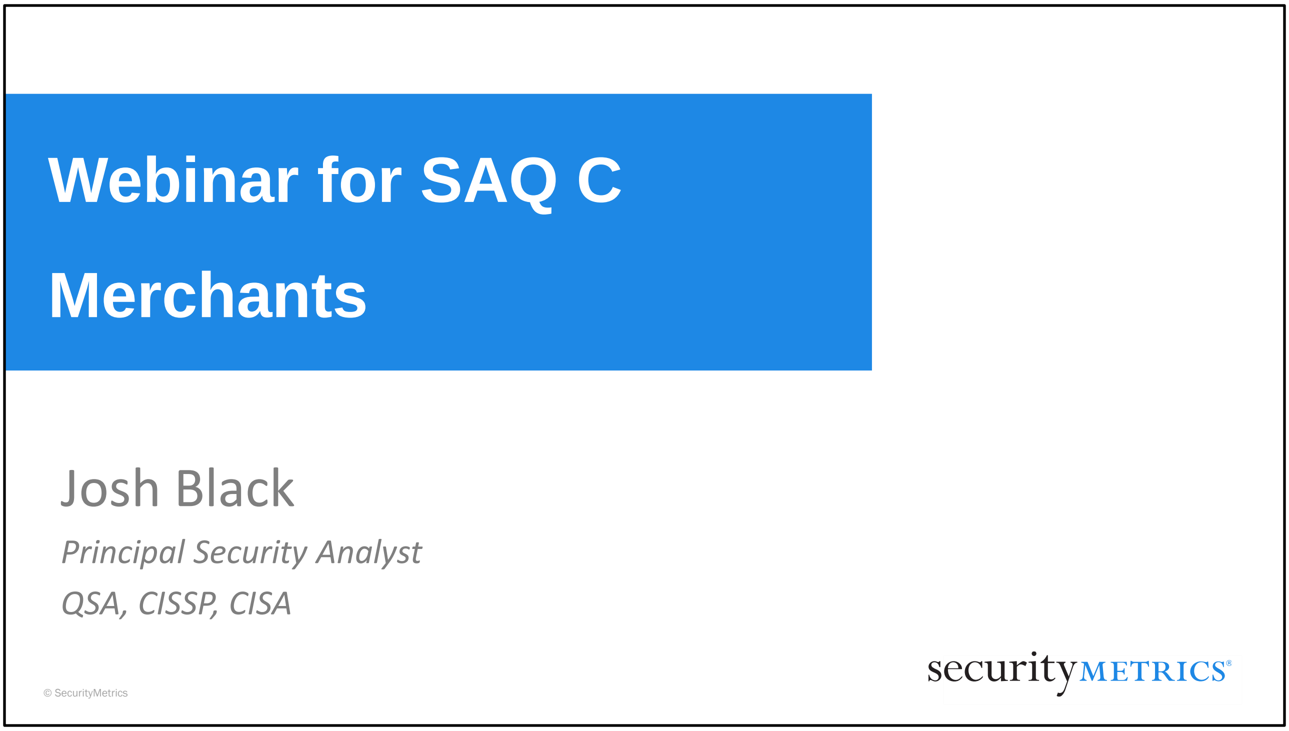


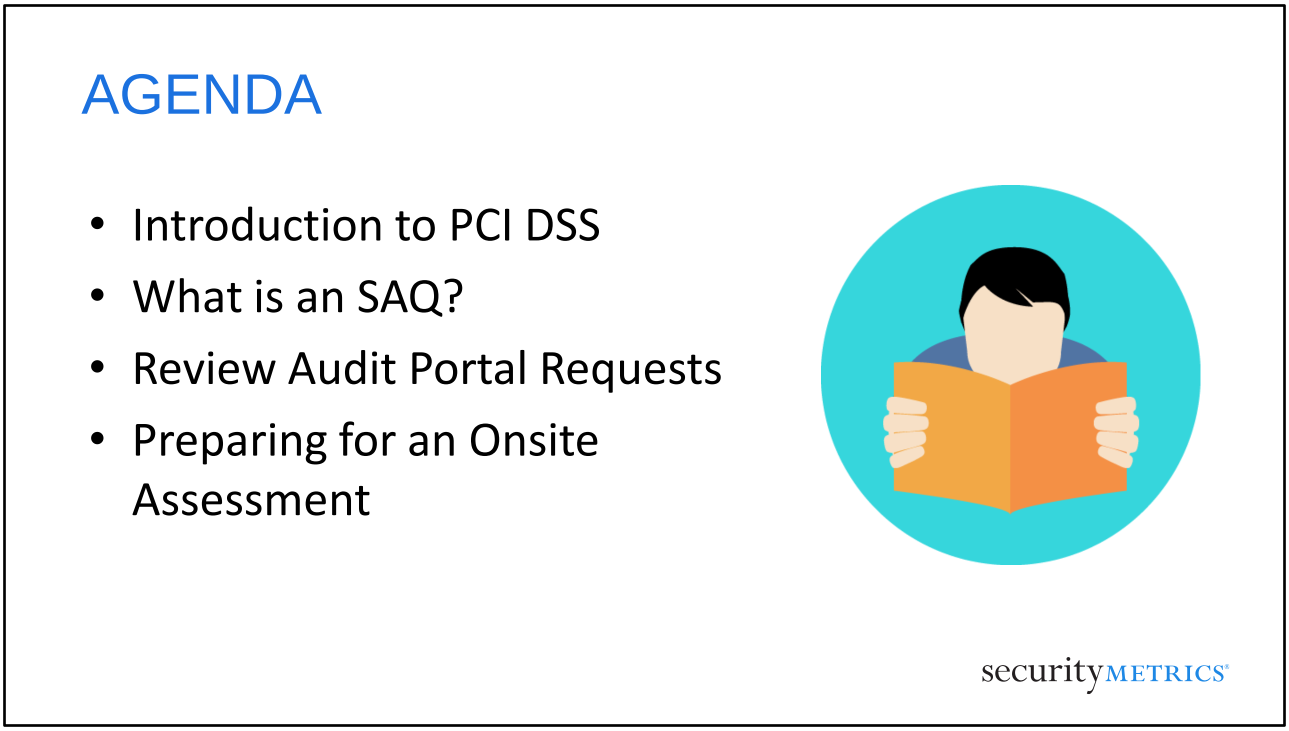
Webinar for SAQ C Merchants

Josh Black

Principal Security Analyst

QSA, CISSP, CISA

