Assessor (QSA) that are trained to provide assessments against the PCI DSS. For a list of QSAs, please visit: https://listings.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

If my business was deemed compliant but my system was still breached and payment account data compromised after the fact, what liability would my business incur?

Article 1019 | April 2012

The PCI Security Standards Council is not responsible for levying any financial or operational consequences on businesses that have either been breached or are suspected of an account data compromise. These businesses should contact the individual payment brands regarding next steps, such as contacting law enforcement, or obtaining other relevant information, including potential consequences should a compromise have occurred.

Do small merchants with limited transaction volumes need comply with PCI DSS?

Article 1022 | July 2015

PCI DSS is intended for all entities involved in payment processing, including merchants, regardless of their size or transaction volume. When compared with larger merchants, small merchants often have simpler environments, with limited amounts of cardholder data and fewer systems that need protecting, which can help reduce their PCI DSS compliance effort.

Whether a small merchant is required to validate compliance is determined by the individual payment brands. For questions regarding compliance validation and reporting requirements, merchants should contact their acquirer (merchant bank) or payment brand they do business with, as applicable.

What are the requirements that have to be satisfied to be in compliance with the PCI Data Security Standard?

Article 1023 | April 2012

The PCI Data Security Standard is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. The PCI Data Security Standard is comprised of 12 general requirements designed to: Build and maintain a secure network; Protect cardholder data; Ensure the maintenance of vulnerability management programs; Implement strong access control measures; Regularly monitor and test networks; and Ensure the maintenance of information security policies.

Is PCI DSS a global standard?

Article 1024 | April 2012

The PCI DSS is a global standard, with compliance expected of any entity that stores, processes or transmit cardholder data regardless of geographic location. Each payment brand manages their PCI DSS compliance and enforcement programs independently of the PCI Security Standards Council. With regard to levels, time lines, and other specific questions about compliance and enforcement, please contact each payment brand to understand programs in the regions in which the company operates.

What are system-level objects?

Article 1034 | December 2022

A system-level object is anything on a computer system required for its operation, including but not limited to application executables and configuration files, system configuration files, static and shared libraries and DLLs, system executables, device drivers and device configuration files, and third-party components.

Refer to the definition of "system-level objects" in the applicable glossary for the version of the standard being used.

How can I provide feedback (negative or positive) about my QSA/ASV?

Article 1036 | April 2012

Merchants or service providers are encouraged to submit feedback about their QSA/ASV through the feedback form available on our website at https://www.pcisecuritystandards.org/program-listings-overview/give_assessor_feedback/. QSAs and ASVs are contractually obligated to provide feedback forms to all of their clients upon completion of services. These completed forms should be submitted directly to the Council at qsa@pcisecuritystandards.org or asv@pcisecuritystandards.org. The PCI Security Standards Council will consider all feedback regarding QSAs/ASVs and will address issues as needed on an individual basis.

Do hosting providers have responsibility for liabilities/fines?

Article 1037 | April 2012

Questions about compliance and possible fines due to a compromise should be addressed directly to the payment card brands and/or acquirers.

Does PCI DSS apply to "hot cards," expired, cancelled or invalid payment account numbers?

Article 1038 | December 2022

PCI DSS applies to any primary account number (PAN), including active, expired, or cancelled PAN, except where the organization can provide documentation which confirms that the PAN is inactive or otherwise disabled and no longer poses a fraud risk to the payment system. However, if the PAN is later reactivated, PCI DSS will again apply.

When payment account numbers expire, the same account number is often reused on the new card with a different expiry date. The PAN must therefore be verified as not being valid before expired payment account numbers are excluded from PCI DSS scope.

Entities should retain PAN based on business/legal needs, as defined in their data retention policy (PCI DSS Requirement 3). Remember: If you don't need it, don't store it.

Does PCI DSS apply to debit cards, debit payments, and debit systems?

Article 1039 | November 2021

Any payment card (credit, debit, prepaid, stored value, gift or chip) bearing the logo of a PCI SSC Participating Payment Brand may be subject to that brand's PCI compliance programs.

Entities should contact the payment brands directly for information about their compliance programs. Contact details for the payment brands can be found in FAQ 1142: How do I contact the payment card brands?

Questions regarding compliance requirements for payment card account data affiliated with other payment networks or brands should be referred to the applicable payment network or brand.

PCI SSC also encourages entities to be aware of potential nuances in local laws and regulations that could affect applicability of the PCI standards.

Should cardholder data be encrypted while in memory?

Article 1042 | December 2022

If the cardholder data is stored in non-persistent memory (e.g. RAM), encryption of cardholder data is not required. However, proper controls must be in place to ensure that memory maintains a non-persistent state. For example, if the data in memory is being written to a file, then appropriate PCI DSS requirements are applicable to that file.

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.

PCI SSC recommends engaging a Qualified Security Assessor (QSA) for guidance as to whether a specific implementation will satisfy this requirement. For a list of QSAs, please visit: https://listings.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

Is frame relay considered a private network and are there any encryption requirements?

Article 1043 | April 2012

In general, frame relay can be considered private if it is dedicated to the customer's traffic. The PCI DSS requires encryption for transmission of cardholder data over public networks, not private networks.

Do ISPs that provide only internet connection need to comply with the PCI DSS?

Article 1044 | April 2012

If the ISP only provides a "pipe" for internet access, then it is not considered a service provider and is not subject to PCI DSS compliance. However, if the ISP is providing additional services such as firewalls or hosting functions, it is considered a service provider and would need to comply with the PCI DSS.

Is MPLS considered a private or public network when transmitting cardholder data?

Article 1045 | December 2022

Whether an MPLS network can be considered a private network is dependent upon the specific provider and configuration of that network. The implementation would need to be evaluated to determine whether the MPLS network provides exposure to the Internet or other untrusted networks, before concluding whether the MPLS network can be considered private. If the MPLS network contains publicly-accessible IP addresses or otherwise provides exposure to the Internet (for example, if an edge router has an Internet port), it may need to be considered an "untrusted" or a public network.

If the MPLS network is determined to be private, transmissions of cardholder data over that network would not need to be encrypted per PCI DSS Requirement 4. However, if there are points of exposure to the Internet or it is a shared connection, the MPLS network could be considered untrusted or public, and Requirement 4 would apply.

MPLS networks that have been verified as being private are still in scope for PCI DSS, and, as with all private networks that are in scope, the MPLS network and associated devices would need to meet the applicable PCI DSS requirements.

Will the PCI Security Standards Council "approve" my organization's implementation of compensating controls in my effort to comply with the PCI DSS?

Article 1046 | April 2012

The PCI Security Standards Council (PCI SSC) is not able to approve specific configurations or compensating controls since we are not onsite doing the assessment and are therefore not able to understand and review the total security environment. Each individual approved as a Qualified Security Assessor (QSA) is trained by the PCI SSC regarding the underlying intent of PCI DSS requirements and the evaluation of compensating controls. QSAs are responsible to determine whether a compensating control is sufficient to meet the intent of a requirement during their review of all other controls in place to satisfy PCI DSS requirements. We recommend that you contact a QSA to review your environment and assist in evaluating any compensating controls you may have in place for meeting the intent of PCI DSS requirements.

I make ATMs, what do I need to do for PTS?

Article 1050 | January 2014

Overall ATM requirements are not currently included in the PTS program so there is no cause for action in this regard. The Encrypting PIN Pad category will still feature in the program, which does impact ATMs. However there is currently no material change to testing procedures or website listings.

Beginning in version 3 of the POI requirements, the security requirements were enhanced to include modules for the Secure Reading and Exchange of Data and for Open Protocols. In version 4, while the security requirements did not significantly change, the underlying testing procedures are much more robust in both what the testing laboratory must do to validate device compliance, and in what support the vendor must provide to support that testing.

Does the PCI Security Standards Council provide information on security breaches, status of investigations, or PCI DSS compliance status?

Article 1054 | March 2017

The PCI Security Standards Council (PCI SSC) does not provide information on the status of security incidents, breach investigations or PCI DSS compliance efforts. The PCI SSC receives information and guidance from the Participating Payment Brands, the PFI community, PCI-recognized laboratories, industry subject matter experts and advisory groups regarding emerging threats and forensics trends. However, the PCI SSC does not participant in forensics investigations or compliance reporting.

Should I complete the Prioritized Approach milestones in sequential order?

Article 1055 | November 2012

The Prioritized Approach was developed to address the highest common risks first in Milestone 1, the next highest risks in Milestone 2, etc. The Prioritized Approach provides a means to address risks quickly by first identifying where payment card data exists, and what parts of the network connect to this data. That being said, each environment is unique, and organizations are encouraged to take a holistic view to payment card security and incorporate their PCI DSS compliance into an overall security strategy.

How would an identified Denial of Service (DoS) vulnerability affect a company's ability to pass a PCI DSS vulnerability scan from an Approved Scanning Vendor (ASV)?

Article 1060 | April 2012

While some ASVs may report DoS vulnerabilities as relatively high risks, the PCI SSC has clearly instructed ASVs to not consider this vulnerability when determining compliance of the ASV scan results. The Exceptions to Scoring Vulnerabilities with the NVD section of the ASV Program Guide states that, "In the case of denial-of-service vulnerabilities (where the vulnerability has both a CVSS Confidentiality Impact of "None" and a CVSS Integrity Impact of 'None'), the vulnerability must not be ranked as a failure. If loss of network availability from an attack such as DoS would not expose cardholder data to the risk of being compromised, the vulnerability would not be relevant to a company's compliance with the PCI DSS.

What is meant by a "payment application" in Part 2d of the Attestation of Compliance?

Article 1062 | July 2015

A payment application is a commercial application that stores, processes, or transmits cardholder data as part of authorization or settlement. A common example of a payment application is the software running on a point-of-sale (POS) terminal. For information about payment applications used in your environment, contact the application vendor. For applications installed on a POS system, the POS terminal provider or your acquirer (merchant bank) may also be able to assist.

Does SAQ C-VT replace SAQ C?

Article 1063 | April 2012

SAQ C-VT does not replace SAQ C. Each SAQ is designed to support a different type of cardholder data environment. At a high level, SAQ C is intended for merchants with payment applications connected to the Internet that are not connected to any other systems. SAQ C-VT is for merchants who manually enter a single transaction at a time into an Internet-based virtual terminal solution provided by a PCI DSS validated service provider. To be eligible for either SAQ, merchants must not have any electronic storage of cardholder data.

Please refer to the PCI DSS SAQ Instructions and Guidelines for more details on the different types of SAQs and eligibility criteria for each.

Merchants should also consult with their acquirer (merchant bank) to determine if they are eligible or required to submit an SAQ, and if so, which SAQ is appropriate for their environment.

What is a VT or Virtual Terminal?

Article 1064 | April 2012

A virtual terminal is web browser-based access to an acquirer, processor or third party service provider website to authorize payment card transactions over the Internet, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual terminals are typically used instead of physical terminals in merchant environments with low transaction volumes. Merchant access to the virtual terminal solution is via a personal computer connected to the Internet, and transactions are manually entered one at a time from the merchant site via a keyboard into the Internet-based virtual terminal solution. Virtual terminals do not store or process cardholder data at the merchant site.

How are third-party service providers (TPSPs) expected to demonstrate PCI DSS compliance for TPSP services that meet customers' PCI DSS requirements or may impact the security of a customer's cardholder data and/or sensitive authentication data?

Article 1065 | November 2024

A TPSP is expected to provide evidence of compliance with applicable PCI DSS requirements.

If the TPSP undergoes its own PCI DSS assessment, it is expected to provide sufficient evidence to its customers to verify that the scope of the TPSP's PCI DSS assessment covered the services applicable to the customer, and that the relevant PCI DSS requirements were examined and determined to be in place. If the provider has an PCI DSS Attestation of Compliance (AOC), it is expected that the TPSP provides the AOC to customers upon request.

If the TPSP does not undergo its own PCI DSS assessment and therefore does not have an AOC, the TPSP is expected to provide specific evidence related to the applicable PCI DSS requirements, so that the customer (or its assessor) is able to confirm that the TPSP is meeting those PCI DSS requirements.

Note: A TPSP that only provides evidence that it meets a limited set of SAQ requirements applicable to a merchant (for example, SAQ A or an SAQ A Attestation of Compliance (AOC)) has not provided sufficient evidence of PCI DSS compliance for its merchant customers. For more information, refer to the PCI DSS section 4 Scope of PCI DSS Requirements, subsection Use of Third-Party Service Providers.

Refer to the following FAQs:

FAQ 1221: To which types of service providers does PCI DSS Appendix A1 apply? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/To-which-types-of-service-providers-does-PCI-DSS-Appendix-A1-apply/)

FAQ 1312: How is an entity's PCI DSS compliance impacted by using third-party service providers (TPSPs)? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-is-an-entity-s-PCI-DSS-compliance-impacted-by-using-third-party-service-providers-TPSPs/)

FAQ 1576: What evidence is a TPSP expected to provide to customers to demonstrate PCI DSS compliance? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/What-evidence-is-a-TPSP-expected-to-provide-to-customers-to-demonstrate-PCI-DSS-compliance/)

What is an "inactive user account" as used in PCI DSS Requirement 8?

Article 1066 | August 2022

An inactive user account is one that has not been used in over 90 days. Inactive accounts are often targets for attackers since they are generally not monitored, and changes to the accounts (such as a changed password) could easily go unnoticed.

Removing or disabling inactive accounts reduces the risk that they will be used to gain unauthorized access to the environment.

Note: The specific sub requirement number(s) and terminology may vary depending on the version of the standard being used.

Are digital leased lines considered public or private?

Article 1068 | August 2022

For PCI DSS Requirement 4, digital leased lines are generally considered to be private since they are dedicated to the individual customer's traffic. This determination, however, is dependent upon the specific implementation and configuration. If a leased line was shared with unknown or untrusted parties, or provided exposure to the Internet, it may be considered an open or public connection.

Note: The specific sub requirement number(s) and terminology may vary depending on the version of the standard being used.

Does PCI DSS apply to paper with cardholder data (for example, receipts, reports, etc.)?

Article 1069 | August 2022

Yes, PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted on or by any media, including paper records. PCI DSS Requirement 9 specifically addresses the safeguarding of physical media, including paper records, containing cardholder data.

Note: The specific sub requirement number(s) and terminology may vary depending on the version of the standard being used.

Are digital images containing cardholder data and/or sensitive authentication data included in the scope of the PCI DSS?

Article 1070 | August 2022

Yes, forms and images containing cardholder data are subject to PCI DSS. PCI DSS Requirement 3 requires that all cardholder data be rendered unreadable. It does not differentiate between how the data is stored or managed. PCI DSS requires that the image and/or paper form must be rendered unreadable (or protected with appropriate compensating controls). In addition, PCI DSS Requirement 3 prohibits the storage of sensitive authentication data after authorization. If the entity collects any sensitive authentication data, they must remove or obfuscate such data before they image it, not storing scanned images with prohibited data.

Note: The specific sub requirement number(s) and terminology may vary depending on the version of the standard being used.

Refer to the definition of "sensitive authentication data" in the applicable glossary for the version of the standard being used.

Can the full payment card number be displayed within a browser window?

Article 1071 | July 2025

PCI DSS requirement 3.4.1 requires that the PAN be masked when it is displayed (for example, on screens, logs, reports, receipts), unless the viewing party has a specific business need to see the full card number. Business needs may exist to validate if the appropriate numbers were entered properly before completing the transaction (for example, for customers and customer service representatives).

Wherever PAN is accessed or displayed, other controls such as Time To Live (TTL) or webpage "timeouts" should be deployed in accordance with PCI DSS Requirement 8.2.8, so that the screen does not display the card numbers indefinitely. Additionally, as with all systems that transmit cardholder data over a public network, the website which displays the PAN should have strong encryption enabled to ensure the data is secured as it is entered and validated.

Do PCI DSS Requirements apply to Bluetooth technology?

Article 1073 | August 2022

Yes. PCI DSS requirements apply wherever payment card account data is stored, processed, or transmitted. For example, PCI DSS Requirement 4 states that strong cryptography and security protocols must be used to safeguard sensitive cardholder data during transmission over open, public networks. Bluetooth technology is included in Requirement 4 guidance as an example of an open, public network, and cardholder data sent over Bluetooth must therefore be protected in accordance with this requirement. If a Bluetooth implementation is unable to meet strong cryptography, compensating controls will need to be implemented to prevent unauthorized access to Bluetooth transmissions to capture cardholder data.

Note: The specific sub requirement number(s) and terminology may vary depending on the version of the standard being used.

Is intrusion detection required if centralized log correlation is in place?

Article 1074 | December 2022

Although log correlation is a valuable tool in a company's information security strategy, it does not replace intrusion detection mechanisms, such as IDS/IPS. Intrusion detection mechanisms provide proactive detection of threats coming into the network by comparing network traffic against known "signatures" or behaviors of different compromise types (e.g. hacker tools, Trojans, and other malware). Intrusion-detection and/or intrusion-prevention techniques are required by PCI DSS Requirement 11. In addition, logs from the intrusion-detection and/or intrusion-prevention mechanisms should be included in the daily log reviews, as required in PCI DSS Requirement 10. Note that the use of log harvesting, parsing, and alerting tools can be used to facilitate the process by identifying log events that need to be reviewed.

Is it permissible to use self-decrypting files for encryption to send cardholder data?

Article 1075 | July 2025

PCI DSS Requirement 4.2 and its sub requirements state that transmission of cardholder data over an open or public network must be secured using strong cryptography and security protocols.

There may also be other protocols and processes that can meet the intent of this requirement. Whichever method is used, it must meet all applicable requirements, including that only secure versions and configurations are supported, and that the proper encryption strength is implemented for the encryption methodology in use.

Refer to the PCI DSS Glossary of Terms, Abbreviations, and Acronyms for additional information regarding 'strong cryptography'.

Is it permissible to use FTP if proper security measures are implemented?

Article 1076 | January 2023

FTP is considered an insecure protocol as it does not provide protection for its communication channel or logon details. PCI DSS Requirement 1 states that network security controls (NSCs), such as firewalls and other network security technologies, must include a business justification for the use of insecure protocols over the network and that appropriate security features must be documented and implemented for the use of such protocols. Additionally, per PCI DSS Requirement 2, system configuration standards must include the implementation of security features for any insecure protocols. Examples of security features may include the use of secure FTP software, or tunneling the FTP connection over a secure channel, such as IPSec, SSH or TLS.

In what circumstances is multi-factor authentication required?

Article 1078 | January 2026

For more information about multi-factor authentication, refer to the Information Supplement: Authentication Guidance, available under Guidance Document in the PCI SSC Document Library.

Our document library can be accessed on our website at:
https://www.pcisecuritystandards.org/document_library/

What is the definition of "merchant"?

Article 1079 | November 2021

For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logo of a PCI SSC Participating Payment Brand as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.

Does PCI DSS Requirement 8.2.2 allow users to share authentication credentials?

Article 1080 | September 2024

Yes, but use of any shared authentication credentials such as group, shared, or generic IDs (including for administrator accounts such as admin or root) must be prevented unless needed for an exceptional circumstance and must be managed in accordance with all elements of PCI DSS Requirement 8.2.2.

PCI DSS Requirement 8.2.2 applies to all shared authentication credentials, not only those used by administrators. The intent of the PCI DSS requirements for strict management of user identification and accounts (requirements under 8.2) and strong authentication (requirements under 8.3) is to ensure each user is uniquely identified such that every action taken is attributable to an individual user ID. This allows organizations to maintain individual accountability for user actions and provide an effective audit trail per user ID. This will help speed issue resolution and containment if misuse or malicious use occurs.

For administrative functions, tools or password vaults can be used to facilitate management, security, and limited use of shared IDs, including confirming the identity of individual users and maintaining individual accountability and audit trails. A password vault is an example of a technology that can be used when a shared ID is needed for emergency use or “break the glass” administrator access.

Does PCI DSS require both database and application logging?

Article 1081 | December 2022

The intent of the PCI DSS logging requirements is to provide a complete record of who did what, where, when, and how, so it can be used for investigation in the event of unexpected or unauthorized activities. Therefore, a combination of operating system logging, database logging, and/or application logging may be implemented as appropriate to record the events defined in Requirement 10. For example, if the operating system and/or installed applications are able and configured to log all individual access to cardholder data within a database, then configuring database logging in addition to these other logs may not be necessary.

If a merchant has multiple processing environments, should the merchant complete multiple SAQ to validate their PCI DSS compliance?

Article 1082 | July 2015

Merchants should always contact their acquirer (merchant bank), or payment brand directly to understand their compliance validation obligations, including which SAQ they may be eligible to use. Contact details for the payment brands can be found in FAQ #1142 'How do I contact the payment card brands'?

For multiple payment channels, it may be possible for a merchant to complete a different SAQ for each payment channel, or for a single SAQ to be used that addresses all the requirements for all channels combined. If different SAQs are used, each channel must meet the eligibility criteria for the applicable SAQ, and adequate network segmentation must be in place to isolate the different channels.

In all cases, details of the environment(s) covered by a SAQ must be documented in the Attestation of Compliance, Part 2: Executive Summary.

What is the mission of the PCI Security Standards Council?

Article 1083 | April 2012

The mission of the PCI Security Standards Council is to enhance payment account security by creating and maintaining PCI Security Standards, as well fostering the education and awareness of these security standards.

Can unencrypted PANs be sent over e-mail, instant messaging, SMS, or chat?

Article 1085 | August 2025

No. PCI DSS Requirement 4.2.2. prohibits the sending of unprotected primary account numbers (PANs) via end-user messaging technologies, whether sent internally or over public networks. E-mail, instant messaging, SMS, and chat are all considered end-user messaging technologies and thus required to meet PCI DSS Requirement 4.2.2. Per PCI DSS Requirement 4.2.1, strong cryptography and security protocols must be used when cardholder data is sent over open, public networks.

Also refer to the following FAQs:

FAQ 1310: Are entities allowed to request that cardholder data be provided over end-user messaging technologies?
(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/are-entities-allowed-to-request-that-cardholder-data-be-provided-over-end-user-messaging-technologies/)

FAQ #1157: What should a merchant do if cardholder data is accidentally received via an unintended channel?
(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-should-a-merchant-do-if-cardholder-data-is-accidentally-received-via-an-unintended-channel/)

How does encrypted cardholder data impact PCI DSS scope?

Article 1086 | March 2026

Encryption of cardholder data with strong cryptography is an acceptable method of rendering the data unreadable according to PCI DSS Requirement 3.5.1. However, encryption alone is insufficient to render the cardholder data out of scope for PCI DSS.

For more information, refer to PCI DSS v4.x section 4 Scope of PCI DSS Requirements, subsection Encrypted Cardholder Data and Impact on PCI DSS Scope.

Refer to the following related FAQs:

FAQ 1233: How does encrypted cardholder data impact PCI DSS scope for third-party service providers?

FAQ 1158: What effect does the use of a PCI-listed P2PE solution have on a merchant's PCI DSS validation?

For vulnerability scans, what is meant by "quarterly" or "at least once every three months"?

Article 1087 | July 2023

The intent of conducting vulnerability scans "quarterly" or "at least once every three months," as defined in PCI DSS v3.2.1 and v4.0 respectively, is to have them conducted as close to three months apart as possible, to ensure vulnerabilities are identified and addressed in a timely manner. To meet the vulnerability scanning requirements in PCI DSS Requirement 11, an entity is required to complete their internal and external scans, and perform any required remediation, at least once every three months.

At least once every three months, or 90 days, is considered the maximum amount of time that should be allowed to pass between quarterly vulnerability scans. If unforeseen circumstances occur that impact an entity's ability to complete scheduled scans, every effort should be made to perform scans as soon as possible (for example, within a day or two) of the scheduled scan date. Where an entity has advance notice of factors that may delay scans or impede their ability to address vulnerabilities (for example, scheduled system downtime, or predefined no-change windows that prevent system updates), the entity should strive to schedule scans before the three-month period is reached.

Entities are encouraged to perform vulnerability scans more frequently than required as it will enhance security by allowing quicker identification and resolution of vulnerabilities. More frequent vulnerability scans also provide entities with earlier awareness of vulnerabilities that need to be resolved, thereby increasing the likelihood that all vulnerabilities are successfully identified and resolved within the three-month period.

PCI DSS also requires vulnerability scans after significant changes. These scans are required in addition to the scans conducted at least once every three months; this means that vulnerability scans are required both 1) at least once every three months and 2) after a significant change.

Also refer to the following related FAQ:

-

FAQ 1572: Can a compensating control be used for requirements with a periodic or defined frequency, where an entity did not perform the activity within the required timeframe?

How can hashing be used to protect Primary Account Numbers (PAN) and in what circumstances can hashed PANs be considered out of scope for PCI DSS?

Article 1089 | March 2026

One-way hashing is a method that can be used to render PAN unreadable in storage. The hashing process and results, as well as the system(s) that perform the hashing, are in scope for a PCI DSS assessment to assure that the process meets applicable PCI DSS requirements.

If the hashing result is transferred and stored within a separate environment, the hashed PAN in that separate environment would no longer be considered cardholder data and would be out of scope for additional PCI DSS requirements. However, if the hashed PAN is stored on the same system or in the same environment that performed the hashing, that system or environment is considered to be storing cardholder data and remains within PCI DSS scope.

PCI DSS requires that hashing be of the entire PAN and be based on strong cryptography. This means that collisions would not occur frequently, and the PAN cannot be recovered or easily determined during an attack. Additionally, PCI DSS v4.x includes Requirement 3.5.1.1 to use keyed cryptographic hashing for hashes used to render PAN unreadable.

Since hashing is used when there is no need to recover the PAN, a recommended practice is to remove the PAN rather than allowing the possibility of a compromise cracking the hash and revealing the original PAN. If the entity intends to recover and use the PAN, then hashing is not an option and an alternative method for rendering the PAN unreadable should be considered.

What are acceptable formats for truncation of primary account numbers?

Article 1091 | June 2022

Acceptable truncation formats vary according to PAN length and Participating Payment Brand requirements.

- A maximum of the first 6 and last 4 digits of the PAN is the starting baseline for entities to retain after truncation, considering the business needs and purposes for which the PAN is used.
- When more digits of the PAN are necessary for business functions, entities should consult the table below for the acceptable formats for each Participating Payment Brand.

PAN / BIN Length

Payment Brand

Acceptable PAN Truncation Formats

16-digit PAN (with either 6- or 8-digit BIN)

Discover

JCB

Mastercard

UnionPay

Visa

At least 4 digits removed. Maximum digits which may be retained:

'First 8, any other 4'

15-digit PAN

American Express

At least 5 digits removed. Maximum digits which may be retained:

'First 6, last 4'

<15-digit PAN

Discover

Maximum digits which may be retained:

'First 6, any other 4'

When using truncation formats for purposes other than storage, or for PAN lengths not covered within this FAQ, entities should confirm that their format is compatible with each of the applicable Participating Payment Brands. Contact information for the Participating Payment Brands can be found in FAQ 1142 How do I contact the payment card brands?

Access to different truncation formats of the same PAN greatly increases the ability to reconstruct full PAN, and the security value provided by an individual truncated PAN

is significantly reduced. Information about the use of different truncation formats of the same PAN can be found in FAQ 1117 Are truncated Primary Account Numbers (PAN) required to be protected in accordance with PCI DSS?

Does PCI DSS apply to merchants who outsource all payment processing operations and never store, process or transmit cardholder data?

Article 1092 | June 2025

Yes. PCI DSS is intended for any entity that stores, processes, or transmits cardholder data — regardless of whether these activities are conducted directly or by a third-party service provider.

When a merchant outsources its payment processing to a third party and does not store, process, or transmit cardholder data, many PCI DSS requirements may not apply directly to the merchant's environment. However, this does not remove the merchant's responsibility to ensure account data is properly protected by the third party.

Merchants remain responsible for:

- Ensuring the provider is PCI DSS compliant for the services offered,
- Maintaining written agreements with the provider that include acknowledgment of their responsibilities (Requirement 12.8.2),
- Monitoring the provider's compliance status at least annually (Requirement 12.8.4),
- Clearly defining and understanding any shared responsibilities.

Merchants are still required to validate PCI DSS compliance, typically through a Self-Assessment Questionnaire (such as SAQ A). Merchants should confirm their compliance obligations with the organization(s) that manage their compliance program—such as their acquirer or payment brand—also referred to as compliance-accepting entities.

Do PCI DSS requirements for protecting stored cardholder data apply to mainframes?

Article 1093 | June 2025

Yes. PCI DSS Requirement 3.5.1 applies to mainframes that store cardholder data. If a company has legitimate business or technical constraints in meeting this or any other requirement, compensating controls may be considered. Compensating controls must address the additional risk introduced by not meeting the original requirement.

Refer to Appendices B and C of PCI DSS v4.0.1 for more information about compensating controls.

Will the PCI Security Standards Council be involved in performing forensics investigations as a result of an account data compromise event?

Article 1094 | April 2012

The PCI Security Standards Council will not conduct forensics investigations either directly or through a third party in the event of an account compromise.

When a QSA or ASV is newly approved, who is the contact at the PCI Security Standards Council to request a press release?

Article 1096 | April 2012

Newly approved QSAs and ASVs should send an e-mail message to info@pcisecuritystandards.org to request a press release.

How does PCI DSS apply to individual PCs or workstations?

Article 1115 | June 2012

All system components in the network are considered part of the cardholder data environment unless adequate network segmentation is in place that isolates systems that store, process, or transmit cardholder data from those that do not. Without proper network segmentation, the entire network is in scope for the PCI DSS. Where there are many PCs or workstations in an environment and all PCs do not need access to the cardholder data environment (CDE), the network segmentation should provide access to the CDE only for the PCs that need access, and should prohibit access for all other PCs. Where segmentation is used to reduce PCI DSS scope, the assessor must verify that the segmentation controls are effective and working as intended. The assessor would need to determine whether the connected systems provide a path for other systems into the CDE. If there are other systems on the network which are not adequately segmented (isolated) from the CDE, they could also be brought into scope. Once it has been validated that adequate segmentation is in place, PCI DSS requirements would be relevant to, and should be applied to, the PC population which is in scope. While all connected systems should be considered in scope for a PCI DSS review, the particular PCI DSS requirements applicable to each system may vary depending on the function of the system and the presence of any additional controls that are implemented. (For example, controls could be in a place that prevents the system from accessing cardholder data or from influencing the security of the CDE in any way). All such controls would need to be verified as part of PCI DSS scope verification.

Are truncated Primary Account Numbers (PAN) required to be protected in accordance with PCI DSS?

Article 1117 | September 2021

Systems that store, process, or transmit only truncated PANs (where a segment of PAN data has been permanently removed) may be considered out of scope for PCI DSS if those systems are adequately segmented from the cardholder data environment, and do not otherwise store, process, or transmit cardholder data or sensitive authentication data. This applies to any truncation that meets the acceptable PAN truncation formats specified in FAQ 1091.

However, the system performing the truncation of the PANs, as well as any connected systems and networks, would be in scope for PCI DSS.

Some entities use solutions that combine truncation with tokenization or encryption to create format-preserving values that can be passed through legacy payment systems. For example, the BIN and the last four digits of the PAN are retained in accordance with FAQ 1091 while the remaining digits are replaced with values generated via a tokenization or encryption operation. Whether such format-preserving values may be considered out of scope for PCI DSS is dependent on a variety of factors and can only be determined in respect of an entity's specific implementation by an Assessor. However, the systems performing encryption or tokenization of the PAN segment and those performing key management for the encrypted or tokenized PANs would be in scope for PCI DSS.

For solutions that combine truncation with tokenization or encryption, factors that indicate the resulting truncation result would be in scope for PCI DSS, include, but are not limited to the following:

- The tokenization or encryption of the PAN segment can be reversed in the environment in which the segment resides.
- The encrypted or tokenized PAN segment is not isolated from related key management processes.
- The encrypted or tokenized PAN segment is present on a system or media that also contains the decryption key.
- The encrypted or tokenized PAN segment is present in the same environment as the decryption key.
- The encrypted or tokenized PAN segment is accessible to an entity that also has access to the decryption key.

Note that access to different truncation formats of the same PAN greatly increases

the ability to reconstruct full PAN, and the security value provided by an individual truncated PAN is significantly reduced. If the same PAN is truncated using more than one truncation format (for example, different truncation formats are used on different systems), additional controls should be in place to ensure that the truncated versions cannot be correlated to reconstruct additional digits of the original PAN. To consider the truncated PAN out of scope, the additional controls must be verified to confirm that correlation is not possible, and that the different truncation formats do not result in more than the maximum allowable digits being present in the environment. If a PAN is truncated using different truncation formats, and this results in more than the allowable number of PAN digits being present in an environment, then that environment would be in scope for PCI DSS.

See also the following FAQs:

FAQ 1091: What are acceptable formats for truncation of primary account numbers?

FAQ 1146: What is the difference between masking and truncation?

What is the scope of the PCI Security Standards Council's activities?

Article 1122 | July 2012

PCI SSC responsibilities include:

- Develop and manage the PCI Security Standards, including maintenance, clarification and revisions of the standards.
- Establish and maintain approval processes for qualified security assessors, approved scanning vendors, and testing laboratories, and routinely evaluate and approve qualified assessors, vendors and laboratories.
- Publish and distribute PCI security standards, including errata and addenda, and all related documents associated with assessor, vendors and laboratory policies and procedures.
- Provide an open forum where all key stakeholders can provide input into the ongoing development of payment security standards and business practices.

In what way does the PCI Security Standards Council make payment card data more secure?

Article 1123 | July 2012

Security of payment card data is the responsibility of every business that participates in payment processing. Single industry-level security standards supported by the members of the PCI Security Standards Council eliminate competing and overlapping brand-specific requirements, thereby simplifying compliance for businesses that store payment card data.

