Webinar for SAQ A & P2PE Merchants

Josh Black

Principal Security Analyst

QSA, CISSP, CISA

securityMETRICS®

Welcome to today's webinar, and thank you for joining us. My name is Josh Black, and I serve as a Principal Security Analyst at SecurityMetrics. I'm privileged to be part of the Enterprise Audit team here, where we specialize in assisting higher education institutions, government entities, and large enterprises with their PCI DSS and HIPAA assessments.

AGENDA

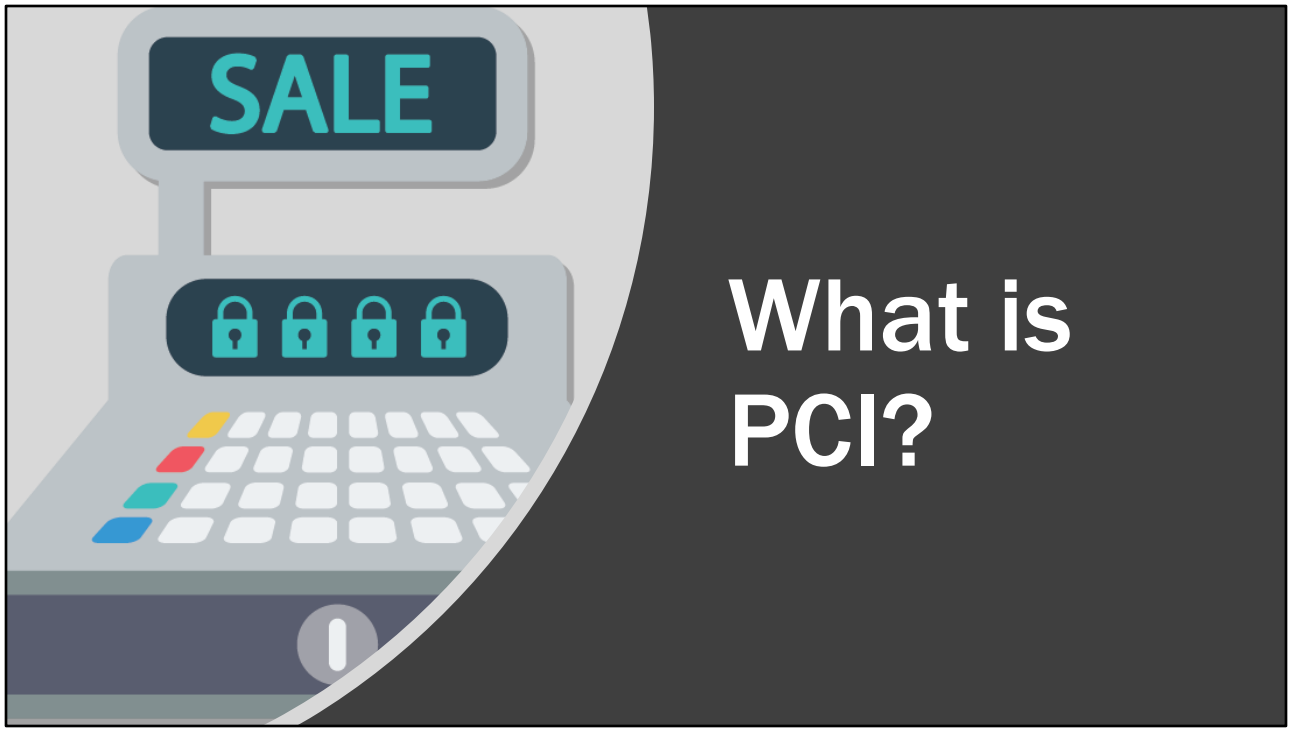
- Introduction to PCI DSS
- What is an SAQ?
- Review Audit Portal Requests
- Preparing for a Remote Assessment

securityMETRICS®

On today's webinar, we'll dive into a brief introduction to PCI DSS and explore how merchants can validate their compliance with this standard.

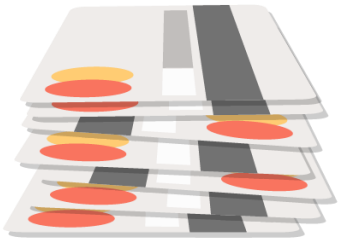
- First, we'll outline the criteria that qualify a merchant for an SAQ A and P2PE type assessment.
- Next, we'll detail the documentation you'll need to provide during your merchant assessment.
- After that, we'll touch upon some common mistakes merchants often make while completing the SAQ.