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

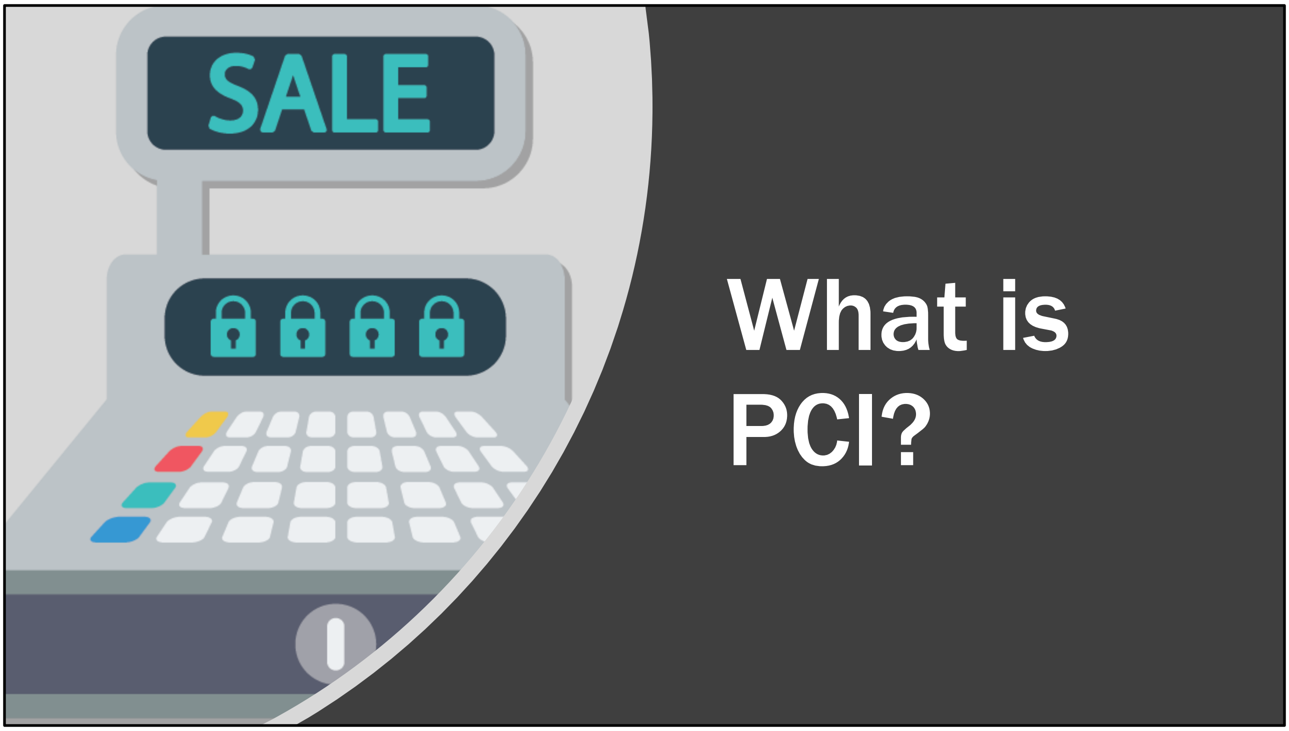
- Introduction to PCI DSS
- What is an SAQ?
- Review Audit Portal Requests
- Preparing for an Onsite Assessment