PCI DSS provides a common data security standard across all payment brands. Are there any plans to provide a common structure of penalties and/or fines for non-compliance to this standard?

Article 1124 | July 2012

The PCI Security Standards Council publishes and distributes PCI Security Standards, including errata and addenda, and all related documents associated with assessor, vendors and laboratory policies and procedures. Any fines and/or penalties associated with non-compliance with the PCI DSS are defined by the payment card brands. For further details, please contact the individual payment card brands directly.

Are there any plans for PCI SSC to be a single point of contact for a merchant, financial institute or processor to send a PCI DSS compliance report to?

Article 1125 | December 2012

Because PCI SSC does not have a contractual relationship with merchants, financial institutes, processors, etc., PCI SSC cannot be the central repository for this information. The Council's focus is to define effective payment-related security standards, as well as to educate and provide resources to the marketplace to drive awareness and adoption of these standards. The payment brands define and manage the compliance programs for these security standards, and entities will continue to send their compliance validation documentation to the payment brands, financial institutions (such as acquirers or merchant banks), or other agents, as applicable for each payment card brand compliance program.

How do I determine whether my business would be required to conduct an independent assessment or a self-assessment?

Article 1126 | July 2012

Merchants should contact the acquiring financial institutions with whom they have merchant agreements (for example, their merchant bank) to determine whether they must validate compliance and the specific requirements for performing and reporting their compliance validation. Service providers should contact the individual payment brands for further information.

Is there opportunity to provide feedback on the PCI Council's standards?

Article 1127 | July 2012

Entities wishing to have early access and input into the PCI security standards are required to join the Council as a participating organization. Non-Participating Organizations will not have access to preliminary drafts, but may submit generic questions and comments on the Council's Web site www.pcisecuritystandards.org.

Are operating systems that are no longer supported by the vendor non-compliant with the PCI DSS?

Article 1130 | June 2013

PCI DSS Requirements 6.1 and 6.2 address the need to keep systems up to date with vendor-supplied security patches in order to protect systems from known vulnerabilities. Where operating systems are no longer supported by the vendor, OEM or developer, security patches might not be available to protect the systems from known exploits, and these requirements would not be able to be met.

However, it may be possible to implement compensating controls to address risks posed by using unsupported operating systems in order to meet the intent of the requirements. To be effective, the compensating controls must protect the system from vulnerabilities that may lead to exploit of the unsupported code. For example, exhaustive reviews may need to be regularly performed to ensure that all known exploits for that operating system are continually identified and that system configurations, anti-virus, IDS/IPS, and firewall rules are continually updated to address those exploits. Examples of controls that may be combined to contribute to an overall compensating control include active monitoring of system logs and network traffic, properly-configured application whitelisting that only permits authenticated system files to execute, and isolating the unsupported systems from other systems and networks. Note that these examples may complement an overall compensating control, but these examples alone would not provide sufficient mitigation.

Additionally, if an unsupported operating system is Internet-facing, it will be detected and reported as an automatic failure by an ASV scan. Detection of unsupported operating systems in an ASV scan will need to be addressed according to Addressing Vulnerabilities with Compensating Controls section of the ASV Program Guide.

The use of compensating controls should be considered a temporary solution only, as the eventual solution is to upgrade to a supported operating system, and the entity should have an active migration plan for doing so. For assistance with compensating controls, and for questions about whether a specific implementation meets PCI DSS requirements, please contact a Qualified Security Assessor.

Does the council have a mapping between PCI DSS and ISO 27002 (formerly ISO 17799) or other standards?

Article 1131 | July 2012

There is no direct correlation between PCI DSS and ISO 27002. The ISO standards provide a framework for implementing an information security program while PCI DSS provides a baseline of technical and operational requirements for the protection of payment card data. Work performed to implement an ISO standard is a good start to becoming PCI DSS compliant, and can provide input and support for PCI DSS compliance efforts. The PCI Security Standards Council does not have a document that maps PCI DSS to other standards. However, other standards organizations may have this type of mapping available.

What is an Attestation of Compliance?

Article 1132 | July 2012

The Attestation of Compliance is the document used to indicate that the appropriate Report on Compliance or Self-assessment Questionnaire has been performed, and to attest to your organization's compliance status with PCI DSS.

Why are there multiple PCI DSS Self-assessment Questionnaires (SAQs)?

Article 1133 | April 2024

There are multiple versions of PCI DSS SAQs to meet various merchant scenarios, depending on how each merchant organization stores, processes, or transmits cardholder data (CHD) and/or sensitive authentication data (SAD). For more information on how to determine which SAQ applies best to a merchant environment and how to complete an SAQ, refer to 'PCI DSS Self-Assessment Questionnaire Instructions and Guidelines', available in the Document Library.

Merchants should consult with their compliance-accepting entity - the entity to which the SAQ will be submitted (typically, an acquirer (merchant bank) or the payment brands) to determine if they are eligible or required to submit an SAQ, and if so, which SAQ is appropriate for their environment.

SAQ D for Service Providers is the ONLY SAQ for SAQ-eligible service providers. All other SAQs are for merchant use only.

Refer to FAQ 1215: What is a PCI DSS Self-Assessment Questionnaire? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-is-a-pci-dss-self-assessment-questionnaire/)

What are the steps needed to perform a self assessment to validate compliance with PCI DSS?

Article 1134 | July 2015

Merchants and service providers that validate PCI DSS compliance using a Self-Assessment Questionnaire (SAQ) will typically complete the following steps:

- Identify the SAQ that applies to your environment, using the Self- Assessment Questionnaire Instructions and Guidelines document (available in the PCI SSC Documents Library) for guidance. Merchants should consult with their acquirer (merchant bank) or the payment brands directly to determine if they are eligible or required to submit an SAQ, and if so, which SAQ is appropriate for their environment.
- Confirm your environment is properly scoped and meets all the eligibility criteria for the SAQ being used.
- Perform the self-assessment activities as described in the Expected Testing column of the SAQ, and enter a response for each requirement included in the SAQ.
- Complete all sections of the SAQ and Attestation of Compliance (AOC). AOCs are included within each SAQ and also provided as separate, standalone documents.
- If required as part of your compliance, complete external vulnerability scans using a PCI SSC Approved Scanning Vendor (ASV), and obtain passing scan reports from the ASV.
- Submit the required documentation to your acquirer or payment brand, in accordance with the applicable payment brand compliance programs. Your compliance documentation may include the full SAQ, AOC, and/or ASV scan reports, as well as other documentation requested by your acquirer or payment brand.

Can VLANs be used for network segmentation?

Article 1135 | July 2012

In general, implementing adequate network segmentation can reduce the scope of the PCI DSS assessment if it isolates systems that store, process, or transmit cardholder data from other systems. While this segmentation can be implemented with, for example, properly-configured internal firewalls, routers with strong access control lists, VLANs, or other technologies that restrict access to a particular network segment, the PCI Security Standards Council is not able to offer an opinion about how your organization can achieve adequate network segmentation since it requires an understanding of security features and controls implemented in your environment. We encourage you to contact a Qualified Security Assessor (QSA) to assist in scoping your cardholder data environment and recommend methods specific to your organization to help reduce the scope of your PCI DSS assessment. Our list of QSAs can be found at: [List of QSA Assessors \(http://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php\)](http://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php)

How can I validate if a number is a legitimate credit card number?

Article 1137 | July 2012

The Luhn formula or Modulus 10 is the algorithm most often used to validate Primary Account Numbers (PAN). The algorithm works as follows:

- double the value of alternate digits of the PAN beginning with the second digit from the right (for any resulting value greater than 10, subtract 9),
- add the calculated values as well as the values skipped in step 1 together,
- the total obtained in step 2 must be divisible by 10. Note that this formula tells you whether the payment card number is a possible and valid number, but not whether it's actually been issued and is active.

Does PCI SSC provide a list of PCI DSS-compliant third-party service providers?

Article 1138 | February 2024

No. PCI SSC does not provide a list of PCI DSS-compliant third-party service providers (TPSPs), nor does PCI SSC manage a program to recognize compliant TPSPs.

PCI DSS is intended for all entities that store, process, or transmit cardholder data and/or sensitive authentication data or could impact security of the cardholder data environment. However, whether an entity is required to comply with or validate their compliance to PCI DSS is at the discretion of those organizations that manage compliance programs (for example, payment brands and acquirers). Some payment brands may provide a list of PCI DSS-compliant TPSPs. Check with the payment brands to understand their compliance programs and whether they provide a list of compliant TPSPs. Contact details for the payment brands can be found in FAQ #1142 [How do I contact the payment card brands?](https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands/) (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands/)

For more information, refer to PCI DSS section 4 Scope of PCI DSS Requirements, subsections Use of Third-Party Service Providers and TPSPs Presence on a Payment Brand List(s) of PCI DSS Compliant Service Providers.

Does PCI DSS allow faxing of payment card numbers?

Article 1139 | August 2025

Any cardholder data that is stored, processed, or transmitted must be protected in accordance with PCI DSS. If faxes are sent or received via modem over a traditional PSTN phone line, these are not considered to be traversing a public network. On the other hand, if a fax is sent or received via the Internet, it is traversing a public network and must be encrypted per PCI DSS Requirement 4.2.1. Any systems, such as fax servers or workstations, that cardholder data passes through must be secured according to PCI DSS. Additionally, any cardholder data on the fax that is stored electronically must be rendered unreadable in accordance with PCI DSS Requirement 3.5.1. If the fax system is combined with an email system (for example, via a fax-to-email gateway), any emails would also be subject to Requirement 4.2.2.

Furthermore, Requirement 3.3 prohibits the storage of sensitive authentication data (full track, card verification codes/values, and PIN block data) after authorization. If sensitive authentication data is received on a fax (for fax transmissions this would only be the 3- or 4- digit card verification codes/values printed on the front or back of payment cards), the data should be blacked-out or removed prior to retaining the fax in paper form. The original fax transmission should be securely deleted from the system in a manner which ensures the data is non-recoverable. Entities should also protect paper documents that contain cardholder data in accordance with PCI DSS Requirements 9.4.

Also refer to the following FAQ:

FAQ 1085: Can unencrypted PANs be sent over e-mail, instant messaging, SMS, or chat?

(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/can-un-encrypted-pans-be-sent-over-e-mail-instant-messaging-sms-or-chat/)

Which Self-assessment Questionnaire (SAQ) should I complete?

Article 1140 | July 2015

The PCI DSS SAQ Instructions and Guidelines document (available from the PCI SSC Documents Library) provides information about the different SAQs and the types of environments that each SAQ is intended for. Merchants should also consult with their acquirer (merchant bank) or payment brand to determine if they are eligible or required to submit an SAQ, and if so, which SAQ is appropriate for their environment.

How do I contact the payment card brands?

Article 1142 | June 2024

Contact the applicable payment brands and/or acquirer (merchant bank) for more information about PCI compliance programs.

Contact details for the PCI SSC Participating Payment Brands are provided below:

American Express

Website: <http://www.americanexpress.com/datasecurity>

Email: AmericanExpressCompliance@securetrust.com

Discover

Website: <https://www.discovernetwork.com/en-us/>

For questions about the DISC program:

<https://www.discovernetwork.com/en-us/business-resources/fraud-security/pci-rules-regulations/>

Email: DISCCompliance@discover.com

JCB

Website: <http://www.global.jcb/en/products/security/data-security-program/>

Email: riskmanagement@info.jcb.co.jp

Mastercard

Website: <http://www.mastercard.com/sdp>

Email: sdp@mastercard.com

UnionPay

Website: <http://unionpayintl.com/en/>

Email: risk@unionpayintl.com

Visa

Website: <https://usa.visa.com/support/small-business/security-compliance.html>

Asia Pacific

Email: vpssais@visa.com - for Merchant Requirement

Email: pciagents@visa.com - for Clients, Third Party Agents and Service Provider Requirements

Canada and the U.S.

Email: pcicap@visa.com - for Merchant Requirement

Email: pciocs@visa.com - for Clients, Third Party Agents and Service Provider Requirement

Central Europe, Middle East, & Africa

Email: pcicemea@visa.com

Europe

Email: datasecuritystandards@visa.com - for Clients and Merchant requirements

Email: pcidsseurope@visa.com - for Clients, Third Party Agents and Service Provider Requirements

Latin America and the Caribbean

Email: aislac@visa.com

Visa PIN Security Program

Website: <http://www.visa.com/pin>

For information about PCI SSC Affiliate Members, please refer to the

following

link:

https://www.pcisecuritystandards.org/get_involved/affiliate_members.php

What is the difference between masking and truncation?

Article 1146 | July 2025

Masking is addressed in PCI DSS Requirement 3.4.1, whereas truncation is one of several options specified to meet PCI DSS Requirement 3.5.1.

Requirement 3.4.1 relates to the protection of primary account number (PAN) that is displayed on screens, paper receipts, printouts, etc. It is not to be confused with Requirement 3.5.1 for the protection of PAN when stored, processed, or transmitted in files, databases, etc.

Masking is a method of concealing a segment of a PAN when displayed or printed (for example, on paper receipts, reports, or computer screens), and is used when there is no business need to view the entire PAN.

Truncation is a method of rendering a full PAN unreadable by removing a segment of PAN data and applies to PANs that are electronically stored (for example, in files, databases, etc.).

Masking is not synonymous with truncation and these terms are not meant to be used interchangeably. Masking refers to concealing certain digits during display or printing, even when the entire PAN is stored on a system. This process differs from truncation, in which the truncated digits are removed and cannot be retrieved within the system. Masked PAN could be 'unmasked', but there is no "un-truncation" without recreating the PAN from another source.

Note that even if a PAN is masked when displayed, the full PAN might still be electronically stored and would need to be protected in accordance with PCI DSS Requirement 3.5.1.

Entities should also be aware of any stricter requirements that may apply to displays of cardholder data, such as specific Payment Brand regulations and regulatory or legislative requirements—for example, restrictions for data displayed on point-of-sale (POS) receipts. PCI DSS does not supersede local or regional laws or other legislative requirements.

See also the following FAQ:

FAQ 1117: Are truncated Primary Account Numbers (PAN) required to be protected in accordance with PCI DSS?
(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/Are-truncated-Primary-Account-Numbers-PAN-required-to-be-protected-in-accordance-with-PCI-DSS)

What is the purpose of PCI DSS Requirement 8.2.8, which requires users to reauthenticate after 15 minutes of idle time?

Article 1147 | November 2025

The intent of this requirement is to prevent an unauthorized person from using an unattended console/PC to gain access to the user's computer and accounts, and potentially to the company's network.

This requirement is not intended to prevent legitimate activities from being performed while the console/PC is unattended. For example, if a user needs to run a program from an unattended computer, they can login to the computer to initiate the program, and then "lock" the computer so that no one else can use their login while the computer is unattended. An example of how to meet this requirement includes configuring an automated screensaver to launch whenever the console has been idle for 15 minutes and requiring the logged-in user to re-authenticate to re-activate the terminal or session.

Note: Requirement 8.2.8 is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.

Can entities be PCI DSS compliant if they have performed vulnerability scans at least once every three months, but do not have four "passing" scans?

Article 1152 | January 2024

PCI DSS requires entities to perform internal and external vulnerability scans at least once every three months, identify and address vulnerabilities in a timely manner, and verify through rescans that vulnerabilities have been addressed. To achieve these objectives, an entity would need to show that "clean" or "passing" scans were performed at least once every three months for the previous four quarters, for both their external and internal environments. A "clean" or "passing" scan generally has the following characteristics:

- No configuration or software was detected that results in an automatic failure (such as the presence of default accounts and passwords, etc.)
- For external scans, no vulnerabilities with a score of 4.0 or higher on the Common Vulnerability Scoring System (CVSS)
- For internal scans, vulnerabilities are resolved by the entity according to PCI DSS Requirement 11.3.1.

With new vulnerabilities continually being identified, scanning becomes an integral part of an organization's vulnerability management process, resulting in a cycle of scanning, patching, and rescanning until a "clean" scan is obtained. However, due to the frequency of new vulnerabilities being identified, it may not always be possible to produce a single, clean scan at least once every three months. Take the example of an entity that performs a scan which identifies several vulnerabilities. The entity then fixes all the identified vulnerabilities and performs a rescan to verify. The rescan shows that the vulnerabilities identified in the first scan have been addressed, but new vulnerabilities that were not present in the original scan have since appeared. In this case, instead of having a single, environment-wide scan report, an entity may verify they have met the scanning requirements through a collection of scan results which together show that all required scans are being performed, and that all applicable vulnerabilities are being identified and addressed at least once every three months.

To verify that the requirement to perform vulnerability scans at least once every three months has been met, the following should occur:

- Scans of all in-scope systems are performed at least once every three months, and all in-scope systems are covered by the entity's scan-remediate-rescan processes.
- Rescans are performed as necessary and show that vulnerabilities identified in the initial scans have been remediated, for all affected systems, as part of that period's scanning process.
- The entity has processes in place to remediate currently identified vulnerabilities.
- Repeated failing scans are not the result of poor remediation practices resulting in previously identified vulnerabilities not being properly addressed.

If, however, an entity does not have four passing scans for the last 12 months, performed at least once every three months, because they didn't schedule the scans properly, or the scans are incomplete, or the identified vulnerabilities have not been addressed from one period to the next, then the entity has not met the requirement.

Note: results from external vulnerability scans may also be required by acquirers and payment card brands as part of an entity's annual compliance validation. Entities should contact their acquirer (merchant bank) and/or the payment brands directly to understand their reporting requirements for external scans.

How does PCI DSS apply to VoIP?

Article 1153 | October 2012

PCI DSS requirements apply wherever payment card account data is stored, processed, or transmitted. While PCI DSS does not explicitly reference the use of VoIP, VoIP traffic that contains payment card account data is in scope for applicable PCI DSS controls, just as other IP network traffic containing payment card account data would be.

VoIP transmissions originating from an external source and sent to an entity's environment are not considered within the entity's PCI DSS scope until the traffic reaches the entity's infrastructure. This is because an entity cannot control the method of inbound phone calls that their customers and other parties may make, including whether any payment card account data sent over that transmission is being adequately protected by the caller.

An entity is considered to have control over the transmission, storage and processing of VoIP traffic within their own network and up to the external perimeter of their infrastructure. The following guidance is intended to assist with PCI DSS scoping for VoIP in different scenarios.

Internal transmissions: VoIP traffic containing payment card account data is in scope for applicable PCI DSS controls wherever that traffic is stored, processed or transmitted internally over an entity's network.

External transmissions to other business entities (business-to-business): Where an entity uses VoIP for transmission of payment card account data to another business—for example, a service provider or payment processor—the entity's systems and networks used for those transmissions are in scope. Where an entity has end-to-end control over the VoIP connection, the transmission is also in scope for applicable PCI DSS controls. Where an entity cannot control the entire connection—for example, where the transmission passes through multiple telephone carriers between the two entities—the VoIP transmission is within the entity's scope only while the transmission is under control of the entity's infrastructure. This is because the entity does not control how the VoIP traffic will be routed outside of the entity's infrastructure or if all the telephone carriers can support secure connections.

External transmissions to/from cardholders: Where VoIP is used for transmissions of payment card account data between a cardholder and an entity, the entity's systems and networks used for those transmissions are in scope. Securing the VoIP transmission outside of the entity's infrastructure is not considered within the entity's scope, as the entity cannot control the methods used by the cardholder to make and receive phone calls. This applies regardless of whether the transmissions are initiated by the entity or the cardholder.

PCI SSC has published an Information Supplement titled "Protecting Telephone-Based Payment Card Data", which provides additional guidance for protecting payment card account data that is received via voice communications. This Information Supplement is available for download from the Guidance Documents section in the PCI SSC

For PCI DSS, can sensitive account data be stored before authorization?

Article 1154 | July 2025

For PCI DSS, account data consists of cardholder data (CHD) and sensitive authentication data (SAD). With respect to SAD, PCI DSS Requirement 3.3.1 prohibits storage of SAD after authorization, even if encrypted. Note that there are no specific rules in PCI DSS regarding how long SAD can be stored before authorization, but such data would need to be protected according to PCI DSS. Use of PCI approved PTS devices and PCI-validated payment software can support PCI DSS compliance for the protection of data prior to authorization.

The individual payment brands determine whether SAD is permitted to be stored before authorization, including any related usage and protection requirements. Additionally, several payment brands have specific rules that prohibit any storage of SAD and do not make any exceptions. To determine payment brand requirements, please contact the individual payment brands directly. Contact information for the payment brands can be found in FAQ 1142 How do I contact the payment card brands?

(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands)

Which service provider category should I use for Part 2 of the PCI DSS Attestation of Compliance (AOC) for Service Providers?

Article 1155 | July 2015

The categories on the service provider Attestation of Compliance (AOC) are provided to assist those completing the AOC to identify their business functions as they deem appropriate and, where applicable, to categorize their services for those payment brands with service provider lists that include such categories. Because there may be different interpretations or uses of these terms in different industries or regions, PCI SSC has not provided specific definitions or criteria for these categories and each service provider is free to use them as appropriate for their particular business. If a service provider performs a function which they feel is not described in this list of categories, they may select the "Other" option, and enter the details of their service(s) in the appropriate field.

If a service provider is unsure whether a category could apply to their service, they should consult with the applicable payment brand. Contact information for the payment brands can be found in FAQ # 1142 How do I contact the payment card brands?

What should a merchant do if cardholder data is accidentally received via an unintended channel?

Article 1157 | October 2012

Merchants sometimes find themselves in a situation where a customer provides their cardholder data unsolicited via an insecure communication channel that was not intended for the purpose of capturing sensitive data.

In this situation, the merchant can choose to either include the channel into the scope of their cardholder data environment (CDE) and secure it according to PCI DSS, or implement measures to prevent the channel from being used for cardholder data.

Some suggestions for merchants to prevent any further capture of cardholder data via unsecured methods include:

- Implementing controls to prevent acceptance of cardholder data via unsecured channels
- Responding to customers in a manner which does not propagate any further unsecured transmissions of cardholder data
- Implementing best practices and customer communications to proactively prevent customer use of unsecured channels for cardholder data

Cardholder data received via an unintended channel should be either immediately removed or secured according to PCI DSS and incorporated into the merchant's CDE. If a merchant does not wish to bring a communication channel and its supporting systems into the scope of their CDE, controls should be in place to prevent the capture of cardholder data and/or to securely delete cardholder data from this channel before the data can be further stored, processed or transmitted.

If unsolicited cardholder data is received via an insecure method, the merchant should take immediate steps to minimize the security impact and prevent further exposure of that data. For example, if a merchant receives cardholder data in an email from a customer, the merchant's personnel should be trained to not 'reply' using the same email that contains the cardholder data. Instead, the merchant's personnel should respond in a manner that does not further propagate the unsecured transmission of cardholder data. This may be accomplished by removing all sensitive data from the email response before replying or by contacting the customer via an alternative communication channel to complete the transaction.

Merchants are encouraged to communicate with their customers on the risks of sending cardholder data through insecure channels, and to ensure their customers are aware of the merchant's secure methods for submitting payment information. By proactively encouraging their customers to use only secure payment methods, merchants can reduce the amount of cardholder data received via unsolicited or insecure channels.

What effect does the use of a PCI-listed P2PE solution have on a merchant's PCI DSS validation?

Article 1158 | February 2024

A PCI-listed P2PE solution can significantly reduce the number of PCI DSS requirements applicable to a merchant's cardholder data environment. However, it does not completely remove the applicability of PCI DSS in the merchant environment.

Refer to FAQ 1247: Who can use SAQ P2PE?

Can merchants use encryption solutions not listed on the PCI Council's website to reduce their PCI DSS validation effort?

Article 1162 | April 2020

Yes, however, PCI SSC recommends the use of PCI-listed P2PE solutions. Reference to [What effect does the use of a PCI-listed P2PE solution have on a merchant's PCI DSS validation?](#)

Merchants using encryption solutions that are not included on PCI SSC's list of Validated P2PE Solutions should consult with their acquirer or the payment brands about the use of these solutions. See [How do I contact the payment card brands?](#) for information regarding contacting the payment brands.

Is a "P2PE Assessor" required for a merchant's PCI DSS assessment if the merchant uses a Council-listed P2PE solution?

Article 1163 | May 2024

No, merchants using PCI-listed P2PE solutions are not required to engage a P2PE assessor [that is, a P2PE Assessor or P2PE Application Assessor] for their PCI DSS assessments.

Merchants should contact their acquirer (merchant bank) or payment brand(s) directly to understand their PCI DSS validation requirements. See FAQ 1142 How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands) for information regarding contacting the payment brands.

Merchants wishing to engage a QSA for their PCI DSS review can find a list of QSAs on the PCI SSC web site - https://www.pcisecuritystandards.org/approved_companies_providers/qa_companies.php

Is the PCI P2PE Standard applicable for merchants that have developed/implemented their own encryption solution?

Article 1164 | April 2020

Yes. Please see the Frequently Asked Questions (FAQ) for Validation Processes for Merchant-Managed Solutions (https://www.pcisecuritystandards.org/documents/P2PEv2_FAQs_for_Merchant-Managed_Solutions.pdf?agreement=true&time=1467151907161) on the PCI SSC website.

Are P2PE solution providers required to have their solutions validated and listed by the Council?

Article 1165 | June 2016

No.

Please reference FAQ 1158 What effect does the use of a PCI-listed P2PE solution have on a merchant's PCI DSS validation? and Can merchants use encryption solutions not listed on the PCI Council's website to reduce their PCI DSS validation effort? for additional information.

What assurances does the Council provide regarding the quality of organizations assessing my systems for compliance with the PCI standards?

Article 1168 | November 2012

The PCI Security Standards Council (PCI SSC) maintains lists of qualified assessors and has implemented a quality assurance program to ensure that services provided by qualified assessors are of an appropriate level. Completion of in-depth training programs and annual re-certifications is required for security companies seeking to become qualified assessors. Details of our training programs can be found on our Website.

Our list of qualified assessors can be found at:
https://www.pcisecuritystandards.org/approved_companies_providers/index.php

What are the Council's requirements for QSA and ASV Companies to maintain a Quality Assurance (QA) manual?

Article 1169 | October 2012

Companies participating in a PCI SSC program, including QSAs and ASVs, must establish and maintain an internal quality assurance (QA) process as set forth by the individual program's qualification or validation requirements. These QA processes must also be formally documented within an internal QA manual. The Council recognizes that each organization has unique needs and therefore does not mandate specific requirements to be included within an organization's QA manual; however, the following items have been identified as a set of best practices which are expected to be present:

- Company name
- List of PCI SSC programs the company participates in
- Descriptions of job functions or responsibilities
- Identification of QA manual process owner
- Approval and sign-off processes
- Requirements for independent quality review of work product
- Requirements for handling and retention of work papers
- QA process flow
- Distribution and availability of the QA manual
- Evidence of annual review by the QA manual process owner

The QA manual should cover all activities relevant to the particular program. QSAs and ASVs should refer to their respective Validation Requirements and Program Guides for information concerning program-specific requirements.

How does the Prioritized Approach work?

Article 1170 | November 2012

The Prioritized Approach tool is intended to help guide non-compliant entities to work through the process of becoming PCI DSS compliant. The Prioritized Approach does not supersede or replace the PCI DSS; rather, it can help to identify the quickest path a non-compliant entity can take to reduce risk to cardholder data.

The Prioritized Approach focuses on six security milestones to incrementally protect against the highest risk factors and escalating threats. The milestones are structured around six core best practices, as follows:

- Milestone One: If you don't need it, don't store it.
- Milestone Two: Secure the perimeter.
- Milestone Three: Secure applications.
- Milestone Four: Control access to your systems.
- Milestone Five: Protect stored cardholder data
- Milestone Six: Finalize your compliance efforts, and ensure all controls are in place.

As the PCI SSC does not enforce compliance, please check with your acquirer or the appropriate payment card brand to identify how the Prioritized Approach can be used in reporting compliance.

Is the Prioritized Approach mandatory?

Article 1171 | November 2012

The PCI SSC does not mandate the use of any one approach to PCI DSS compliance. The Prioritized Approach is designed as a reporting tool to help entities understand where they can act to reduce risk earlier in the compliance process, and to provide a means to track their progress towards compliance.

In some cases, acquirers (merchant banks) or the payment brands may require use of this reporting tool as part of the payment brands' compliance programs. Organizations should check with their acquirer or payment brand, to determine if the Prioritized Approach reporting tool should be included in their compliance reporting.

Does the Prioritized Approach replace the PCI DSS?

Article 1172 | November 2012

The Prioritized Approach is not a replacement for PCI DSS; rather, it reorganizes the PCI DSS requirements into security milestones, and is designed to help organizations working towards PCI DSS compliance to identify higher-risk requirements and reduce risk to cardholder data earlier in the compliance process. The Prioritized Approach Reporting Tool also provides a means to track an entity's progress towards compliance.

Entities that store, process or transmit payment card data are required to maintain PCI DSS compliance as required by the payment card brands— compliance programs.

How does an organization maintain compliance when a standard changes?

Article 1176 | August 2021

PCI SSC updates its standards to address changes in payment industry threats, risks, and best practices. To ensure organizations have enough time to transition to a new standard, the previous version will remain active for a period of time (typically between 12 and 18 months) after a major version of a standard is published. The period of time will depend on factors such as the volume of changes in a standard and the impact to stakeholders. This ensures a gradual, phased introduction of any updated requirements, and helps to prevent organizations from becoming noncompliant when changes are published. To ensure that organizations can maintain compliance with updated versions of the standards, new requirements may also be phased in with future effective dates. Future-dated requirements are considered best practices until the future date is reached, after which those requirements will be effective and applicable.

Are audio/voice recordings permitted to contain sensitive authentication data?

Article 1210 | June 2025

PCI DSS Requirement 3.3.1 prohibits storage of sensitive authentication data (SAD), including card validation codes and values, after authorization even if the data is encrypted. Storage of card validation codes or values (referred to as CAV2, CVC2, CVV2 or CID) in any form of digital audio recording—for example, .wav or .mp3 files—after authorization is therefore a violation of this requirement.

If SAD is collected during a call, every effort must be made to prevent the data from being recorded. Where technology exists to suppress or redact audio during data entry, it should be enabled.

If it is not possible to prevent SAD from being recorded, the data should be securely deleted immediately upon authorization of the transaction. If secure deletion is not possible due to legitimate technical or business constraints, compensating controls should be implemented to mitigate the risk associated with storing the data. At a minimum, the compensating control process should include:

- Comprehensive risk assessments, annually and upon significant changes to the environment.
- Securing SAD in accordance with applicable PCI DSS requirements.
- Controls preventing SAD access and call recording queries
- Documentation of controls, detailed justifications, risk assessment results, and evidence of compliance

These controls are validated during annual PCI DSS assessments and shared with acquirers/payment brands as needed.

PCI DSS does not override local or regional audio retention laws. Refer to the Information Supplement: Protecting Telephone-Based Payment Card Data for further guidance.

To whom should media inquiries or requests for interviews about the PCI Security Standard Council be directed?

Article 1211 | January 2013

For media inquiries or to request an interview, please send an email message to press@pcisecuritystandards.org.

What is the involvement of the PCI SSC on the compliance validation processes for PCI DSS assessments and scan reports?

Article 1212 | January 2013

While the PCI Security Standards Council (PCI SSC) manages the security standards and provides training for security assessors, we do not enforce compliance or define validation reporting requirements. Compliance validation programs are maintained by the individual payment brands, including requirements on how and who needs to validate compliance. The PCI SSC recommends that entities contact their acquirer and/or the payment brands directly, as applicable, to understand their validation reporting requirements. Please contact the payment brands directly.

Which PCI standards apply to card manufacturers, embossers, card personalizers, or entities that prepare data for card manufacturing?

Article 1214 | January 2024

Organizations that participate in data preparation, manufacturing, personalizing, and/or embossing for plastic cards are considered Card Production Vendors and are typically required to adhere to the Card Production and Provisioning Standards.

Entities should contact the payment brands directly for information about their compliance programs and reporting requirements, and to understand if additional PCI standards apply based upon the specific services they perform. Contact details for the payment brands can be found in FAQ 1142: How do I contact the payment card brands?

What is a PCI DSS Self-Assessment Questionnaire?

Article 1215 | April 2024

PCI DSS Self-Assessment Questionnaires (SAQs) are validation tools for use by SAQ-eligible merchants and service providers to perform and report the results of their PCI DSS self-assessments. There are several different SAQs, developed for specific types of environments as defined in each SAQ's eligibility criteria.

Each SAQ contains a "Completing the Self-Assessment Questionnaire" section, which outlines the type of environment that the SAQ is intended for. All the eligibility criteria for a particular SAQ must be met to use that SAQ.

Additional guidance is also provided in PCI DSS Self-Assessment Questionnaire Instructions and Guidelines, available in the Document Library.

Merchants should consult with their compliance-accepting entity - the entity to which the SAQ will be submitted (typically, an acquirer (merchant bank) or a payment brand) to determine if they are eligible or required to submit an SAQ, and if so, which SAQ is appropriate for their environment.

SAQ D for Service Providers is the ONLY SAQ for SAQ-eligible service providers. All other SAQs are for merchant use only.

Refer to FAQ 1133: Why are there multiple PCI DSS Self-Assessment Questionnaires (SAQs)?

(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/why-are-there-multiple-pci-dss-self-assessment-questionnaires-saqs/)

Does the PCI DSS apply to acquirers?

Article 1216 | January 2013

PCI DSS applies to any entity that stores, processes, or transmits cardholder data and any such entity is expected to comply with PCI DSS, including acquirers. However, each payment card brand manages their own PCI DSS compliance programs that may include, for example, who must validate compliance, merchant and service provider levels, and due dates. At their discretion, payment card brands may require acquirers to validate PCI DSS compliance. For more specific information on PCI DSS compliance validation requirements, please contact the payment brands directly.

