Marshall & Sterling
INSURANCE

Payment Card Industry Data Security Standard Compliance Guide

Provided by: Marshall & Sterling

110 Main Street
Poughkeepsie
Tel: (845) 454-0800

TABLE OF CONTENTS

This guide is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance. Consult your licensed Commercial Property and Casualty representative at Marshall & Sterling, Inc. or legal counsel to address possible compliance requirements.

INTRODUCTION

In today's world, customers have serious concerns about the security of their personal data, particularly their credit card information—and for good reason. The 2015 Nilson Report, which provides statistics on the payment card industry, found that credit, debit and prepaid card fraud contributed to global losses in excess of $16 billion. Just in the United States, card issuers lost $4.91 billion and merchants lost $2.95 billion to fraud. What's worse, those losses don't include the related costs that issuers and merchants incur.

To help protect customers, it's critical that any organization that accepts payment cards understands the payment card industry's (PCI) Data Security Standards (DSS).*

Navigating the PCI DSS can be taxing for the average merchant, as an overview of PCI DSS compliance specifics and best practices are rarely found under one, all-encompassing source. Moreover, the PCI DSS itself is over 100 pages and is filled with acronyms and terminology that can be confusing. At Marshall & Sterling, Inc., we are here to help simplify the PCI DSS compliance process, translating information so that it's easy to understand—particularly for those without a PCI background.

**Note:* *While this guide focuses specifically on PCI DSS, there are a number of other PCI standards that merchants may need to comply with, depending on the type and complexity of their businesses. For example, manufacturers must follow the PIN Transaction Security Requirements (PTS) while software developers must adhere to the Payment Application Data Security Standard (PA-DSS). You can find out more information on those standards here.*

GLOSSARY OF TERMS

To improve your understanding of the PCI DSS, it is helpful to first understand the following terms you will come across throughout this guide:

- **Acquirers/acquiring banks:** These are broad terms for banks that issue payment cards, as well as payment processors. These bodies are responsible for enforcing the PCI DSS and for working with payment card brands, particularly because they have established relationships with individual merchants seeking the right to process credit cards.
- **Approved Scanning Vendors (ASVs):** These organizations provide security services and possess tools that can be used to conduct external vulnerability scans for merchants. These organizations are often the strongest choice for merchants looking to conduct a gap analysis because ASVs are audited and approved by the PCI Security Standards Council (PCI SSC) and are equipped to scan systems for issues related to the most up-to-date version of the PCI DSS.
- **Merchants:** For the purposes of this guide, a merchant refers to any establishment—whether it's a brick-and-mortar retailer or an e-commerce retailer—that processes payment cards as part of its operations. It's the merchant's responsibility to implement the PCI DSS and demonstrate compliance at all times.
- **Payment card industry (PCI):** The PCI refers to all organizations that store, process and transmit cardholder data. In general, these cards are most often debit, credit, prepaid, e-purse, ATM and point-of-sale (POS) cards.
- **Payment card industry's Data Security Standards (PCI DSS):** The PCI DSS is the standard that all organizations that handle cardholder information need to follow. This is to guard against payment card fraud and misuse.
- **Qualified Security Assessors (QSAs):** QSAs are organizations that assist merchants in reviewing the security of their payment transaction systems. In addition, these organizations have trained and certified personnel that can assess and validate compliance with the PCI DSS.
- **Report on Compliance (ROC):** An ROC is a formal PCI DSS assessment that can only be issued by a certified QSA.
- **Self-assessment Questionnaire (SAQ):** An SAQ is a validation tool that merchants and service providers use to report the results of their PCI DSS self-assessments.

PCI DSS OVERVIEW—HISTORY AND IMPORTANCE

The **PCI DSS is a set of requirements designed to ensure that all entities that process, store or transmit credit card information maintain a secure environment.** In essence, the PCI DSS establishes a minimum set of requirements for protecting the account information of cardholders. Regardless of whether a merchant processes one credit card a year or 1 million, they must adhere to the PCI DSS.

It should be noted that local laws and regulations may require additional protections for personal information or other data elements. The PCI DSS does not supersede or replace local or regional laws, government regulations, or other legal requirements. The PCI DSS should be thought of as industry standards.

History

Prior to the implementation of the PCI DSS, the major payment card companies maintained their own rules related to data protections and payment processing. This meant that there were multiple standards that merchants had to follow to secure cardholder information. Under this system, compliance was often confusing and unmanageable for merchants.