Throughout the webinar, we encourage you to ask questions. Kindly submit them via the meeting interface, and we'll address them later in the presentation.
Thank you for your active participation, and let's make this a productive session!



The Payment Card Industry Data Security Standard, commonly referred to as PCI DSS, is a set of security controls specifically designed to safeguard cardholder data. Its primary goal is to ensure that businesses process, store, and transmit credit card information in a secure manner.

Payment Card Industry (PCI) Data Security Standard (DSS)

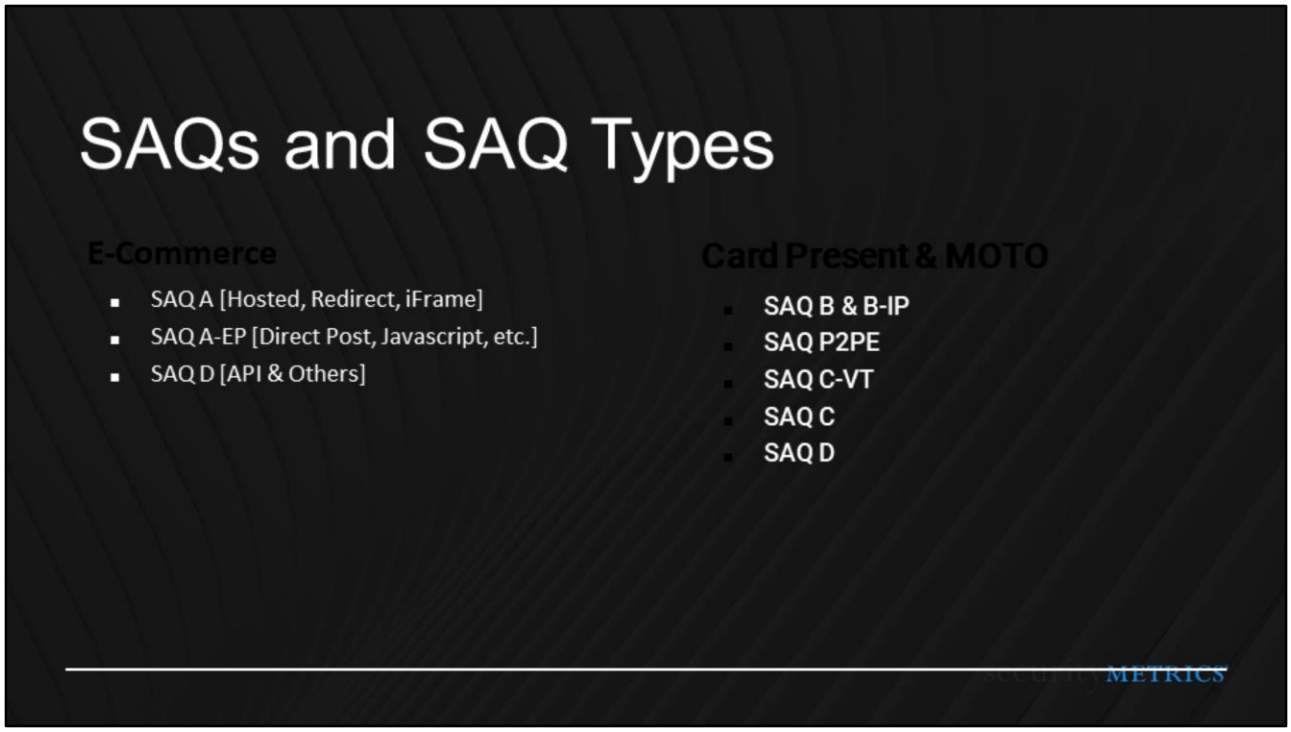


Level 1 and Level 2 Merchants must:

- Have their PCI DSS compliance status validated annually.
- Have assessments performed by someone qualified by the PCI Security Standards Council (SSC).

securityMETRICS®

Your organization falls under the 'Level 2' merchant category based on the annual volume of credit card transactions. As a Level 2 merchant, you have an annual obligation to your merchant bank. This obligation entails providing documentation that confirms a third-party Qualified Security Assessor (QSA) has thoroughly reviewed your merchant environment. The QSA ensures that all requisite PCI-DSS security controls are effectively implemented to safeguard customer cardholder data.