Does the PCI DSS apply to issuers?

Article 1217 | January 2013

PCI DSS applies to any entity that stores, processes, or transmits cardholder data and any such entity is expected to comply with PCI DSS, including issuers. However, each payment card brand manages their own PCI DSS compliance programs that may include, for example, who must validate compliance, merchant and service provider levels, and due dates. At their discretion, payment card brands may require issuers to validate PCI DSS compliance. For more specific information on PCI DSS compliance validation requirements, please contact the payment brands directly.

Are compliance certificates recognized for PCI DSS validation?

Article 1220 | August 2023

No. The only documentation recognized for PCI DSS validation are the official form documents from the PCI SSC website. Any other form of certificate or documentation issued for the purposes of documenting compliance to PCI DSS or any other PCI SSC standard are not authorized or validated by PCI SSC, and their use is not acceptable for evidencing compliance. The use of certificates or other non-authorized documentation to validate compliance with PCI DSS requirements according to PCI DSS Requirements 12.8 and/or Requirement 12.9 is also not acceptable.

The PCI SSC website is the official source for reporting templates and forms that are approved by PCI SSC for the purposes of documenting compliance to PCI DSS or any other PCI SSC standard. These include template versions of the Report on Compliance (ROC), Attestations of Compliance (AOC), Self-Assessment Questionnaires (SAQ), and Attestations of Scan Compliance for ASV scans.

Entities that receive certificates or documents that purport to indicate compliance to PCI DSS or other PCI SSC standards, which are not in the form of the above templates available from the PCI SSC website, should request that documentation be provided using the official PCI SSC templates. Any organization issuing, providing, or using certificates or other documents not provided by PCI SSC as an indication of compliance with PCI DSS or other PCI SSC standards must also be able to provide corresponding documentation using the official PCI SSC forms and templates.

To which types of service providers does PCI DSS Appendix A1 for Multi-Tenant Service Providers apply?

Article 1221 | November 2025

All service providers are expected to meet PCI DSS requirements as applicable to the services offered to their customers. In addition, PCI DSS Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers includes requirements specific to multi-tenant service providers, which is a type of third-party service provider (TPSP) that offers various shared services to merchants and other service providers.

Appendix A1 for Multi-Tenant Service Providers applies to service providers with customers in shared services environments, where customers manage their own environment or have administrative control over their own segment.

Multi-tenant service providers offer various shared services to merchants and other service providers, where customers share system resources (such as physical or virtual servers), infrastructure, applications (including Software as a Service (SaaS)), and/or databases. Services may include, but are not limited to, hosting multiple entities on a single shared server, providing e-commerce and/or “shopping cart” services, web-based hosting services, payment applications, various cloud applications and services, and payment gateway and processor services offered in a shared environment. *

It is not the intent that all or even most TPSPs are categorized as multi-tenant service providers. For example, the following are not considered multi-tenant service providers and are not subject to Appendix A1:

- TPSPs that offer a single, unified environment where customers access only their own data through a common platform, and the provider manages all access and infrastructure.
- TPSPs that offer only shared data center services (often called co-location or “co-lo” providers), where equipment, space, and bandwidth are available on a rental basis.
- TPSPs with servers that are dedicated to a single customer.

Note that all other applicable PCI DSS requirements do apply to the above TPSPs.

Whether a service provider is required to validate PCI DSS compliance is determined by the organizations that manage compliance programs (for example, an acquirer, payment brand, or other entity). Entities should always contact the entity that manages their compliance program directly to determine their compliance requirements. Contact details for the payment brands can be found in FAQ #1142: How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands/)

* For additional information and applicable requirements for these TPSPs, refer to PCI DSS Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers.

Does cardholder name, expiration date, etc. need to be rendered unreadable if stored in conjunction with the PAN (Primary Account Number)?

Article 1222 | June 2025

No. Only the Primary Account Number (PAN) must be rendered unreadable when it is stored, in accordance with Requirement 3.5.1. Other elements of cardholder data, such as cardholder name, expiration date, or service code, do not need to be rendered unreadable, even if stored with the PAN.

However, if these elements are stored, processed, or transmitted with the PAN or are otherwise present in the cardholder data environment (CDE), they must be protected in accordance with the PCI DSS requirements applicable to cardholder data.— such as network security controls, access controls, vulnerability management, and other security measures.

Please refer to the “PCI DSS Applicability Information” section of PCI DSS v4.0.1 for more details.

Who are the founders of the PCI Security Standards Council?

Article 1227 | November 2021

The founders of the PCI Security Standards Council are American Express, Discover Financial Services, JCB, Mastercard, and Visa Inc.

What is SAQ C-VT?

Article 1229 | February 2013

SAQ C-VT is a self-assessment questionnaire designed for brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants that process cardholder data via virtual terminals on personal computers connected to the Internet, and that do not store cardholder data on any computer system. This SAQ option is intended to apply only to merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution. SAQ C-VT applies to merchant environments that meet all of the following criteria —

- The only payment processing is done via a virtual terminal accessed by an Internet connected web browser;
- The virtual terminal solution is provided and hosted by a PCI DSS validated third party service provider;
- The PCI DSS compliant virtual terminal solution is accessed via a computer that is isolated in a single location, and is not connected to other locations or systems within the merchant environment (this can be achieved via a firewall or network segmentation to isolate the computer from other systems);
- The merchant's computer does not have software installed that causes cardholder data to be stored (for example, there is no software for batch processing or store-and-forward);
- The merchant's computer does not have any attached hardware devices that are used to capture or store cardholder data (for example, there are no card readers attached);
- The merchant's does not otherwise receive or transmit cardholder data electronically through any channels (for example, via an internal network or the Internet);
- The merchant retains only paper reports or paper copies of receipts; and
- The merchant does not store cardholder data in electronic format.

Merchants using virtual terminal solutions should consult with their acquirer (merchant bank) to determine if they are eligible or required to submit an SAQ, and if so, whether SAQ C-VT is appropriate for their environment.

How does encrypted cardholder data impact PCI DSS scope for third-party service providers?

Article 1233 | March 2026

Where a third-party service provider (TPSP) receives and/or stores only data encrypted by another entity, and where they do not have the ability to decrypt the data, the TPSP may be able to consider the encrypted data out of scope if the TPSP has no access to the decryption keys or to the clear-text data.

For more information, refer to PCI DSS v4.x section 4 Scope of PCI DSS Requirements, subsection Use of Third-Party Service Providers.

Refer to FAQ 1086: How does encrypted cardholder data impact PCI DSS scope? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-does-encrypted-cardholder-data-impact-PCI-DSS-scope/)

I have had an external vulnerability scan completed by an ASV - does this mean I am PCI DSS compliant?

Article 1234 | June 2025

PCI DSS Requirement 11.3.2.1 addresses the need for quarterly external vulnerability scans to be performed by a PCI SSC Approved Scanning Vendor (ASV). The ASV will produce a scan report that details the results of the vulnerability scan — this scan report is not an indication that any other PCI DSS requirements have been reviewed or are in place.

ASVs are required to provide scan reports on official templates as defined in the ASV Program Guide. Any additional documentation provided by the ASV (for example, certificates, letters or other documentation) should be clearly identified as supplemental materials provided by the ASV Company - these supplemental materials have not been endorsed by the PCI SSC, nor should they be considered replacements for the official PCI SSC templates and forms.

Quarterly ASV scan reports, in addition to providing evidence of meeting a PCI DSS requirement, may also be requested by acquirers and/or payment brands. Entities should consult with the organization(s) that manage the entity's compliance program (such as payment brands and acquirers), also called compliance-accepting entities, to understand any specific reporting requirements.

If a merchant or service provider has internal corporate credit cards used by employees for company purchases like travel or office supplies, are these corporate cards considered "in scope" for PCI DSS?

Article 1235 | February 2013

PCI DSS applies to any entity that stores, processes, or transmits cardholder data. Whether entities with cardholder data on their own corporate cards need to validate compliance is determined by each payment brand individually. Depending on the marks on those corporate cards, please contact the applicable payment brands directly.

Can a QSA that is not also a P2PE Assessor validate an encryption solution meets P2PE Requirements?

Article 1246 | May 2024

No. Only P2PE Assessors are qualified by the PCI Security Standards Council to evaluate P2PE Solutions, P2PE Components and P2PE Applications. Note that only a P2PE Assessor is qualified to evaluate P2PE Solutions (including Merchant-Managed Solutions) and P2PE Components, while a P2PE Application Assessor is additionally qualified to evaluate P2PE Applications.

Who can use SAQ P2PE?

Article 1247 | September 2020

SAQ P2PE is intended for SAQ-eligible merchants or merchant environments (as determined by the individual payment card brands), that process cardholder data only via a validated PCI-listed P2PE solution. Whether a merchant is eligible to use an SAQ is determined by the individual payment card brands and/or merchant acquirers. Merchants wishing to use SAQ P2PE must meet payment brand requirements for using an SAQ, and must also confirm that they:

- Are using a validated * PCI P2PE solution (per the PCI P2PE Program Guide).
- Do not store, process, or transmit any cardholder data on any system or electronic media (for example, on computers, portable disks, or audio recordings) outside of the payment terminal used as part of the validated PCI P2PE solution.
- Do not store any cardholder data in electronic format. This includes verifying that there is no legacy storage of cardholder data from other payment devices or systems.
- Have implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.

* Expired P2PE solutions are listed on PCI's list of Point-to-Point Encryption Solutions with Expired Validations. These solutions are no longer considered "validated" per the P2PE Program Guide. Because these P2PE solution providers did not renew their listings in accordance with PCI SSC requirements, the validations are therefore expired. Merchants using an expired P2PE solution should check with their acquirer or individual payment brands about their eligibility to complete SAQ P2PE.

In P2PE, how do "hybrid" decryption environments differ from "hardware" decryption environments?

Article 1248 | April 2020

In a hardware decryption environment, all decryption operations are performed only by PCI listed or FIPS approved HSMs.

In a hybrid decryption environment, the decryption of account data is performed on a "Host System", outside of an HSM. The solution provider's decryption environment may consist of multiple Host Systems in one or more locations. When the Host System is required to decrypt encrypted account data received from a POI, the account-data decryption key (DDK) is retrieved from a key store protected by the HSM, then passed to the Host System. The Host System temporarily retains account-data decryption keys (DDKs) in volatile memory for the purpose of decrypting account data. When the DDK reaches the end of its cryptoperiod, it will be erased from memory. These DDKs are the only keys permitted to exist in the clear outside of the HSM and only for the purpose of decrypting account data. All other cryptographic keys, functions and key management operations must still occur within the secure cryptographic devices (HSMs).

In both hardware and hybrid decryption environments, all HSMs used in the solution must be approved to either FIPS140-2 (or 140-3) Level 3 or higher, or to PTS HSM. Refer to the P2PE Standard for further information.

What is the process to use previously-deployed POI devices in a PCI P2PE Solution?

Article 1251 | April 2020

(Note the term "solution provider" below can be used interchangeably with "component provider," depending on the entity managing the POI devices.)

Please refer to the latest P2PE glossary for definitions of terms used in this FAQ.

This FAQ provides guidance concerning previously-deployed POI devices that can be followed by a P2PE solution provider and a P2PE Assessor as a means to help meet the applicable PCI P2PE requirements.

The P2PE standard contains various requirements regarding the establishment and enablement of POI devices in merchant locations for use in a validated P2PE solution. If these requirements are not specifically adhered to, it may be difficult or impossible for a P2PE Assessor to verify the applicable requirements in P2PE Domains 1, 2, and 5 have been satisfied, especially when the POI devices were deployed either without knowledge of the requirements and/or prior to a P2PE assessment. POI devices already deployed as part of a PCI-listed P2PE v2 solution that are being assessed to the current P2PE Standard should still adhere to this guidance, though, the effort and/or concern is likely minimal.

P2PE solution providers should engage a P2PE Assessor as soon as possible to assess the status of the previously-deployed POI devices. The P2PE Assessor can assess the solution provider's documented processes for POI deployment and note any potential deficiencies requiring remediation.

The following table depicts various scenarios and associated guidance for both a P2PE solution provider and a P2PE Assessor.

"NOTE: It is acceptable for the POI devices to retain the necessary keying material to facilitate remote loading (including firmware loading and remote key injection.) If, however, there is any indication there has been a compromise of these keys or the firmware itself, the POI devices must be sent back for re-initialization."

SCENARIO

PROCESS

NEW P2PE ASSESSMENTS

A P2PE Assessor has been engaged to perform an initial assessment of a solution provider's new P2PE solution. There are POI device type(s) that need to be assessed that have already been deployed to merchant locations.

The P2PE solution provider engages a P2PE Assessor to assess their solution as required by the PCI P2PE Standard and Program Guide.

- If the P2PE Assessor determines the applicable P2PE requirements regarding the previously-deployed POI devices have been satisfied, the P2PE Assessor will document the P-ROV accordingly, which per the P2PE Program Guide, can be submitted to the PCI Council upon completion of a successful P2PE assessment.

- If the solution provider lacks sufficient evidence to verify the applicable P2PE requirements have been satisfied (as determined by a P2PE Assessor during the course of a P2PE assessment), then all firmware, cryptographic keysNOTE, configurations, and software must be reloaded into the POI devices in accordance with applicable P2PE requirements. At this point, the P2PE Assessor can reassess the applicable requirements.

ADDING A NEW MERCHANT WITH THE SAME POI DEVICE TYPES TO A PCI-LISTED SOLUTION

A solution provider with a PCI-listed P2PE solution wants to add a merchant that has already deployed POI devices of the same POI device type as those approved for use in their P2PE solution (as shown as device dependencies on the P2PE approval listing).

The P2PE solution provider follows their documented processes that were assessed previously as part of their P2PE solution assessment.

- If the applicable P2PE requirements regarding the previously-deployed POI devices have been satisfied, the results must be documented by the solution provider and retained for future review.
- If the solution provider lacks sufficient evidence to verify the applicable P2PE requirements have been satisfied, then all firmware, cryptographic keysNOTE, configurations, and software must be reloaded into the POI devices in accordance with applicable P2PE requirements.

ADDING A NEW MERCHANT WITH DIFFERENT POI DEVICE TYPES TO A PCI-LISTED SOLUTION

A solution provider with a PCI-listed P2PE solution wants to add a merchant that has already deployed POI devices of a different POI device type as those approved for use in their P2PE solution.

- The solution provider must engage a P2PE Assessor. The P2PE Assessor must follow the P2PE Program Guide Change process to add the new POI device type(s) to the associated PCI P2PE listing.
- The P2PE solution provider follows their documented processes that were assessed previously as part of their P2PE solution assessment.
- If the applicable P2PE requirements regarding the previously-deployed POI devices have been satisfied, the results must be documented by the solution provider and retained for future review.
- If the solution provider lacks sufficient evidence to verify the applicable P2PE requirements have been satisfied, then all firmware, cryptographic keysNOTE, configurations, and software must be reloaded into the POI devices in accordance with applicable P2PE requirements.

Do all PCI DSS requirements apply to every system component?

Article 1252 | July 2025

PCI DSS requirements apply to all system components, unless it has been verified that a requirement is not applicable for a particular system. Decisions about the applicability of PCI DSS requirements are not to be based on an entity's perception of the risk of not implementing the requirement. Organizations may not choose which PCI DSS requirements they want to implement, and risk assessments cannot be used as a means of avoiding or bypassing applicable PCI DSS requirements.

The applicability of specific PCI DSS requirements to a particular system will vary according to the function of that system. For example, PCI DSS Requirements 3.5 - 3.7 for the secure storage of cardholder data would not be applicable to systems that do not store or manage the storage of cardholder data. It would also have to be verified that the system does not have any access to stored cardholder data, cryptographic keys, or the encryption/decryption mechanisms for those requirements to be considered "not applicable" for that system.

In another example, PCI DSS Requirement 2.3.1 for securing wireless technologies would not apply to a system component that was verified as not having any wireless technology.

Some PCI DSS requirements may also be applied at the network level rather than on every system. For example, requirements for intrusion-detection and/or intrusion-prevention systems to monitor traffic in the CDE may be implemented at the network level rather than on every system in the environment. The assessor would need to verify that the network-level control provides coverage for all systems to which the requirement applies.

Determining that any PCI DSS requirement is not applicable to a system must be verified and supported with documented evidence. Any controls used to reduce the applicability of PCI DSS requirements (for example, controls to ensure a system component cannot access cardholder data) must also be verified to be implemented properly and working as intended.

Does hashing of passwords meet the intent of PCI DSS Requirement 8.3.2?

Article 1253 | July 2025

Yes. Using strong cryptography to hash the password meets the intent of the PCI DSS Requirement 8.3.2, which requires that all authentication factors be rendered unreadable during transmission and storage using strong cryptography.

This requirement is designed to prevent unauthorized access to these authentication factors, both in storage and as they traverse the network. When implemented properly, hashing ensures that passwords cannot be easily recovered or misused, even if the data is compromised.

Please refer to the PCI DSS Glossary of Terms, Abbreviations, and Acronyms for additional information on hashing.

Can I report on my Prioritized Approach progress instead of producing a Report on Compliance or Attestation of Compliance?

Article 1257 | August 2013

The PCI SSC does not manage the process for reporting PCI DSS compliance. Please check with your acquiring bank or payment card brands for this information.

Does PCI SSC endorse specific products to meet PCI DSS requirements?

Article 1258 | August 2013

PCI SSC does not endorse or approve specific security products, such as firewalls, anti-virus software, or web application firewalls, that may be used to help meet PCI DSS requirements. Wherever such products are used to meet PCI DSS requirements, they must be able to meet the specified requirements in full, as well as other applicable PCI DSS requirements (for example, authentication of users and administrative personnel, audit logging, etc.).

Since PCI SSC is not present to assess different environments, we cannot determine whether implementations of specific solutions or products meet PCI DSS requirements. For information on how PCI DSS applies to a specific solution or product implementation, please consult with a Qualified Security Assessor for assistance.

It should be noted that no single product can provide PCI DSS compliance or replace the need for organizations to validate their PCI DSS compliance. Organizations should consult with their acquirer (merchant bank) or the payment brands directly to understand their PCI DSS compliance obligations.

Can I combine sections from different versions of the PCI DSS?

Article 1265 | May 2015

No. When validating compliance, either through a Report on Compliance (ROC) or a self-assessment questionnaire (SAQ), requirements should not be "combined" from two versions of the standard ? validation must be to one version in its entirety.

When the PCI DSS is updated, it is understood that organizations may need time to complete their transition from a previous version to the current one. During this transition, their environment may reflect aspects of both versions of the standard. However, when it comes to reporting and validating compliance, only one version can be used.

As always, entities with specific questions about how to report their compliance validation should consult with their acquirer (merchant bank) or payment brand, as applicable..

If an entity is in the middle of a PCI DSS assessment when a new version of the standard is released — should the assessment be started again using the new version?

Article 1266 | March 2023

Entities should always contact their acquirer or the payment brands directly for information about their compliance programs and reporting requirements. Contact details for the payment brands can be found in FAQ #1142 How do I contact the payment card brands?

As clarifications and additional guidance provided in updated PCI DSS versions may facilitate the implementation of requirements and address current threats, organizations are strongly encouraged to complete their transition to the most current PCI DSS version as early as possible.

Also refer to the following related FAQs:

-

FAQ 1564: How does an entity report the results of a PCI DSS assessment for new requirements that are noted in PCI DSS as best practices until a future date?

-

FAQ 1563: What should an entity do if its PCI DSS assessment will not be complete prior to that standard's retirement date? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-should-an-entity-do-if-its-pci-dss-assessment-will-not-be-complete-prior-to-that-standard-s-retirement-date/)

-

FAQ 1328: Where can I find the current version of PCI DSS? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/where-can-i-find-the-current-version-of-pci-dss/)

-

FAQ 1565: Does an entity's PCI DSS assessment result expire when the standard against which the entity was assessed is retired?

Are merchants required to meet PCI DSS Requirement 12.9?

Article 1277 | June 2014

PCI DSS Requirement 12.9 applies only if the entity being assessed is a service provider. Merchants and other entities that use service providers should review PCI DSS Requirement 12.8 and its sub-requirements, as this is where the controls for managing service provider relationships are defined. Requirement 12.9 provides a corresponding control for service providers to support their customers' need to meet Requirement 12.8.2.

Requirement 12.9 therefore does not apply to merchants, and should be marked "N/A" for a merchant's PCI DSS assessment.

Can card verification codes be stored for card-on-file or recurring transactions?

Article 1280 | October 2023

No. It is not permitted to retain card verification codes once the specific purchase or transaction for which it was collected has been authorized. Card verification codes are typically used for authorization in card-not-present transactions. PCI DSS does not prohibit the collection of card verification codes prior to authorization of a specific purchase or transaction.

A card verification code (also referred to a CAV2, CVC2, CVN2, CVV2, or CID, depending on the payment brand) is the 3- or 4- digit number printed on the front or back of a payment card. —These values are considered sensitive authentication data (SAD), which, in accordance with PCI DSS Requirement 3, cannot be stored after authorization*.

Card verification codes are not needed for card-on-file or recurring transactions (for example, for a recurring gym membership payment), and PCI DSS prohibits storage for these purposes. PCI DSS also prohibits storage of card validation codes for concierge-style services, where cardholder details are retained by an entity to facilitate potential future transactions on behalf of a consumer (for example, for making restaurant reservations or purchasing theatre tickets).

All card verification codes must be completely removed from the entity's systems to comply with Requirement 3. The requirement that prohibits retaining sensitive authentication data after authorization applies even if that data is encrypted. Any service or process that claims to "remove" card verification codes from storage, yet is able to retrieve them for future authorization, would need to be assessed (for example, by a QSA or ISA), to confirm that all card verification codes have been truly removed from the entity's systems and are not being stored in any way, shape, or form.

It should also be noted that it is not permissible to store card verification codes regardless of any permission the entity may have received from their customer to store the sensitive authentication data on their behalf. A customer's request or approval for an entity to retain a card verification code has no validity for PCI DSS and does not constitute an allowance to store the data.

Merchants and their service providers should contact organizations that manage compliance programs, such as their acquirer (merchant bank), the payment brands, or other entity directly, as applicable, for guidance on how to process recurring or card-on-file transactions without requiring transmission or storage of the card verification codes. Contact details for the payment brands can be found in FAQ #1142 How do I contact the payment card brands?

See also the following related FAQs:

FAQ 1574: If an organization provides software or functionality that runs on a consumer's device (for example, smartphones, tablets, or laptops) and is used to

accept payment account data, can the organization store card verification codes for those consumers?

FAQ1533: For PCI DSS, why is storage of sensitive authentication data (SAD) after authorization not permitted even when there are no primary account numbers (PANs) in an environment?

* Only issuers or those companies supporting issuing services with a legitimate issuing business need may store SAD after transaction authorization.

Are point-of-interaction devices required to be physically secured (for example, with a cable or tether) to prevent removal or substitution to meet PCI DSS Requirement 9.5?

Article 1281 | July 2025

No, PCI DSS Requirement 9.5 does not require devices to be fixed in place or physically attached to a surface. Requirement 9.5 and its three sub-requirements address three areas of device security:

- Maintaining an up-to-date list of POI devices,
- Periodically inspecting POI devices to detect tampering and unauthorized substitution, and
- Providing training for personnel in POI environments to be aware of attempted tampering or replacement of POI devices.

Note that Requirement 9.5 applies only to deployed POI devices used in card-present transactions (that is, a payment card form factor such as a card that is swiped, tapped, or dipped).

These requirements do not apply to, but are recommended best practices for:

- Components used only for manual PAN key entry.
- Commercial off-the-shelf (COTS) devices (for example, smartphones or tablets), which are mobile merchant-owned devices designed for mass-market distribution.

Can an entity be PCI DSS compliant if they use a third-party service provider (TPSP) that is validated to a previous version of PCI DSS?

Article 1282 | November 2022

Yes. When a new version of PCI DSS is available and as entities transition to the newer version of PCI DSS there may be situations where an entity relies on a TPSP that is validated to the older PCI DSS version. In this situation, the TPSP's validation must have been completed prior to the retirement of the version of the standard to which they were validated, and their validation must still be current (that is, 12 months have not passed since the service provider's validation).

Entities should always contact their acquirer or the payment brands directly to determine their compliance reporting requirements, including how to report any TPSPs. Contact details for the payment brands can be found in [FAQ #1142 How do I contact the payment card brands?](#)

How do PCI standards apply to organizations that develop software that runs on a consumer's device (for example, a smartphone, tablet, or laptop) and is used to accept payment card data?

Article 1283 | October 2023

If the consumer is also the cardholder and is using the device solely for their own cardholder data entry, and the software is only used by that cardholder using his own credentials, then the device is treated similarly to a cardholder's payment card. The consumer's environment in which the software runs is not in scope for the organization's PCI DSS assessment.

Even though the consumer's environment is outside of the organization's PCI DSS scope, the development of the software is in scope, as the software is being developed for the purpose of facilitating a merchant's payment acceptance process. The software should therefore be developed in accordance with industry best practices and applicable PCI DSS requirements — for example, those included in Requirement 6. Additionally, if the software developer stores, processes, or transmits payment account data on the consumer's behalf, then PCI DSS will apply to the developer's environment.

It is recommended that software be developed using the Software Security Framework (SSF) standards (the Secure Software Standard and Secure SLC Standard) as a baseline for the protection of payment account data. Sources of industry guidance for developing mobile applications include ENISA and OWASP, as well as the PCI Mobile Payment Acceptance Security Guidelines for Developers.

For information about whether software that runs on a consumer's device is eligible for listing as Validated Payment Software according to the PCI Secure Software Standard, or whether the software vendors are eligible for listing as a Secure SLC-Qualified Vendor according to the PCI Secure SLC Standard, refer to the Secure Software Program Guide or the Secure SLC Program Guide, respectively, on the PCI SSC website.

Note that, while PCI DSS does not require the use of Validated Payment Software or a Secure SLC-Qualified Vendor, some payment brands may have specific requirements. Entities should contact organizations that manage compliance programs, such as their acquirer (merchant bank) the payment brands, or other entity directly for information about any such requirements. Contact details for the payment brands can be found in FAQ #1142 How do I contact the payment card brands?.

See also the following related FAQ:

FAQ 1574: If an organization provides software or functionality that runs on a consumer's device (for example, smartphones, tablets, or laptops) and is used to accept payment account data, can the organization store card verification codes for those consumers?

Are acquirers considered service providers for the purpose of PCI DSS Requirements 12.8 and 12.9?

Article 1284 | July 2014

Service providers include business entities that are not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This includes organizations providing acquiring services — for example, payment gateways, PSPs, ISOs etc.

However, an entity that acquires a merchant's payment transactions and is defined by a payment brand to be an acquirer is not considered a service provider for that particular merchant's PCI DSS compliance for the purpose of Requirements 12.8.

If the acquirer provides other services to the merchant, for example management of the merchant's payment terminals, then the merchant and acquirer should work together to understand which party is responsible for managing the applicable PCI DSS requirements for the services provided.

Whether acquirers are required to validate PCI DSS compliance, including Requirement 12.9, is determined by the individual payment brands.

Does PCI DSS apply to one-time or single-use PANs?

Article 1285 | November 2021

PCI DSS applies to all primary account numbers (PANs) that represent a PCI SSC Participating Payment Brand. Whether a one-time PAN is in scope for PCI DSS will depend on the particular restrictions around their usage as defined by the payment brands. Entities should contact the applicable payment brand to determine how PCI DSS applies.

Does PCI DSS apply to virtual (electronic-only) PANs?

Article 1286 | November 2021

PCI DSS applies to all primary account numbers (PANs) that represent a PCI SSC Participating Payment Brand. This includes PANs that are only provided electronically (virtual PANs) as well as PANs that correspond to a physical payment card.

If the virtual PAN is also a one-time or single-use PAN, refer to FAQ 1285: Does PCI DSS apply to one-time or single-use PANs?

If an entity uses a third-party service provider (TPSP) that has been validated as PCI DSS compliant, is the entity's assessor required to go onsite to the TPSP's location and retest the PCI DSS requirements?

Article 1290 | February 2024

No. PCI SSC does not require that an entity's assessor go onsite to the entity's TPSP and retest PCI DSS requirements that have already been covered in the TPSP's current PCI DSS assessment.

Refer to the following FAQs:

FAQ 1065: How are third-party service providers (TPSPs) expected to demonstrate PCI DSS compliance for TPSP services that meet customers' PCI DSS requirements or may impact the security of a cardholder data environment? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-are-third-party-service-providers-TPSPs-expected-to-demonstrate-PCI-DSS-compliance-for-TPSP-services-that-meet-customers-PCI-DSS-requirements-or-may-impact-the-security-of-a-cardholder-data-environment/)

FAQ 1312: How is an entity's PCI DSS compliance impacted by using third-party service providers (TPSPs)? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-is-an-entity-s-PCI-DSS-compliance-impacted-by-using-third-party-service-providers-TPSPs/)

FAQ 1576: What evidence is a TPSP expected to provide to customers to demonstrate PCI DSS compliance? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/What-evidence-is-a-TPSP-expected-to-provide-to-customers-to-demonstrate-PCI-DSS-compliance/)

Why is SAQ A-EP used for Direct Post while SAQ A is used for iFrame or URL redirect?

Article 1291 | August 2015

There is a distinct difference in terms of how payment data is accepted between Direct Post & iFrames/redirects, which is why there are different SAQs. In a Direct Post implementation, the merchant website produces some or all of the web page that is used to accept payment data, and then passes it directly to the third-party payment processor. In this implementation, the consumer (cardholder) never leaves the merchant website. Conversely, with a redirect or iFrame, the third-party payment processor produces the webpage that accepts payment data. The merchant website is not directly involved in the acceptance of payment data as this is directly accepted by the third-party payment processor. In these implementations, the consumer leaves the merchant website and goes to the payment processor for payment acceptance and processing.

This data flow is a key difference between the different methods, and is reflected in the eligibility criteria for SAQ A and SAQ A-EP as follows:

-

SAQ A: All elements of the payment page(s) delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s)

- SAQ A-EP: Each element of the payment page(s) delivered to the consumer's browser originates from either the merchant's website or a PCI DSS compliant service provider(s)

Why is there a different approach for Direct Post implementations than for iFrame and URL redirect - what are the technical differences and how do they impact the security of e-commerce transactions?

Article 1292 | August 2015

The way that criminals attempt to hijack card data from e-commerce transactions depends on the way that the merchant's website accepts cardholder data, the difficulty of gaining access to the transaction, and how likely it is that the criminal will receive an ongoing supply of cardholder data. PCI DSS aims to reduce the probability that a criminal can steal cardholder data from a merchant's e-commerce transaction. In the last three years, the industry has seen two types of attacks against merchant websites which do not directly process cardholder data but which work in conjunction with a payment service provider. Typically these merchants completed SAQ A as they believed that all their payment processing was outsourced. Because of the nature of the attacks, the payment card brands and PCI SSC have clarified the conditions where a merchant can legitimately consider processing to be outsourced.

To be eligible for PCI DSS v3 SAQ-A, the e-commerce environment must be fully outsourced such that: "The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s)." A merchant website can either redirect the consumer to a third-party payment page, or embed the third-party payment page in an iFrame. In either method, the main attack a criminal has against this is to change the code on the merchant's website so the consumer is re-directed to the criminal's payment page and not the legitimate payment page — this is commonly known as a "man-in-the-middle" (MITM) attack. The disadvantage for the criminal is that this attack is usually detected reasonably quickly and minimal cardholder data is put at risk. Additionally some payment service providers are developing solutions that help to detect when a MITM attack has occurred and to notify the merchant accordingly.

Alternatively, there are a number of e-commerce acceptance methods where the merchant website generates the payment page used to collect cardholder data before posting it directly from the consumers' browser to the payment processor. The form elements on this page may be created by HTML loaded from the merchant's website or by JavaScript loaded by the consumer's browser from a third party. From the merchant's perspective this is an attractive solution as it gives the merchant greater control over the look-and-feel of the payment page and the payment flow than what is provided in a redirect or iFrame method. The common criminal attack against this scenario is to compromise the payment page by including criminal-provided JavaScript that simply takes a copy of the cardholder data as it is being entered and sends it to a criminal's server. The actual payment flow is not affected, and therefore this attack is very hard to detect and will often provide an ongoing supply of cardholder data to the criminal. It is primarily for these types of environments that the Council developed SAQ A-EP to provide a level of assurance

that the merchant's website was appropriately protected.

The Council understands that the various ways that merchants can make e-commerce transactions is continually evolving. Merchants and QSAs receive often conflicting advice from vendors which can be especially confusing when the difference between using an iFrame and embedding a payment form in a <DIV> appears to be minimal. However, the difference in security is substantial: fully-hosted payment pages and payment pages loaded into an iFrame are resistant to the transparent theft of cardholder data as it is entered by the consumer; techniques such as Direct Post and JavaScript forms are not. The Council is aware that a MITM attack against a redirect or iFrame is viable, but in the payment brands' experience these are detected before significant volumes of cardholder data are lost. The Council is working with Payment Service Providers to encourage tamper-resistance and tamper-detection which will also reduce the viability of a MITM-type attack.

Where merchants or QSAs are unsure whether the correct SAQ to be completed is SAQ A or SAQ A-EP, they are advised to firstly determine whether "The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s)". If any element of a payment page originates from the merchant's website, the implementation is not eligible for SAQ A. If any element of a payment page originates from a non-compliant service provider, the implementation is not eligible for either SAQ A or SAQ A-EP. If it is unclear whether this condition has been met, merchants or QSAs are advised to contact the acquirer or payment brand.