As a result, **the PCI Security Standards Council (SSC)** was formed in 2004 by the world's five leading payment brands—American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Later in 2004, the members of the PCI SSC agreed to align their individual information security standards under the PCI DSS. Merchants must now abide by PCI DSS, and acquirers, like banks and large payment processors, must help enforce these standards.

The Importance of Compliance

Failure to comply with the PCI DSS can result in serious consequences for merchants. If a merchant experiences a data breach and is found to be non-compliant with the PCI DSS, it may be subject to hefty fines.

Depending on the circumstances, a merchant may be required to pay anywhere from $5,000 to $100,000 a month until it addresses all compliance issues. What's more, if non-compliance persists, a merchant may lose its ability to process payment cards.

Beyond the threat of fines, PCI DSS non-compliance can jeopardize the vital relationships a merchant has established with its customers. Following a data breach, brand loyalty is easily lost, especially when a merchant is trusted to keep personal identifiable information out of the hands of fraudsters. This can result in months and even years of lost revenue.

Other potential fallout from failed PCI DSS compliance could include legal action, mandatory audits and remediation costs.

To avoid financial damages and business interruption, you should make compliance with the PCI DSS a priority.

This guide is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance. Consult your licensed Commercial Property and Casualty representative at Marshall & Sterling, Inc. or legal counsel to address possible compliance requirements.

PCI DSS GOALS AND REQUIREMENTS

Unfortunately, becoming PCI DSS compliant isn’t as easy as checking off a few boxes. There are a number of specific security requirements, most with their own sub-requirements. Validating compliance with acquirers and payment card brands can be equally difficult, as the process can differ depending on a variety of factors, including the number of payment card transactions a merchant performs in a year.

First and foremost, understanding the PCI DSS goals and requirements will provide merchants with a general action plan to follow. The following is a quick overview of the 12 major goals and requirements outlined by the PCI DSS:

Goals	PCI DSS Requirements
Build and maintain a secure network and systems.	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect cardholder data.	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a vulnerability management program.	5. Protect all systems against malware and regularly update antivirus software or programs. 6. Develop and maintain secure systems and applications.
Implement strong access control measures.	7. Restrict access to cardholder data to individuals on a need-to-know basis. 8. Identify and authenticate access to system components. 9. Restrict physical access to cardholder data.
Regularly monitor and test networks.	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an information security policy.	12. Maintain a policy that addresses information security for all personnel.

Note: *The above requirements have multiple sub-requirements. Please see Appendix C for more details.*

These standards apply to merchants of any size. In response to the 12 PCI DSS requirements, most organizations implement a Written Information Security Program (WISP) or Data Security Policy that incorporates the requirements of the PCI DSS. These policies and programs should:

- Be easy to implement and understand;
- Address the 12 main goals and requirements of the PCI DSS;
- Take into account operational controls, like employee training and incident response plans; and
- Detail methods for leveraging any lessons learned from an incident to ensure that any gaps in compliance are addressed in a timely fashion.

This guide is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance. Consult your licensed Commercial Property and Casualty representative at Marshall & Sterling, Inc. or legal counsel to address possible compliance requirements.

THE 4 STEPS TO PCI DSS COMPLIANCE

There are four major steps to compliance, as outlined by the PCI SSC. If followed closely, these steps can help merchants of any size integrate PCI DSS standards into their businesses. Those steps include the following:

1. **Determine Merchant Level.** This step involves determining which merchant level applies to your organization as determined by the payment card brands you accept.
2. **Assess.** This process involves identifying vulnerabilities in your IT assets and payment card processing systems.
3. **Remediate.** After you have assessed all PCI DSS issues, you must remediate any security vulnerabilities you have found.
4. **Report.** Once you have assessed and remediated vulnerabilities, you must document your compliance efforts and submit them to the acquirers and payment card companies you are working with.

Remember, PCI DSS compliance is an ongoing process, so it’s important that merchants assess, remediate and report at least annually.

This guide is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance. Consult your licensed Commercial Property and Casualty representative at Marshall & Sterling, Inc. or legal counsel to address possible compliance requirements.