While all merchants accepting credit card payments must adhere to relevant PCI-DSS security controls, the PCI Security Standards Council recognizes the varying needs of different merchants. To simplify the compliance documentation process, the Council introduced Self-Assessment Questionnaires (SAQs). These SAQs are tailored to spotlight key security controls pertinent to specific, lower-risk payment environments. There are various SAQ designations, each crafted for a distinct payment environment. If your setup aligns with one of these lower-risk categories, you're entitled to use the corresponding SAQ for your annual compliance validation.

Self-Assessment Questionnaire Differences

SAQ Level	Requirements
SAQ P2PE	20
SAQ A	19
SAQ A-EP	134
SAQ B	33
SAQ B-IP	86
SAQ C	104
SAQ C-VT	54
SAQ D	259

securityMETRICS®

Here's a very high-level view of the effort required for each SAQ type.

Now let’s discuss the SAQ P2PE. This SAQ is designed for merchants who use a validated Point-to-Point encrypted solution for all processing of cardholder data. To qualify for this SAQ, all cardholder data entry and transmission must be performed by P2PE validated terminals.

Eligibility Criteria – SAQ P2PE

Part 2g. Eligibility to Complete SAQ P2PE	
Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:	
☐	All payment processing is via the validated PCI P2PE solution approved and listed by the PCI SSC (per above).
☐	The only systems in the merchant environment that store, process or transmit account data are the Point of Interaction (POI) devices that are approved for use with the validated and PCI-listed P2PE solution.
☐	Merchant does not otherwise receive or transmit cardholder data electronically.
☐	Merchant verifies there is no legacy storage of electronic cardholder data in the environment.
☐	If Merchant does store cardholder data, such data is only in paper reports or copies of paper receipts and is not received electronically, **and**
☐	Merchant has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.

securityMETRICS®

On pg4 of the SAQ P2PE, you will find a list of criteria that must be true to qualify to use the SAQ P2PE to validate your merchant PCI DSS status. Let's look at what each of these mean.

1. **All payment processing is via the validated PCI P2PE solution approved and listed by the PCI SSC.** [A list of validated P2PE solutions can be found on the PCI SSC website. To use the SAQ P2PE, you must be processing payments using a validated and listed solution]
2. **The only systems in the merchant environment that store, process or transmit account data are the Point of Interaction (POI) devices that are approved for use with the validated and PCI-listed P2PE solution.**
3. **Merchant does not otherwise receive or transmit cardholder electronically.** [Receiving or processing data electronically on any other system would disqualify merchants from using the SAQ P2PE]
4. **Merchant verifies there is no legacy storage of electronic cardholder data in the environment.** [Remember how cardholder data was processed prior to implementing the P2PE solution. Verify that there are no instances of stored cardholder data on legacy systems.]
5. **If Merchant does store cardholder data, such data is only in paper receipts and is not received electronically**
6. **Merchant has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.** [Be sure to look through the PIM provided by your P2PE solution provider and make sure all requirements listed

within the manual are in place.]

SAQ P2PE Solution Validation

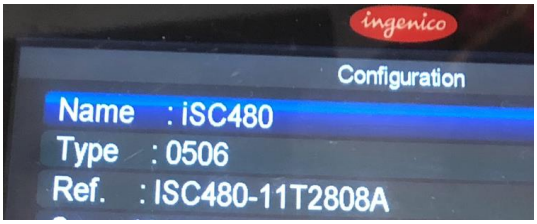
Part 2d. P2PE Solution	
Provide the following information regarding the validated PCI P2PE solution your organization uses:	
Name of P2PE Solution Provider:	
Name of P2PE Solution:	
PCI SSC Reference Number	
Listed P2PE POI Devices used by Merchant (PTS Device Dependencies):	

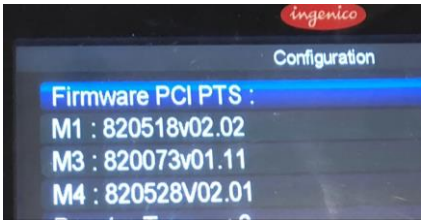
securityMETRICS®

When completing the SAQ P2PE, you will notice that you must include specific details surrounding the P2PE solution in use. This information can be found in the P2PE Instruction Manual or PIM provided by your solution provider. This can also be found on the PCI SSC website at www.pcisecuritystandards.org