If a merchant's e-commerce implementation meets the criteria that all elements of payment pages originate from a PCI DSS compliant service provider, is the merchant eligible to complete SAQ A or SAQ A-EP?

Article 1293 | June 2014

To be eligible for SAQ A, all elements of the payment pages must only originate from PCI DSS compliant service provider(s), and no single element of a payment page can originate from the merchant's website.

To be eligible for SAQ A-EP, each individual element of the payment page must originate from either the merchant website or from a PCI DSS compliant service provider. If any element of the payment page originates from a source other than the merchant website or the PCI DSS compliant service provider, then the implementation is not eligible for SAQ A-EP.

It should be noted that all eligibility criteria for a particular SAQ must be met in order to use that SAQ. For example, a merchant could have a website where all payment page elements originate from a PCI DSS compliant service provider; however, if the merchant does not also meet all the other eligibility criteria for SAQ A or for SAQ A-EP, then they would not be eligible for either SAQ.

How does PCI DSS apply to payment terminals?

Article 1300 | March 2026

Payment terminals (sometimes referred to as point-of-sales systems, point-of-interaction devices, or payment devices) are physical devices that capture payment card data to process transactions. Because these devices are directly involved in storing, processing and/or transmission of account data, they are part of an entity's cardholder data environment (CDE) and are in scope for PCI DSS.

The PCI DSS requirements applicable to these devices will vary depending on the type of device being used. For example, a more complex point-of-sale system with multiple applications and configuration options would require a greater number of PCI DSS controls than a simple payment terminal that has been locked down and secured by the manufacturer, or one that is connected via a dial-out phone line rather than connecting to a data network.

Merchants should ensure that they are managing their devices per the applicable PCI DSS requirements — for example, PCI DSS v4.x Requirement 9.5 — and that any account data output from the device is suitably protected. Merchants should review the vendor documentation for their payment device to understand if the device needs additional configuration to meet PCI DSS requirements. For example, if the device is configured to output account data in clear text, the merchant will need to implement their own encryption before sending the data over the Internet.

Payment devices must also be reviewed during a PCI DSS assessment to confirm that they are configured properly and that the security functions and settings have not been disabled. For example, the assessor would verify that the terminal has not been configured by the merchant to store sensitive authentication data after authorization.

While PCI DSS does not specify the types of payment devices to be used, some payment brands require the use of PTS-approved devices. Entities should contact the organization that manages their compliance program, such as acquirers, payment brands, or other entity directly for information about any such requirements. The list of PTS-approved devices can be found on the PCI SSC website under 'Products & Solutions Listings (https://listings.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices)'.

See also the following related FAQ:

FAQ 1301: How should payment terminals be considered during a PCI DSS assessment?

How should payment terminals be considered during a PCI DSS assessment?

Article 1301 | August 2023

The PCI PIN Transaction Security (PTS) standards define physical and logical security requirements for different types of payment devices, including PIN-entry devices (PEDs) and other point of interaction (POI) devices. The PTS POI standard protects the PIN, which is the original objective of the PTS standard. Devices approved to PTS with SRED (Secure Reading and Exchange of Data) have additionally been assessed to provide the option to encrypt account data. PCI PTS devices with SRED, when used as part of a PCI-listed Point-to-Point Encryption (P2PE) solution, can facilitate PCI DSS scope reduction for merchants. However, for many PCI PTS devices the use of SRED is optional and this may be controlled by the payment application resident in the payment terminal. These payment applications can be expected to vary based on the merchant, terminal model, acquirer, and region/location. Therefore, unless included as part of a validated PCI P2PE Solution, or assessed against the PCI Secure Software requirements, an assessor should not assume that any payment terminal is encrypting cardholder data without further validation.

While use of PTS-approved payment devices can facilitate PCI DSS compliance, such devices do not by themselves guarantee PCI DSS compliance or reduce the scope of a merchant's cardholder data environment. The boundaries of the cardholder data environment are not affected by the presence or absence of a PTS-approved terminal, and any payment terminal interactions with the merchant's environment are in scope for a merchant's PCI DSS implementation. Payment terminals, regardless of whether they are validated to the PCI PTS POI standard, must be reviewed during a PCI DSS assessment to confirm that payment account data is protected during storage, processing, and transmission; either through encryption within the terminal, or by PCI DSS controls maintained across the interfacing merchant systems.

Often, the payment terminals will be managed by a third party (for example, the merchant's acquiring bank), and not by the assessed entity. Also, a terminal management system (TMS) may be used to manage the terminals and to update software and configurations on those payment terminals. The entity or assessor should determine if a TMS is in use, and if so, which entity is responsible for the TMS and whether the TMS is a connected-to system that needs to be included in scope for the merchant's PCI DSS assessment. The assessed entity should work with the third-party as part of its regular business-as-usual processes to maintain compliance of the payment terminals, and to prepare the appropriate evidence to demonstrate compliance with the applicable PCI DSS requirements to its assessor.

Assessors conducting these assessments are expected to possess sufficient knowledge and experience to conduct technically complex assessments associated with payment devices in the CDE to confirm the applicable PCI DSS requirements are met, or to work with an individual who possesses the required knowledge (for example, an entity employee, employee of a third-party managing the payment

terminals, or another employee of the QSAC).

For all instances where payment terminals are used in the cardholder data environment (CDE), the assessor is expected to include those payment terminals in the PCI DSS assessment. Where there are large numbers of payment terminals in the population being tested, the assessor may choose to select samples, as long as they are representative samples of the population that include all payment terminal types, locations, acquirers, and payment applications used.

The following activities can be performed to determine if cardholder data is being output in the clear from the payment terminal:

- Capture network traffic from the payment terminal during test transactions,

- Capture traffic from the payment terminal to any attached systems (for example, cash registers or point-of-sale systems).

In addition, the assessor should perform the following:

- Confirm that the payment terminals are included in the merchant's inventory of POI devices and that they are configured in accordance with vendor instructions, including that vendor default passwords are changed (Requirement 2).

- Confirm that any cardholder data stored by the merchant is rendered unreadable (Requirement 3).

- Confirm that transmitted account data is either rendered unreadable in the payment terminal or in merchant interfacing systems, prior to transmission (Requirement 4).

- Determine which applications are installed on the payment terminal.

- Confirm that the device and installed applications are still supported by the vendor(s), and that vendor-supplied security patches/updates have been applied (Requirement 6).

- Confirm that multi-factor authentication is in place for any access in to the CDE, including for remote access to the payment terminals and the TMS, as applicable (Requirement 8).

- Confirm that any payment devices used in card-present transactions and that capture payment card data via direct physical interaction with a payment card are protected from tampering and substitution (Requirement 9).

Where the payment terminals are managed by a third-party (for example, via a TMS), the assessor should also confirm with the third-party which of the above bullets they are responsible for, and which are the responsibility of the merchant.

Assessors should be familiar with PCI standards related to security of payment terminals, security of payment applications residing in the payment terminals, and payment solutions that include secure payment devices, cryptographic processes, and solution provider management processes, and have a good understanding of how compliance with these standards can facilitate compliance with applicable PCI DSS requirements. These PCI standards include PIN Transaction Security (PTS) Point-of-Interaction (POI), Secure Software, and Point-to-Point Encryption (P2PE). The lists of devices and solutions for these standards can be found at:

- Approved PIN Transaction Security (PTS) Devices
(https://listings.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement?return=%2Fassessors_and_solutions%2Fpin_transaction_devices)

- Validated Payment Software
(https://listings.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement?return=%2Fassessors_and_solutions%2Fpayment_software)

- Point-to-Point Encryption (P2PE) Solutions
(https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions)

It should be noted that while PCI DSS does not require the use of PTS-approved devices, some payment brands have requirements for the use of PTS-approved devices. Entities should contact their acquirer or the payment brands directly for information about any such requirements. Contact details for the payment brands can be found in FAQ #1142 How do I contact the payment card brands?.

How does use of an expired PTS device affect my PCI DSS compliance?

Article 1302 | March 2020

While PCI DSS does not require that PCI PTS-approved devices be used, some payment brands have their own requirements for using PTS-approved devices, including whether PTS devices with expired approvals may be purchased or used beyond the expiry date. The impact of using expired PTS devices should be discussed with the merchant's acquirer or the payment brand.

When implementing a new payment device, merchants are encouraged to review the PCI PTS listing to determine whether the device is approved to PTS and when the approval expires. Click [here](https://listings.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement?return=%2Fassessors_and_solutions%2Fpin_transaction_devices) to see list of PTS-approved devices and their expiry dates (https://listings.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement?return=%2Fassessors_and_solutions%2Fpin_transaction_devices). Note that devices with expired approvals may not be able to withstand the latest generations of attacks. Entities using expired devices should contact their acquirer or payment brand. Contact details for the payment brands can be found in FAQ #1142: How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands)

To which devices does PCI DSS Requirement 10.4.2 apply?

Article 1304 | July 2025

PCI DSS Requirement 10.4.1 defines several events and system types that require daily log reviews, but Requirement 10.4.2 allows the organization to determine the log review frequency for all other in-scope events and systems that do not fall under Requirement 10.4.1.

For some environments, all in-scope systems could fall under the system categories defined in Requirement 10.4.1, meaning that daily log reviews are required for all in-scope systems. In other environments, there may be systems that are considered in scope, but which do not meet the bullets specified in Requirement 10.4.1. Some examples could be stock-control or inventory-control systems, print servers, or certain types of workstations.

Requirement 10.4.2.1 specifies that the frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.

How do individuals obtain examination accommodation or adjustments for PCI SSC programs?

Article 1305 | November 2025

Individuals with a physical or mental impairment, or a limitation described as a disability under the Americans with Disabilities Act (ADA) or other applicable law, may request examination accommodations or adjustments for any program organized by the PCI Security Standards Council (PCI SSC). Click [here](https://www.pcisecuritystandards.org/wp-content/uploads/2025/11/Examination_Accommodation_Request_Form_ver1.pdf) (https://www.pcisecuritystandards.org/wp-content/uploads/2025/11/Examination_Accommodation_Request_Form_ver1.pdf) to download the Examination Accommodation Request Form (https://www.pcisecuritystandards.org/wp-content/uploads/2025/11/Examination_Accommodation_Request_Form_ver1.pdf).

Are PCI Forensic Investigators (PFIs) permitted to enter into retainer-type agreements with merchants and service providers?

Article 1306 | April 2017

PCI Forensic Investigators (PFIs) are required to use independent judgment in performing PFI investigations for entities which have been subject to compromise or where a compromise is suspected. It is of paramount importance that PFIs are not subject to any influences that may affect their independent judgment.

It is permissible for an entity to have a PFI on a retainer-type contract, in readiness to provide a rapid incident response, providing that all of the PFI Program independence requirements continue to be met.

PFIs must adhere to the independence requirements documented in Section 2.3 of the PFI Qualification Requirements

How can an entity ensure that hashed and truncated versions cannot be correlated?

Article 1308 | June 2025

PCI DSS Requirement 3.5.1 states that if hashed and truncated versions of the same PAN, or different truncation formats, are present in the environment, additional controls must be implemented to prevent correlation.

The simplest solution is not to store both hashed and truncated PANs. If both must be retained, the following controls can help:

- Use of strong, unique, secret salts for hashing
- Separate storage systems for hashed and truncated values, isolated with segmentation, and distinct access controls
- Preventing cross-references or database links between values
- Real-time monitoring to detect correlation attempts

These are examples only. Controls should be suitable for the environment and ensure that full PAN reconstruction is not possible.

As per the guidance listed in PCI DSS implementing keyed cryptographic hashes with associated key management processes and procedures in accordance with Requirement 3.5.1.1 is a valid additional control to prevent correlation.

Are entities allowed to request that cardholder data be provided over end-user messaging technologies?

Article 1310 | August 2025

PCI DSS does not prevent the use of end-user technologies (such as email, SMS, chat, etc.) to request or receive cardholder data. However, if an end-user messaging technology is used to receive or send PAN, then that entity's channel must be protected according to all applicable PCI DSS requirements, including but not limited to Requirements 4.2.1 and 4.2.2. Additionally, the entity's systems related to end-user technologies (for example, e-mail servers) would be in-scope for PCI DSS.

Also refer to the following FAQs:

FAQ 1085: Can unencrypted PANs be sent over e-mail, instant messaging, SMS, or chat?

(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/can-unencrypted-pans-be-sent-over-e-mail-instant-messaging-sms-or-chat/)

FAQ1157: What should a merchant do if cardholder data is accidentally received via an unintended channel?

(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-should-a-merchant-do-if-cardholder-data-is-accidentally-received-via-an-unintended-channel/)

Are PFI Companies which are "in remediation" permitted to perform investigations?

Article 1311 | December 2014

Yes, "In Remediation" status indicates that a PFI organization has elected to participate in the PFI Remediation Program, after determination by the PCI SSC Quality Assurance review team that the organization did not meet all applicable program requirements. PFIs "In Remediation" are permitted to perform PFI Investigations in accordance with the PFI Program Guide and may be actively seeking to do so with the objective of successfully completing remediation.

For additional information regarding the status of a specific PFI organization, please contact that organization's Primary Contact as listed on the PCI SSC website. For general information about remediation, please contact the PCI SSC Program Manager at pfi@pcisecuritystandards.org.

How is an entity's PCI DSS compliance impacted by using third-party service providers (TPSPs)?

Article 1312 | February 2024

When an entity (the TPSP customer) uses one or more TPSPs for functions within or related to the customer's cardholder data environment, it will impact the customer's PCI DSS compliance, specifically with PCI DSS Requirement 12.8 and with any PCI DSS requirements the TPSP is meeting on the customer's behalf.

In all scenarios where a TPSP is used, the customer must manage and oversee all their TPSP relationships and monitor the PCI DSS compliance status of their TPSPs in accordance with Requirement 12.8. This includes performing due diligence, having appropriate agreements in place, identifying which requirements apply to the customer and which apply to the TPSP, and monitoring the compliance status of TPSPs at least annually. Requirement 12.8 does not specify that the customer's TPSPs must be PCI DSS compliant, only that the customer monitors their compliance status as specified in the requirement. Therefore, TPSPs do not need to be validated as PCI DSS compliant for the customer to meet Requirement 12.8.

However, if a TPSP provides a service that meets a PCI DSS requirement(s) on behalf of the customer, then those requirements are in scope for the customer's assessment and the TPSP's compliance of that service will impact the customer's compliance. For example, if a customer engages a TPSP to manage their network security controls, and the TPSP does not provide evidence that it meets the applicable PCI DSS requirements in PCI DSS Requirement 1, then those requirements are not in place for the customer's assessment. As another example, TPSPs that store cardholder data on behalf of customers need to meet the applicable requirements related to access controls, physical security etc., for their customers to consider those requirements in place for their assessments.

Whether a TPSP is required to undergo a PCI DSS assessment is determined by organizations that manage compliance programs (for example, an acquirer, payment brand, or another entity). Entities should contact the organization that manages their compliance program directly to understand the requirements for TPSPs. Contact details for the payment card brands can be found in FAQ #1142: How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands/)

Refer to FAQ 1576: What evidence is a TPSP expected to provide to customers to demonstrate PCI DSS compliance? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/What-evidence-is-a-TPSP-expected-to-provide-to-customers-to-demonstrate-PCI-DSS-compliance/)

Can SAQ B-IP be used if cardholder data is transmitted over wireless?

Article 1313 | December 2014

SAQ B-IP is intended for merchants who use PCI PTS-approved point-of-interaction (POI) devices that communicate to the payment processor over an IP-based (Internet Protocol) network. The list of PTS-approved devices can be found here (https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php). If a POI device that uses cellular or wireless connections is PTS-approved, and the merchant meets all the eligibility criteria for SAQ B-IP, then SAQ B-IP may be appropriate for that environment. However, merchants should always consult with their acquirer (merchant bank) or the payment brands, as applicable, to determine if their environment is eligible for SAQ B-IP or any other SAQ. Contact details for the payment brands can be found in FAQ #1142.

Each SAQ contains a "Before You Begin" section that provides guidance on the type of environment each SAQ is intended for. Entities must meet all the eligibility criteria for a particular SAQ in order to be eligible to use that SAQ.

Is storage of encrypted cardholder data considered "cardholder data" per the SAQ eligibility criteria?

Article 1314 | January 2015

Yes, encrypted cardholder data is considered cardholder data for the purposes of the SAQ eligibility criteria.

Merchants must meet all the defined eligibility criteria for a particular SAQ in order to use that SAQ. The eligibility criteria for all SAQs, except SAQ D, include an attestation by the merchant that they do not store cardholder data in electronic format. As SAQ D is the only SAQ that includes PCI DSS requirements for protecting stored cardholder data, including encryption and key management requirements, SAQ D could apply to scenarios where only encrypted cardholder data is stored.

Merchants should consult with their acquirer or the payment brands directly (as applicable) to determine which SAQ they should use. Contact details for the payment brands can be found in FAQ #1142 - How do I contact the payment card brands?

See also FAQ # 1086 Is encrypted cardholder data in scope for PCI DSS?

Is storage of truncated PAN considered storage of "cardholder data" per the SAQ eligibility criteria?

Article 1315 | January 2015

An entity that receives and stores only truncated PAN does not need to consider this storage of cardholder data for the purposes of the SAQ eligibility criteria.

Merchants must meet all the defined eligibility criteria for a particular SAQ in order to use that SAQ. Merchants should consult with their acquirer or the payment brands directly (as applicable) to determine which SAQ they should use. Contact details for the payment brands can be found in FAQ #1142 How do I contact the payment card brands?

See also FAQ #1117 Are truncated Primary Account Numbers (PAN) required to be protected in accordance with PCI DSS?

Are merchants required to perform the "Expected Testing" in the SAQs?

Article 1316 | January 2015

Yes. The Expected Testing column of each SAQ provides a high-level description of the types of testing activities that should be performed in order to determine whether a requirement is in place. The individual(s) responsible for performing the self-assessment (that is, the merchant or service provider, or their QSA) is expected to perform these testing activities.

The instructions in the "Expected Testing" column are based on the testing procedures in the PCI DSS, and allows the entity to determine whether the requirement is properly implemented, thus enabling them to accurately complete the SAQ. Refer to the section "Understanding the Self-Assessment Questionnaire" in the applicable SAQ for further guidance.

What is meant by "significant change" in PCI DSS?

Article 1317 | April 2023

There are several PCI DSS requirements that specify performance upon a significant change in an entity's environment. While what constitutes a significant change is highly dependent on the configuration of a given environment, each of the following activities are included under "Significant Change" in the "Description of Timeframes Used in PCI DSS Requirements" section in PCI DSS v4.0:

- New hardware, software, or networking equipment added to the CDE.
- Any replacement or major upgrades of hardware and software in the CDE.
- Any changes in the flow or storage of account data.
- Any changes to the boundary of the CDE and/or to the scope of the PCI DSS assessment.
- Any changes to the underlying supporting infrastructure of the CDE (including, but not limited to, changes to directory services, time servers, logging, and monitoring).
- Any changes to third party vendors/service providers (or services provided) that support the CDE or meet PCI DSS requirements on behalf of the entity.

Each of these activities, at a minimum, have potential impacts on the security of an entity's cardholder data environment (CDE), and must be considered and evaluated to determine whether a change is significant for that entity and in the context of related PCI DSS requirements.

What is the maximum period of time that cardholder data can be stored?

Article 1318 | July 2025

PCI DSS does not define minimum or maximum times for how long cardholder data may be stored. PCI DSS Requirement 3.2.1 specifies that a data retention and disposal policy must be implemented to limit data storage to that which is necessary for legal, regulatory, and/or business purposes. It should be noted that any storage of sensitive authentication data (including full track data, card verification codes/values, and PIN block data) is prohibited after authorization per PCI DSS Requirement 3.3.1.

Wherever cardholder data is stored, it must be protected in accordance with applicable PCI DSS Requirements, including Requirements 3.5 — 3.7 (electronic storage) and 9.4 (storage on physical media). Once cardholder data is no longer required, it must be securely deleted or rendered unrecoverable.

Are merchants allowed to request card-verification codes/values from cardholders?

Article 1319 | June 2025

Yes. Card verification codes/values (e.g., CVV2, CVC2, CID, or CAV2) are commonly requested during card-not-present (CNP) transactions such as e-commerce or mail order/telephone order (MOTO) to help verify that the customer is in possession of the card. Card verification codes/values are normally three- or four- digit code printed on the front or back of a payment card.

These codes/values are considered Sensitive Authentication Data (SAD). PCI DSS Requirement 3.3.1.2 strictly prohibits storing them after authorization — even if encrypted.

Merchants must ensure:

- These codes are collected only when necessary for authorization
- They are never stored post-authorization
- Systems and processes are configured to prevent retention

Who do I report insecure merchant behavior to?

Article 1320 | January 2015

It is recommended that you discuss any concerns you have with the merchant in question. In many cases, once merchants have become aware of issues identified to them by their customers, they have worked to correct the issues.

If working with the merchant directly does not resolve the issue, and you suspect fraud, you should contact your card Issuer (for example, using the phone number provided on the back of the card) and report the possible fraud.

Do parent/subsidiary companies validate as a single entity or as separate entities?

Article 1321 | January 2015

Each payment brand determines their own compliance validation requirements, which may include specific requirements for companies comprised of multiple or separate entities. Organizations should contact their acquirer (merchant bank) and/or the payment brands directly, as applicable, to determine how to validate their compliance. Contact information for the payment brands is in FAQ #1142 How do I contact the payment card brands?.

What are the expiry dates for PTS POI device approvals?

Article 1322 | May 2024

Details regarding PTS-approved POI device expiry can be found in the PCI PTS 'Device Testing and Approval Program Guide,' located in the PCI SSC Document Library (https://www.pcisecuritystandards.org/document_library/).

Whether or not the purchase and use of devices is acceptable beyond their PTS approval expiry date is determined by the individual payment brands. Entities should contact their acquirer or payment brand about the use of devices with expired approvals. Contact details for the payment brands can be found in FAQ #1142 How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands?)

For more information about the use of PTS devices with expired approvals, refer to FAQ #1302 How does use of an expired PTS device affect my PCI DSS compliance? ([https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-does-use-of-an-expired-PTS-device-affect-my-PCI-DSS-compliance/](https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-does-use-of-an-expired-PTS-device-affect-my-PCI-DSS-compliance?)) And FAQ #1434 How do PCI PTS-approved POI device expiry dates affect a PCI-listed P2PE solution? ([https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-PCI-PTS-approved-POI-device-expiry-dates-affect-a-PCI-listed-P2PE-solution/](https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-PCI-PTS-approved-POI-device-expiry-dates-affect-a-PCI-listed-P2PE-solution?))

Are disaster-recovery (DR) sites in scope for PCI DSS?

Article 1323 | March 2015

Whether a disaster-recovery (DR) site is in scope for PCI DSS will largely depend on how the site is configured and used. For example; "hot standby" or "warm standby" approaches, where a DR site contains a live or ready-to-use copy of CDE systems and data, or backups of cardholder data, or other component that impacts the security of cardholder data (such as cryptographic keys), are in scope for PCI DSS.

Alternatively, "cold standby" approaches, where the DR site does not contain any CDE systems or cardholder data and does not connect to the CDE, may be excluded from scope while the DR site is not in use. However, in the event that the DR site is activated, the entity must ensure that the DR site is configured to maintain all applicable PCI DSS requirements for the duration that it is used, and that all cardholder data is securely deleted from the DR site upon completion of its use.

Any testing activity performed on a DR site (for example, to simulate activation of the site) that includes the presence of cardholder data or other component that impacts the security of cardholder data, are also in scope for PCI DSS requirements.

What changes are PFI companies allowed to make to the PFI Reporting Templates?

Article 1324 | May 2020

PCI SSC recognizes that there may be a need for PFIs to personalize the PFI Report Templates, such as adding a company logo or add rows for more detail. However, such changes must be limited per the following:

- Personalization, such as inclusion of corporate logos, must be limited to the title page of the document.
- The format and content of the PFI Report Templates must be maintained with no deletions — the only permitted format change is the addition of rows as needed to facilitate complete and accurate responses. Changes to the order or content of sections, reporting instructions, guidance notes or other static text are not permitted.
- Removal or omission of any static text, including section headers, guidance notes and instructions is prohibited. Where a section or requirement is determined to be not applicable, those sections and/or requirements must remain in the completed PFI reports with any "not applicable" results documented.
- The addition of content, such as legal verbiage or additional reporting, is allowed in a limited manner; such additional content/reporting sections should be treated as addendum sections that are attached at the end of the PFI Report following the appendices. If a PFI would like to include more information than they feel can be included in the allotted space, they must put an addendum reference in the report at the location where expansion is needed, and identify where (in the addendum) that data can be found. Additions of addendum content should be carefully considered, as the affected payment brand(s) have the right to reject such changes.
- PFIs must also ensure that any content added by the PFI is visually evident and discernable from the original PCI SSC Report Template. Any additional reporting must not be duplicated information, but rather, must be additional details that add context or clarification to the responses provided in the main body of the report.

Does PCI SSC provide a "PCI DSS Compliant" logo?

Article 1325 | April 2015

PCI SSC does not issue an official PCI seal, mark or logo that companies can use when they achieve PCI DSS compliance. Please note that the PCI logo is a registered trademark and may not be used without authorization. You may not use the marks PCI Compliant, PCI Certified, PCI DSS Compliant, PCI DSS Certified or PCI with check marks or any other mark or logo that suggests or implies compliance or conformance with our standards. If your company is a member of one of PCI SSC's programs, i.e. PO, QSA, ASV, ISA, or QIR, please contact your Program Manager who can provide a program logo that can be used for members of that program only. Note that authorized use of an applicable PCI logo by a program member is not an indication of that organization's PCI compliance status or an endorsement by PCI SSC.

How does PCI DSS apply to EMVCo Payment Tokens?

Article 1326 | May 2015

Payment Tokens, as defined by EMVCo in the "EMVCo Payment Tokenisation Specification - Technical Framework", are provided to merchants and acquirers in lieu of the cardholder's PAN. They are routed through the payment networks in the same way as a PAN and allow transactions to occur without the merchant being exposed to the underlying PAN.

Payment Tokens must be used in conjunction with a dynamic token cryptogram and/or other sufficient domain controls that are enforced during a payment transaction (as defined by the EMVCo Payment Tokenisation Specification - Technical Framework) to adequately prevent fraud. It is also not feasible to recover the PAN value associated with the Payment Token through knowledge of only the Payment Token, multiple Payment Tokens, or other Payment Token to PAN combinations.

Applicability of PCI DSS to Payment Tokens is described below.

For entities designated by EMVCo as Token Service Providers:

PCI SSC has published Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens), which is intended for Token Service Providers (TSPs) as defined by EMVCo. Within the TSP's token data environment, PCI DSS and the Additional Security Requirements for TSPs apply for the protection of Payment Tokens and payment card data. For more information about TSP requirements and the token data environment, refer to the Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens) and accompanying FAQ.

For all other entities (including merchants and acquirers):

A Payment Token that is defined and used in accordance with the EMV Payment Tokenisation Specification and that exists outside of the Token Service Provider's token data environment is not considered Account Data and is therefore not in scope for PCI DSS.

PCI DSS still applies anywhere Account Data is stored, processed, or transmitted. If any system storing, processing, or transmitting Payment Tokens also stores, processes, or transmits Account Data (such as a PAN), or is connected to systems that store, process or transmit Account Data, those systems remain in scope for PCI DSS requirements.

Please note that while some EMV-compliant chip cards and mobile phones may use Payment Tokens for payment, the use of an EMV-capable terminal or the acceptance of mobile or EMV chip transactions is not an indication that Payment Tokens are necessarily in use. Payment Tokens may be used in multiple types of payment transactions, including from chip cards, mobile devices, and card-on-file services. For more information about Payment Tokens, refer to the EMVCo website — www.emvco.com (<http://www.emvco.com>).

Do PANs need to be masked on cardholder statements sent by issuers to customers?

Article 1327 | August 2022

PCI DSS Requirement 3 is not intended to apply to individual account statements sent by issuing banks to cardholders. Full PAN displays in individual account statements are not required to be masked or rendered unreadable. The reference to "paper reports" in Requirement 3 is intended to apply to back-office reports and other internal paper reports that are not intended for distribution to individual cardholders.

With that said, Issuers should strongly consider masking or truncating PAN on any account statements, whether in paper or electronic form, as the presence of full PAN in addition to other information listed on account statements (such as name, address, telephone number, etc.) could provide a malicious individual with enough information to masquerade as the cardholder.

Issuers with a legitimate business need to display full PAN on account statements can do so, but may wish to contact the payment brands directly to discuss possible alternatives. Contact details for the payment brands can be found in [FAQ 1142 - How do I contact the payment card brands?](#)

Note: The specific sub requirement number(s) and terminology may vary depending on the version of the standard being used.

Where can I find the current version of PCI DSS?

Article 1328 | October 2024

The current version of PCI DSS can be found in the PCI SSC Document Library. All retired versions are also available as archived documents in the Document Library.

Compliance questions, including questions about whether it is acceptable to submit a PCI DSS assessment report for a retired version of that standard, should be directed organizations that manage compliance programs (for example, payment brands and acquirers).

Contact details for the payment brands can be found in FAQ #1142: How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/how-do-i-contact-the-payment-card-brands/)

Also refer to the following related FAQs:

- FAQ 1564: How does an entity report the results of a PCI DSS assessment for new requirements that are noted in PCI DSS as best practices until a future date? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/how-does-an-entity-report-the-results-of-a-pci-dss-assessment-for-new-requirements-that-are-noted-in-pci-dss-as-best-practices-until-a-future-date/)
- FAQ 1563: What should an entity do if its PCI DSS assessment will not be complete prior to that standard's retirement date? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-should-an-entity-do-if-its-pci-dss-v3-2-1-assessment-will-not-be-complete-prior-to-that-standard-s-retirement-date-of-31-march-2024/)
- FAQ 1565: Does an entity's PCI DSS assessment result expire when the standard against which the entity was assessed is retired? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/Does-an-entity-s-PCI-DSS-assessment-result-expire-when-the-standard-against-which-the-entity-was-assessed-is-retired/)
- FAQ 1266: If an entity is in the middle of a PCI DSS assessment when a new version of the standard is released – should the assessment be started again using the new version? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/If-an-entity-is-in-the-middle-of-a-PCI-DSS-assessment-when-a-new-version-of-the-standard-is-released-should-the-assessment-be-started-again-using-the-new-version/)

Can SAQ eligibility criteria be used as a guide for determining applicability of PCI DSS requirements for merchant assessments documented in a Report on Compliance?

Article 1331 | May 2025

Service providers cannot use SAQ eligibility criteria to determine applicability of PCI DSS requirements for assessments documented in a Report on Compliance (ROC). The only acceptable SAQ for service providers is SAQ D for Service Providers. All other SAQs are intended for merchant use only.

Merchants should work with their QSA to fully understand the merchant's environment. If they are able to reach agreement that applying only the requirements included in an SAQ is an acceptable approach to secure that merchant's environment, then that SAQ may be used as a relevant guide for applicability of PCI DSS requirements for that environment. If an environment meets some but not all eligibility criteria for a particular SAQ, then the SAQ should not be considered a relevant guide for applicability of requirements. This approach must be clearly documented by the QSA in "Description of Scope of Work and Approach Taken" section 3.1 of the (ROC).

The assessor will need to perform appropriate testing and validation to verify the non-applicability of any PCI DSS requirements. As an example: If an e-commerce merchant has a webserver using a server-side redirect (for example, HTTP response with a status code 301 or 302) to a PCI DSS compliant third-party payment processor, the assessor could consider requirement 6.4.3 and 11.6.1 as not applicable since the redirection mechanism is not susceptible to script-based attacks.

This approach must be clearly documented by the QSA in "Description of Scope of Work and Approach Taken" section 3.1 of the ROC. Any PCI DSS requirements verified by the assessor to be not applicable should be reported as "Not Applicable" in accordance with instructions in the ROC Template. Assessors should refer to the ROC Template and ROC Template FAQs for the version of the standard being used for relevant guidance.

In all cases, the merchant is still expected to include PCI DSS Requirement 12.5.2 to document and confirm their PCI DSS scope at least once every 12 months. The merchant's assessor is expected to include an assessment of Requirement 12.5.2 and document results in the merchant's ROC. See PCI DSS v4.x "Annual PCI DSS Scope Confirmation" for more details.

Merchants should always consult with the organizations that manage compliance programs (for example, payment brands and acquirers) to confirm their PCI DSS validation and reporting method. If a detailed assessment and ROC is the appropriate method, merchants meeting the eligibility criteria from an SAQ should also confirm that the approach outlined above is acceptable. Contact information for the payment brands can be found in FAQ #1142 How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-d

o-I-contact-the-payment-card-brands)

Is a merchant website still in scope for PCI DSS if it meets all the criteria for SAQ A?

Article 1332 | July 2015

Yes. The merchant web server must be included in scope so the assessor can examine its configuration and verify the redirection mechanism used. Once verified, the applicable requirements will then need to be implemented. If the merchant environment and web server redirection meet all criteria for SAQ A, then the minimum applicable requirements can be considered as those within that SAQ.

See also FAQ 1331 Can SAQ eligibility criteria be used as a guide for determining applicability of PCI DSS requirements for merchant assessments in a Report on Compliance?

(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/can-saq-eligibility-criteria-be-used-as-a-guide-for-determining-applicability-of-pci-dss-requirements-for-merchant-assessments-documented-in-a-report-on-compliance/)

Can PCI DSS compliance be determined by testing only pre-production environments using test data?

Article 1333 | July 2015

No. There are many tests the assessor would be unable to perform in a pre-production or test environment, and it is unlikely that such testing would meet the intent of a PCI DSS assessment.