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.

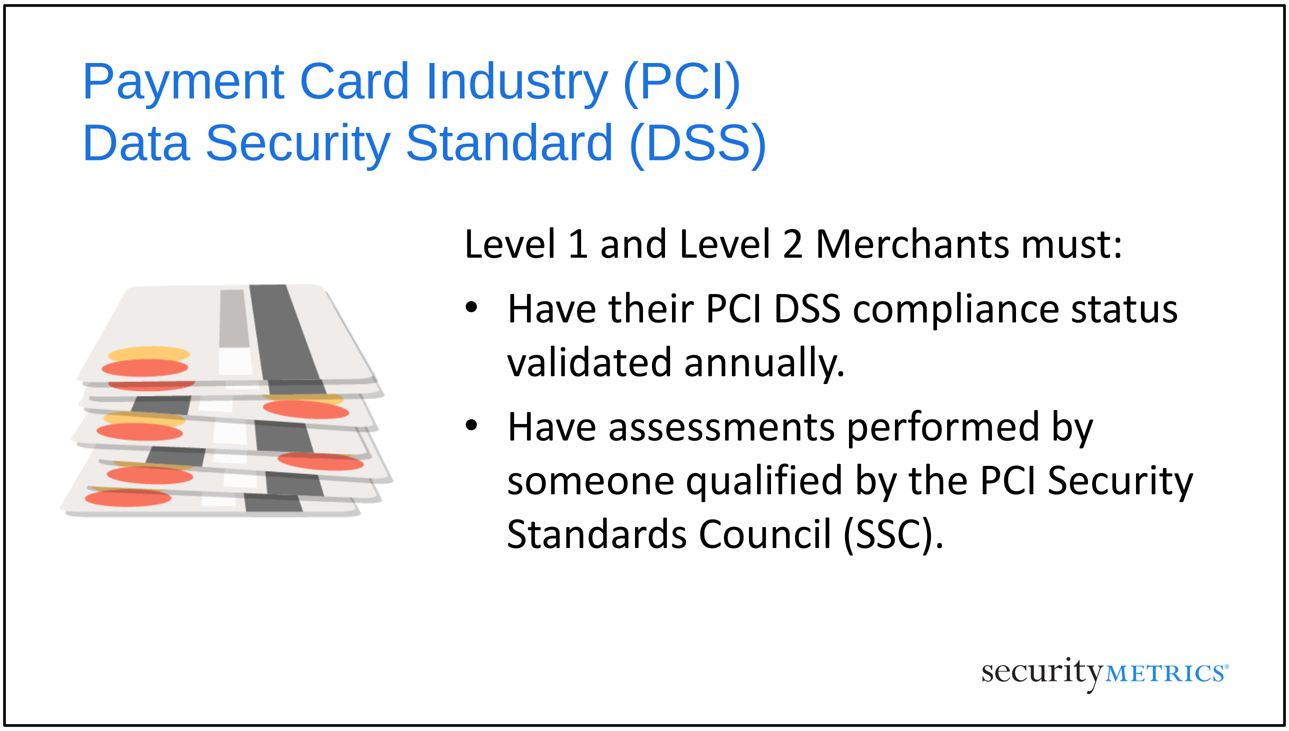
- First, we'll outline the criteria that qualify a merchant for an SAQ C type assessment.
- Next, we'll detail the documentation you'll need to provide during your merchant assessment.
- After that, we'll touch upon some common mistakes merchants often make while completing the SAQ.

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!



What is PCI?

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.