STEP 1: Determine Merchant Level

While the PCI DSS has aligned the data security requirements for protecting cardholder data, each payment card brand still maintains its own data security and compliance program. Therefore, it is critical that merchants understand what each payment card brand requires in order to achieve PCI DSS compliance.

Payment card brands rely on a tiered system to assign compliance requirements to merchants. These tiers, which are more commonly referred to as merchant levels, are determined by the aggregate number of transactions processed by a merchant annually. In general, as the number of payment card transactions a merchant processes rises, so too does the number and complexity of validation and reporting requirements the merchant must comply with.

Depending on an organization’s merchant level, it may be required to perform periodic network scans, vulnerability scans, self-assessments or on-site security assessments. These PCI DSS compliance methods will be reviewed in detail later in the next section.

For a comprehensive look at the merchant levels and associated validation and reporting requirements for each of the five major payment card brands, please consult the charts found in Appendix A of this guide.

This guide is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance. Consult your licensed Commercial Property and Casualty representative at Marshall & Sterling, Inc. or legal counsel to address possible compliance requirements.

STEP 2: ASSESS

The assessment stage of compliance is one of the most important, as it allows merchants to obtain a holistic view of their security weaknesses. The primary goal of this stage is to identify vulnerabilities in the merchant's technologies or processes that could jeopardize the security of cardholder data. Assessments must take into account all technologies and systems that transmit, process or store cardholder data as part of a merchant's operations. Accordingly, the following are some important tips related to assessments:

- Identify all systems—network components, servers, applications, etc.—that handle cardholder data. Utilize card data scanning tools to further address all applicable touchpoints.
- Consider ways to reduce your compliance burden. In practice, this refers to methods merchants can use to separate or remove cardholder data from the rest of their business processes. This can be accomplished through tactics like outsourcing or network segmentation.
- Create a cardholder data matrix to record the systems that store, process or transmit cardholder data. This matrix should identify the following:
    - System name
    - Cardholder data stored
    - Reason for storage
    - Retention period
    - Protection mechanism

Methodology

There are several methods for completing an assessment, some of which may carry over into the later compliance steps. The methodology or methodologies a merchant must use are determined by its merchant level.

Self-assessments

In many instances, a merchant will be required to evaluate their own PCI DSS compliance by completing a self-assessment. Self-assessments are guided by a Self-assessment Questionnaire (SAQ), which is an assessment tool that merchants use to report the results of the PCI DSS self-assessments. There are eight different SAQs available to meet different merchant environments. Entities are encouraged to contact their acquiring banks for assistance if they are unsure which SAQ is applicable to their operations.

Each SAQ contains a series of "yes or no" questions for the applicable PCI DSS requirements. If an organization answers no to any one of the SAQ questions, it may be required to state the future remediation date and associated actions. The various SAQ templates are available through the PCI SSC's Document Library. If you are unsure about any of your SAQ responses, it's best to assume non-compliance until you can find clarification.

It should be noted that, in some cases, SAQs are also considered validation tools that allow merchants to report compliance with acquirers and payment card companies. As such, an SAQ can go a long way in identifying and addressing PCI DSS gaps, in turn, giving merchants a method of verifying compliance.

Please see Appendix B for a detailed list of the different types of SAQs and who they apply to.

Vulnerability Scans

Merchants may also be required to perform vulnerability scans at least quarterly and after any significant change to a network (such as new system component installations, changes in network topology, firewall rule modifications or product upgrades). However, depending on the payment card brand you partner with, you may not need to complete a vulnerability scan as part of your compliance duties.

In either case, it could be beneficial to perform regular scans because they can help confirm that your business has no gaps in data security and that you are fit to process payments.

A vulnerability scan is a combination of automated or manual tools, techniques and methods that are run against external and internal network devices and servers. They are designed to expose potential vulnerabilities that could be found and exploited by malicious individuals. There are two major types of scans to be aware of:

1. **Internal scans.** For internal scanning, the testing procedures must verify that four quarterly internal scans took place within the past 12 months and that rescans occurred until all "high-risk" vulnerabilities were resolved. Internal scans may be performed by internal staff or by a firm specializing in vulnerability scanning.
2. **External scans.** External scans, like internal scans, must be performed at least quarterly. However, all external scans must be executed by an Approved Scanning Vendor (ASV), approved by the PCI SSC. The PCI SSC maintains a list of ASVs, which can be found here.