If an assessment is planned prior to the production environment going 'live', reviewing the pre-production environment may help the assessor gain advance understanding of how the environment will actually function, which may assist with the assessment when the environment is in production. However, the assessor could not complete a PCI DSS assessment nor could they state that all applicable requirements are "in place" until the environment is in use. As an example, the assessor would be unable to confirm whether audit logs are capturing the necessary information if the environment is not operational.

Where can I find unlocked versions of the AOCs and SAQs?

Article 1334 | July 2015

The Self-Assessment Questionnaires (SAQs) and Attestations of Compliance (AOCs) are official validation forms and are not provided in an unlocked format.

If there is a need to include additional information than that permitted by the SAQ/AOC format, entities are encouraged to consult with their compliance-accepting entity (e.g. acquirer or payment brand) to identify a suitable method for providing the information.

Does PCI DSS apply to bank account data?

Article 1335 | June 2023

PCI DSS applies for the protection of cardholder data (primary account number (PAN), cardholder name, service code and expiration date) and sensitive authentication data (full track data from the magnetic stripe or equivalent data on the chip, CAV2/CVC2/CVV2/CID/CVN2, and PIN/PIN block), from a payment card representing a PCI SSC Participating Payment Brand (American Express, Discover, JCB, Mastercard, UnionPay, or Visa).

Bank account data, such as branch identification numbers, bank account numbers, sort codes, routing numbers, etc., are not considered payment card data, and PCI DSS does not apply to this information. However, if a bank account number is also a PAN or contains the PAN, then PCI DSS applies.

It should also be noted that some bank account numbers may contain PAN digits. If the number of included PAN digits is in excess of the truncation formats defined by the particular payment brand (see FAQ 1091), then PCI DSS applies.

Even if PCI DSS does not apply to a particular account number containing elements of PAN, it is strongly recommended that the account number be protected to avoid unauthorized persons from being able to derive the full PAN from the account number.

Refer to FAQ 1091 for more information on truncation formats: What are acceptable formats for truncation of primary account numbers?

What is the difference between POI firmware and additional software that may be present on the POI device?

Article 1338 | September 2015

PTS devices inherently require firmware to function. "Firmware" as defined in the PTS standard is "... any code within the device that provides security protections needed to comply with (PTS) device security requirements or can impact compliance to these (PTS) security requirements. Firmware may be further segmented by code necessary to meet the PTS Core, OP (Open Protocols) or SRED (Secure Reading and Exchange of Data). Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware. Any software intended for use in a P2PE solution that does not meet the PTS definition of "firmware" must be assessed in accordance with the PCI P2PE standard and is subject to all applicable P2PE security requirements. Note that reassessing the PTS firmware as part of the P2PE assessment is not required nor allowed. See also FAQ entitled Are POI devices with only the PTS-approved firmware (i.e., no additional software) eligible for use in a PCI P2PE solution?.

Are POI devices with only PTS-approved firmware (i.e., no additional software) eligible for use in a PCI P2PE solution?

Article 1339 | April 2020

Yes. However, while it may be possible for a PCI POI device to implement all the necessary functionality for use in a P2PE solution solely within its existing PTS-approved firmware, generally the POI device will contain additional software. Any software (whether it has access to cardholder data or not) that is present or intended to be present on the POI device within the P2PE solution that was not included in the PTS-evaluation and approval of the POI device's firmware must be assessed in accordance with the PCI P2PE Standard. Note that it may be possible for additional (non-firmware) software to be present on the POI device during its PTS assessment. However, any software that does not meet the PTS POI definition of firmware is not reviewed as part of the PTS POI assessment or included in the PTS approval. The assessor must be diligent in identifying any non-firmware on the POI device(s). If the POI device contains ANY software that was not included in the POI device's PTS-approved firmware, then that software **MUST** be assessed to the applicable PCI P2PE requirements. See also FAQ 1338 entitled What is the difference between POI firmware and additional software that may be present on the POI device?.

Can sensitive information be redacted from the PCI DSS Attestation of Compliance before it is shared with other entities?

Article 1354 | April 2023

Yes, an entity may redact sensitive information from their PCI DSS Attestation of Compliance (AOC), providing that the resulting document contains, unredacted, all information relevant to the purpose for which the AOC is being shared.

While AOCs are intended to be shared, an AOC might contain sensitive information about the entity's internal environment or security implementation that is not relevant to every organization the entity shares their AOC with. For example, it may not be necessary for a servicer provider's customers to know the city where a data center is located, or details about the technologies present in the service provider's cardholder data environment (CDE). Conversely, details about the scope and services covered by the PCI DSS assessment, the requirements assessed, and the findings of the assessment, are relevant to the service provider's customers and should be included in the service provider's AOC.

Examples of AOC sections that should not be redacted because they include information relevant to the purpose of sharing AOCs include:

-

Section 1: Part 1: Contact Information

-

Section 1: Part 2a: Scope Verification (in Service Provider AOCs)

-

Section 1: Part 2f: Third-Party Service Providers

-

Section 1: Part 2g: Summary of Assessment

-

Section 2: Report on Compliance/Self-Assessment Questionnaire

-

Section 3: Validation and Attestation Details

Sharing the AOC may be preferred to sharing the full Report on Compliance (ROC) or Self-Assessment Questionnaire. However, for the AOC to serve its purpose, the information contained within must provide a meaningful summary of the assessed environment and, in the case of service provider AOCs, clearly identify the services covered by the assessment.

Where information relevant to the services offered is sensitive or confidential, entities may consider having a confidentiality agreement in place so that such information can be shared.

Entities providing a redacted AOC to a payment brand or acquirer for compliance

validation purposes are advised to consult with the brand or acquirer for information about their reporting requirements, because requirements regarding redaction of AOCs can vary. Contact details for the payment brands can be found in FAQ 1142: How do I contact the payment card brands?

See also FAQ #1220: Are compliance certificates recognized for PCI DSS validation?

What does "Duly Authorized Officer" mean?

Article 1356 | June 2023

In the context of PCI SSC-related validation and compliance reports, the intent of requiring a signature from a "duly authorized officer" is to ensure the Company is aware of and has formally signed off on the work being done together with all associated Company liability for that work. A "duly authorized officer" must have authority to legally bind the company for purposes of the report. Although the signatory's job title need not include the term "officer," the signatory must be formally authorized by the Company to sign such documents on the Company's behalf and should be competent and knowledgeable regarding the applicable PCI SSC program and related requirements and duties. Each organization is different and is ultimately responsible for defining its own policies and job functions based on the Company's needs and culture.

Examples of signatories that are not "duly authorized officers" include non-employees, attestants or notaries, and any other individual (whether employed by the Company or not) who either is not authorized to make binding commitments on the Company's behalf and/or are merely attesting to the genuineness of the document or signature by adding their own signature. Signature authority for materials submitted to PCI SSC may not be outsourced to any third party.

This FAQ applies to all PCI SSC programs. Refer to each applicable PCI SSC program guide, available on the PCI SSC website, for any additional context for a duly authorized officer.

Which version of the P2PE Standard should be used for a P2PE assessment?

Article 1358 | May 2024

The latest version of the PCI P2PE Standard is v3.1, September 2021.

Can PCI-listed P2PE v2.0 applications be used in PCI P2PE v3 solutions/components?

Article 1367 | April 2020

Yes. P2PE applications currently listed as a valid PCI P2PE v2.0 application can be used in a PCI P2PE v3 solution or component and must be included as part of the overall solution assessment. The P2PE v2.0 application's listing will retain its existing properties and will still be governed by version 2 of the PCI P2PE Program Guide, including the P2PE application's associated reassessment date .

Can PCI-listed P2PE v3 applications be used in PCI P2PE v2 listed solutions/components?

Article 1368 | May 2020

Yes, a PCI-listed P2PE application validated to P2PE v3 can be used as part of a P2PE solution or component validated to P2PE v2. Note that the associated P2PE Program Guide must be used (i.e, in this case the P2PE v3 Program Guide for the P2PE v3 application and the P2PE v2 Program Guide for the P2PE v2 solution/component).

Does PCI P2PE allow for partial assessments of third parties with services that will be used in one or more P2PE solutions?

Article 1369 | May 2020

No. PCI P2PE allows for P2PE component providers to formalize the process of assessing third parties. Therefore, it is not allowable to perform partial P2PE assessments and reuse (for example, via a partial P-ROV) those partial assessments for either P2PE component provider and/or solution provider assessments.

All third parties providing services to P2PE solution providers must be assessed against the P2PE standard. As stated in the PCI P2PE standard: There are two options for third-party entities performing functions on behalf of solution providers to validate compliance:

- Undergo a P2PE assessment of relevant P2PE requirements on their own and submit the applicable P2PE Report of Validation (P-ROV) to PCI SSC for review and acceptance. Upon acceptance, the P2PE component is listed on PCI SSCs list of Validated P2PE Components.

Or:

- Have their services reviewed during the course of each of their solution-provider customers P2PE assessments.

There is considerable information regarding component providers and third parties in the standard, specifically in the section 'P2PE Solutions and Use of Third Parties and/or P2PE Component Providers'.

Is Payment Account Reference (PAR) as defined by EMVCo considered PCI Account Data?

Article 1374 | January 2016

Payment Account Reference (PAR) is a new data element introduced by EMVCo in Specification Bulletin No. 167 January, 2016. PAR is a new data element that is associated with the EMVÆ Payment Tokenisation Specification — Technical Framework. As detailed in the EMVCo Bulletins, PAR is a value that is intended to allow acquirers and merchants to link tokenized transactions to transactions that are based on the underlying PAN. PAR is generated and linked to a PAN (and successor PANs associated with the underlying issuer customer account) and will also be associated with all affiliated Payment Tokens when a PAN is tokenized.

PAR cannot be used to initiate transactions and no authorization, capture, clearing or settlement message can be initiated with PAR alone. The guidelines for PAR also indicate that a PAR value must be generated in such a way as to ensure that it cannot be reverse engineered to obtain a PAN or other PCI Account Data. The data structure of PAR is also intentionally designed to ensure that PAR cannot be confused for PAN, Payment Token or other PCI Account Data.

Based on the underlying EMVCo description of PAR and its intended functions including the underlying guidelines for PAR generation, PAR data is not considered to be PCI Account Data and on its own is not subject to the underlying requirements for protecting PCI Account Data as specified in PCI DSS. PCI DSS still applies anywhere PCI Account Data is stored, processed, or transmitted. If any system storing, processing, or transmitting PAR also stores, processes, or transmits Account Data (such as a PAN), or is connected to systems that store, process or transmit Account Data, those systems remain in scope for PCI DSS requirements.

Can an Attestation of Compliance (AOC) be provided to an assessed entity before the Report on Compliance (ROC) is finalized?

Article 1375 | February 2016

No, an Attestation of Compliance (AOC) cannot be provided to an assessed entity before the Report on Compliance (ROC) is finalized. The AOC must be completed as a declaration of the results of the assessment with the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS). Within "Section 2: Report on Compliance" of the AOC, it is stated that the AOC "reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC)" and there the assessor must provide the date of the assessment documented in the attestation and in the ROC, which again enforces the intent that the ROC is finalized prior to the execution of the AOC.

Can a partial PCI DSS assessment be documented in a Report on Compliance (ROC)?

Article 1382 | August 2024

Yes. Where an entity wants its assessor to conduct a PCI DSS assessment against only a subset of PCI DSS requirements, it is acceptable to document this partial assessment using the Report on Compliance (ROC). The Attestation of Compliance (AOC) is also completed after a PCI DSS assessment to summarize and attest to the results of the assessment.

There are a number of reasons why an entity may want to undergo a partial assessment, including:

- An entity only needs to validate a subset of requirements to their acquirer (for example, using the prioritized approach to validate only certain milestones);
- An entity wants to validate a new security control that impacts only a subset of requirements (for example, a new encryption methodology requiring assessment to PCI DSS Requirements 3 and 4);
- A service provider identifies which PCI DSS requirements are included in the scope of their service offering and only wants those covered in the assessment (for example, a data center hosting provider only wants to validate physical security controls per PCI DSS Requirement 9 for their hosting facility);
- During a Token Service Provider (TSP) engagement, the TSP assessor determines that a partial PCI DSS assessment will adequately address the additional considerations for PCI DSS Requirements 1-12 that affect TSPs.

When documenting such an assessment, the assessor is expected to clearly communicate that testing of all requirements has not been performed by documenting which specific requirements were tested and which were not tested within both the ROC and the AOC.

The PCI DSS ROC Template provides detailed instructions on how to properly define the scope of the assessment, and how to properly document the findings from the testing performed, including the difference between "Not Tested" and "Not Applicable" responses. Accurate documentation of assessment activities performed and related findings provides readers of the report a clear understanding of the report and removes any ambiguity about the scope of the assessment review.

Note that whether a "Not Tested" response can result in PCI DSS compliance is treated differently between PCI DSS v3.2.1 and v4.0 - QSAs must refer to the ROC Template and ROC Template FAQs for the version of the standard being used for relevant guidance.

See also:

FAQ 1473: What is the role of compliance-accepting entities and assessors in determining the applicability of PCI DSS requirements for merchant and service provider PCI DSS assessments?
(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/What-i

s-the-role-of-compliance-accepting-entities-and-assessors-in-determining-the-applicability-of-PCI-DSS-requirements-for-merchant-and-service-provider-PCI-DSS-assessments)

FAQ 1331: Can SAQ eligibility criteria be used as a guide for determining applicability of PCI DSS requirements for merchant assessments in a Report on Compliance? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/can-saq-eligibility-criteria-be-used-as-a-guide-for-determining-applicability-of-pci-dss-requirements-for-merchant-assessments-documented-in-a-report-on-compliance/)

To whom do the PCI Token Service Provider Security Requirements apply?

Article 1383 | April 2016

The PCI Token Service Provider (TSP) Security Requirements are intended for entities that have registered with EMVCo as a Token Service Provider for Payment Tokens. The PCI TSP Security Requirements cover Payment Tokens as defined by EMVCo, and do not address acquiring tokens or other types of tokens. While entities that provide services for acquiring tokens (for example, by tokenizing PAN after it is received from the cardholder during a transaction) may choose to implement the PCI TSP Security Requirements, they are not required to do so.

Entities that are registered as Token Service Providers by EMVCo should confirm their compliance and validation requirements with the applicable payment brand(s).

For more information, refer to the PCI TSP Security Requirements and Frequently Asked Questions for PCI TSP Security Requirements in the PCI SSC Document Library.

What is the difference between 'acquiring tokens', 'issuer tokens', and 'Payment Tokens'?

Article 1384 | April 2016

Each of these types of tokens replace the PAN with an alternative or surrogate value.

Acquiring tokens are created by the acquirer, merchant, or a merchant's service provider after the cardholder presents their PAN and/or other payment credentials. Acquiring tokenization solutions are proprietary and are not based on an industry-standard approach to token generation, format, request or provisioning[1]. Acquiring Tokens cannot be used for new authorizations. They can be used for card-on-file and recurring payments. The PCI Tokenization Product Security Guidelines offers guidance on acquiring tokens.

Issuer tokens, also known as virtual card numbers, are created by issuers and provide the means to reduce risk in specific use cases, including commercial card applications, as well as consumer-oriented services. These tokens resemble the PAN, so merchants and acquirers are unlikely to know that they are using a token[2] .

Payment tokens are created by TSPs that are registered with EMVCo. Payment Tokens and their usage are defined by EMVCo in the EMVCo Technical Framework. Payment Tokens are issued to a cardholder in lieu of a PAN, and the cardholder presents the Payment Token to the merchant when making a purchase. During a Payment Token transaction, the merchant and acquirer do not receive or have access to the corresponding PAN.

[1] U.S. Payments Security Evolution and Strategic Road Map. Developed by the working groups of the Payments Security Taskforce, December 11, 2014.

[2] U.S. Payments Security Evolution and Strategic Road Map. Developed by the working groups of the Payments Security Taskforce, December 11, 2014.

Which types of tokens are addressed by the PCI SSC tokenization documents?

Article 1385 | April 2016

PCI SSC has published a number of documents and supporting FAQs that are each intended for a specific type(s) of tokens. An overview of the documents and the applicability is provided below.

-

Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens) (2015): An additional standard intended for entities designated by EMVCo as Token Service Providers for Payment Tokens. These requirements apply in addition to PCI DSS for the protection of the environment where the Token Service Provider performs tokenization services (token data environment). Assessment and validation against these requirements may be required by payment brands for registered Token Service Providers

-

Tokenization Product Security Guidelines (2015): Technical best practices for the development of tokenization solutions for acquiring tokens. The Tokenization Product Security Guidelines are intended as guidance only; there is no program or validation associated with the guidelines.

-

PCI DSS Information Supplement: PCI DSS Tokenization Guidelines (2011): General guidance on the use of acquiring tokens in the payment industry. These guidelines provide a high-level introduction to tokenization concepts and security considerations, and do not define any technical specifications or implementation requirements. This document is intended as general guidance only.

For more information about types of tokens used in the payment industry, refer to [What is the difference between 'acquiring tokens', 'issuer tokens', and 'Payment Tokens'?](#)

Are OEMs and/or hardware/software resellers considered third-party service providers for PCI DSS Requirements 12.8 and 12.9?

Article 1427 | November 2025

Original equipment manufacturers (OEMs) and equipment resellers may provision equipment initially for the cardholder data environment (CDE), but once the equipment has been provisioned, they may no longer be involved in the day-to-day operation of the product. If the OEM simply provides a product and is not involved in its operation or maintenance, they are not considered third-party service providers (TPSPs) for the purposes of meeting Requirements 12.8 and 12.9.

However, if the OEM or reseller also provides additional ongoing services—such as supporting the ongoing operation of the equipment or software—or has access to their customer's CDE, then they would be TPSPs for their customers and the agreements described in 12.8 and 12.9 would be applicable for the TPSP services being offered.

Refer to the PCI DSS Glossary in Appendix G for the full definition of Service Providers.

How do PCI PTS-approved POI device expiry dates affect a PCI-listed P2PE solution?

Article 1434 | May 2024

For details regarding PTS-approved POI device expiry in regard to the PCI P2PE Standard and Program, refer to the current P2PE Technical FAQs found in the PCI SSC Document Library (https://www.pcisecuritystandards.org/document_library/?category=p2pe).

What is the Council's guidance on the use of SHA-1?

Article 1435 | January 2026

For more information about strong cryptography, refer to the Information Supplement: PCI Cryptography Guidance, available under Guidance Document in the PCI SSC Document Library.

Our document library can be accessed on our website at:
https://www.pcisecuritystandards.org/document_library/

Where do I direct questions about complying with PCI standards?

Article 1436 | December 2022

Each of PCI SSC's Participating Payment Brand members (American Express, Discover, JCB International, Mastercard, UnionPay, and Visa) currently have their own PCI compliance programs for the protection of their affiliated payment card account data. Entities should contact the payment brands directly for information about their compliance programs and reporting requirements. Contact details for the payment brands can be found in FAQ 1142: How do I contact the payment card brands?

Questions regarding compliance and reporting requirements for payment card account data affiliated with other payment networks should be referred to the applicable payment network .

PCI SSC also encourages entities to be aware of potential nuances in local laws and regulations that could affect applicability of the PCI standards.

Can PCI DSS be used to protect non-payment card data?

Article 1437 | August 2016

PCI DSS provides a solid baseline of security requirements that can be used to protect non-payment card data. However, entities should consult with the applicable regulatory body and/or the data owner, as appropriate, to understand the suitability of using PCI DSS requirements to protect the data in question.

How is the payment page determined for SAQ A merchants using iframe?

Article 1438 | September 2016

To be eligible for SAQ A, all elements of the payment page delivered to the consumer's (cardholder's) browser must originate only and directly from a PCI DSS validated third-party service provider(s). The term "payment page" refers to a collection of web elements used to collect and/or process payment card data. Payment pages can exist as a standalone web page or be embedded into another web page using iframe.

An iframe can appear as a section within a larger web page or it could be sized to encompass the entire web page. Where an iframe encompasses the entire web page, all content is typically delivered via the iframe. Where an iframe appears as a section of a larger web page, content is delivered via the iframe and also via the web page on which the iframe resides.

Payment pages can be as simple as input fields collecting payment information, or they could also be used to display additional information, such as the list of items being purchased, shipping information, and promotional materials. All web elements located within the same iframe as elements associated with payment card data are considered part of the payment page.

Where the payment page is embedded within an iframe on a page on the merchant's website, all fields and web elements associated with capturing payment card data must be contained within the iframe to be eligible for SAQ A. If any element involved in the collection or processing of payment card data is present on or provided by the merchant website, the merchant is not eligible for SAQ A.

Web page elements that are unrelated to the capture of payment card data, and that exist on the merchant website outside of the iframe, are not considered part of the payment page. SAQ A may therefore be used where the merchant website delivers content unrelated to the payment process, as long as all elements of the payment page originate from a compliant service provider via an embedded iframe, and all other SAQ eligibility criteria are met.

How do PCI DSS Requirements 2, 6 and 8 apply to SAQ A merchants

Article 1439 | May 2019

Merchants eligible to complete SAQ A are e-commerce or mail-order/telephone-order (MOTO) merchants that outsource all payment processing and do not store, process or transmit cardholder data on their premises or systems. E-commerce merchants eligible for SAQ A include those that completely outsource all website operations, including those using URL redirect or another mechanism that meets SAQ A criteria to redirect consumers to a compliant third party for payment processing.

Where URL redirection mechanisms to third-party payment processing systems reside on merchant-managed websites, those mechanisms must be protected from ongoing threats, such as man-in-the-middle attacks that aim to manipulate URL redirection mechanisms to direct traffic to malicious sites without the consumers' knowledge. For this reason, requirements for changing default passwords (Requirement 2); implementing basic authentication, such as requiring a unique user ID and strong password (Requirement 8); and installing applicable security patches and ensuring critical patches are applied within one month of release (Requirement 6) are included in SAQ A. These requirements are intended to help protect merchant websites from compromise and maintain the integrity of the redirection mechanism.

In a simple e-commerce environment where the merchant webserver contains the mechanism that redirects customers from their website to a third party for payment processing, the merchant will need to validate these requirements for the webserver upon which the redirection mechanism is located.

It is also possible for a SAQ A merchant to have a more complex e-commerce environment, where additional system components (such as application servers, database servers, and web proxies) control or could impact the integrity of the redirection mechanism. In these scenarios, the requirements would apply to all system components comprising or managing the redirection mechanism.

MOTO or e-commerce merchants that have completely outsourced all operations, including all management of their website, may not have any systems in scope for SAQ A and, in such circumstances, these requirements could be considered "not applicable." If a requirement is deemed not applicable, the merchant should select the "N/A" option for that requirement, and complete the "Explanation of Non-Applicability" worksheet in Appendix C for each "N/A" entry.

How does PCI DSS Appendix A2 apply after the SSL/early TLS migration deadline?

Article 1440 | August 2018

Prior to 30 June 2018, PCI DSS v3.2 Appendix A2 applied to all scenarios where SSL/early TLS was used as a security control to protect cardholder data or the cardholder data environment. As of 1 July 2018, SSL/early TLS may only be used as a security control by POS POI terminals that are verified as not being susceptible to known exploits and the termination points to which they connect; Appendix A2 was updated to reflect this in PCI DSS v3.2.1.

While Appendix A2 identifies PCI DSS Requirements 2.2.3, 2.3, and 4.1 as examples of requirements directly affected by the use of SSL/early TLS, applicability of the Appendix is not limited to these three requirements. The impact to all requirements must be considered. For example; per Requirement 8.2.1, strong cryptography must be used to render all authentication credentials unreadable during transmission and storage on all system components. Since SSL/Early TLS does not constitute strong cryptography, it cannot be used to satisfy this requirement except as allowed by POS POI terminal connections.

After 30 June 2018, organizations using SSL/early TLS to meet any PCI DSS requirement, except as allowed by POS POIs and their termination points, must have compensating controls in place to mitigate the risks associated with using SSL/early TLS. Merchants and service providers using SSL/early TLS to meet a PCI DSS requirement for POS POI terminal connections should complete the applicable requirements in Appendix A2. Additionally, because SSL/early TLS is considered an insecure protocol, its allowed use through firewalls must be documented and approved, with security features documented and implemented, in accordance with Requirement 1.1.6. Similarly, the presence of SSL/Early TLS on a system component must be justified in accordance with documented configuration standards per Requirement 2.2.2. If SSL/early TLS is enabled but is not necessary for the function of the system, it must be disabled.

If SSL/early TLS is present but is not being used as a security control, Appendix A2 would not apply. However, the use of SSL/early TLS must still be documented and addressed in accordance with applicable requirements surrounding the presence of insecure protocols.

All organizations are strongly encouraged to replace SSL/early TLS with a strong cryptographic protocol as soon as possible.

Additional guidance can be found in the Information Supplements: Use of SSL/Early TLS and Impact on ASV Scans and Use of SSL/Early TLS for POS POI Terminal Connections, available in the PCI SSC Document Library.

Can merchants using non-console administrative access be eligible for SAQ B-IP, C-VT, or C?

Article 1442 | November 2016

Yes, as long as all SAQ eligibility criteria are met. For example, SAQ B-IP, SAQ C and SAQ C-VT are each intended for environments using only permitted system types, as defined in the eligibility criteria for each SAQ. A brief description for each SAQ is provided below:

- SAQ B-IP: Environments using only PTS-approved point-of-interaction (POI) devices (excludes SCRs). This is the only permitted system type for this SAQ.
- SAQ C-VT: Environments using only web-based virtual payment terminals on a personal computer connected to the Internet. This is the only permitted system type for this SAQ.
- SAQ C: Environments using only payment application systems (for example, point-of-sale systems) connected to the Internet. This is the only permitted system type for this SAQ.

The SAQ criteria is not intended to prohibit more than one of the permitted system types being on the same network zone, as long as the permitted systems are isolated from other types of systems (e.g. by implementing network segmentation). In these types of environments, a merchant may wish to administer a defined system/device from the same type of system/device located within the same network. This would be considered non-console administrative access, and, in this scenario, the PCI DSS requirements for protecting non-console administrative access would apply.

Merchants that do not support non-console administrative access should select "N/A" for the affected requirements and complete Appendix C, as directed in the Before You Begin section of the applicable SAQ.

If any type of system other than that defined by the SAQ criteria is used to administer a SAQ-defined system, the environment would not be eligible for that SAQ. As an example, use of a back-office server to administer a PTS-approved POI device does not meet the eligibility criteria of SAQ B-IP.

What is the intent of the SAQ eligibility criteria?

Article 1443 | November 2016

Each Self-Assessment Questionnaire (SAQ) was created to support a specific type of environment, depending on how the entity stores, processes, and/or transmits cardholder data. All SAQs (except for SAQ D) are intended for merchants with less complex environments, and each SAQ defines specific criteria that must be met in order to be eligible to use that SAQ. For example; SAQ B-IP is intended for environments using only PTS-approved point-of-interaction (POI) devices (excludes SCRs), SAQ C-VT for environments using only web-based virtual payment terminals on a personal computer, and SAQ C for environments using only payment application systems (for example, point-of-sale systems) connected to the Internet. In accordance with payment brand compliance programs, entities that meet all eligibility criteria for a particular SAQ may then assess and validate to the subset of PCI DSS requirements included within that SAQ.

In order for a merchant environment to meet SAQ eligibility criteria, only system types defined in the eligibility criteria may be used in that environment. Additionally, these SAQs explicitly state that the defined system type must not be connected to any other systems, and that segmentation may be used to isolate the permitted system type from all other systems*.

The SAQ criteria is not intended to prohibit more than one of the permitted system types being on the same network zone, as long as the permitted systems are all isolated from other types of systems (e.g. by implementing network segmentation). For example, an environment eligible for SAQ B-IP may have more than one PTS-approved POI device on a network that does not contain any other type of system. Similarly, SAQ C merchants may have more than one point-of-sale system on the same local network.

The intent of this criteria is to ensure that the environment is properly scoped and is suitable for validation against the subset of PCI DSS requirements contained in the SAQ. Environments containing any other types of systems would not be eligible for the particular SAQ, as they would likely be subject to different and/or additional PCI DSS requirements than those included in the SAQ.

Merchants should always consult with their acquirer (merchant bank) or the payment brands directly to determine if they are eligible or required to submit an SAQ, and if so, which SAQ is appropriate for their environment.

* This criteria is not intended to prevent the defined system type from being able to transmit transaction information to a third party for processing, such as an acquirer or payment processor, over a network.

Can a PFI Company perform subsequent PFI investigations for the same entity?

Article 1444 | August 2024

PFI Companies must adhere to the independence requirements of the PFI program as defined in the PFI Qualification Requirements and PFI Program Guide. Whether a PFI Company can conduct a PFI investigation more than once on the same entity will depend on circumstance. For example; if during an investigation the PFI Company carried out work which impacted the PCI DSS compliance status of the entity, and the entity subsequently identifies or suspects a breach, that PFI Company may not be able to satisfy the independence requirements for a subsequent investigation.

Each payment brand has their own rules when a PFI must be engaged, and merchants should consult their compliance-accepting entity (acquirer and/or the payment brands) concerning any issues which may influence a PFI Company's ability to perform an independent investigation, including instances where there is continuation of breach/re-breach after a PFI Final Report has been issued.'

Payment brand contact details are provided in FAQ #1142 How do I contact the payment card brands?

How should QSA assistance with completion of Self-Assessment Questionnaire (SAQs) be documented?

Article 1445 | February 2017

PCI SSC does not define specific reporting requirements for QSAs assisting merchants with Self-Assessment Questionnaires (SAQs).

Before beginning any engagement, the QSA should have a clear understanding of their expected role for the engagement. If the QSA's client is requesting assistance with their self-assessment, the type and level of assistance should be clearly defined and understood by both parties. Similarly, if a merchant's acquirer stipulates that a QSA must be involved in the merchant's self-assessment, the QSA and merchant should confirm with the acquirer what activities the QSA is expected to perform, including the level of testing and documentation, as applicable. For example, the QSA may be requested to provide guidance to help the merchant determine their PCI DSS scope, or assist with interpretation of PCI DSS requirements, or perform testing to validate that controls were in place. It is important that responsibilities are clearly defined for all parties — including the acquirer, merchant, and QSA — and that each party understands their responsibilities in the process.

In all instances, the QSA should clearly document the role they performed in the QSA Acknowledgement section (Part 3c) in the applicable SAQ. Similarly, Part 3d of the SAQ provides the ability for an ISA to document their involvement, if applicable, in the assessment.

What is meant by "At-Risk Timeframe" and at risk referenced in the Final PFI Report?

Article 1448 | September 2024

The At-Risk Timeframe refers to the period of time data elements, such as account data, were at risk for this Entity Under Investigation during the incident under investigation. A data element is considered at risk if evidence indicates the data element was exposed (i.e. per the Final PFI Report template v3.3, Section 3.4 "a data element was accessible to the Entity under investigation or any unauthorized entity, process, source, etc.") during the incident under investigation.

The "At-Risk Timeframe" as identified in the Final PFI Report template, Appendix C refers to the period of time during the incident under investigation when data was vulnerable. For example, consider a scenario where evidence (e.g., system/access logs) indicates that an unauthorized entity breached the cardholder data environment's security controls on 2024-04-14T18:30:00 and was discovered by the breached entity (who subsequently took the system offline to limit the exposure) 2024-04-17T07:15:00.

The at-risk timeframe is considered to have been from 6:30PM on April 14th when the breach occurred, through 7:15AM on April 17th when the breached system was taken offline (approximately 60 hours).

Further considering the scenario above, suppose the breached entity had several years' worth of data elements stored in the environment. In this case, regardless of how many data elements were exposed or how long they were stored, the at-risk timeframe:

- would not date back to the oldest data element stored, and
- only refers to the timeframe itself — the period of time the data elements were at risk (approximately 60 hours in this scenario).

For additional information please contact your case-specific Payment Brand representative.

Is two-step authentication acceptable for PCI DSS Requirement 8.4?

Article 1449 | January 2026

For more information about multi-factor authentication, refer to the Information Supplement: Authentication Guidance, available under Guidance Document in the PCI SSC Document Library.

Our document library can be accessed on our website at:
https://www.pcisecuritystandards.org/document_library/

Where can I find more information about the Assessment Guidance for Non-listed Encryption Solutions (aka NESAs)?

Article 1450 | August 2017

When the Council published the Assessment Guidance for Non-listed Encryption Solutions a document containing multiple FAQs was subsequently published. This document can be retrieved here (https://www.pcisecuritystandards.org/documents/FAQS_Assessment_Guidance_Non-listed_Encryption_Solutions.pdf).

The aim of the Assessment Guidance for Non-listed Encryption Solutions is to provide a consistent approach for evaluating existing non-listed encryption solutions in use by merchant customers, and to reinforce that only PCI P2PE Solutions are tested and validated against the PCI P2PE Standard to provide the strongest protection for card data and reduce PCI DSS compliance responsibilities.

It is important to note that this is guidance only, not requirements. P2PE QSAs can use the guidance to evaluate existing solution providers' non-listed encryption solutions and document their suggested applicable PCI DSS controls for merchants that use these solutions. The aim of a non-listed encryption solution assessment is to identify the gaps between the solution and the PCI P2PE Standard and to show how use of the solution impacts a merchant's PCI DSS assessment.

Can PFIs provide reports to their clients before sending the report to the affected payment brands?

Article 1451 | November 2021

No. It is not acceptable for reports (draft or final) to be issued to clients, acquirers, issuers, or other parties for review/amendment before being sent to payment brands and/or acquirers. PCI Forensic Investigators (PFIs) are obliged under the terms of the PFI Program Guide to provide Preliminary Incident Response Reports and Final PFI Reports to their client, each affected payment brand, and their client's affected acquirer(s). The reports must be sent to all parties (clients, affected payment brands and all affected acquirer(s) identified in Appendix C of the Final PFI Report) at the same time.

