securityMETRICS®

White paper

HOW TO BECOME COMPLIANT WITH PCI DSS 3.2

WHAT'S NEW AND HOW TO PREPARE

HOW TO BECOME COMPLIANT WITH PCI DSS 3.2

WHAT'S NEW AND HOW TO PREPARE

INTRODUCTION

Payment Card Industry Data Security Standard (PCI DSS) version 3.2 PCI DSS 3.2 received minimal changes (and future versions will likely contain similar incremental changes), which were specifically related to security threats rather than large-scale updates. Many of the 3.2 updates were minor clarifications to existing requirements or geared towards testing procedures.

PCI DSS 3.2 and supporting documents were released on April 28, 2016. On October 31, 2016, PCI DSS 3.1 will retire, and at this time all assessments will need to use version 3.2 self-assessment questionnaires (SAQs). By February 1, 2018, organizations need to implement all new 3.2 requirements (which are currently considered best practices).

Key changes in PCI DSS 3.2 are:

- Revised SSL and early TLS sunset dates as outlined in the Bulletin on Migrating from SSL and Early TLS
- Expansion of requirement 8.3 to include use of multi-factor authentication for administrators accessing the cardholder data environment
- Additional security validation steps for service providers and others, including the "Designated Entities Supplemental Validation" (DESV) criteria, which was previously a separate document

In this white paper, you will learn about these and other key PCI DSS 3.2 changes as well as tips to help you understand and implement PCI compliance.

KEY PCI DSS 3.2 UPDATES

UPDATED MIGRATION DATES

In December 2015, the migration dates for organizations to move from SSL and early TLS to the latest version of TLS (e.g., TLS 1.2 or better) were moved back from June 2016 to June 2018. Because as of June 30, 2016, service providers are required to provide a secure service offering, the PCI Council wanted to reflect that date change in the latest version of PCI DSS.

Many businesses are opting to stick to the original 2016 date so they don't have to deal with the extra exposure. Using SSL encryption is very risky to security since it has many exploitable vulnerabilities. So even though the deadline has been extended, it's a good idea to update to TLS 1.2 as soon as possible.

If you use SSL and early TLS and need to continue using these tools, remember not to add any new systems or technologies that use SSL and early TLS. If you need to continue them for regular business operations, the following examples explain some options:

- Upgrade to a current, secure version of TLS configured not to accept fallback to SSL or early TLS.
- Encrypt data with strong cryptography before sending over SSL/early TLS (for example, use field-level or application-level encryption to encrypt data prior to transmission).
- Set up a strongly-encrypted session first (e.g. IPsec tunnel), then send data over SSL within the secure tunnel.
- Check firewall configurations to see if SSL can be blocked.
- Check that all application and system patches are up-to-date.
- Check and monitor systems to identify suspicious activity indicating a security issue.

You need to establish a formal Risk Mitigation and Migration Plan, where you detail your plans to migrate to TLS 1.2 (or better) and describe controls in place to reduce the risk associated with SSL/early TLS until the migration is complete. For example, new vulnerabilities could emerge at any time, and it's up to you to remain up-to-date with vulnerability trends and determine if your organization is susceptible to any known exploits.

For Point of Sale (POS) Point of Interaction (POI) terminals using SSL and/or early TLS, you need to verify that the terminals (and the SSL/TLS termination points to which they connect) are not susceptible to any known exploits. If you find vulnerabilities in your POS POI environment, plan for migration to the latest version of TLS immediately. Although you are allowed to use SSL/early TLS for POIs after June 30, 2018, you should consider upgrading your POI environments to the latest version of TLS.

INCORPORATING DESIGNATED ENTITIES SUPPLEMENTAL VALIDATION INTO PCI DSS

PCI DSS 3.2 incorporates some extra validation procedures in the Appendix. An entity is required to undergo an assessment according to this Appendix ONLY if instructed to do so by an acquirer or a payment brand. Designated entities are those who:

- Store, process, and/or transmit large volumes of cardholder data
- Provide aggregation points for cardholder data
- Have suffered significant or repeated breaches of cardholder data

If you're unsure if you're a designated entity, you likely aren't one. Acquirers and payments brands should notify you if you are and what you are required to do. For example, in addition to full PCI DSS validation, designated entities must have some additional validation that determines whether a business's day-to-day practices are reflective of their compliance.