Audit Portal – P2PE Version Example

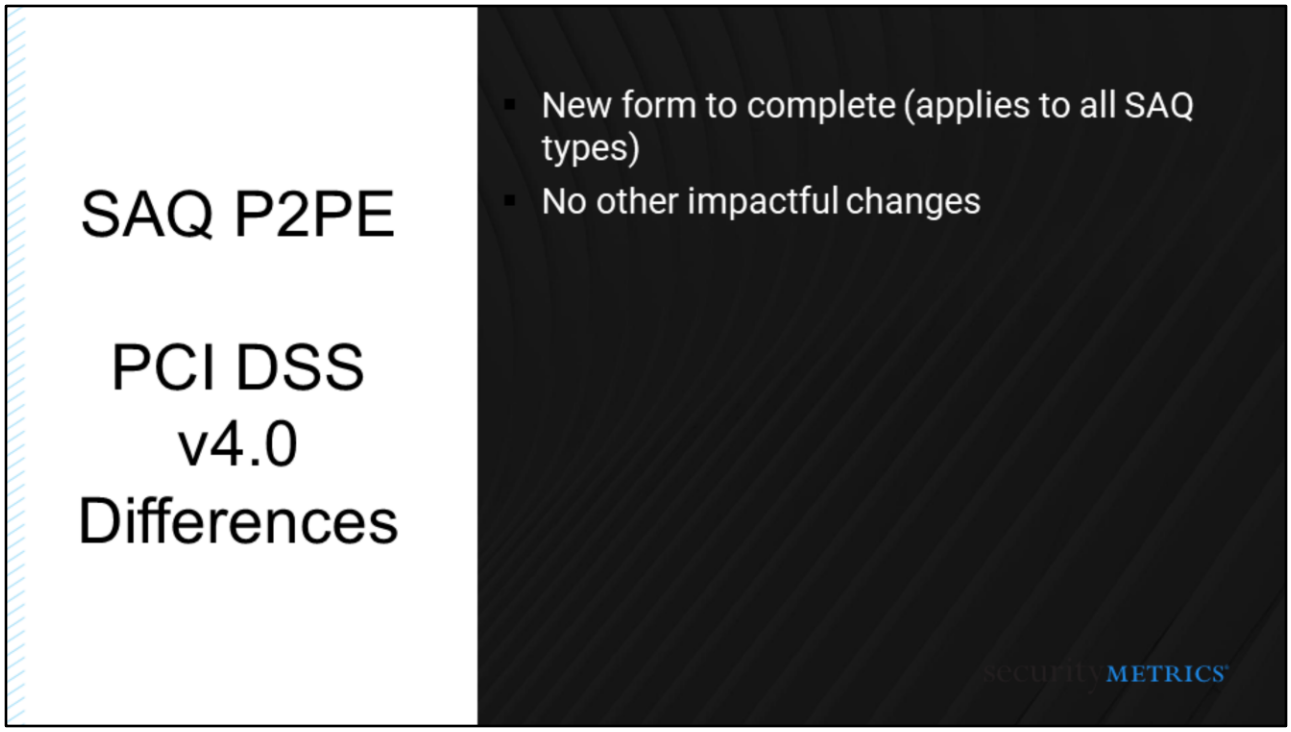
POI device vendor:	*Ingenico*
POI device model name and number:	*ISC Touch 480 (v4)*
Hardware version #(s):	ISC4xx-01Txxxxx, ISC4xx-11Txxxxx
Firmware version #(s):	820518 V11.xx, 820518 V12.xx, SRED (CTLS): 820528V02.xx
PCI PTS Approval #(s):	4-30125





securityMETRICS®

Here's an example of what we want to see in order to verify the device you're using qualifies for the SAQ P2PE. This step is critical.



Those with the SAQ P2PE are in luck, besides a new form to fill out there are no impactful changes to the SAQ P2PE in PCI DSS v4.0

SAQ A

The SAQ A is designed for e-commerce environments where the collection and processing of cardholder data has been fully outsourced to a PCI DSS compliant third-party provider. To qualify for the SAQ A, the university cannot be involved in the electronic collection or transmission of cardholder data.