Appendix A of the PFI Program Guide describes the provisions PFI Companies must include in their contracts to support the report delivery requirements. Appendix C: Impacted Entities should be broken out into separate lists for each acquirer (if more than one acquirer is involved), with a complete "master list" provided to each affected payment brand.

The judgements, conclusions, and findings in PFI reports must be based solely on the factual evidence obtained during the investigation and reflect the independent judgement, findings, and conclusion of the PFI company. If an amendment is required to a Final PFI Report post-issue, for example to correct a factual error or omission, the amendment must be clearly evidenced in the Table of Changes in the revised report and the report version number incremented appropriately.

How does Triple DEA (TDEA) impact ASV Scan results?

Article 1452 | September 2017

Triple DEA (Data Encryption Algorithm)'also referred to as TDEA, TDES or 3DES'is a cryptographic cipher used in TLS, SSH, IPSec and other protocols and products. TDEA is susceptible to a known vulnerability that is currently ranked as Medium severity by the Common Vulnerability Scoring System (CVSS). As defined in PCI DSS Requirement 11.2.2, vulnerabilities ranked as Medium or High risk by the CVSS must be corrected and the affected systems re-scanned after the corrections to show the issue has been addressed.

ASVs are permitted to re-rank a vulnerability's risk assignment if they disagree with the CVSS (see ASV Program Guide section 6.3.3 'Exceptions to Scoring Vulnerabilities with the NVD'), or if they are able to confirm that the risk level is lower in a particular environment. When making this type of adjustment to the scan report, the ASV should consider the scan customer's unique environment, systems, and controls, and not make adjustments based on general trends or assumptions.

Scan customers are also permitted to dispute the scan findings if they determine a vulnerability was incorrectly reported or if compensating controls or environment-specific factors exist that reduce or eliminate the risk. Refer to ASV Program Guide sections 7.7 "Managing False Positives and Other Disputes" and 7.8 "Addressing Vulnerabilities with Compensating Controls" for details. In all cases, scan customers and ASVs should work together to determine the level of risk that a particular vulnerability may present in a specific environment or configuration.

TDEA has been superseded by the Advanced Encryption Algorithm (AES). Entities using TDEA are encouraged to review their implementations to determine the potential risk that TDEA may present to their environments, and consider transitioning toward a more secure alternative.

Can a PFI Company provide QSA services to an entity after performing a PFI investigation for that entity?

Article 1453 | August 2022

Yes. All PFI Companies are also QSA Companies. A PFI Company may provide QSA Services (as defined in the QSA Agreement) to an entity after performing a PFI investigation for that entity.

However, it should be noted it is highly unlikely the PFI Company could perform a subsequent PFI investigation for the entity (should that become necessary) without violating the independence requirements of the PFI program.

With that being said, compliance programs are managed by the payment brands. PFI Companies should contact the payment brands directly to understand compliance program requirements when asked to provide QSA Services after performing a PFI investigation. Contact details for the payment brands can be found in FAQ #1142?How do I contact the payment card brands?

What is the intent of "administrative access" in PCI DSS?

Article 1454 | October 2017

Accounts with administrative access are those assigned with specific privileges or abilities in order for that account to manage systems, networks and/or applications. As a general rule, the functions or activities considered to be administrative are beyond those performed by regular users as part of routine business functions. For example, activities related to normal processing of card payments and providing customer service would not be considered administrative.

Examples of accounts that are typically considered as administrative include:

- Accounts used for system administration. Depending on the operating system (OS), common names for these accounts might include root, administrator, admin or supervisor.
- Accounts with the ability to make unrestricted, potentially adverse, or system-wide changes.
- Accounts with the ability to install, remove or edit executable files.
- Accounts with the ability to assign or take ownership of sensitive data, system files, and/or programs.
- Accounts with ability to directly access or query databases containing cardholder data – for example, Database Administrators.
- Accounts with the ability to override or change security controls – for example;
- Turn security controls on or off, such as anti-virus software, firewalls, IDS/IPS or audit logs.
- Change or configure security policy settings, such as password policies (session timeouts, password expiry, etc.), role definitions, or firewall rules.
- Change other administrative accounts or passwords, including elevating privileges to administrator-level.
- Maintain logs, including setting log retention periods or changing or deleting logs.
- Alter access permissions to systems and/or data.
- Change cryptographic keys or encryption settings.

In addition to the above, each entity should identify any roles within their organization with elevated privileges that require additional protection. When determining whether an account should be considered administrative, the entity should consider the potential impact if that account is compromised. For example, an application-level account that creates user IDs only within the application, where those user IDs do not impact other systems or applications, might not be considered administrative. Conversely, an account with the ability to create or edit other accounts that themselves perform administrative tasks, or that have access to multiple applications or systems, would be considered administrative.

Some solutions encapsulate administrative access to a system component within a single sign-on solution, such as a remote access portal, that also provides

non-administrative access to other system components. If a single sign-on account provides administrative access to any system component(s), this account would be considered administrative only for access to that system component(s).

Does a QSA need to be onsite at the client's premises for all aspects of a PCI DSS assessment?

Article 1455 | January 2018

Per the QSA Qualification Requirements and QSA Program Guide, "QSA Companies and their QSA Employees" responsibilities in connection with the Program include, but are not limited to— Performing PCI DSS Assessments in accordance with the PCI DSS, including but not limited to— Being on-site at assessed entity during the PCI DSS Assessment.

PCI SSC intends for on-site testing to be the norm, with the majority of PCI DSS assessment testing completed at the physical client location. Though the entire PCI DSS Assessment may not require being on-site, required validation methods like "observe" — meaning the assessor watches an action or views something in the environment — are difficult to complete remotely. Examples of observation subjects include personnel performing a task or process, system components performing a function or responding to input, system configurations/settings, environmental conditions and physical controls.

Ultimately, the QSA is responsible for ensuring that any validation that is performed remotely is reasonably defensible, including that the remote validation is appropriate for the requirement being assessed and for each entity's particular implementation. For example, a QSA may request an onsite physical presence to observe physical security controls, attempting to "open doors," etc. Similarly, in some cases a QSA might have a convincing case for relying on screen shots provided to the QSA by the assessed entity – for example, if the QSA defined the system sample themselves and then directed the assessed entity's employee to specific settings while sharing a screen via conference call. Alternative ways to meet the onsite objective could include QSAs engaging qualified local QSA resources to do onsite visits on their behalf if it is not feasible for the primary QSA to travel to the onsite location, in accordance with the QSA program requirements related to sub-contracting. While most interviews should be conducted on-site, there may be scenarios where doing so may seem unreasonable and unnecessary. For example, it may not be reasonable for a QSA to fly to another country solely to conduct interviews on training in secure coding if the information obtained on-site at the primary and other locations describing the training is consistent with and supported by the answers provided by the employees by phone or video interview.

The QSA is expected to be physically on-site for each PCI DSS Assessment, though the duration of the on-site visit will vary. PCI SSC recognizes that outlier scenarios may exist where validation of individual requirements can be reasonably achieved remotely without on-site visit, but these are expected to be the exception and if such an approach is used, the QSA must be able to sufficiently document and defend why this approach was used for those individual requirements.

Can PCI SSC revoke a QSA Company's eligibility to participate in the Associate QSA Program due to quality concerns in connection with that program, and not revoke qualification as a QSA Company?

Article 1456 | April 2018

Yes. Per the PCI DSS Qualification Requirements for Qualified Security Assessors, PCI SSC reserves the right to revoke AQSA Program qualification or reject any future AQSA Program application from a QSA Company that PCI SSC determines has committed conduct that constitutes a "Violation" for purposes of applicable AQSA Program requirements, including but not limited to failure to meet AQSA Program quality standards or comply with applicable AQSA Program requirements. The period of ineligibility is a minimum of one (1) year, as determined by PCI SSC in a reasonable and non-discriminatory manner.

For example, if PCI SSC determines that a QSA Company failed to provide required resources to support an AQSA in their development with a mentor as required per AQSA Program requirements, under the QSA Qualification Requirements that conduct would constitute a "Violation" and "failure to comply with...applicable Program Qualification Requirements (defined in the QSA Agreement)... or program guides...", and result in Associate QSA Program ineligibility for at least one (1) year.

Are Mobile Payments on COTS (MPoC) solutions, Software-based PIN Entry on COTS (SPoC)[™] solutions, or Contactless Payments on COTS (CPoC[™]) solutions eligible for a P2PE Solution approval?

Article 1457 | April 2024

No. The Mobile Payments on COTS (MPoC) Standard, Software-based PIN Entry on COTS (SPoC)[™] Standard, Contactless Payments on COTS (CPoC[™]) Standard and the P2PE Standard are all separate PCI SSC standards intended for unique use cases.

Note that devices used as part of an MPoC, SPoC, and/or CPoC Solution may coexist in the same merchant environment as devices used as part of a P2PE Solution.

What date should be used for "Date of Report" in the ROC?

Article 1458 | July 2019

The "Date of Report" indicates the completion date of the ROC, and therefore must be no earlier than the date on which the QSA completed collection and validation of corresponding evidence to support the QSA's findings documented in the ROC.

Further, the ROC should not be considered complete until all reporting within the ROC is finalized, including completion of all internal quality assurance activities.

Note: Per the QSA Program Guide, the dates of the ROC and AOC cannot predate completion of the PCI DSS Assessment, and the date of the AOC cannot predate the corresponding ROC. As a matter of accuracy, the date of the ROC and AOC should not be in the future. See also Can an Attestation of Compliance (AOC) be provided to an assessed entity before the Report on Compliance (ROC) is finalized?

Where should reports be sent when the PFI investigation has concluded there is no evidence of a breach?

Article 1460 | November 2018

Where the entity under investigation is a merchant, all completed work products (e.g. Preliminary and Final reports) must be distributed to all participating payment brands accepted by the merchant. Where the entity under investigation is a service provider, all completed work products must be distributed to all participating payment brands whose products the service provider handles.

Please contact the PFI Program Manager at PFI@pcisecuritystandards.org for further information.

What are the security considerations for TLS 1.3?

Article 1461 | January 2019

Transport Layer Security (TLS) is a protocol that provides security over networks and is widely used for internet communications and online transactions. TLS version 1.3 introduces protocol changes that may improve security and performance while removing complexities and streamlining the protocol stack. These changes, however, also introduce new considerations for organizations using TLS for security controls.

Organizations implementing TLS 1.3 will need to ensure their implementation is properly configured. Factors to consider when evaluating a TLS implementation include the services and options enabled, the cryptographic algorithms supported, and the strength of the cryptographic keys used.

Organizations should also be aware that the features of TLS 1.3 could affect the functionality for some types of security solutions, such as those that rely on decryption to inspect the packets before they reach the endpoint. For example, organizations using web application firewalls and intrusion detection/prevention systems may find that these systems no longer function as expected, as they may not be able to analyze the encrypted TLS 1.3 connections. This may require changes in the way organizations satisfy certain PCI DSS requirements.

Additionally, devices that do not yet support TLS 1.3 may react differently when presented with TLS 1.3 encrypted traffic. The result could be that traffic is allowed to pass through without inspection, potentially leaving malicious payloads or activities undetected. Other devices could fallback to an earlier or insecure version of the protocol, resulting in data having a lower level of protection than intended. These issues may result in organizations needing to reconfigure or adapt their systems so that they continue to perform as expected.

As with all new technologies, organizations should evaluate and review the possible implications that TLS 1.3 may have on their environment. Organizations are encouraged to contact their security solution vendors to determine any potential impact and whether alternative configurations or other workarounds are recommended.

PCI SSC continues to monitor the evolution of security protocols and their impact on security solutions for the payment industry, and will keep stakeholders informed as updates become available.

What does "Window of Payment Card Data Storage" mean in the Final PFI Report template?

Article 1462 | January 2019

Window of Payment Card Data Storage (section 3.1 of the Final PFI Report template) indicates:

- The timeframe for which account or payment card data was being stored – this may include expired accounts and/or card data. It answers the question, 'What is the date range of all accounts and/or payment card data stored, including expired account/payment card data'?
- Overall timeframe of exposed account/card data. Note the Window of payment card data storage is not limited to the "at-risk timeframe" which refers to the period of time the account numbers were at risk (see Section 3.4 of the Final PFI Report template and FAQ 1448). The Window of payment card data storage includes the full date range (time window) of the actual accounts/card data that were exposed during the at-risk timeframe.

Example: The at-risk timeframe is Jan 1 – Jan 31, 2019 (31 days). The unauthorized data disclosure includes account/payment card data dating back to March 2012. The Window of payment card data storage would be March 1, 2012 - January 31, 2019.

Does the use of expired PTS POI devices meet eligibility criteria for SAQ B-IP?

Article 1464 | March 2019

Whether the purchase and use of devices with expired PTS approval is acceptable beyond their expiry date and whether such devices meet the eligibility criteria for SAQ B-IP is determined by the individual payment brands. For specific information regarding payment brand mandates for expired devices, entities should contact the applicable payment brand(s) directly. Contact information for the payment brands can be found in FAQ 1142 'How do I contact the payment card brands'?

Can organizations use alternative password management methods to meet PCI DSS Requirement 8?

Article 1467 | May 2019

The password requirements in PCI DSS include a minimum level of complexity and strength intended to be met by all types of organizations using a range of technologies. PCI SSC encourages organizations to implement stronger controls or additional security measures as appropriate to meet their security needs.

PCI DSS allows organizations to implement alternative controls than those defined in the standard, as long as the intent of the PCI DSS requirements is met. When considering alternative methods, it is important not to view individual recommendations in isolation but to take all the recommendations as a complete set of controls. For example, when considering the alternative controls described in NIST Special Publication 800-63B, the exclusion of periodic password changes without implementing additional compensating controls would not meet the intent of either the NIST Special Publication or PCI DSS.

Any variation to an authentication method that has been defined in PCI DSS will require that the organization consider how the approach could impact other settings and processes as well as the overall impact to security. Organizations wishing to follow a different combination of password complexity and change frequency than those defined in PCI DSS should document their approach as a compensating control. As part of this process, the organization will need to demonstrate how the risk is mitigated and how the intent of the requirement is met through the implementation of other controls.

PCI SSC continually monitors changes in technologies and payment environments and may incorporate updates in future PCI DSS revisions as needed to support evolving industry best practices.

Can I have the same assessor company or individual assessor perform a PCI DSS and PIN Assessment for our organization?

Article 1468 | September 2019

An assessor that is listed as a QSA for PCI DSS and QPA for PCI PIN on the PCI SSC website may be eligible to perform both types of assessments, subject to meeting the requirements of both programs. However, while PCI SSC manages the PCI security standards and assessor programs, PCI compliance programs and validation requirements are defined and managed by the individual payment card brands. We recommend you contact the payment brands directly to discuss their individual compliance rules, validation criteria and processes, etc. Contact information for the payment brands can be found in FAQ #1142 titled, "How do I contact the payment brands?" on the PCI SSC website at <https://www.pcisecuritystandards.org/faqs>.

How do PCI PTS-approved HSM expiry dates affect a PCI-listed P2PE Solution or Component?

Article 1469 | May 2024

For details regarding PTS-approved POI device expiry in regard to the PCI P2PE Standard and Program, refer to the current P2PE Technical FAQs found in the PCI SSC Document Library

(https://www.pcisecuritystandards.org/document_library?category=p2pe)

Are PFIs required to fill out all the fields in the Final PFI Report?

Article 1470 | November 2019

Yes, per the Final PFI Report template instructions, the report template must be completed fully. Therefore, all fields are mandatory; any exceptions must be discussed with and approved by the affected payment brands.

What does "Servicing Markets" on the QSA listing mean?

Article 1471 | November 2019

The Servicing Markets element of the Qualified Security Assessor (QSA) listing indicates the geographic regions or countries for which the QSA Company is authorized by PCI SSC to perform PCI DSS assessments and QSA-related duties. Under no circumstances may QSA Companies perform PCI DSS Assessments—or act as a QSA Company in any capacity—outside of the regions or countries for which they are qualified.

Questions about which countries are included in a particular region should be addressed to the QSA Program Manager via qsa@pcisecuritystandards.org.

How can I determine whether a QSA is authorized to perform PCI DSS assessments in all countries that are in scope for my company's PCI DSS assessment?

Article 1472 | November 2019

The Servicing Markets element of the Qualified Security Assessor (QSA) listing indicates the geographic regions or countries for which the QSA Company is authorized by PCI SSC to perform PCI DSS assessments and QSA-related duties. Under no circumstances may QSA Companies perform PCI DSS Assessments—or act as a QSA Company in any capacity—outside of the regions or countries for which they are qualified.

The Place of Business element of the QSA listing indicates the QSA Company has a physical presence in that country. This is provided for information only and does not supersede the Servicing Markets element of the listing.

If QSA-related tasks must be performed outside of the geographic regions or countries for which the QSA Company is qualified, it may be necessary to engage a QSA Company qualified for that region/country to perform the related tasks. Further information is available in the QSA Program Guide available on the PCI SSC website.

Questions about which countries are included in a particular region should be addressed to the QSA Program Manager via qsa@pcisecuritystandards.org.

What is the role of compliance-accepting entities and assessors in determining the applicability of PCI DSS requirements for merchant and service provider PCI DSS assessments?

Article 1473 | March 2023

Compliance-accepting entities (typically, payment brands and acquirers) are responsible for determining the PCI DSS validation and reporting methods of their merchants and service providers, including how compliance is to be evidenced—for example, whether via a Report on Compliance (ROC) or a Self-Assessment Questionnaire (SAQ). Compliance-accepting entities may also provide direction to their customers about which PCI DSS requirements to include in the assessment—for example, they may require that only a specific subset of PCI DSS requirements, such as those included in an SAQ, be tested and the results documented in a ROC.

Assessors are responsible for validating that the scope of the assessment and that applicability of PCI DSS requirements is accurately defined and documented. To report a PCI DSS requirement as 'Not Applicable', the assessor must first confirm through testing that the requirement is truly not applicable to that environment. This confirmation must be performed and documented for all "Not Applicable" responses before a compliant result can be considered for the assessment.

Alternatively, a "Not Tested" response is used for assessments where a requirement (or a single aspect of a requirement) is not tested in any way – this means the requirement (or aspect thereof) is completely excluded from the assessment without any consideration as to whether it does or could apply.

If a compliance-accepting entity directs an assessed entity or its assessor to exclude any PCI DSS requirement(s) from an assessment, that requirement(s) must be marked as 'Not Tested.'

The PCI DSS ROC Template provides detailed instructions on how to properly document the findings from the testing performed, including the difference between "Not Tested" and "Not Applicable" responses.

Note that whether a "Not Tested" response can result in PCI DSS compliance is treated differently between PCI DSS v3.2.1 and v4.0?QSAs must refer to the ROC Template and the ROC Template FAQs for the version of the standard being used for relevant guidance.

Entities should contact the payment brands directly for information about their compliance programs and reporting requirements. Contact details for the payment brands can be found in FAQ 1142: How do I contact the payment card brands?

See also:

FAQ 1382: Can a partial PCI DSS assessment be documented in a Report on Compliance (ROC)?

FAQ 1331: Can SAQ eligibility criteria be used as a guide for determining applicability of PCI DSS requirements for merchant assessments in a Report on Compliance?

(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/can-saq-eligibility-criteria-be-used-as-a-guide-for-determining-applicability-of-pci-dss-requirements-for-merchant-assessments-documented-in-a-report-on-compliance/)

Can PCI-listed P2PE v2 components be used as part of a P2PE v3 solution?

Article 1474 | April 2020

Yes. P2PE solutions validated to P2PE v3.0 can contain P2PE components and applications validated using P2PE v2.0. Note the P2PE v2 components are governed by the P2PE v2 Program Guide. The v3 solution assessment is governed by the P2PE v3 Program Guide.

See also FAQ Can PCI-listed P2PE v3 Components be used as part of a P2PE v2 Solution assessment? and Which P2PE Program Guide do I use?

Can PCI-listed P2PE v3 components be used as part of a P2PE v2 solution?

Article 1475 | April 2020

Only the PCI-listed P2PE v3 component types that also exist in P2PE v2 may be used in a P2PE v2 solution assessment, which are:

- Encryption Management
- Decryption Management
- KIF
- CA/RA

The new P2PE v3 component types (POI Deployment, POI Management, Key Management, Key Loading) can only be used as part of a P2PE v3 component or solution assessment.

Which P2PE Program Guide version do I use?

Article 1476 | April 2020

P2PE v2 Program Guide: Used for the assessment and management of P2PE v2 solutions, applications, and components.

P2PE v3 Program Guide: Used for the assessment and management of P2PE v3 solutions, applications, and components.

Are software vendors wishing to undergo validation to the PCI Secure Software Lifecycle (Secure SLC) Standard also required to have payment software listed or in the process of being validated to the PCI Secure Software Standard?

Article 1477 | May 2020

It is not necessary for a software vendor to have payment software listed or in the process of being validated to the PCI Secure Software Standard in order to become a Secure SLC qualified vendor.

Can PCI-listed P2PE v3 components be used as part of a P2PE v2 solution?

Article 1478 | May 2020

Only the PCI-listed P2PE v3 component types that also exist in P2PE v2 may be used in a P2PE v2 solution assessment, which are:

- Encryption Management
- Decryption Management
- KIF
- CA/RA

The new P2PE v3 component types (POI Deployment, POI Management, Key Management, Key Loading) can only be used as part of a P2PE v3 component or solution assessment.

Can PCI-listed P2PE v2 components be used as part of a P2PE v3 solution?

Article 1479 | May 2020

Yes. P2PE solutions validated to P2PE v3.0 can contain P2PE components and applications validated using P2PE v2.0.

Note, the P2PE v2 components are governed by the P2PE v2 Program Guide. The v3 solution assessment is governed by the P2PE v3 Program Guide.

See also FAQ 1478 Can PCI-listed P2PE v3 components be used as part of a P2PE v2 solution?

Which P2PE Program Guide version do I use?

Article 1480 | May 2020

P2PE v2 Program Guide: Used for the assessment and management of P2PE v2 solutions, applications, and components.

P2PE v3 Program Guide: Used for the assessment and management of P2PE v3 solutions, applications, and components.

What type of assessor signatures are allowable for PCI SSC attestation documentation?

Article 1481 | June 2020

Attestation documents, including AOCs, AOVs, and program-related attestations, that are provided by the PCI SSC require an assessor's signature. The assessor's signature signifies the individual has knowledge, approval, and acceptance of the document's contents. The signature should guarantee non-repudiation. Acceptable forms of signature currently are wet signature (performed with ink) or PCI SSC-accepted electronic/digital signature (cryptographically protected, such as under the US Federal ESIGN Act, the Uniform Electronic Transactions Act (UETA), or European Union Regulation NO 910/2014 on Electronic Identification, Authentication and Trust Services (eIDAS)).

Please note the payment brands themselves manage their own associated compliance programs and may have their own mandates for what types of signatures they will accept. For information please contact the payment brands directly. Contact details for the payment brands can be found in [FAQ #1142 How do I contact the payment card brands?](#)

Are P2PE Products (P2PE Solutions, P2PE Components, P2PE Applications) on the P2PE Expired Listings still considered "validated" per the P2PE Program Guide?

Article 1482 | October 2020

No, they are no longer considered validated. However, please contact the payment brands regarding the use of P2PE Solutions on the P2PE Expired List (How do I contact the payment card brands?).

As a reminder, reassessment dates shown in orange or red on the PCI SSC website for P2PE products represent products that have not been revalidated in accordance with P2PE program requirements.

Dates in orange indicate the P2PE Product revalidation is up to 90 days overdue and dates in red indicate that the P2PE product revalidation is more than 90 days overdue. These colors and their meaning are described at the bottom of each product listings page and are defined in the P2PE Program Guide. If a P2PE Product's Listing has been in a Red status for more than 90 days, the P2PE Product will be moved to the P2PE Expired Listings.

Refer to the P2PE v3 Program Guide for further details in the PCI SSC Document Library (https://www.pcisecuritystandards.org/document_library?category=p2pe).

You may also be interested in the following FAQs:

1483: If a P2PE Solution is on PCI's list of Point-to-Point Encryption Solutions with Expired Validations, does the solution meet the eligibility criteria for SAQ P2PE?

1484: If a P2PE Solution is shown as red or orange on PCI's list of Validated P2PE Solutions, does the solution meet the eligibility criteria for SAQ P2PE?

If a P2PE Solution is on PCI's list of Point-to-Point Encryption Solutions with Expired Validations, does the solution meet the eligibility criteria for SAQ P2PE?

Article 1483 | September 2020

P2PE solutions on the PCI list of Point-to-Point Encryption Solutions with Expired Validations are no longer considered "validated" per the P2PE Program Guide. Because these P2PE solution providers did not renew their listings in accordance with PCI SSC requirements, the validations are therefore expired.

Merchants using an expired P2PE solution should check with their acquirer or individual payment brands about their eligibility to complete SAQ P2PE.

If a P2PE Solution is shown as red or orange on PCI's list of Validated P2PE Solutions, does the solution meet the eligibility criteria for SAQ P2PE?

Article 1484 | September 2020

Yes, P2PE solutions with dates shown as red or orange are considered validated P2PE solutions and meet the eligibility criteria for SAQ P2PE. Dates shown in colors on the PCI SSC list of Validated P2PE Solutions indicate that the solution has not been revalidated in accordance with P2PE program requirements. Orange means that the P2PE Solution revalidation is up to 90 days overdue and red means that the P2PE Solution revalidation is more than 90 days overdue. These colors and their meaning are described at the bottom of each listings page and are defined in the P2PE Program Guide.

P2PE Solutions that are red for more than 90 days will be moved to PCI's list of Point-to-Point Encryption Solutions with Expired Validations. Expired P2PE solutions are no longer considered "validated" per the P2PE Program Guide and the validations are therefore expired. Refer to [If a P2PE Solution is on PCI's list of Point-to-Point Encryption Solutions with Expired Validations, does the solution meet the eligibility criteria for SAQ P2PE?](#) for more information.

SAQ P2PE is intended for SAQ-eligible merchants or merchant environments as determined by the individual payment card brands. Refer to [Who can use SAQ P2PE?](#) for more information.

What is the meaning of 'initial PCI DSS assessment'?

Article 1485 | January 2024

Where an entity is being assessed for the first time against a PCI DSS requirement with a defined timeframe, it is considered an initial PCI DSS assessment for that requirement. This means the entity has never undergone a prior assessment to that requirement, where the assessment resulted in submission of a compliance validation document (for example, an AOC, SAQ, or ROC).

For an initial assessment against a requirement that has a defined timeframe (for example, with an activity that is to be performed once every three or six months), it is not required that the activity has been performed for every such timeframe during the previous year, if the assessor verifies that:

- The activity was performed in accordance with the applicable requirement within the most recent timeframe (for example, the most recent three-month or six-month period), and

- The entity has documented policies and procedures for continuing to perform the activity within the defined timeframe.

All other applicable PCI DSS requirements are expected to be in place at the time of the assessment.

If an entity has previously submitted a formal validation document, subsequent assessments of the requirements reviewed in prior assessments cannot be considered an initial assessment. Examples of situations that do not change or reset an entity's initial assessment date include where the entity:

- Misses a subsequent assessment date,
- Changes assessor companies,
- Reports to a different compliance entity, or
- Changes or introduces new technologies to the environment.

Where an entity is being assessed to a PCI DSS requirement with a defined timeframe for the first time—for example, if the addition of a new payment acceptance channel results in an additional PCI DSS requirement(s) becoming applicable or where a PCI DSS requirement(s) with a defined timeframe is added to a ROC or SAQ —the first assessment of the additional requirement(s) could be considered an initial assessment for that specific requirement(s).

Entities should always consult with their acquiring bank or payment brand(s) to

confirm how to report their compliance. Contact information for the payment brands is provided in FAQ 1142 How do I contact the payment card brands?

Internal gap assessments and pre-production assessments that do not result in a formal compliance document are not considered initial assessments. For further guidance on PCI DSS compliance in pre-production environments, refer to FAQ 1333 Can PCI DSS compliance be determined by testing only pre-production environments using test data?

Can the "Compliant but with Legal exception" option in the AOC be used to identify where a testing procedure could not be performed due to a legal constraint?

Article 1486 | December 2020

No. The "Compliant but with Legal exception" option in Part 3 of an Attestation of Compliance (AOC) allows an entity to document that they could not implement one or more requirements because doing so would contravene a local or regional law or regulation. In such circumstances, the requirements that cannot be met must be marked as "Not in Place" in the accompanying ROC (Report on Compliance) or SAQ (Self-Assessment Questionnaire), as applicable. Use of the "Compliant but with Legal exception" option also requires additional review from the acquirer or payment brand to whom compliance is being reported.

Where the assessor is unable to complete testing of a requirement because of a legal constraint—for example, due to government enforced travel restrictions, local or regional lockdowns, or other factors impacting the assessor's ability to gain access or complete a testing activity—the affected requirements must be marked as 'Not Tested'. Because the assessor was unable to determine whether the requirement has been met, Part 3 of the AOC must be marked as 'Non-Compliant.'

In situations where testing procedures cannot be completed, assessors are encouraged to document in the report why the requirement could not be tested, and entities encouraged to consult with their acquirer and/or payment brand to understand expectations regarding partial or incomplete assessments.

Can a 3DS entity outsource the hosting and management of its HSMs to a third-party service provider?

Article 1487 | December 2020

Yes, a 3DS entity may choose to outsource the hosting and management of its HSM infrastructure to a third-party service provider as long as all applicable requirements are met. The 3DS entity should work with their service provider to determine which requirements are covered by the service provider and which are covered by the 3DS entity. The 3DS entity remains ultimately responsible for ensuring that all applicable requirements regarding the hosting and management of HSMs are met. Please refer to the "Use of Third-Party Service Providers / Outsourcing" section in the PCI 3DS Core Security Standard for more information.

What types of 3DS components are in scope for Requirement P2-7 in the PCI 3DS Core Security Standard?

Article 1488 | December 2020

Requirements P2-7.1 and P2-7.2, which relate to data center and CCTV security, apply to 3DS Directory Server (DS) and 3DS Access Control Server (ACS) systems.

As noted in the Overview section of Requirement P2-7, the DS and ACS systems are critical components of the 3DS infrastructure that require a secure facility with elevated physical security controls to restrict, manage, and monitor all physical access.

The requirements in P2-7 are recommended, but not required, for locations where only a 3DS Server (3DSS) is present. Refer to the PCI 3DS Core Security Standard for information about the different 3DS components.

Is an EMVCo Letter of Approval required prior to conducting a PCI 3DS Assessment?

Article 1489 | December 2020

No, an EMVCo Letter of Approval (LOA) is not required for a PCI 3DS Assessor to perform an assessment to the PCI 3DS Core Security Standard. If an EMVCo LOA is not obtained prior to completing the PCI 3DS Assessment, the assessed entity should select the "other" option in Part 2a of the PCI 3DS Attestation of Compliance (AOC) and explain why the 3DS functions or services being assessed do not have an associated EMVCo LOA.

Whether a completed PCI 3DS Report on Compliance (ROC) will be accepted without an EMVCo LOA is determined by the individual payment brands. Contact details for the payment brands can be found in [FAQ #1142 How do I contact the payment card brands?](#)

Can a PCI 3DS Assessment result in a finding of "Compliant" if some requirements are not tested?

Article 1490 | December 2020

No. The PCI 3DS Attestation of Compliance (AOC) can only document a "Compliant" finding if all requirements are tested and found to be "In Place" or a combination of "In Place," 'In Place w/CCW' (in place with compensating controls worksheet), and/or "N/A" (not applicable). Where the assessor has marked requirements as "In Place w/CCW" or "N/A," the assessor would also need to perform appropriate testing and complete the appropriate appendixes of the PCI 3DS Report on Compliance (ROC).

Version 1.0 of the PCI 3DS ROC and AOC do not include an option to report requirements as 'not tested'. Because the assessor has not determined whether such requirements could be applicable or whether they have been met, any PCI 3DS requirements that have not been tested must be marked as "Not in Place" and the overall compliance status marked as 'Not Compliant'.

Support for "not tested" responses is planned for inclusion in a future update to the PCI 3DS ROC and AOC. Requirements identified as "not tested" would also result in a finding of 'Not Compliant'.

Does PCI DSS define which versions of TLS must be used?

Article 1491 | January 2021

No. However, PCI DSS does not consider SSL or early TLS to be strong cryptography.

Transport Layer Security (TLS) is a protocol that encrypts traffic between two endpoints to provide privacy and reliability of transmitted data and is widely used for internet communications and online transactions. Current available versions of TLS include TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. PCI DSS does not allow the use of SSL or early TLS as a security control, with one exception. For allowed uses of early TLS, see the PCI SSC Information Supplement, Use of SSL /Early TLS for POS POI Terminal Connections.

The term "early TLS" does not refer to a specific version(s) of the protocol, but rather it encompasses any version or implementation of TLS that is vulnerable to a known exploit. This categorization is intended to help entities identify and prioritize mitigation efforts for TLS implementations known to be inherently vulnerable. Entities should have processes to monitor threats as they continue to evolve and as new versions of the protocol are released to address those threats, and to keep the entity's cryptographic implementations up to date to prevent them becoming vulnerable to known exploits.

All cryptographic implementations, including TLS, must use and support modern cryptographic algorithms, secure configuration settings, and other features as needed to meet the intent of strong cryptography. This means that every TLS implementation, irrespective of the protocol version, must apply strong cryptography using an appropriate cipher suite to implement a secure key exchange algorithm, strong cryptography, and an appropriate message authentication for strong cryptography and security protocols.