The additional validation procedures are for designated entities to ensure they are PCI compliant on a day-to-day basis.

An example would be looking at a list of all the change controls in a merchant's environment for the past year. These procedures could include anything that shows the day-to-day compliance.

CLARIFYING MASKING CRITERIA (REQ. 3.3)

PCI DSS 3.2 clarifies masking criteria for primary account numbers (PAN) when displayed. Masking is described as hiding information from view; this is not the same as encryption. When displaying a credit card number or bank identification number (BIN), you are allowed to display, at a maximum, the first 6 and last 4 numbers.

Although you can display the first 6 and last 4 numbers of sensitive data, only display what is necessary to perform a specific business function. For example, if a job only needs the last 4 digits, mask the rest of the information.

Additionally, you're required to document who needs access to more than the first six/last four numbers of sensitive data (including full PAN). You must log all access to cardholder data, specially what data was viewed by which user.

REMEMBER, IF YOUR BUSINESS STORES PAN, YOU'RE ALSO REQUIRED TO ENCRYPT AND PROPERLY SECURE IT.

CHANGE MANAGEMENT PROCESS (REQ. 6.4.6)

PCI DSS 3.2 explains that you need to have a change management process to ensure that all new or changed systems and networks implement all relevant PCI DSS requirements, upon completion of a significant change. Your documentation should include what qualifies as a 'significant change' and these process updates.

Examples of possible requirements that could be impacted:

- Network diagram is updated to reflect changes
- Systems are configured per configuration standards, with all default passwords changed and unnecessary services disabled
- Systems are protected with required controls—e.g., file-integrity monitoring (FIM), anti-virus, patches, audit logging
- Sensitive authentication data (SAD) is not stored and all cardholder data (CHD) storage is documented and incorporated into data-retention policy and procedures
- New systems are included in the quarterly vulnerability scanning process

MULTI-FACTOR AUTHENTICATION REQUIRED IN AND OUT (REQ. 8.3)

PCI DSS 3.2 requires additional multi-factor authentication for administrators within a Cardholder Data Environment (CDE). Multi-factor authentication is an effective way to secure your CDE, and is a requirement under PCI DSS. To properly configure multi-factor authentication, you must have at least two of three things:

- Something you know (username, password, etc.)
- Something you have (getting a code from your phone)
- Something you are (Fingerprint and other biometrics)

Prior to PCI DSS 3.2, multi-factor authentication was previously required for remote access to the network (e.g., external network access) by employees, administrators, and third parties. But now, all non-console administrative access into the CDE requires multi-factor authentication. As with all PCI DSS requirements, this is a reflection of the current threat landscape. This change helps strengthen security within your CDE as well as outside it.

Additionally, make sure you "incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network."

ALL NON-CONSOLE ADMINISTRATIVE ACCESS TO CDE REQUIRES MULTI-FACTOR AUTHENTICATION.

SERVICE PROVIDER WRITTEN AGREEMENT (REQ. 12.8.2)

PCI DSS 3.2 has further explained that "the extent to which the service provider is responsible for the security of cardholder data will depend on the particular service and the agreement between the provider and assessed entity." You should obtain a written security acknowledgement from the service provider, where they acknowledge their responsibility to protect cardholder data that they're storing, processing, transmitting, or can affect your organization's security.

NEW SERVICE PROVIDER REQUIREMENTS

This section contains the most important new and revised requirements specifically for service providers. A service provider is an organization that's not a payment brand, but is directly involved in the processing, storage, or transmission of cardholder data on behalf of another organization (e.g., managed firewalls, merchant processor).

Until January 31, 2018, these new/revised service provider requirements will be considered best practice and become requirements starting February 1, 2018.

CRYPTOGRAPHIC ARCHITECTURE (REQ. 3.5.1)

Service providers need to maintain a documented description of cryptographic architectures, including:

- Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date
- Description of the key usage for each key
- Inventory of any HSMs and other SCDs used for key management

You need to keep pace with evolving threats to your architecture by planning for and documenting updates (e.g., different algorithms/key strengths changes). Maintaining such documentation helps you detect lost or missing keys or key-management devices, and identify unauthorized additions to your cryptographic architecture.