Other important considerations to be aware of are as follows:

- Merchants that fail a vulnerability scan will have to address any issues found and then do a rescan.
- Some acquiring banks require those that have failed a vulnerability test to submit a detailed plan for remediation. This plan typically identifies what the original compliance issues were and a timeline for addressing them.
- Acquirers may have strict guidelines related to remediation response time. This may vary from bank to bank, but, in general, issues flagged as high vulnerabilities must be remediated within 24 hours. After that, moderate vulnerabilities must be remediated within 72 hours and low vulnerabilities must be remediated by the next quarterly scan.

On-site Assessments

For the overwhelming majority of merchants, a self-evaluation using a SAQ is sufficient to validate PCI DSS compliance. However, there are a number of circumstances under which an entity may be required

This guide is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance. Consult your licensed Commercial Property and Casualty representative at Marshall & Sterling, Inc. or legal counsel to address possible compliance requirements.

to undergo an on-site assessment. An on-site assessment is a detailed review of an organization's card data environment using a standard methodology and reporting format that results in a Report on Compliance (ROC)—which is formally used as a validation tool (*see "Step 4: Report" for more information on ROCs*).

Typically, on-site assessments must be conducted by qualified security assessors (QSAs). QSAs assist merchants in reviewing the security of their payment transaction systems. In addition, these individuals have been trained and certified to assess and validate compliance with PCI DSS.

Assessments by QSAs are required on an annual basis to ensure compliance with the PCI DSS. The PCI SSC maintains the certification process for companies and their employees seeking QSA certification. More information on QSAs and a list of qualified QSA companies can be found on the PCI SSC's website.

STEP 3: REMEDIATE

In general, there are no set rules for remediation defined by the PCI DSS as it relates to timing and tactics. Typically, merchants will work with the vendors they have already identified for an assessment to help address any concerns. ASVs and QSAs are especially helpful in this instance.

Outside of utilizing established relationships with accredited PCI DSS vendors, it's recommended that merchants complete the following four steps:

1. Have your network scanned with software tools to discover vulnerabilities in your data infrastructure. This is essentially the assessment phase of compliance.
2. Classify and rank the different vulnerabilities found during the initial scan. This will help prioritize the remediation process.
3. Remediate your payment systems by applying patches, bug fixes, workarounds and other changes to unsafe processes and workflows.
4. Rescan your system to ensure that the issues identified in your initial assessment have been addressed effectively.

Most experts recommend that remediation tactics be segmented into phases to help reduce the load. Some merchants find that outsourcing aspects of their payment systems to approved PCI DSS vendors can reduce the strain of remediation, as the onus for remediation falls on the third party.

Again, contacting the PCI SSC or a QSA can help you clarify the remediation process, helping you find an effective solution tailored to your business.

STEP 4: REPORT

The reporting (validation) process confirms your status as a PCI DSS compliant organization to acquiring banks and payment card companies. To do this, merchants have to provide evidence that they have taken appropriate steps to protect cardholders' information.

There are several ways of going about this, and there's often some overlap in tactics from the assessment process. This is because many of the vendors used for an initial scan, like QSAs, can also validate compliance.

In general, merchants can validate their compliance through a report on compliance or an SAQ (attestation of compliance).

Reports on Compliance (ROCs)

ROCs are generally considered the most formal attestation of PCI DSS compliance. Generally reserved for large merchants, an ROC is typically completed with the assistance of a QSA following an on-site assessment and includes the following information:

1. An executive summary
2. Specifics on the scope of work; this should take into account things like a description of how the assessment was conducted, what the data environment was like, what types of network segmentation were used, how each sample set was selected and tested, etc.
3. A deeper look at the cardholder data environment, including diagrams of each network, a list of hardware and software used, details on any third-party payment applications, etc.
4. General information on the report, including key contact information and the date the ROC was conducted
5. Vulnerability scan results
6. Other findings and observations

For more information on ROC reporting, please visit the PCI SSC.

Attestation of Compliance

For all other merchants, it's critical to know and understand what your payment card brand is expecting of you. As you may have determined from the assessment portion of this guide, card brands typically have their own set of rules related to reporting.

Most of these guidelines tie back to your merchant level, or annual transaction volumes. For the majority of merchants, completing an annual attestation of compliance, which arises following an SAQ, is sufficient for reporting.