Eligibility Criteria – SAQ A

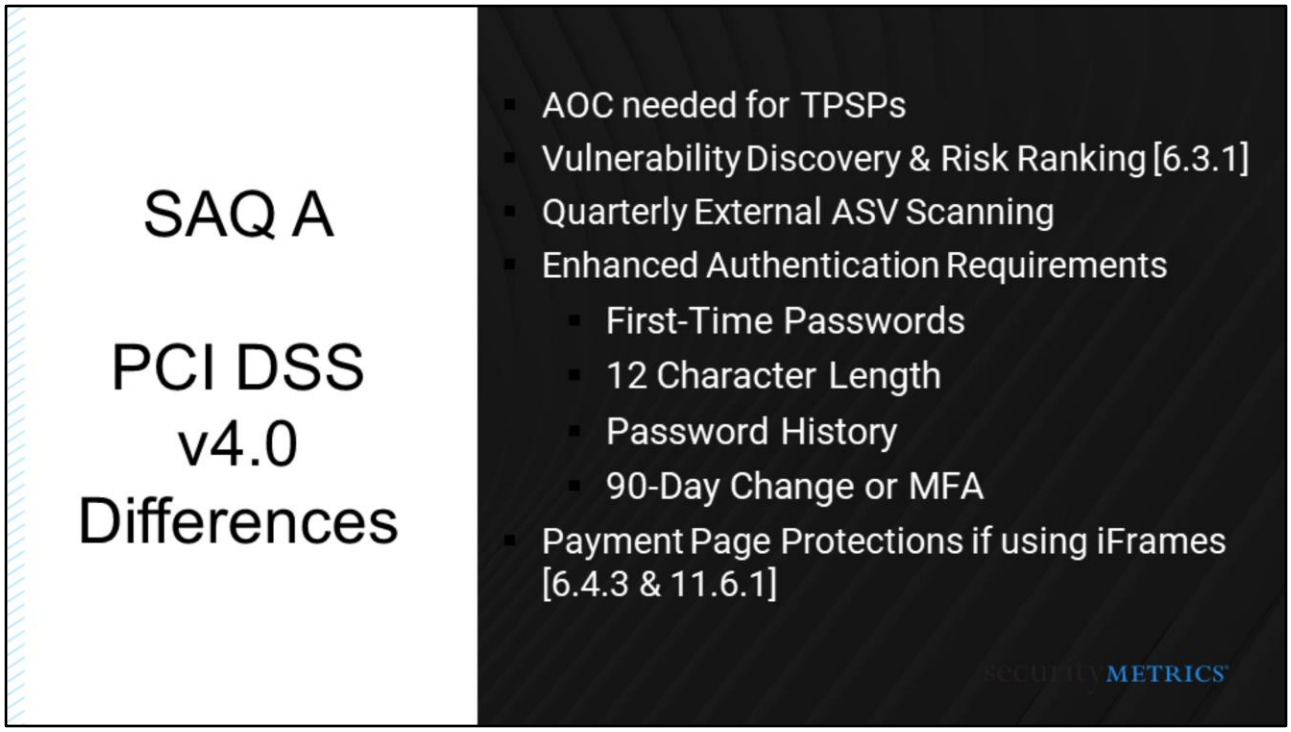
Part 2g. Eligibility to Complete SAQ A	
Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:	
☐	Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions);
☐	All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;
☐	Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;
☐	Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
☐	Any cardholder data the merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.
☐	*Additionally, for e-commerce channels:* All elements of the payment page(s) delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s).