Entities using TLS should review their implementations against industry references (such as the current version of NIST SP 800-52) for guidance on configuration options that meet the intent of strong cryptography. Note that, while industry guidelines such as NIST SP 800-52 may provide additional insight into specific configurations and implementations and provide the rationale for implementing particular controls, PCI DSS does not mandate the use of external standards or guidance in meeting strong cryptography. In addition to monitoring specific threats to cryptographic implementations, entities should monitor changes in industry best practices and standards, and where applicable, entities should apply modifications to minimum cryptographic standards used within their environments to ensure that sensitive information such as account data and authentication credentials remain secured.

It is expected that systems conducting negotiation of TLS protocols use the strongest cipher suites first, with subsequent negotiation to mutually supported cipher suites only if needed, but always within the bounds of the minimum standard of strong cryptography and security protocols.

For the definition of "strong cryptography" as used in PCI DSS, refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms available in PCI SSC's

Document Library, under the PCI DSS drop-down menu.

How can an entity meet PCI DSS requirements for PAN masking and truncation if it has migrated to 8-digit BINs?

Article 1492 | April 2024

There are two PCI DSS requirements that may be affected when considering 8-digit BINs.

Requirement 3.4.1 pertains to masking (concealing) digits of the PAN so that the full PAN is not displayed, and Requirement 3.5.1 is for rendering PAN unreadable when stored. These requirements are different and distinct and therefore it is important to understand each requirement and how it pertains to the entity's implementation.

PCI DSS Requirement 3.4.1 requires that no more than the BIN and last four digits of the PAN are displayed on computer screens, reports, etc. unless there is a documented business justification for seeing more digits. The documented business justification should explain why that person (or role) needs to see more digits of PAN, be approved by management, and available for an assessor to review as part of the PCI DSS assessment.

PCI DSS Requirement 3.5.1 applies when PAN is stored (i.e., data at rest). This requirement specifies four acceptable methods for rendering PAN unreadable when stored. One of the techniques is truncation, which permanently removes the middle digits of the PAN, leaving the rest of the PAN to be stored in the clear. FAQ #1091 What are acceptable formats for truncation of primary account numbers? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/What-a-re-acceptable-formats-for-truncation-of-primary-account-numbers) provides information about acceptable truncation formats for each payment brand based on the length of PAN/BIN. Because each payment brand has different PAN/BIN lengths and different requirements, questions about payment brand truncation requirements should be directed to the applicable payment brands. Contact details for the payment brands are provided in FAQ #1142 How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-d-o-I-contact-the-payment-card-brands)

Please note that truncation is only one acceptable method for rendering PAN unreadable during storage; other options include encrypting the entire PAN, using index tokens, or using one-way hashes. All hashes generated after 31 March 2025 must be keyed cryptographic hashes according to PCI DSS Requirement 3.5.1.1.

What is the PCI 3DS (3D Secure) Core Security Standard?

Article 1493 | April 2021

The PCI SSC document library contains an overview that answers numerous questions about the PCI 3DS Core Security Standard (otherwise known as the PCI 3DS Security Requirements and Assessment Procedures for EMVÆ 3-D Secure Core Components: ACS, DS, and 3DS Server.)

This overview document answers various questions, from "What is 3DS"?, questions about the PCI 3DS Security Standard itself, in addition to relationships with other PCI SSC Standards. The overview document can be found here (<https://www.pcisecuritystandards.org/documents/Overview-PCI-3DS-Core-Security-Standard.pdf?agreement=true&time=1617729076719>).

For personnel working from home, is the work-from-home environment considered a "sensitive area" for PCI DSS Requirement 9?

Article 1494 | May 2021

No. An individual's private work-from-home (WFH) environment is not considered a "sensitive area," and personnel working from home are not required to meet PCI DSS Requirements 9.1.1 or 9.3 for their WFH environments.

"Personnel working from home" refers to individuals that are employed by an entity to perform business duties from the individual's private residence; this does not include individuals running their own home-based business.

A sensitive area is typically a subset of the cardholder data environment (CDE) and is any area that houses systems considered critical to the CDE. This includes data centers, server rooms, back-office rooms at retail locations, and any area that concentrates or aggregates cardholder or account data storage, processing, or transmission. Sensitive areas also include areas housing systems that manage or maintain the security of the CDE (for example, those providing network security or that manage physical or logical security).

As a WFH environment is not considered a sensitive area, it is not expected that video cameras and/or access control mechanisms are in place to monitor or physically restrict access within these environments. Personnel working from home are expected to adhere to their organization's security policies and procedures, including limiting access to cardholder data within their WFH environments - for example, using only company-authorized devices to access cardholder data, locking computer screens when stepping away from the computer, securing any storage of paper copies of cardholder data to prevent unauthorized access, and following the organization's policies for securing network and computer equipment used at home for work purposes.

See also the following FAQs:

FAQ 1495: Is an assessor required to visit work-from-home environments to determine if personnel are meeting PCI DSS requirements?

FAQ 1496: Are entities expected to do onsite audits of personnel work-from-home environments?

Is an assessor required to visit work-from-home environments to determine if personnel are meeting PCI DSS requirements?

Article 1495 | May 2021

No, PCI SSC does not require QSAs or ISAs to visit personnel private residences for any purpose, including the review of work-from-home (WFH) environments to validate PCI DSS requirements.

Entities should have policies and procedures implemented to provide assurance that applicable PCI DSS controls are in place for WFH personnel and that such personnel are aware of and adhering to the entity's secure practices.

Assessors should work with the entity to understand the processes and controls the entity has implemented to secure connections from personnel in WFH environments. This includes understanding how the entity ensures that account data is stored, processed, or transmitted from WFH environments in accordance with applicable PCI DSS requirements, and how the entity gains assurance that those controls continue to function effectively to protect the entity's network and cardholder data.

See also the following FAQs:

FAQ 1494: For personnel working from home, is the work-from-home environment considered a "sensitive area" for PCI DSS Requirement 9?

FAQ 1496: Are entities expected to do onsite audits of personnel work-from-home environments?

Are entities expected to do onsite audits of personnel work-from-home environments?

Article 1496 | May 2021

No, entities are not expected to conduct onsite assessments of work-from-home (WFH) environments, as home environments are not owned or controlled by the entity.

Entities are expected to have controls and processes in place governing how personnel working from home access payment card account data. Controls and processes should also be implemented to provide assurance that payment card account data is protected in accordance with applicable security requirements.

See also the following FAQs:

FAQ 1494: For personnel working from home, is the work-from-home environment considered a "sensitive area" for PCI DSS Requirement 9?

FAQ 1495: Is an assessor required to visit work-from-home environments to determine if personnel are meeting PCI DSS requirements?

For PCI DSS, why is storage of sensitive authentication data (SAD) after authorization not permitted even when there are no primary account numbers (PANs) in an environment?

Article 1533 | July 2021

In the PCI DSS Applicability Information section of the standard, it is stated that sensitive authentication data must not be stored after authorization even if encrypted, and that this applies even for environments where there is no PAN present.

Sensitive authentication data (SAD) is used by the issuer of a card to authenticate the card and the cardholder, specifically the card verification code and the PIN/PIN block.

The card verification codes that are found in the track data, the track data equivalent in the chip or, for an e-commerce transaction, that are printed on the front or back of a payment card, are validated by the issuer during authorization to give them confidence that the card they issued is being used for the transaction.

The PIN or PIN block is validated by the issuer during authorization to give them confidence that the cardholder is making the transaction.

If an entity stores sensitive authentication data even where there is no PAN in the entity's environment, there is the risk that the SAD could be compromised by an attacker and subsequently correlated with other data to give an attacker the PAN and SAD together, which would reduce an issuer's ability to determine whether a transaction was genuine or fraudulent. For example, a customer is often identified by its email address; criminals may use correlation databases to correlate a PAN and email address stolen from one merchant with a card verification code and the same email address stolen from a second merchant.

Similarly, if a merchant stores a card verification code alongside a token that can be used to make a payment transaction, the merchant (or an attacker with access to the merchant's environment) is misrepresenting to the card issuer that the cardholder provided the card verification code during the transaction, limiting the issuer's ability to protect their cardholder from fraud. Transactions that use stored cardholder data with the cardholder's permission (referred to as account on file, card on file, and credential on file), including recurring transactions and additional charges in the travel industry, do not require the merchant to provide the card verification code. For more information on card-on-file or recurring transactions, see [FAQ #1280 Can card verification codes/values be stored for card-on-file or recurring transactions?](#)

What is a compliance-accepting entity?

Article 1536 | October 2021

When assessment results are associated with compliance programs defined and managed by one or more payment brands, the compliance-accepting entity is the entity to which those assessment results (for example, a Report on Compliance) are submitted. The compliance-accepting entity is typically a payment brand or acquirer.

Are remote assessments permitted for PCI DSS?

Article 1537 | October 2021

While onsite assessments continue to be the expected method for PCI SSC assessments, the use of remote assessment methods may provide a suitable alternative in legitimate scenarios where an onsite assessment is not feasible. In such scenarios, entities should consult with the compliance-accepting entity to confirm whether remote assessments are allowed and any requirements they may have around performing remote assessments or the submission of remote assessment reports.

PCI SSC has developed a set of guidelines and procedures outlining the appropriate use of remote assessment methods when an onsite assessment is not feasible and where remote assessments are permitted by the compliance-accepting entity. The PCI SSC Remote Assessment Guidelines and Procedures can be found in the PCI SSC Document Library. If remote assessment methods are used in place of onsite assessment, the Assessor may be required to complete the Addendum for ROC/ROV: Remote Assessments, if requested by the compliance-accepting entity.

What is the process to initiate a software evaluation to the PCI Secure Software Standard?

Article 1538 | November 2021

Vendors that want to have their software assessed to the PCI Secure Software Standard initiate the process by engaging a qualified Secure Software assessor from the PCI SSC list of Software Security Framework Assessors (https://www.pcisecuritystandards.org/assessors_and_solutions/software_security_framework_assessors).

A detailed overview of the assessment process, including roles and responsibilities, is provided in the Secure Software Program Guide available in the Document Library (https://www.pcisecuritystandards.org/document_library).

See also the following FAQs:

FAQ 1539: Who is qualified to perform assessments to the PCI Secure Software Standard?

FAQ 1540: What software is eligible for validation to the PCI Secure Software Standard?

Who is qualified to perform assessments to the PCI Secure Software Standard?

Article 1539 | November 2021

Secure Software Assessors are qualified by PCI SSC to validate payment software adherence to the Secure Software Standard.

Qualified Secure Software Assessors will have the Assessment Type of "Secure Software" noted in their listing in the PCI SSC list of Software Security Framework Assessors

(https://www.pcisecuritystandards.org/assessors_and_solutions/software_security_framework_assessors).

See also the following FAQs:

FAQ 1538: What is the process to initiate a software evaluation to the PCI Secure Software Standard?

FAQ 1540: What software is eligible for validation to the PCI Secure Software Standard?

What software is eligible for validation to the PCI Secure Software Standard?

Article 1540 | November 2021

The eligibility criteria for software validation to the PCI Secure Software Standard is defined in the Secure Software Program Guide, available in the Document Library (https://www.pcisecuritystandards.org/document_library).

Whether an entity is required to use software validated to the Secure Software Standard is determined by individual payment brand mandates, and not by PCI SSC. For information about payment brand requirements for use of Secure Software validated applications, please contact the payment brands directly. Payment brand contact details can be found in FAQ 1142 How do I contact the payment card brands?

See also the following FAQs:

FAQ 1538: What is the process to initiate a software evaluation to the PCI Secure Software Standard?

FAQ 1539: Who is qualified to perform assessments to the PCI Secure Software Standard?

When must validated payment software be revalidated?

Article 1541 | November 2021

Subject to early expiry and the terms of the Software Security Framework Vendor Release Agreement (VRA), validations to the Secure Software Standard are valid for three years. Further information on revalidations and the process for managing changes to validated payment software can be found in the Secure Software Program Guide. Both the VRA and Secure Software Program Guide are available in the Document Library (https://www.pcisecuritystandards.org/document_library).

What is the process for PCI Secure SLC Qualification?

Article 1542 | November 2021

Vendors that want to have their software development processes assessed to the Secure SLC standard may initiate the process by engaging a qualified Secure SLC assessor from the PCI SSC list of Software Security Framework Assessors (https://www.pcisecuritystandards.org/assessors_and_solutions/software_security_framework_assessors).

A detailed overview of the assessment process, including roles and responsibilities, is provided in the Secure SLC Program Guide available in the Document Library (https://www.pcisecuritystandards.org/document_library).

See also FAQ 1543: Who is qualified to perform assessments to the PCI Secure SLC Standard?

Who is qualified to perform assessments to the PCI Secure SLC Standard?

Article 1543 | November 2021

Secure SLC Assessors are qualified by PCI SSC to validate software vendor adherence to the Secure SLC Standard.

Qualified Secure SLC Assessors will have the Assessment Type of "Secure SLC" noted in their listing in the PCI SSC list of Software Security Framework Assessors (https://www.pcisecuritystandards.org/assessors_and_solutions/software_security_framework_assessors).

See also FAQ 1542: What is the process for PCI Secure SLC Qualification?

Does PCI SSC provide a list of software vendors whose software development process(es) have been validated to the Secure SLC Standard?

Article 1544 | November 2021

Yes. Vendors whose software development practices have been validated to the Secure SLC Standard are added to the list of Secure SLC Qualified Vendors (https://www.pcisecuritystandards.org/assessors_and_solutions/software_lifecycle?agree=true).

Are there prerequisite PCI SSC program requirements to meet before qualifying as an SSF Assessor Company?

Article 1545 | November 2021

No, companies are not required to participate in other PCI SSC programs before becoming an SSF Company.

Can multiple changes for a Secure Software listing be submitted within a single change submission?

Article 1546 | November 2021

Yes, it is possible to submit multiple changes to a software listing, however, details of each change must be provided separately using Section C1 of the Change Impact Template (located in the Secure Software Program Guide, which is available in the Document Library (https://www.pcisecuritystandards.org/document_library)) as appropriate.

Are currently listed PA-DSS payment applications required to be revalidated using the Secure Software Standard?

Article 1547 | November 2021

After 28 October 2022, all previously validated PA-DSS applications will be expired and moved to the "Acceptable Only for Pre-existing Deployments" list on the PCI SSC website. Payment application vendors wishing to maintain active payment application listings after 28 October 2022 should have their payment applications validated to the Secure Software Standard for inclusion on the PCI SSC's List of Validated Payment Software.

Whether the use of payment software validated to the Secure Software Standard is required is determined by the individual payment brand compliance programs. Please contact the applicable payment brand or acquirer to understand any compliance requirements they may have. Payment brand contact details can be found in FAQ 1142 —How do I contact the payment card brands?.

Are Secure Software Assessors or Secure Software Lifecycle Assessors required to report Continuing Professional Education (CPE) credits to PCI SSC?

Article 1548 | November 2021

No. Secure Software Assessors and Secure SLC Assessors in good standing do not need to report CPEs to PCI SSC. The CPEs that these Assessors are required to obtain and report to other certification bodies in order to maintain their industry-recognized certifications are sufficient to ensure they stay current in their field of practice.

Is software-as-a-service (SaaS) eligible for Secure Software Standard validation and listing?

Article 1549 | November 2021

Yes, if the software in question meets all stated eligibility criteria in effect at the time of submission, software-as-a-service may be validated to the Secure Software Standard and listed on the PCI SSC list of Validated Payment Software (https://www.pcisecuritystandards.org/assessors_and_solutions/payment_software).

More information on the eligibility for the Secure Software Program is located in the Secure Software Program Guide available in the Document Library (https://www.pcisecuritystandards.org/document_library).

What is a PCI SSC Participating Payment Brand?

Article 1554 | November 2021

A PCI SSC Participating Payment Brand is a payment brand that, as of the time in question, is then formally admitted as (or an affiliate of) a member of PCI SSC pursuant to its governing documents. At the time of writing, Participating Payment Brands include PCI SSC Founding Members and Strategic Members.

What impact does the inclusion of UnionPay in PCI DSS documents have on an entity's PCI DSS assessment?

Article 1561 | October 2022

Whether the inclusion of UnionPay in PCI DSS documents impacts an entity's PCI DSS assessment is determined by the PCI SSC Participating Payment Brands (American Express, Discover, JCB International, Mastercard, UnionPay, and Visa). Each Participating Payment Brand currently has their own PCI compliance programs for the protection of their affiliated payment card account data. Entities should always contact their acquirer or the payment brands directly to determine their compliance reporting requirements, including any potential impacts to a PCI DSS assessment. Contact details for the payment brands can be found in [FAQ #1142 How do I contact the payment card brands?](#)

PCI DSS v3.2.1 documents have been updated to include UnionPay as a Participating Payment Brand, and UnionPay is now included in both PCI DSS v3.2.1 and v4.0 documents.

Is a QSA Employee that designs, develops, or implements specific controls for a customer also permitted to assess those same controls?

Article 1562 | November 2022

No. As per section 2.2 of the QSA Qualification Requirements, "The QSA Company must have separation of duties controls in place to ensure Assessor-Employees conducting or assisting with PCI SSC Assessments are independent and not subject to any conflict of interest." If a QSA Employee(s) recommends, designs, develops, provides, or implements controls for an entity, it is a conflict of interest for the same QSA Employee(s) to assess that control(s) or the requirement(s) impacted by the control(s).

Another QSA Employee of the same QSA Company (or subcontracted QSA) - not involved in designing, developing, or implementing the controls - may assess the effectiveness of the control(s) and/or the requirement(s) impacted by the control(s). The QSA Company must ensure adequate, documented, and defensible separation of duties is in place within its organization to prevent independence conflicts.

What should an entity do if its PCI DSS assessment will not be complete prior to that standard's retirement date?

Article 1563 | October 2024

Compliance questions, including questions about whether it is acceptable to submit a PCI DSS assessment report after that standard's retirement date, should be directed to organizations that manage compliance programs (for example, payment brands and acquirers).

Contact details for the payment brands can be found in FAQ #1142: How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/how-do-i-contact-the-payment-card-brands/)

-

FAQ 1564: How does an entity report the results of a PCI DSS assessment for new requirements that are noted in PCI DSS as best practices until a future date?

-

FAQ 1328: Where can I find the current version of PCI DSS? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/where-can-i-find-the-current-version-of-pci-dss/)

-

FAQ 1565: Does an entity's PCI DSS assessment result expire when the standard against which the entity was assessed is retired?

-

FAQ 1266: If an entity is in the middle of a PCI DSS assessment when a new version of the standard is released - should the assessment be started again using the new version?

How does an entity report the results of a PCI DSS assessment for new requirements that are noted in PCI DSS as best practices until a future date?

Article 1564 | March 2023

Where a future-dated requirement has not yet been implemented by an entity and the Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ) is completed prior to the effective date of the new requirement, the future-dated requirement can be marked as "Not Applicable."

Where an entity relies on a third-party service provider (TPSP) to meet PCI DSS requirements on the entity's behalf, and:

-

The TPSP has not yet been assessed against the new version of the standard,
Or

-

The TPSP has been assessed to the new version of the standard, but the assessment was prior to the effective date of new requirements that the TPSP is meeting on the entity's behalf, and did not include those new requirements,

Then, providing that the TPSP has a current PCI DSS assessment (within the last 12 months) against a version that was current at the time of the assessment, the entity's assessor may mark those requirements upon which the entity relies as "Not Applicable."

If an entity or TPSP has implemented a future-dated requirement prior to its effective date and wants to include it in its PCI DSS assessment, they may choose to do so.

In all cases, commencing on the effective date of new PCI DSS requirements, all new requirements applicable to an entity's assessment (including those met by a TPSP on the entity's behalf) must be fully considered as part of the entity's PCI DSS assessment.

Also refer to the following related FAQs:

-

FAQ 1563: What should an entity do if its PCI DSS assessment will not be complete prior to that standard's retirement date?
(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-should-an-entity-do-if-its-pci-dss-assessment-will-not-be-complete-prior-to-that-standard-s-retirement-date/)

-

FAQ 1328: Where can I find the current version of PCI DSS?
(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/where-can-i-find-the-current-version-of-pci-dss/)

-

FAQ 1565: Does an entity's PCI DSS assessment result expire when the standard against which the entity was assessed is retired?

-

FAQ 1266: If an entity is in the middle of a PCI DSS assessment when a new version of the standard is released — should the assessment be started again using the new version?

Does an entity's PCI DSS assessment result expire when the standard against which the entity was assessed is retired?

Article 1565 | March 2023

No. The period for which an entity's PCI DSS assessment result is valid does not change if the standard against which the entity was assessed has been retired. However, how long an assessment result is valid and how frequently an entity must be reassessed is determined by organizations that manage compliance programs (for example, payment brands and acquirers).

Entities should always contact their acquirer or the payment brands directly for information about their compliance programs and reporting requirements. Contact details for the payment brands can be found in FAQ #1142 How do I contact the payment card brands?

Also refer to the following related FAQs:

- FAQ 1564: How does an entity report the results of a PCI DSS assessment for new requirements that are noted in PCI DSS as best practices until a future date?
- FAQ 1563: What should an entity do if its PCI DSS assessment will not be complete prior to that standard's retirement date?
(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-should-an-entity-do-if-its-pci-dss-assessment-will-not-be-complete-prior-to-that-standard-s-retirement-date/)
- FAQ 1328: Where can I find the current version of PCI DSS?
(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/where-can-i-find-the-current-version-of-pci-dss/)
- FAQ 1266: If an entity is in the middle of a PCI DSS assessment when a new version of the standard is released — should the assessment be started again using the new version?

Can a Qualified Security Assessor (QSA) ask an auditor from the same company (for example, one conducting a SOC 2 or SOC 3 audit) to collect evidence for a PCI DSS assessment?

Article 1566 | March 2023

Yes. However, regardless of how the QSA obtains evidence to support a PCI DSS assessment, the QSA conducting the PCI DSS assessment has the ultimate responsibility for their client's assessment and the accuracy and relevance of the information and evidence provided in the Report on Compliance and related workpapers.

This responsibility includes that the QSA evaluates the evidence and confirms that:

- Collected evidence is specific to the scope of the PCI DSS assessment,
- Collected evidence directly relates to the specific PCI DSS requirement under review,
- The date of the evidence is within the scope of the assessment and meets any specifics called out in related PCI DSS testing procedures, and
- The QSA can effectively render an opinion based on the collected evidence about whether the relevant controls are "in place."

See also FAQ 1567: Can a Qualified Security Assessor (QSA) rely on the results from non PCI DSS assessment (for example, a SOC 2 or SOC 3 audit) for a PCI DSS assessment?

Can a Qualified Security Assessor (QSA) rely on the results from non PCI DSS assessment (for example, a SOC 2 or SOC 3 audit) for a PCI DSS assessment?

Article 1567 | March 2023

No, due to the variability of scope coverage and assessor validation procedures, a QSA cannot rely on reports from other attestation engagements (like SOC 2 or SOC 3) for a PCI DSS assessment. However, a QSA may be able to use the evidence generated during those assessments for a PCI DSS assessment, but only after independently reviewing the evidence and gaining assurance that:

-

The scope of the assessment includes the relevant payment environment(s) and payment account data,

-

What was covered directly maps to PCI DSS requirements,

-

The evidence is within the timeframe of the PCI DSS assessment and meets any specifics called out in related PCI DSS testing procedures, and

-

That relevant PCI DSS controls are "in place."

See also FAQ 1566: Can a Qualified Security Assessor (QSA) ask an auditor from the same company (for example, one conducting a SOC 2 or SOC 3 audit) to collect evidence for a PCI DSS assessment? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/can-a-qualified-security-assessor-qa-ask-an-auditor-from-the-same-company-for-example-one-conducting-a-soc-2-or-soc-3-audit-to-collect-evidence-for-a-pci-dss-assessment/)

Is the PCI DSS Attestation of Compliance intended to be shared?

Article 1568 | April 2023

Yes. The PCI DSS Attestation of Compliance is intended to be shared externally to requesting entities, according to applicable Participating Payment Brand rules and as noted in the Qualified Security Assessor Program Guide.

Entities should contact the payment brands directly for information about their compliance programs and reporting requirements. Contact details for the payment brands can be found in FAQ 1142: How do I contact the payment card brands?

Is sampling allowed in PCI DSS v4.x?

Article 1569 | March 2026

Yes. Assessors have two options when performing PCI DSS testing procedures; they can either: 1) test a representative sample of the population according to the assessor's defined sampling methodology, or 2) test 100% of the given population.

Sampling is not mandatory; it is an option for assessors to facilitate the assessment process when there are large numbers of items in a population being tested. If sampling is not used, 100% of the population must be tested. Where sampling is used, each sample must be a representative selection of all variants of the population and be sufficiently large to provide the assessor with assurance that controls are implemented as expected across the entire population.

The use of sampling for PCI DSS testing procedures has not changed in PCI DSS v4.x. Previously, sampling was mentioned in some, but not all, testing procedures. In PCI DSS v4.x, mention of sampling was removed from all testing procedures for consistency.

When considering whether the use of sampling is appropriate for a particular testing procedure, the assessor should consider the size of the population being tested as well as the overall scope and complexity of the environment.

For more information, see PCI DSS v4.x Section 6, For Assessors: Sampling for PCI DSS Assessments.

Does TDEA meet the requirements of "strong cryptography" as defined in PCI DSS?

Article 1570 | August 2023

At the end of 2023, NIST disallows the use of three-key TDEA for use in protecting security sensitive data within US Federal information systems. However, as per NIST SP800-57 part 1, TDEA using three keys can still provide an effective strength of 112 bits when applied using appropriate key management and modes of operation.

The definition of 'strong cryptography' was updated in PCI DSS v4.0 to reference the effective key size of the algorithm/key combination rather than any specific algorithms - specifically the effective key strength is a minimum of 112 bits, with a recommendation to use systems that provide 128 bits of effective strength. Additionally, "strong cryptography" requires the use of industry-tested and accepted algorithms and proper key-management practices.

For other PCI SSC standards, refer to the subject standard for whether and how use of three-key TDEA is allowed.

Is the expectation that any PFI investigation initiated must result in a PFI Final Report?

Article 1571 | August 2024

Yes, a PFI Final Report is required. The expectation is that the PFI must complete the merchant's PFI Investigation and produce the Final PFI Report, with details of adequate evidence to support claims.

PCI SSC has received multiple inquiries on how to move forward on a third-party service provider case where the breach has been confirmed to have occurred and affected merchants, particularly where some affected merchants may have already begun their own PFI engagements. While there is no "one size fits all" response to such inquiry, PCI SSC can provide the following guidance to PFIs in determining next steps:

- When a PFI investigates a third-party service provider incident, scoping should include steps to identify and include any third-party connections as part of incident validation and assessment, including affected merchants and their sponsoring acquirers.
- In the example of a merchant for which a PFI has already completed the PFI Preliminary Incident Response Report and delivered it to each affected Participating Payment Brand before evidence that a third-party service provider was in fact responsible for the breach affecting the merchant is produced, PFIs are expected to fully complete a Final PFI Report for the merchant. The PFI is expected to complete the merchant investigation and provide confirmation and document in the final PFI report that the breach is related to the third-party service provider incident. It would be reasonable to explain what was investigated, at what point the PFI became aware of the findings for the third-party service provider, and to clearly communicate what was assessed at the merchant and report those findings (conclusive or inconclusive).
- Whether the same PFI Company did or did not assess the third-party service provider and the merchant may affect the level of reporting; if the same PFI Company assessed both, they would reasonably have access to more relevant data than a PFI Company who did not assess the third-party service provider but is assessing an affected merchant.
- Where a third-party service provider PFI investigation has identified affected merchants and no PFI has been engaged for any affected merchant, it is recommended to consolidate the merchant cases into the third-party provider case as a matter of efficiency instead of opening an individual merchant PFI if required by a different workstream or regulatory agency. While the final decision does not rest with the PFI, the PFI must consult with Participating Payment Brands and affected acquirers on how to proceed with the investigation.
- Where there is sufficient evidence, based on one or more merchant PFI investigation(s) that indicate the breach was caused by the third-party service provider, and the third-party service provider is not cooperative and/or has not engaged a PFI, the PFI must inform the Participating Payment Brands and affected acquirers.

Payment Brand contact details are provided in FAQ #1142 How do I contact the payment card brands?

Can a compensating control be used for requirements with a periodic or defined frequency, where an entity did not perform the activity within the required timeframe?

Article 1572 | June 2025

No.

Several PCI DSS requirements specify that a security activity is to be performed periodically or at a defined frequency. If an entity fails to perform the control on one or more of the defined timeframes, there is no way for them to perform the control retroactively or backdate a later occurrence of the control to an earlier period.

A common example is external ASV scans, which are required at least once every three months. If an ASV scan was missed, the entity will not have sufficient ASV scan reports to provide as evidence during the assessment. Other examples include not installing a critical security patch within 30 days of release and not reviewing network security control configurations at least once every six months.

In these scenarios, an assessor can determine a requirement to be “In Place” if the entity has implemented corrective actions and successfully performed the control in accordance with the requirement, and the assessor has assurance that:

- The entity has a repeatable and documented process for performing the control,
- The entity demonstrates that the activity was missed due to an exceptional circumstance (poor security practices and recurring failures are not “exceptional circumstances”),
- The entity shows that they have addressed the issue that led to the exception, and
- The entity has included steps in their process to prevent recurrence.

If the entity cannot demonstrate the above, or the assessor does not have assurance that the entity has processes in place to continue to meet the requirement, the assessor can consider whether a “Not in Place” finding would be the appropriate result.

To document these situations, assessors should follow assessment best practices to determine whether a requirement can be considered in place, and document it in their work papers and in the Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ). This should include the corrective actions the entity implemented, that the entity has successfully performed the control in accordance with the requirement, and how the assessor has assurance that the entity meets the bullets outlined above.

Do PCI DSS requirements for keyed cryptographic hashing apply to previously hashed PANs?

Article 1573 | September 2023

No. The PCI DSS requirement for keyed cryptographic hashing is a new requirement for PCI DSS v4.0 and is a best practice until the new requirements become effective on 31 March 2025. After that date, all hashing processes used to render primary account numbers unreadable are required to meet the PCI DSS requirements for keyed cryptographic hashing.

For the definitions of "hashing" and "keyed cryptographic hashing" refer to the PCI DSS Glossary of Terms, Abbreviations, and Acronyms in PCI DSS v4.x, Appendix G.

See also FAQ 1089: Are hashed Primary Account Numbers (PAN) considered cardholder data that must be protected in accordance with PCI DSS?

If an organization provides software or functionality that runs on a consumer's device (for example, smartphones, tablets, or laptops) and is used to accept payment account data, can the organization store card verification codes for those consumers?

Article 1574 | October 2023

No. PCI DSS prohibits storage of card verification codes, for example, after transaction authorization or to facilitate potential future transactions.

There are four common scenarios where organizations may want to, or think it is necessary to, store card verification codes for consumers, due to software or functionality on a consumer's device:

- Applications that facilitate consumers' online purchases and where the merchant or service provider stores card verification codes for use on behalf of consumers. Examples include merchant online store applications, gaming applications, and web browsers for auto fill of payment transactions.
- Functionality where a service provider stores card verification codes on behalf of consumers, including password vaults.
- Issuing functions that provision a consumer's account data into a consumer's device (which may include card verification codes). Not the subject of this FAQ. Only issuers or companies supporting issuing services with a legitimate issuing business need may store SAD after transaction authorization.
- Consumers that enter their own payment account data into their device (which may include card verification codes). Not the subject of this FAQ. In this case, the device is treated similarly to a consumer's payment card.

This FAQ applies only to the first two bullets above.

Card verification codes are typically used for authorization in card-not-present transactions.— PCI DSS does not prohibit the collection of card verification codes prior to authorization of a specific purchase or transaction. However, it is not permitted to retain card verification codes once the specific purchase or transaction for which it was collected has been authorized.

It is not permissible to store card verification codes regardless of any permission the entity may have received from their customer to store the sensitive authentication data on their behalf. A customer's request or approval for an entity to retain a card verification code has no validity for PCI DSS and does not constitute an allowance to store the data.

Generally, PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). This includes all entities involved in payment card account processing—including merchants, processors, acquirers, issuers, and other service providers.

Note that whether such an entity is required to undergo a PCI DSS assessment is determined by organizations that manage compliance programs, such as acquirers (merchant banks), payment brands, or other entities. Entities should contact these organizations directly for information about any such requirements. Contact details for the payment brands can be found in FAQ #1142 'How do I contact the payment card brands'?.

See also the following related FAQs:

FAQ 1280: Can card verification codes/values be stored for card-on-file or recurring transactions?

FAQ 1283: How do PCI standards apply to organizations that develop software that runs on a consumer's device (for example, a smartphone, tablet, or laptop) and is used to accept payment card data?

FAQ 1533: For PCI DSS, why is storage of sensitive authentication data (SAD) after authorization not permitted even when there are no primary account numbers (PANs) in an environment?

Does PCI SSC consider guidance from other standards organizations when making updates to PCI standards?

Article 1575 | December 2023

Yes. PCI SSC considers the guidance provided from many different standards organizations when updating our standards, balancing the guidance against the unique needs and challenges of the payments industry.

There may be differences between PCI standards and specific recommendations from other standards organizations due in part to the industries they were written for and the information they are designed to protect. PCI standards have long been focused on providing specific direction and guidance on meeting security outcomes for payment environments and solutions, providing security requirements that can be implemented by a broad range of stakeholders throughout the payment ecosystem.

What evidence is a TPSP expected to provide to customers to demonstrate PCI DSS compliance?