Sometimes referred to simply as an AOC, an attestation of compliance is a form that both merchants and payment processors use to confirm the results of a PCI DSS assessment—like a vulnerability scan or SAQ.

There are a number of different AOC forms available, and you should speak to your acquiring bank to determine what specific documents you need to complete.

This guide is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance. Consult your licensed Commercial Property and Casualty representative at Marshall & Sterling, Inc. or legal counsel to address possible compliance requirements.

CONTINUED COMPLIANCE

PCI DSS compliance is an ongoing process—one that needs to be taken seriously.

To help promote this concept, merchants should adopt PCI DSS compliance steps into business-as-usual processes. In practice, this means that merchants should treat PCI DSS compliance as part of an overall security initiative. Doing so can help businesses ensure that compliance is maintained between scans and assessments, rather than having to remediate issues every quarter.

To incorporate PCI DSS into business-as-usual activities, merchants should do the following:

- Monitor security controls on a regular basis to ensure that they are working effectively
- Respond to any lapses in security controls in a timely manner
- Review the scope of their PCI DSS requirements any time new technology or network configurations are implemented; these requirements should also be reviewed in the event of a merger or acquisition
- Conduct periodic reviews of personnel and communications to confirm continued PCI DSS compliance
- Institute annual reviews of hardware and software to ensure that they are still supported by their original vendors. This not only improves data security infrastructure, but it confirms that technology is up to date on the most recent PCI DSS.

ADDITIONAL RESOURCES

PCI DSS compliance is not something that can be easily addressed on your own—especially if you are a merchant with limited resources. Luckily, there are variety of tools and resources that you can use to provide help or answers to your questions.

The following are just some of the sources available to you online:

Item	Link
General Information	
Membership Information	www.pcisecuritystandards.org/get_involved/join.php
Webinars	www.pcisecuritystandards.org/news_events/events.shtml
FAQs	www.pcisecuritystandards.org
Payment Card Brand Compliance	
American Express	https://www209.americanexpress.com/merchant/services/en_US/data-security
Discover	http://www.discovernetwork.com/merchants/data-security/disc.html
JCB International	http://partner.jcbcard.com/security/jcbprogram/
MasterCard	https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/site-data-protection-PCI.html
Visa Inc.	http://www.visa.ca/merchant/security/account-information-security/index.jsp
Training	
QSA Training	www.pcisecuritystandards.org/training/qsa_training.php
PA-QSA Training	www.pcisecuritystandards.org/training/pa-dss_training.php
Other Training Programs	https://www.pcisecuritystandards.org/training/index.php
Products, Solutions and Vendors Approved by the PCI SSC	
Pin Transaction Security Devices	www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php
Payment Applications	www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php
P2PE Solutions	https://www.pcisecuritystandards.org/approved_companies_providers/validated_p2pe_solutions.php
QSAs	https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php

This guide is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance. Consult your licensed Commercial Property and Casualty representative at Marshall & Sterling, Inc. or legal counsel to address possible compliance requirements.

ASVs	https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php
Documentation	
PCI DSS	https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
Supporting Documents	https://www.pcisecuritystandards.org/security_standards/documents.php
SAQs	https://www.pcisecuritystandards.org/documents/Understanding_SAQs_PCI_DSS_v3.pdf
Glossary	https://www.pcisecuritystandards.org/security_standards/glossary.php

APPENDICES

APPENDIX A: MERCHANT LEVELS BY PAYMENT CARD BRAND

American Express	
Merchant Level	**Requirements**
Level 1: 2.5 million transactions or more per year	1. Quarterly network scan 2. Annual on-site security assessment
Level 2: 50,000 to 2.5 million transactions per year	1. Quarterly network scan 2. Annual SAQ
Level 3 (designated): Less than 50,000 transactions per year and designated by American Express as being required to submit validation documents	1. Quarterly network scan 2. Annual SAQ
Level 3: Less than 50,000 transactions per year	1. Quarterly network scan (not required, but recommended) 2. Annual SAQ (not required, but recommended)
Level EMV: 50,000 or more chip-enabled card transactions per year with at least 75 per cent made on an EMV-enabled (chip-enabled) terminal capable of processing contact and contactless American Express transactions	1. Annual EMV Attestation (AEA)
More information: https://www209.americanexpress.com/merchant/services/en_US/data-security	

Discover		
Merchant Level	**Validation**	**Reporting**
Level 1: 6 million or more card transactions annually	1. Full on-site assessment using the PCI DSS Requirements and	Attestation of compliance from an ROC (submission of scan results is not required)

This guide is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance. Consult your licensed Commercial Property and Casualty representative at Marshall & Sterling, Inc. or legal counsel to address possible compliance requirements.