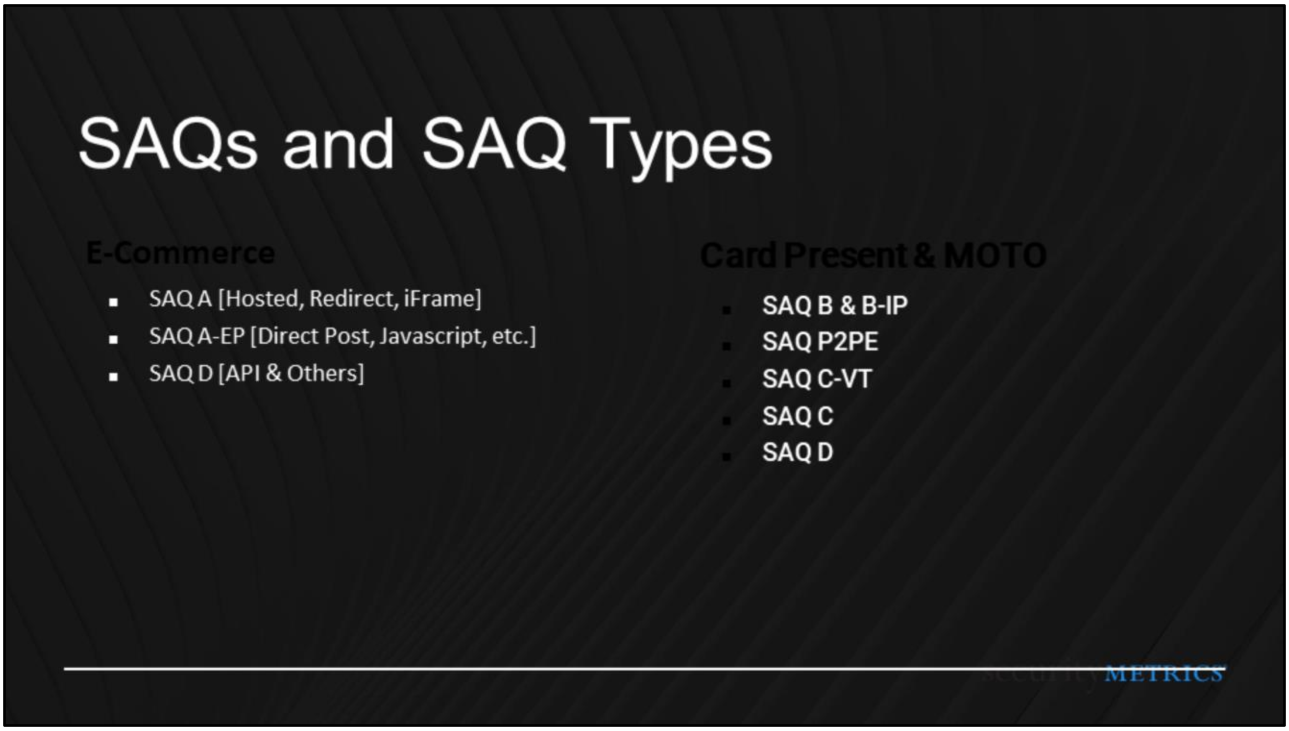
Payment Card Industry (PCI) Data Security Standard (DSS)

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.