TIMELY DETECTION AND REPORTING (REQ. 10.8, 10.8.1)

Service providers are required to "implement a process for the timely detection and reporting of failures of crucial security control systems," including, but not limited to, failure of:

- Firewalls
- IDS/IPS
- FIM
- Anti-virus
- Physical access controls
- Logical access controls
- Audit logging mechanisms
- Segmentation controls (if used)

Service providers need to respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:

- Restoring security functions
- Identifying and documenting the duration (date and time start to end) of the security failure
- Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause
- Identifying and addressing any security issues that arose during the failure
- Performing a risk assessment to determine whether further actions are required as a result of the security failure
- Implementing controls to prevent cause of failure from reoccurring
- Resuming monitoring of security controls

Document that processes and procedures are in place to respond to security failures. Make sure staff are aware of their responsibilities in the event of a failure. If you are breached, document your organization's actions and responses to the security failure.

IF SECURITY FAILURES ARE NOT QUICKLY AND EFFECTIVELY RESPONDED TO, ATTACKERS MAY USE THIS TIME TO INSERT MALWARE, TAKE SYSTEM CONTROL, AND/OR STEAL DATA FROM YOUR ENVIRONMENT.

PENETRATION TESTING REQUIREMENTS (REQ. 11.3.4.1)

By February 1, 2018, service providers who use segmentation will be required to perform penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.

Validation of PCI DSS scope should be performed as frequently as possible to ensure PCI DSS scope remains up to date and aligned with changing business objectives.

AS A SERVICE PROVIDER, IF YOU USE SEGMENTATION, PERFORM PENETRATION TESTING ON SEGMENTATION CONTROLS AT LEAST EVERY SIX MONTHS AND AFTER ANY CHANGES.

This penetration testing should be performed by a qualified internal resource or third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). The purpose of the penetration testing is to test segmentation controls/methods in use to verify whether segmentation controls/methods are operational and effective.

Although this requirement only applies to service providers, any organization can request a penetration test whenever they wish to measure their business security. Helping you find security weaknesses, penetration testers analyze network environments, identify potential vulnerabilities, and try to exploit those vulnerabilities (or coding errors) just like a hacker would.

The time it takes to conduct a penetration test varies based on network size, network complexity, and the individual penetration test staff members assigned. A small environment can be completed in a few days, but a large environment can take several weeks.

Penetration testers should be well versed in:

- Black hat attack methodologies (e.g., remote access attacks, SQL injection)
- Internal and external testing (i.e., perspective of someone within the network, perspective of hacker over Internet)
- Web front-end technologies (e.g., JavaScript, HTML)
- Web application programming languages (e.g., Python, PHP)
- Web APIs (e.g., restful, SOAP)
- Network technologies (e.g., firewalls, IDS)
- Networking protocols (e.g., TCP/UDP, SSL)
- Operating systems (e.g., Linux, Windows)
- Scripting languages (e.g., Python, Pearl)
- Testing tools (e.g., Nessus, Metasploit)
- Segmentation testing

Typically, penetration test reports contain a detailed description of attacks used, testing methodologies, and suggestions for remediation.

ESTABLISH RESPONSIBILITIES FOR PCI AND DATA (REQ. 12.4.1)

Executive management needs to establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:

- Overall accountability for maintaining PCI DSS compliance
- Defining a charter for a PCI DSS compliance program and communication to executive management

Smaller organizations should add these roles to an individual's job responsibilities, while larger organizations might need to establish a PCI compliance team (e.g., a compliance team made up of IT, accounting, and management). Whichever is the case, management should give their PCI officer/team power to act and implement necessary changes to become PCI compliant, as well as have monthly (or weekly) meetings with executive management.

QUARTERLY PERSONNEL REVIEWS (REQ. 12.11, 12.11.1)

Service providers need to perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:

- Daily log reviews
- Firewall rule-set reviews
- Applying configuration standards to new systems
- Responding to security alerts
- Change management processes

In addition, you need to maintain documentation of quarterly review process, including:

- Documenting results of the reviews
- Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program

SAQ UPDATES

On April 29, 2016, PCI Security Standards Council (SSC) released the revised 3.2 version of existing Self-Assessment Questionnaires (SAQ), which didn't contain new SAQ types or change SAQ descriptions. PCI DSS 3.2 brought minimal change for most SAQ types, except for SAQ A-EP, SAQ C, and SAQ D (for both merchants and service providers).