	Security Assessment Procedures 2. Quarterly external network vulnerability scans	
Level 2: 1 million to 6 million card transactions annually	1. SAQ 2. Quarterly external network vulnerability scans	Attestation of compliance from an SAQ (submission of scan results is not required)
Level 3: 20,000 to 1 million card-not-present only transactions annually	1. SAQ 2. Quarterly external network vulnerability scans	Attestation of compliance from an SAQ (submission of scan results is not required)
Level 4: All other merchants	1. SAQ 2. Quarterly external network vulnerability scans	Attestation of compliance from an SAQ (submission of scan results is not required)
More information: http://www.discovernetwork.com/merchants/data-security/determining-organizations.html		

JCB ***(if you handle cardholder data and transaction data via the internet or an internet-accessible network)***		
	1 million transactions or more per year	**Less than 1 million transactions per year**
Self-assessment	N/A	Required
Security Scan	Quarterly	Quarterly
On-site Review	Yearly	N/A
More information: http://partner.jcbcard.com/security/jcbprogram/index.html		

This guide is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance. Consult your licensed Commercial Property and Casualty representative at Marshall & Sterling, Inc. or legal counsel to address possible compliance requirements.

JCB

(if you do not handle cardholder data and transaction data via the internet or an internet-accessible network)

	1 million transactions or more per year	Less than 1 million transactions per year
Self-assessment	N/A	Required
Security Scan	N/A	N/A
On-site Review	Yearly	N/A
More information: http://partner.jcbcard.com/security/jcbprogram/index.html		

MasterCard

Merchant Level	Criteria	Requirements
Level 1	• Any merchant that has suffered a hack or an attack that resulted in an account data compromise • Any merchant that has more than 6 million total combined MasterCard and Maestro transactions annually • Any merchant meeting the Level 1 criteria of Visa • Any merchant that MasterCard, in its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system	1. Annual on-site assessment 2. Quarterly network scan conducted by an ASV

Level 2	- Any merchant with more than 1 million but less than or equal to 6 million total combined MasterCard and Maestro transactions annually - Any merchant meeting the Level 2 criteria of Visa	1. Annual self-assessment 2. On-site assessment at the discretion of the merchant 3. Quarterly network scan conducted by an ASV
Level 3	- Any merchant with more than 20,000 combined MasterCard and Maestro e-commerce transactions annually but less than or equal to 1 million total combined MasterCard and Maestro e-commerce transactions annually - Any merchant meeting the Level 3 criteria of Visa	1. Annual self-assessment 2. Quarterly network scan conducted by an ASV
Level 4	All other merchants	1. Annual self-assessment 2. Quarterly network scan conducted by an ASV
More information: https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html		

Visa	
Merchant Level	**Requirements**
Level 1: 6 million transactions or more per year	1. File an ROC completed by a QSA annually 2. Submit an attestation of compliance form annually 3. Have a quarterly network scan completed
Level 2: 1 million to 6 million transactions per year	
Level 3: 20,000 to 1 million e-commerce	

transactions annually	by an ASV
Level 4: Less than 20,000 transactions per year and all other merchants	
More information: https://usa.visa.com/support/small-business/security-compliance.html?ep=v_sym_cisp	

APPENDIX B: SAQ CATEGORIES

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing or transmission of any cardholder data on the merchant's systems or premises. *Not applicable to face-to-face channels.*
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have websites that don't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing or transmission of any cardholder data on the merchant's systems or premises. *Applicable only to e-commerce channels.*
B	Merchants using only: • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. *Not applicable to e-commerce channels.*
C	Merchants with payment application systems connected to the internet; no electronic cardholder data storage. *Not applicable to e-commerce channels.*
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*

D	SAQ D for merchants: All merchants not included in descriptions for the above SAQ types. SAQ D for service providers: All service providers defined by a payment card brand as eligible to complete a SAQ.