Article 1576 | February 2024

If the TPSP undergoes its own PCI DSS assessment, it is expected to provide sufficient evidence to its customers to verify that the scope of the TPSP's PCI DSS assessment covered the services applicable to the customer, and that the relevant PCI DSS requirements were examined and determined to be in place. If the TPSP has a PCI DSS Attestation of Compliance (AOC), it is expected to provide the AOC to customers upon request. This AOC should be applicable to the services the TPSP provides to the customer(s) and provide evidence that the PCI DSS requirements relevant to those services are met. The customer may also request relevant sections of the TPSP's PCI DSS Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ) D for Service Providers.

If the TPSP does not undergo its own PCI DSS assessment and or otherwise does not have an applicable AOC, the TPSP is expected to provide specific evidence related to the applicable PCI DSS requirements, so that the customer (or its assessor) is able to confirm that the TPSP is meeting those PCI DSS requirements.

In addition, in accordance with PCI DSS Requirement 12.9.1 and 12.9.2, the TPSP is obligated to provide information to its customers about which PCI DSS requirements for which the TPSP is responsible, and which are the responsibility of the customer. One tool that can be used to document and share this information is a responsibility matrix, a sample of which can be found in Appendix B of the Information Supplement: Third-Party Security Assurance (https://docs-prv.pcisecuritystandards.org/Guidance%20Document/PCI%20DSS%20General/ThirdPartySecurityAssurance_March2016_FINAL.pdf) on the PCI SSC website.

For more information, refer to the PCI DSS section 4 Scope of PCI DSS Requirements, subsection Use of Third-Party Service Providers.

Refer to the following FAQs:

FAQ 1312: How is an entity's PCI DSS compliance impacted by using third-party service providers (TPSPs)? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-is-an-entity-s-PCI-DSS-compliance-impacted-by-using-third-party-service-providers-TPSPs/)

FAQ 1354: Can sensitive information be redacted from the PCI DSS Attestation of Compliance before it is shared with other entities? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/Can-sensitive-information-be-redacted-from-the-PCI-DSS-Attestation-of-Compliance-before-it-is-shared-with-other-entities/)

FAQ 1290: If an entity uses a third-party service provider (TPSP) that has been validated as PCI DSS compliant, is the entity's assessor required to go onsite to the TPSP's location and retest the PCI DSS requirements?

(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/If-an-entity-uses-a-third-party-service-provider-TPSP-that-has-been-validated-as-PCI-DSS-compliant-is-the-entity-s-assessor-required-to-go-onsite-to-the-TPSP-s-location-and-retest-the-PCI-DSS-requirements/)

What does “console access” mean for PCI DSS Requirements 8.4.1 and 8.4.2?

Article 1577 | May 2024

Console access refers to a system with a direct physical connection to another system component, where that connection does not rely on a networked connection (meaning that access is from the “console” to the system component via a physical cable). Console access is a mechanism typically used by system administrators, to connect via physical cable to a system component that resides in the CDE or sensitive area for purposes of managing that system (for example, editing a sensitive configuration file on that system component). This is considered a more secure form of access because it cannot be easily intercepted by an unauthorized user.

Console access does not include situations where the system is used to access other system components over a networked connection. For example, access via a laptop or workstation using a physically connected keyboard is not considered “console access” if that system requires a networked connection to access any other system component.

Can service providers use eligibility criteria from a merchant Self-Assessment Questionnaire (SAQ) to determine applicable PCI DSS requirements for the service provider's assessment?

Article 1578 | June 2024

No. It was never the intent that a service provider uses a merchant SAQ to determine applicable requirements for a service provider's PCI DSS assessment. The only correct SAQ for a service provider is SAQ D for Service Providers. All other SAQs are intended only for merchants.

Certain merchant SAQs include a reduced set of applicable requirements because, to be eligible for that SAQ, the merchant must have outsourced all storage, processing, and transmission of account data to a PCI DSS compliant service provider. Many requirements with important security controls are not included in those SAQs specifically because it is expected that the service providers used by these merchants are meeting those PCI DSS requirements on the merchant's behalf. A service provider that only meets the reduced set of requirements in these SAQs will be missing these important security controls. In addition, there are numerous requirements noted as "Additional requirement for service providers only" in SAQ D for Service Providers - these requirements are not included in any merchant SAQ.

All PCI DSS requirements must be considered when scoping a service provider's assessment to determine which requirements are applicable to the service being provided and the systems providing that service. To the extent that a given service provider offers a limited service for merchants, for example one that only indirectly facilitates storage, processing, or transmission of payment data, those service providers are still expected to comply with all applicable PCI DSS requirements related to the service and the systems that provide that service.

If a given PCI DSS requirement is truly not applicable to a service provider (for example, the software development ones in Requirement 6 because the service provider does not develop software), those requirements can be marked as N/A.

A service provider that provides a merchant SAQ or a merchant Attestation of Compliance (AOC) as evidence of its PCI DSS compliance has not provided sufficient evidence for its customers.

Does PCI DSS apply to service providers that can impact the security of payment account data, if the service provider does not directly store, process, or transmit payment account data?

Article 1579 | June 2024

Yes. PCI DSS is intended for all entities that store, process, or transmit cardholder data and/or sensitive authentication data or could impact the security of payment account data (which consists of cardholder data and/or sensitive authentication data). This includes all entities involved in payment account processing—including service providers that can impact the security of a cardholder data environment (CDE). Examples of ways a service provider may impact the security of a CDE include, but are not limited to, where the service provider:

- Has direct or indirect access to a customer's CDE, payment account data, and/or system components that may allow access to a customer's CDE.
- Provides a service that directly or indirectly meets a PCI DSS requirement(s) on behalf of another entity (for example, provision of network security controls or anti-malware services).
- Provides a service that directly or indirectly facilitates storage, processing, and/or transmission of another entity's payment account data (for example, passing a URL redirect from one entity to another).

Also refer to the following FAQs:

- FAQ 1233: How does encrypted cardholder data impact PCI DSS scope for third-party service providers? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/how-does-encrypted-cardholder-data-impact-pci-dss-scope-for-third-party-service-providers/)
- FAQ 1580: What is the scope of a PCI DSS assessment for service providers that can impact the security of payment account data, if the service provider does not directly store, process, or transmit payment account data? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-is-the-scope-of-a-pci-dss-assessment-for-service-providers-that-can-impact-the-security-of-payment-account-data-if-the-service-provider-does-not-directly-store-process-or-transmit-payment-account-data/)

What is the scope of a PCI DSS assessment for service providers that can impact the security of payment account data, if the service provider does not directly store, process, or transmit payment account data?

Article 1580 | June 2024

The scope of a PCI DSS assessment for service providers that can impact the security of payment account data (which consists of cardholder data and/or sensitive authentication data), but which do not directly store, process, or transmit payment account data includes all people, processes, and technology involved in providing the service provider's services.

While the applicable PCI DSS requirements for these service provider assessments will depend on the services provided and the access the service provider may have into a CDE or to payment account data, here are some considerations when scoping a service provider's PCI DSS assessment:

- If the service provider has access to a customer's CDE, to a customer's payment account data, and/or to system components that may allow access to a customer's CDE, the applicable PCI DSS requirements are those that verify network and security controls effectively limit the service provider's access to only that which is necessary.
- If a service provider's services directly or indirectly meet a PCI DSS requirement(s) on behalf of another entity, the applicable PCI DSS requirements are those specific to the service being met by the service provider.
- If a service provider's service that directly or indirectly facilitates storage, processing, and/or transmission of another entity's payment account data, the applicable PCI DSS requirements are those related to the security of the service and systems.

The service provider and its assessor should work together to confirm the applicable PCI DSS requirements, based on an analysis of the service provider's services and the access the service provider has, or may have, to another entity's payment account data, and how and whether that service provider may be able to impact the security of another entity's payment account data.

Where a service provider is completing SAQ D for Service Providers and is not using an external assessor, the applicable PCI DSS requirements should be confirmed by internal staff responsible for compliance.

All PCI DSS requirements determined to be not applicable must be thoroughly justified and documented, either 1) in the ROC along with each requirement for which "Not Applicable" is selected or 2) in SAQ D for Service providers, Appendix C: Explanation of Requirements Noted as Not Applicable.

For any entity seeking to outsource payment or security-related services to a service provider where that service could impact the security of the entity's payment account data, it is important to establish agreements about how PCI DSS compliance information will be shared between both parties and what type of information the

service provider will share to verify that all applicable PCI DSS requirements are being met.

For guidance on nested service providers (where one service provider uses other service providers), refer to the Third-Party Security Assurance Information Supplement.

Also refer to the following FAQs:

- FAQ 1233: How does encrypted cardholder data impact PCI DSS scope for third-party service providers?
(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/how-does-encrypted-cardholder-data-impact-pci-dss-scope-for-third-party-service-providers/)
- FAQ 1579: Does PCI DSS assessment apply to service providers that can impact the security of payment account data, if the service provider does not directly store, process, or transmit payment account data?
(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/does-pci-dss-apply-to-service-providers-that-can-impact-the-security-of-payment-account-data-if-the-service-provider-does-not-directly-store-process-or-transmit-payment-account-data/)

How does PCI DSS Requirement 6.4.3 apply to 3DS scripts called from a merchant check-out page as part of 3DS processing?

Article 1581 | August 2024

The objective of PCI DSS Requirement 6.4.3 is to ensure that unauthorized code cannot be executed in the payment page as it is rendered in the consumer's browser.

In a typical 3DS implementation, 3DS Server fetches and stores URLs to scripts from an EMV 3DS Access Control Server (ACS), EMV 3DS Directory Server (DS), or services connected to the ACS or DS, on behalf of an issuer, issuer agent, or payment network. During the checkout process, a merchant website serves a web page with an iframe using a URL provided by the 3DS Server with an applicable script to support 3DS functionality.

For merchants using a 3DS solution, validation to PCI DSS Requirement 6.4.3 for 3DS scripts is not required due to the inherent trust relationship between the 3DS service provider and the merchant, as established in the merchant's due diligence and onboarding processes, and the business agreement between the entities.

Any script run outside of the purpose of performing a 3DS functionality is subject to PCI DSS requirement 6.4.3.

What is the completion date for PCI DSS assessments documented in a Self-Assessment Questionnaire and its related Attestations of Compliance?

Article 1582 | August 2024

For PCI DSS assessments documented in a Self-Assessment Questionnaire (SAQ), the Self-Assessment completion date denotes the date the PCI DSS self-assessment was completed, either by the entity, or, if applicable, by a Qualified Security Assessor (QSA) or Internal Security Assessor (ISA). The Self-Assessment completion date can be found at the start of Section 2 in each SAQ, and in the SAQ Attestations of Compliance (AOCs) in Section 3 at the start of Part 3.

Each SAQ Attestation of Compliance (AOC) also includes Part 3b Merchant (or Service Provider) Attestation, for the Merchant or Service Provider Executive officer's signature and signing date. This signature date is expected to be the same date as, or within a reasonable timeframe after (for example, within two or three weeks), the Self-Assessment completion date. The signature acknowledges that the SAQ and Self-Assessment completion date are accurate; this date does not indicate the completion date for the assessment.

Refer any questions about these dates, including about acceptable reasonable timeframes between dates, to the entity to which the document (the SAQ or AOC) will be submitted. This is typically an acquirer (merchant bank) or the payment brands. Contact details for the payment brands can be found in [FAQ 1142 How do I contact the payment card brands?](#)

What is the completion date for PCI DSS assessments documented in a Report on Compliance and its related Attestations of Compliance?

Article 1583 | August 2024

For PCI DSS assessments documented in a Report on Compliance (ROC), the Date of Report is considered the completion date for the PCI DSS assessment. This denotes the date when the QSA Company and assessed entity agree on the final version of the ROC.

The Date of Report can be found in the:

- ROC, in Section 1.2.
- ROC Attestations of Compliance (AOCs), on the AOC cover page and in Section 3 at the start of Part 3.

The ROC AOC also includes the following:

- Part 3b Merchant (or Service Provider) Attestation, for the Merchant or Service Provider Executive officer's signature and signing date.
- Part 3c Qualified Security Assessor (QSA) Acknowledgement, for the Duly Authorized Officer of the QSA Company's signature and signing date.

The signature dates noted above are expected to be the same date as, or within a reasonable timeframe after (for example, within two or three weeks), the Date of Report. These signature dates acknowledge that the ROC and ROC Date of Report are accurate; these dates do not indicate the completion date for a PCI DSS assessment.

Refer any questions about these dates, including about acceptable reasonable timeframes between dates, to the entity to which the document (the ROC or AOC) will be submitted. This is typically an acquirer (merchant bank) or the payment brands. Contact details for the payment brands can be found in FAQ 1142 How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/how-do-i-contact-the-payment-card-brands/)

Refer to the following related FAQs:

FAQ 1458: What date should be used for "Date of Report" in the ROC? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-date-should-be-used-for-date-of-report-in-the-roc/)

FAQ 1356: What does "Duly Authorized Officer" mean? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-does-duly-authorized-officer-mean/)

FAQ 1375: Can an Attestation of Compliance (AOC) be provided to an assessed entity before the Report on Compliance (ROC) is finalized? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/can-an-attestation-of-compliance-aoc-be-provided-to-an-assessed-entity-before-the-report-on-compliance-roc-is-finalized/)

For PCI DSS, can multi-factor authentication (MFA) implementations indicate the success of a factor prior to presentation of subsequent factors?

Article 1584 | September 2024

Yes. PCI DSS v4.x requires the success of all authentication factors before access is granted. However, it is acceptable under PCI DSS to indicate that one factor has been successful before presentation of subsequent authentication factors.

It is recommended that systems either 1) provide no feedback about the success of any factor until all factors are provided, or 2) authenticate with a session-unique factor (for example, a one-time password (OTP) or phishing-resistant factor) before authenticating any factor that is the same across different sessions (such as a password). However, MFA implementations where the success of one factor is indicated prior to the entry of subsequent factor(s) meet applicable PCI DSS requirements for MFA.

When should an entity implement PCI DSS requirements noted as best practices until a future date?

Article 1585 | October 2024

Updates to PCI DSS are intended to address evolving threats in the payments ecosystem, therefore, entities are strongly encouraged to complete their transition to the most current PCI DSS version, including the adoption of new requirements, as early as possible.

Future-dated requirements that have not yet been implemented by the entity may be marked as “Not Applicable” in any Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ) completed prior to the requirement’s effective date. However, commencing on the new requirements’ effective date, all requirements applicable to an entity’s assessment, including the newly effective requirements, must be fully considered as part of the entity’s PCI DSS assessment.

Note that questions about compliance programs and reporting requirements, including whether there are any specific reporting requirements for new requirements, should be directed to compliance-accepting entities, which are the entities to which those assessment results (for example, a Report on Compliance) are submitted. The compliance-accepting entity is typically a payment brand or acquirer.

Contact details for the payment brands can be found in FAQ #1142: How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/how-do-i-contact-the-payment-card-brands/)

Also refer to the following FAQs:

- FAQ 1485: What is the meaning of ‘initial PCI DSS assessment’? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-is-the-meaning-of-initial-pci-dss-assessment/)
- FAQ 1266: If an entity is in the middle of a PCI DSS assessment when a new version of the standard is released-should the assessment be started again using the new version? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/if-an-entity-is-in-the-middle-of-a-pci-dss-assessment-when-a-new-version-of-the-standard-is-released-should-the-assessment-be-started-again-using-the-new-version/)
- FAQ 1564: How does an entity report the results of a PCI DSS assessment for new requirements that are noted in PCI DSS as best practices until a future date? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-does-an-entity-report-the-results-of-a-PCI-DSS-assessment-for-new-requirements-that-are-noted-in-PCI-DSS-as-best-practices-until-a-future-date/)
- FAQ 1573: Do PCI DSS requirements for keyed cryptographic hashing apply to previously hashed PANs? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/do-pci-dss-requirements-for-keyed-cryptographic-hashing-apply-to-previously-hashed-pans/)

How does an e-commerce merchant meet the SAQ A eligibility criteria for scripts?

Article 1588 | February 2025

This FAQ is only intended to clarify the specific SAQ A eligibility criteria called out below. The contents of this FAQ should not be interpreted to impact or contradict any other eligibility criteria in SAQ A or in any other SAQ.

PCI DSS v4.0.1 Self-Assessment Questionnaire (SAQ) A r1 includes the following eligibility criteria for e-commerce channels:

The merchant has confirmed that their site is not susceptible to attacks from scripts that could affect the merchant's e-commerce system(s). *

* Refer to the latest version of PCI DSS SAQ A for the complete list of eligibility criteria.

The above SAQ A eligibility criteria only applies to e-commerce merchants with a webpage that includes a TPSP's/payment processor's embedded payment page/form (for example, one or more inline frame(s) (iframes)).

The above SAQ A eligibility criteria does not apply to e-commerce merchants with a webpage that redirects customers from the merchant's webpage to a TPSP/payment processor (for example, including but not limited to, with an HTTP 30x redirect, a meta redirect tag, or a JavaScript redirect) or e-commerce merchants that fully outsource payment functions to a TPSP/payment processor (for example, by providing customers with an email with a link to a TPSP's website to pay).

The merchant can confirm that the merchant's webpage is not susceptible to script attacks by either:

- Using techniques such as, but not limited to, those detailed in PCI DSS Requirements 6.4.3 and 11.6.1 to protect the merchant's webpage from scripts targeting account data. These techniques may be deployed by the merchant or a third party.

Or

- Obtaining confirmation from the merchant's PCI DSS compliant TPSP/payment processor providing the embedded payment page/form(s) that, when implemented according to the TPSP's/payment processor's instructions, the TPSP's/payment processor's solution includes techniques that protect the merchant's payment page from script attacks.

Merchants are encouraged to work with the merchant's TPSP to obtain guidance about how to implement the TPSP's solution securely.

A provider of third-party scripts is not considered a third-party service provider (TPSP) for purposes of SAQ A, if the provider's only service is providing scripts not related to payment processing and where those scripts cannot impact the security of cardholder data and/or sensitive authentication data.

Merchants should continue to consult with their compliance-accepting entity, the

entity to which the SAQ will be submitted (typically, an acquirer (merchant bank) or the payment brands), to determine if the merchant is required to submit an SAQ, and if so, which SAQ is appropriate for the merchant's environment.

Contact information for the payment brands can be found in FAQ #1142 How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/how-do-i-contact-the-payment-card-brands/)

See also:

FAQ 1133: Why are there multiple PCI DSS Self-Assessment Questionnaires (SAQs)? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/why-are-there-multiple-pci-dss-self-assessment-questionnaires-saqs/)

Is the cardholder in scope for PCI DSS?

Article 1589 | March 2025

No.

Do PCI DSS Requirements 8.3.9 and 8.3.10.1 apply to all system components?

Article 1590 | March 2025

No. PCI DSS Requirements 8.3.9 and 8.3.10.1 do not apply to in-scope system components where multi-factor authentication (MFA) is used.

Requirements 8.3.9 and 8.3.10.1 apply if passwords/passphrases are used as part of a single-factor authentication implementation; neither of these requirements apply to in-scope system components where MFA is used.

PCI DSS v4.x Requirement 8.3.10.1 is like requirement 8.3.9, except that it is specific for "service providers only" and for access by service provider customers. Both requirements 8.3.9 and 8.3.10.1 specify that, if passwords/passphrases are used as the only authentication factor for user access** (i.e., in any single-factor authentication implementation), then either:

- Passwords/passphrases are changed at least every 90 days or
- The security posture of accounts is dynamically analyzed, and real-time access to resources automatically determined accordingly.

If an entity has implemented MFA for access to all in-scope system components (including those in the CDE, and those that are connected-to or security-impacting system components), then the entity does not have single-factor authentication implemented for any in-scope system components. For such entities, the assessor can mark Requirements 8.3.9 and 8.3.10.1 as "not applicable." For any requirements marked "not applicable," QSAs are expected to follow the ROC Template instructions to confirm and document why "not applicable" is the appropriate response.

Refer to the following FAQ:

FAQ 1591: Why do requirements 8.3.9 and 8.3.10.1 focus on passwords/passphrases used for single-factor authentication, when multi-factor authentication is required for all access into the CDE? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/why-do-requirements-8-3-9-and-8-3-10-1-focus-on-passwords-passphrases-used-for-single-factor-authentication-when-multi-factor-authentication-is-required-for-all-access-into-the-cde/)

Why do requirements 8.3.9 and 8.3.10.1 focus on passwords/passphrases used for single-factor authentication, when multi-factor authentication is required for all access into the CDE?

Article 1591 | March 2025

PCI DSS Requirement 8.4.2 for multi-factor authentication (MFA) is not mandatory for access to in-scope system components outside of the CDE. If a user's access to a system component can be used to connect into the CDE, then MFA is required.

For Requirements 8.3.9 and 8.3.10.1, passwords/passphrases are still allowed as "the only authentication factor for user access (i.e., in any single-factor implementation)" if all the following are true:

- The system component being accessed is in scope but is not in the CDE, and
- The system component is a connected-to or a security impacting system, and
- The user's access to that system component cannot be used to connect into the CDE.

Passwords/passphrases may also be "the only authentication factor for user access" within the CDE, where a user has been granted access into the CDE via MFA, and is subsequently accessing a system component within the CDE.

If an entity has implemented MFA for access to all in-scope system components (including those in the CDE, and those that are connected-to or security-impacting system components), then the entity does not have single-factor authentication implemented for any in-scope system components. For such entities, the assessor can mark Requirements 8.3.9 and 8.3.10.1 as "not applicable." For any requirements marked "not applicable," QSAs are expected to follow the ROC Template instructions to confirm and document why "not applicable" is the appropriate response.

Refer to the following FAQ:

FAQ 1590: Do PCI DSS Requirements 8.3.9 and 8.3.10.1 apply to all system components?

(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/do-pci-dss-requirements-8-3-9-and-8-3-10-1-apply-to-all-system-components/)

Are providers of third-party scripts for e-commerce environments considered third-party service providers for PCI DSS Requirements 12.8 and 12.9?

Article 1592 | March 2025

A provider of third-party scripts is not considered a third-party service provider (TPSP) for PCI DSS Requirements 12.8 and 12.9 as part of an entity's assessment of the entity's e-commerce environment, if the entity confirms that:

- The provider's only service is providing scripts not related to payment processing, and
- The provider's scripts cannot impact the security of cardholder data and/or sensitive authentication data.

Refer to the following FAQ:

FAQ 1588: How does an e-commerce merchant meet the SAQ A eligibility criteria for scripts?

(https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/how-does-an-e-commerce-merchant-meet-the-saq-a-eligibility-criteria-for-scripts/)

How should PCI DSS v4.x requirements noted as superseded by another requirement be reported after 31 March 2025?

Article 1593 | March 2025

After 31 March 2025, superseded requirements should be marked as Not Applicable (N/A) in a Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ).

Three PCI DSS v4.x requirements include a note that the requirement will be superseded by another requirement as of 31 March 2025.

The table below shows the three requirements, with the effective requirement and superseded requirement noted in each case.

Requirement Number and Description *

Effective as of

31 March 2025

Superseded – N/A after 31 March 2025

6.4.2 - For public-facing web applications, deploy an automated technical solution to detect and prevent web-based attacks.

X

6.4.1 - Review public-facing web application via manual or automated application vulnerability security assessment tools/methods or deploy an automated technical solution to detect and prevent web-based attacks.

X

8.3.10.1 - If passwords/passphrases are used as the only authentication factor for customer user access, service providers change customer passwords at least once every 90 days or determine access to resources based on dynamic analysis of accounts' security posture.

X

8.3.10 - If passwords/passphrases are used as the only authentication factor for customer user access, service providers provide guidance to customers about frequency, when, and under which circumstances to change passwords/passphrases.

X

10.7.2 - Failures of critical control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical control systems:

· <10 bullets>

X

10.7.1 - Failures of critical control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical control systems:

· <8 bullets>

X

* Refer to PCI DSS v4.x for the exact wording of the requirement.

Are passkeys synced across devices, implemented according to the FIDO2 requirements, acceptable for use as phishing-resistant authentication to meet PCI DSS Requirement 8.4.2?

Article 1595 | May 2025

Yes. Passkeys synced across devices (also called synced passkeys), implemented according to the FIDO2 requirements, are considered phishing-resistant authentication, and may be used as a single authentication factor in place of multi-factor authentication (MFA) to meet PCI DSS Requirement 8.4.2. This aligns with the Applicability Note in Requirement 8.4.2. Passkeys not implemented according to the FIDO2 requirements must include an additional factor to meet PCI DSS Requirements 8.4.1, 8.4.2, and 8.4.3 for MFA.

See also:

FAQ 1596: Is phishing-resistant authentication alone acceptable as multi-factor authentication for PCI DSS Requirements 8.4.1 and 8.4.3 (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/is-phishing-resistant-authentication-alone-acceptable-as-multi-factor-authentication-for-pci-dss-requirements-8-4-1-and-8-4-3/)?

Is phishing-resistant authentication alone acceptable as multi-factor authentication for PCI DSS Requirements 8.4.1 and 8.4.3?

Article 1596 | May 2025

No, phishing-resistant authentication cannot be used without an additional authentication factor to meet Requirements 8.4.1 or 8.4.3 because of the increased risk with these types of access.

Use of phishing-resistant authentication is encouraged and recommended; however, to meet Requirements 8.4.1 and 8.4.3 for MFA, phishing-resistant authentication must be used with another factor (for example, a password, PIN, or biometric).

See also:

FAQ 1595: Are passkeys synced across devices, implemented according to the FIDO2 requirements, acceptable for use as phishing-resistant authentication to meet PCI DSS Requirement 8.4.2 (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/are-passkeys-synced-across-devices-implemented-according-to-the-fido2-requirements-acceptable-for-use-as-phishing-resistant-authentication-to-meet-pci-dss-requirement-8-4-2/)?

What are the expectations for entities when assigning risk rankings to vulnerabilities and resolving or addressing those vulnerabilities?

Article 1597 | May 2025

There are several PCI DSS requirements that govern vulnerability management and reference related timeframes. These requirements are described under the general topics of 1) identifying and risk ranking vulnerabilities, and 2) resolving or addressing vulnerabilities.

Vulnerability Management Infographic
(<https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/Vulnerability%20Management%20Infographic.pdf>)

Identify and risk-rank vulnerabilities:

Requirements 11.3.1 and 11.3.1.1 specify internal vulnerability scans. The information from an entity's internal vulnerability scans should be used as one of the inputs into the entity's processes for identifying and risk-ranking vulnerabilities at Requirement 6.3.1.

After finding the vulnerabilities, Requirement 6.3.1 specifies that entities manage security vulnerabilities, including assigning risk rankings based on impact to the entity and identifying at a minimum those vulnerabilities considered to be high-risk or critical to the entity's environment. Note that Requirement 6.3.1 does not require that an entity accepts risk rankings assigned by external sources; rather the entity may evaluate external risk rankings considering the entity's risk and environment and then assign the appropriate risk ranking for the entity's environment.

Resolve or address vulnerabilities:

Requirements 11.3.1 and 11.3.1.1 also specify that critical and high-risk vulnerabilities are resolved*, and that lower-ranked vulnerabilities are addressed** in accordance with the entity's risk as defined and documented in a targeted risk analysis (TRA).

PCI DSS Requirement 6.3.3 specifies time frames for installing security patches/updates – those for critical vulnerabilities must be resolved within one month of release. Additionally, all other applicable security patches/updates must be installed within appropriate time frames determined by the entity's assessment of the risk to their environment. The appropriate time frames defined by the entity should align with the risk ranking of vulnerabilities assigned in Requirement 6.3.1 (for example, resolving high-risk vulnerabilities more quickly than lower-ranked vulnerabilities). Refer to the Requirement 6.3.3 Guidance column under Examples for more information.

* Resolved – the entity solves or fixes the vulnerability.

** Addressed - the entity determines whether to resolve the vulnerability or to mitigate the risk by addressing the vulnerability in another way (e.g., with a compensating control or by disabling a vulnerable service).

Are Approved Scanning Vendors and Qualified Security Assessors considered third-party service providers for PCI DSS Requirements 12.8 and 12.9?

Article 1598 | June 2025

No, Approved Scanning Vendors (ASVs) and Qualified Security Assessors (QSAs) are not considered third-party service providers (TPSPs) for purposes of PCI DSS Requirements 12.8 and 12.9, if an ASV or QSA company's only service is performing ASV scans or conducting PCI DSS assessments, respectively. Where ASV or QSA companies provide other services, they may be considered a TPSP for those services.

ASV and QSA companies are qualified by the PCI Security Standards Council's (PCI SSC) to offer ASV and QSA related services. The PCI SSC qualification processes ensure that:

- ASV companies and their ASV tools meet specific criteria necessary to perform external vulnerability scans for PCI DSS Requirement 11.3.2.
- QSA companies and individual QSAs meet specific criteria necessary to perform PCI DSS assessments.

These companies have a direct relationship with PCI SSC through the ASV and QSA programs and are subject to PCI SSC's quality programs to remain in good standing and be included on PCI SSC's lists of qualified professionals.

Regardless of the relationship these companies have with PCI SSC, entities should follow their internal third-party due diligence processes when engaging with an ASV or QSA company.

What is the impact if an entity uses a third-party service provider (TPSP) to meet a PCI DSS requirement(s), when that TPSP's PCI DSS assessment completion date is close to a year ago, as documented in the TPSP's Attestation of Compliance (AOC)?

Article 1601 | November 2025

Any evidence reviewed as part of a PCI DSS assessment, where the assessor deems it to be valid when it is reviewed, remains valid for that assessment and does not need additional review before finalization of the ROC. As part of the PCI DSS assessment, the assessor is expected to additionally confirm that the assessed entity has defined and implemented processes that result in timely updates to documentation that supports PCI DSS controls.

Any questions about whether a TPSP's AOC can be accepted as evidence to support an entity's assessment should be directed to the organizations that manage compliance programs (for example, acquirers, payment brands, or other entities). Contact details for the payment brands can be found in FAQ #1142: How do I contact the payment card brands? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands/)

Please refer to the following FAQs:

FAQ 1312: How is an entity's PCI DSS compliance impacted by using third-party service providers (TPSPs)? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-is-an-entity-s-PCI-DSS-compliance-impacted-by-using-third-party-service-providers-TPSPs/)

FAQ 1576: What evidence is a TPSP expected to provide to customers to demonstrate PCI DSS compliance? (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/What-evidence-is-a-TPSP-expected-to-provide-to-customers-to-demonstrate-PCI-DSS-compliance/)

Should entities with enterprise or internal service providers, used to provide internal services to other corporate entities, conduct separate PCI DSS assessments of these service providers or include them as part of each corporate entity's PCI DSS assessment?

Article 1602 | February 2026

Assessed entities have the discretion to either have enterprise functions assessed separately as an internal service provider or include those functions in each individual corporate entity's PCI DSS assessment. Regardless of the entity's decision, the appropriate validation tool for a service provider is either Self-Assessment Questionnaire (SAQ) D for Service Providers or a PCI DSS Report on Compliance (ROC), as directed by their compliance accepting entity (typically a merchant acquirer or a payment brand).

Are authentication values from a 3DS transaction considered sensitive authentication data for PCI DSS purposes?

Article 1603 | March 2026

No. PCI DSS sensitive authentication data (SAD) consists of full magnetic-stripe data, card verification codes or values, and PINs or PIN blocks. PCI DSS specifically prohibits storage of SAD after completion of the authorization process.

The 3-D Secure (3DS) authentication value is a cryptographic value generated by the 3DS Access Control Server that allows the authorization system to validate the integrity of the authentication result during authorization processing. This 3DS value is also referred to as the cardholder authentication value (CAVV) and the accountholder authentication value (AAV). The authentication value is one of the data elements identified as 3DS sensitive data in the PCI 3DS Data Matrix in Table 1: 3DSS, DS, and ACS Sensitive Data Elements. Data elements included in this table are subject to the requirements in the PCI 3DS Core Security Standard that apply to 3DS sensitive data.

3DS authentication values and other 3DS sensitive data are not considered to be SAD from a PCI DSS perspective and PCI DSS does not prohibit 3DS sensitive data from being stored after the authorization process is complete.

Entities performing or providing any of the following 3DS functions: 3DS Server, 3DS Directory Server, and/or 3DS Access Control Server should confirm with the payment brand(s) for which they perform these 3DS functions whether they are required to meet the requirements in the PCI 3DS Core Security Standard.

Do ASV scans in SAQ A apply to merchants with webpages that redirect to TPSPs or include TPSPs' embedded iframes?

Article 1604 | June 2026

Yes. SAQ A for PCI DSS v4.x includes requirements for external vulnerability scanning by a PCI SSC Approved Scanning Vendor (ASV) for merchant e-commerce webpages, even where payment processing is fully outsourced to a third party. Requirements 11.3.2 and 11.3.2.1 were added to SAQ A to address risks where a merchant's webpage could be compromised and thereby result in compromise of the payment process.

Merchants with e-commerce webpages that complete SAQ A, even where payment processing is outsourced to TPSPs, still have responsibility for the PCI DSS requirements included in SAQ A, including the requirements for ASV scanning. This includes merchants with webpages that:

- Redirect transactions to a TPSP (or to another third-party redirection server which then redirects to a TPSP).
- Include a TPSP's embedded iframe (or an iframe that includes another TPSP's iframe).

PCI ASV scans for purposes of satisfying PCI DSS Requirement 11.3.2 must be performed by a PCI Approved Scan Vendor (ASV) listed as an Approved Scanning Vendor

(https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors/) on the PCI SSC website, using the ASV scan solution from that vendor.

The two-page ASV Resource Guide (<https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI%20SSC%20ASV%20Resource%20Guide.pdf>), created in 2024, provides information to help understand this requirement and how it applies to merchants, including those completing SAQ A.