Here are the basic changes:

- SAQ A added 8 more requirements (e.g., multi-factor authentication, improved user access controls)
- SAQ A-EP added 52 more requirements (e.g., firewall configuration and documentation rules, coding procedures, intrusion detection and prevention systems, multi-factor authentication)
- SAQ B remained the same
- SAQ B-IP added 1 more requirement (e.g., multi-factor authentication)
- SAQ C-VT added 6 more requirements (e.g., multi-factor authentication, improved user access controls)
- SAQ C added 21 more requirements (e.g., multi-factor authentication, improved user access controls)
- SAQ D added 15 more requirements (e.g., multi-factor authentication, cryptographic architecture documentation, semi-annual penetration tests on segmentation)
- SAQ P2PE removed 2 requirements (e.g., masking and emailing unencrypted PAN data)

PCI DSS 3.2 SAQ TYPES

SAQ	Description	# of Questions	Vulnerability Scan	Penetration Testing
A	**E-commerce website (third party)** • Fully outsourced card acceptance and processing • Merchant website provides an iframe or URL that redirects a consumer to a third-party payment processor • Merchant cannot impact the security of the payment transaction	22	N	N
A-EP	**E-commerce website (direct post)** • Merchant website accepts payment using direct post or transparent redirect service	191	Y	Y
B	**Processes cards via:** • Analog phone, fax, or stand-alone terminal • Cellular phone (voice), or stand-alone terminal • Knuckle buster/imprint machine	41	N	N
B-IP	**Processes cards via:** • Internet-based stand-alone terminal isolated from other devices on the network	82	Y	N
C-VT	**Processes cards:** • One at a time via keyboard into a virtual terminal • On an isolated network at one location • No swipe device	79	N	N
C	**Payment application systems connected to the Internet:** • Virtual terminal (Not C-VT eligible) • IP terminal (Not B-IP eligible) • Mobile device (smartphone/tablet) with a card processing application or swipe device • View or handle cardholder data via the Internet • POS with tokenization	160	Y	N
D	**E-commerce website** • Merchant website accepts payment and does not use a direct post or transparent redirect service **Electronic storage of card data** • POS system not utilizing tokenization or P2PE • Merchant stores card data electronically (email, e-fax, recorded calls, etc.)	329	Y	Y
P2PE	**Point-to-point encryption** • Validated PCI P2PE hardware payment terminal solution only • Merchant specifies they qualify for the P2PE questionnaire	33	N	N

PCI DSS 3.2 TAKEAWAYS

Whether you're new to PCI or a veteran, take time to review your past PCI compliance efforts and plan your future PCI DSS 3.2 efforts. Here are five basic payment security elements on which to build your PCI DSS 3.2 compliance program and avoid fines that may result from noncompliance.

1. DOCUMENT EVERYTHING

PCI DSS 3.2 emphasizes the importance of documentation throughout the PCI process. You need to have your policies and procedures physically documented.

Documenting your policies is important because it helps employees and management comprehend what has been done, what still needs to be done, and where problems exist in your environment. It's the failsafe that keeps your security efforts organized. If you don't document your plan for PCI DSS, it will never happen.

Not only does documentation simplify your PCI DSS process, it also provides a great baseline for security training materials. Use your plan to educate employees on important security principles and procedures that apply to them.

If you document throughout your PCI DSS process, you'll save time and maintain a greater level of security.

2. DETERMINE YOUR SCOPE

Although PCI DSS 3.2 didn't add new scoping requirements, it's vital for organizations to know and regularly assess what is 'in-scope.' In-scope means if a particular person/process/technology/component stores, processes, handles, or transmits payment card data, or is connected to systems that do, they must be PCI DSS compliant.

For instance, if your call center agents take credit card payments via phone, enter that data in a computer, and if that information is captured in call recordings, your recordings, the servers that hold the recordings, your call center computers, your call center wireless network, and your call center agents may all be individually in scope.