APPENDIX C: DETAILED PCI DSS REQUIREMENTS

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

1.1	Establish and implement firewall and router configuration standards that do the following: Formalize testing whenever configurations change; Identify all connections between the cardholder data environment and other networks (including wireless) with documentation and diagrams; Document business justification and various technical settings for each implementation; Diagram all cardholder data flows across systems and networks; and Stipulate a review of configuration rule sets at least every six months.
1.2	Build firewall and router configurations that restrict all traffic, inbound and outbound, from "untrusted" networks (including wireless) and hosts, and specifically deny all other traffic except for protocols necessary for the cardholder data environment.
1.3	Prohibit direct public access between the internet and any system component in the cardholder data environment.
1.4	Install personal firewall software on any mobile and/or employee-owned devices that connect to the internet when outside the network, and which are also used to access the network.
1.5	Ensure that related security policies and operational procedures are documented, in use and known to all affected parties.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

2.1	Always change ALL vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This includes wireless devices that are connected to the cardholder data environment or are used to transmit cardholder data.
2.2	Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted definitions. Update system configuration standards as new vulnerability issues are identified.
2.3	Using strong cryptography, encrypt all non-console administrative access such as browser/web-based management tools.
2.4	Maintain an inventory of system components that are in scope for PCI DSS.

2.5	Ensure that related security policies and operational procedures are documented, in use and known to all affected parties.
2.6	Shared hosting providers must protect each entity’s hosted environment and cardholder data.

Requirement 3: Protect stored cardholder data.

3.1	Limit cardholder data storage and retention time to that which is required for business, legal and/or regulatory purposes, as documented in your data retention policy. Purge unnecessary stored data at least quarterly.
3.2	Do not store sensitive authentication data after authorization (even if it is encrypted). Render all sensitive authentication data unrecoverable upon completion of the authorization process. Issuers and related entities may store sensitive authentication data if there is a business justification and if the data is stored securely.
3.3	Mask primary account numbers (PANs) when displayed (the first six and last four digits are the maximum number of digits you may display), so that only authorized people with a legitimate business need can see the full PAN. This does not supersede stricter requirements that may be in place for displays of cardholder data, such as on a POS receipt.
3.4	Render PANs unreadable anywhere they are stored—including on portable digital media, backup media, in logs, and in data received from or stored by wireless networks. Technology solutions for this requirement may include strong one-way hash functions of the entire PAN, truncation, index tokens with securely stored pads or strong cryptography. (See PCI DSS Glossary for definition of strong cryptography).
3.5	Document and implement procedures to protect any keys used for encryption of cardholder data from disclosure and misuse.
3.6	Fully document and implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.
3.7	Ensure that related security policies and operational procedures are documented, in use and known to all affected parties.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

4.1	Use strong cryptography and security protocols such as transport layer security (TLS), secure shell (SSH) or internet protocol security (IPSec) to safeguard sensitive cardholder data during transmission over open, public networks (e.g., the internet, wireless technologies, cellular technologies, General Packet Radio Service [GPRS] and satellite communications). Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for

	authentication and transmission. The use of wired equivalent privacy (WEP) as a security control is prohibited.
4.2	Never send unprotected PANs by end-user messaging technologies (for example, via email, instant message, SMS or chat).
4.3	Ensure that related security policies and operational procedures are documented, in use and known to all affected parties.

Requirement 5: Protect all systems against malware and regularly update antivirus software or programs.

5.1	Install antivirus software on any systems vulnerable to malicious software, especially personal computers and servers.
5.2	Ensure that all antivirus mechanisms are current, actively running and capable of generating audit logs.
5.3	Ensure that antivirus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.
5.4	Ensure that related security policies and operational procedures are documented, in use and known to all affected parties.

Requirement 6: Develop and maintain secure systems and applications.

6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, “high,” “medium” or “low”) to newly discovered security vulnerabilities.
6.2	Protect all system components and software from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.
6.3	Develop internal and external software applications based on industry standards and in a secure fashion.
6.4	Follow change control processes and procedures for all changes to system components.
6.5	Prevent common coding vulnerabilities in software development processes by training developers in secure coding techniques and by developing applications based on secure coding guidelines—including how sensitive data is handled in memory.

6.6	Review public-facing web applications. This can be accomplished via manual or automated application vulnerability security assessment tools or methods. This must be done at least annually to address new threats and vulnerabilities recurrently.
6.7	Ensure that related security policies and operational procedures are documented, in use and known to all affected parties.

Requirement 7: Restrict access to cardholder data on a need-to-know basis.