securityMETRICS®

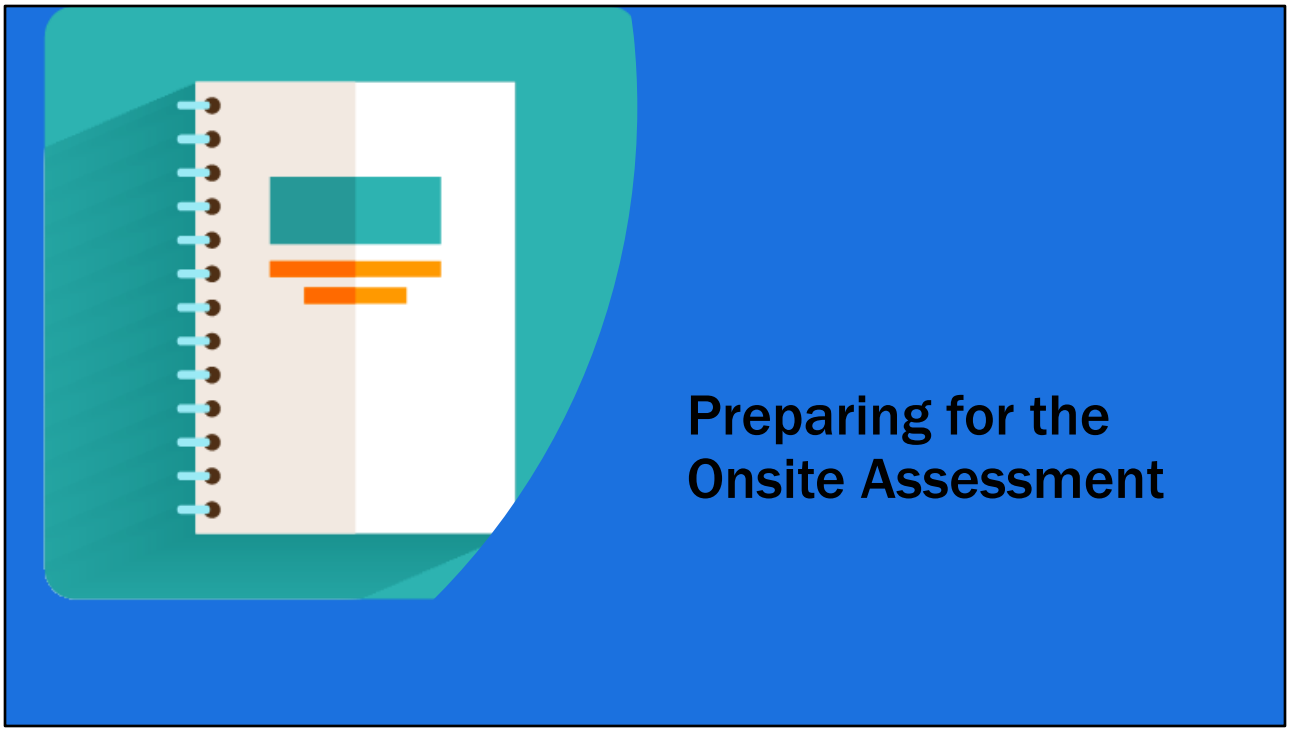
On pg3 of the SAQ A, you will find a list of criteria that must be true to qualify to use the SAQ A to validate your merchant PCI DSS status. Let's look at what each of these mean.

1. **Merchant accepts only card-not-present transactions.** [This means you cannot accept any data in person. If you are taking credit card data at your location and entering it into your own payment website, you would not qualify for the SAQ A.]
2. **All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers** [This means you are not involved in the collection or transmission of cardholder data. A third-party provider, like PayPal, Authorize.net, or Stripe must be fully responsible for collection and processing. If your website collects credit card data and uses an API to forward it to the gateway, you will not qualify for SAQ A]
3. **Merchant does not electronically store, process or transmit any cardholder data…**
4. **Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant.** [You must receive an Attestation of Compliance or AOC from each of your third-party service provider annually to ensure they are continuing to be compliant to the PCI security controls.]
5. **Any cardholder data the merchant retains is on paper…** [This is just another way to say there is no electronic storage of CHD]
6. **All elements of the payment page(s) delivered to the customer's browser**

originate only and directly from a PCI DSS validated third-party service provider. [You must either fully redirect the customer's browser to the payment gateway for collection or implement an iFrame provided by your PCI DSS validated third-party provider to collect the CHD.]



Sounds like a lot of new requirements but many are not “brand new”, but are enhancements of previous requirements.



Now let’s discuss how you can be the most prepared for the onsite assessment.

How to Prepare for the Onsite Assessment

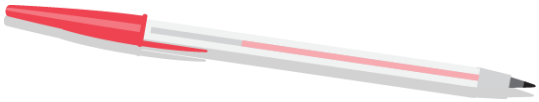
- Have all audit portal requests submitted prior to the assessment
- Be sure appropriate staff members have been invited and can attend

securityMETRICS®

To be ready for the onsite assessment:
1. Before the assessment begins, it's best to have all evidence submitted to the assessor via the audit portal. The assessor will review it before meeting with you and will greatly speed up the onsite portion. The evidence requested will be the main talking points of the assessment.
2. Make sure the right people will be attending. Those people include not only those who are able to answer technical questions related to the evidence requested in the audit portal, but also people familiar with the how the business works, and more importantly, how they take credit/debit card payments.

QUESTIONS?

www.securitymetrics.com



securityMETRICS®