System components most likely in scope for your environment may include:

- Networking devices
- Servers
- Switches
- Routers
- Computing devices
- Applications

Understanding your PCI DSS scope can save you a lot of trouble. If you understand which pieces of your environment fall under the standard's requirements, you won't unnecessarily work towards compliance on systems that don't need to be compliant or leaving something out.

The only true way to understand your scope is to document it. PCI DSS Requirement 1.1.3 requires the creation of a cardholder data flow diagram for all in scope networks. Data flow diagrams are simply the graphical representations of cardholder data flow throughout your business.

ONCE YOU KNOW YOUR FLOWS AND KNOW WHAT SYSTEMS THEY INTERACT WITH, YOU CAN EASILY CREATE A CARD FLOW DIAGRAM OF HOW CARD DATA MOVES WITHIN YOUR NETWORK.

3. SEGMENT YOUR NETWORK

Segmentation is *not* required to be compliant with PCI DSS 3.2. However, if you're looking for the easiest way to reduce cost, effort, and time spent on getting in-scope systems compliant, you may want to consider segmentation.

Network segmentation can be achieved by physically or virtually separating environment systems that store, process, or transmit cardholder data from those that don't via firewalls or physical gaps.

For example, you install and configure a multi-interface firewall at the edge of your network. From there, you create one interface on the firewall dedicated just to the systems that store/process/transmit cardholder data. If that interface doesn't allow any other traffic into or out of any other zones, this is proper network segmentation.

Segmentation can be extremely tricky, especially for those without a technical security background. Consider having a security professional double check all your segmentation work. For some SAQ types (e.g., SAQ D service providers), you will have additional requirements, such as Requirement 11.3.4.1 requiring penetration testing on segmentation controls at least every six months and after any changes.

4. SPEND MONEY AND TIME TO TRAIN ALL STAFF MEMBERS

Most individuals believe bad technology causes data breaches. However, according to PwC, employees and corporate partners are responsible for 60% of data breaches.

Employees are normal people. They haven't had years of cyber security training (let alone are up-to-date with PCI DSS 3.2), and are therefore more likely to be vulnerable than most technologies, so educate your employees.

Create tailored data security training to individual employee roles. For example, your IT director requires different training than your front desk manager. Your IT director must be trained on how to protect cardholder data within your firewalls and servers, and what to do in the event of a breach. Your front desk manager who processes credit cards should be taught security awareness, how to identify a tampered point of sale system, and the acceptable use of technology.

To help employees retain what you've taught them, train monthly instead of yearly. Remember to require policy documentation signatures annually, and consistently enforce the policy with strict and appropriate sanctions. You only protect your business and customers if you hold employees accountable.

5. ASK A SECURITY PROFESSIONAL

With any updates to PCI DSS (e.g., PCI DSS 3.2), you should *always* consult with a security professional. You or your IT guys are *not* the experts on PCI compliance. PCI DSS Qualified Security Assessors (QSAs) are.

QSAs go through very intense training to understand everything there is to know about PCI DSS and the best ways to comply with many unique and different environments. They have the technical expertise to assist you through the process and to let you know if and how certain requirements apply to your evolving environment and business.

If you're a small business, you probably won't need a PCI DSS audit, but you should still talk to a PCI security professional to verify that you're on the right compliance path for PCI DSS 3.2. Although this requires money up front, it may save you in the long run.

CONCLUSION

The deadline for PCI DSS 3.2 is getting closer. After October 31, 2016, organizations will need to use version 3.2 for all assessments. By February 1, 2018, all new 3.2 requirements need to be implemented. While you have some time to prepare, you should implement the new standard as soon as possible to ensure your organization's security and compliance.

Start by creating and working through your PCI compliance program; you'll also want to add the new and revised requirements to your new/existing program. Keep contact with a trained security professional to help you with compliance throughout the year, especially when you're making changes to your PCI program and cardholder data environment.

By updating your PCI program to comply with 3.2, you help avoid fines and better secure your business's data. The longer you wait, the longer your business could be vulnerable.

ABOUT SECURITYMETRICS

SecurityMetrics has helped over 800,000 organizations comply with PCI DSS, HIPAA, and other mandates. Our solutions combine innovative technology that streamlines compliance validation with the personal support you need to fully understand compliance requirements.

consulting@securitymetrics.com

801.705.5656