7.1	Limit access to system components and cardholder data to only those individuals whose jobs require such access.
7.2	Establish an access control system for system components that restricts access based on a need-to-know basis, and is set to "deny all" unless specifically allowed.
7.3	Ensure that related security policies and operational procedures are documented, in use and known to all affected parties.

Requirement 8: Identify and authenticate access to system components.

8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all systems.
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components.
8.3	Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, including vendor access for support or maintenance.
8.4	Document and communicate authentication procedures and policies to all users.
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods.
8.6	Use of other authentication mechanisms such as physical security tokens, smart cards and certificates must be assigned to an individual account.
8.7	All access to any database containing cardholder data (including access by applications, administrators and all other users) is restricted.
8.8	Ensure that security policies and operational procedures for identification and authentication are documented, in use and known to all affected parties.

Requirement 9: Restrict physical access to cardholder data.

9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
9.2	Develop procedures to easily distinguish between on-site personnel and visitors.
9.3	Control physical access for on-site personnel to sensitive areas.
9.4	Implement procedures to identify and authorize visitors.
9.5	Physically secure all media.
9.6	Maintain strict control over the internal or external distribution of any kind of media.
9.7	Maintain strict control over the storage and accessibility of media.
9.8	Destroy media when it is no longer needed for business or legal reasons.
9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.
9.10	Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use and known to all affected parties.

Requirement 10: Track and monitor all access to network resources and cardholder data.

10.1	Implement audit trails to link access to system components to each individual user.
10.2	Implement automated audit trails for all system components for reconstructing these events: All individual user access to cardholder data; All actions taken by any individual with root or administrative privileges; Access to all audit trails; Invalid logical access attempts; Use of and changes to identification and authentication mechanisms (including the creation of new accounts, elevation of privileges), and all changes, additions and deletions to accounts with root or administrative privileges; Initialization, stopping or pausing of the audit logs; and The creation and deletion of system-level objects.
10.3	Record audit trail entries for all system components for each event, including at a minimum:

This guide is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance. Consult your licensed Commercial Property and Casualty representative at Marshall & Sterling, Inc. or legal counsel to address possible compliance requirements.

	User identification Type of event Date and time Success or failure indication Origination of event Identity or name of affected data System component Resource
10.4	Using time synchronization technology, synchronize all critical system clocks and times and implement controls for acquiring, distributing and storing time.
10.5	Secure audit trails so they cannot be altered.
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.
10.7	Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.
10.8	Ensure that related security policies and operational procedures are documented, in use and known to all affected parties.

Requirement 11: Regularly test security systems and processes.

11.1	Implement and utilize processes that help test for authorized and unauthorized wireless access points. This should be done at least quarterly.
11.2	Carry out internal and external vulnerability scans at least quarterly. These should also be done following a significant change in the network (like new technology, firewall modifications, updates, etc.).
11.3	Create a method for penetration testing. This should include testing from both inside and outside the network.
11.4	Utilize intrusion-detection systems to monitor and prevent unwanted network access.
11.5	Deploy a change-detection mechanism—such as a file-integrity monitoring tool—to alert key individuals to unauthorized modifications.
11.6	Ensure that related security policies and operational procedures are documented, in use and

	known to all affected parties.

Requirement 12: Maintain a policy that addresses information security for all personnel.

12.1	Establish, publish, maintain and disseminate a security policy; review the security policy at least annually and update it when the environment changes.
12.2	Implement a risk assessment process that is performed at least annually and after significant changes are made to the environment, which identifies critical assets, threats and vulnerabilities, and results in a formal assessment.
12.3	Develop usage policies for critical technologies to define their proper use by all personnel. These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and internet.
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
12.5	Assign the information security management responsibilities to an individual or team.
12.6	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
12.7	Screen potential personnel prior to hire to minimize the risk of internal attacks. Example screening includes researching previous employment history, criminal records and credit history, and conducting reference checks.
12.8	Maintain and implement policies and procedures to manage service providers with which cardholder data is shared, or that could affect the security of cardholder data.
12.9	**Additional requirement for service providers only:** Service providers acknowledge in writing to customers that they are responsible for the security of the cardholder data that they possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.

This guide is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance. Consult your licensed Commercial Property and Casualty representative at Marshall & Sterling, Inc. or legal counsel to address possible compliance requirements.