SAQs and SAQ Types

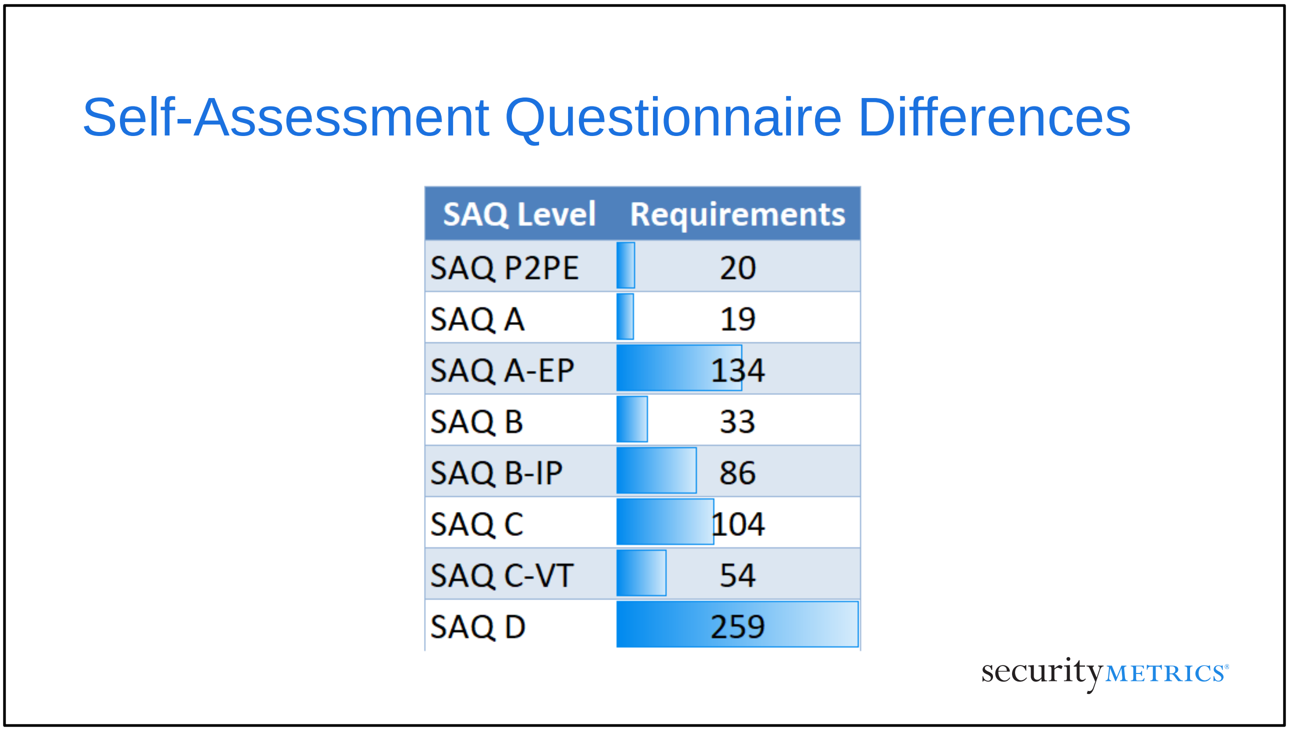
E-Commerce

- SAQ A [Hosted, Redirect, iFrame]
- SAQ A-EP [Direct Post, Javascript, etc.]
- SAQ D [API & Others]

Card Present & MOTO

- SAQ B & B-IP
- SAQ P2PE
- SAQ C-VT
- SAQ C
- SAQ D

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

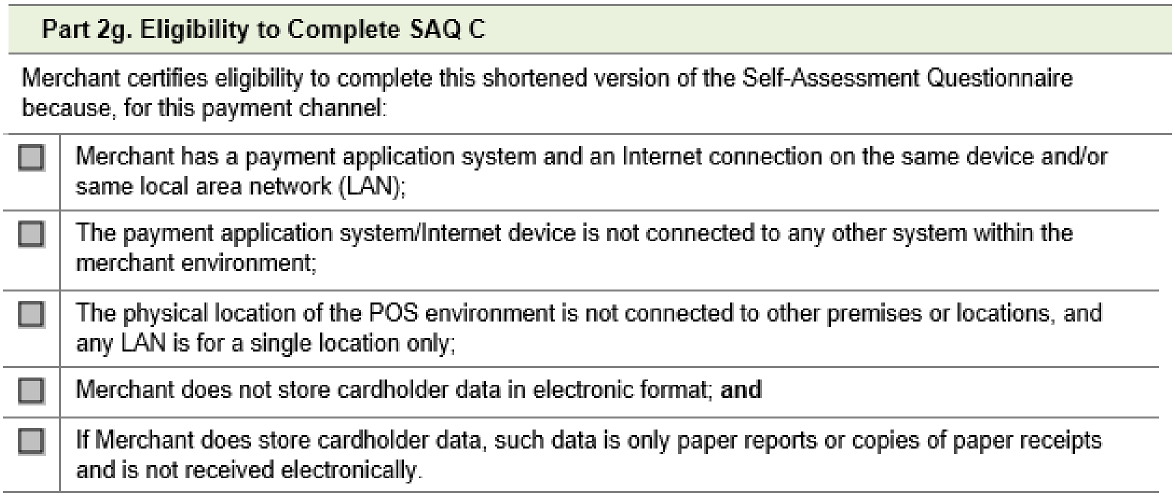
SAQ Level	Requirements
SAQ P2PE	20
SAQ A	19
SAQ A-EP	134
SAQ B	33
SAQ B-IP	86
SAQ C	104
SAQ C-VT	54
SAQ D	259

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

SAQ C

Let's explore the characteristics of SAQ C.

Eligibility Criteria – SAQ C



Part 2g. Eligibility to Complete SAQ C

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:

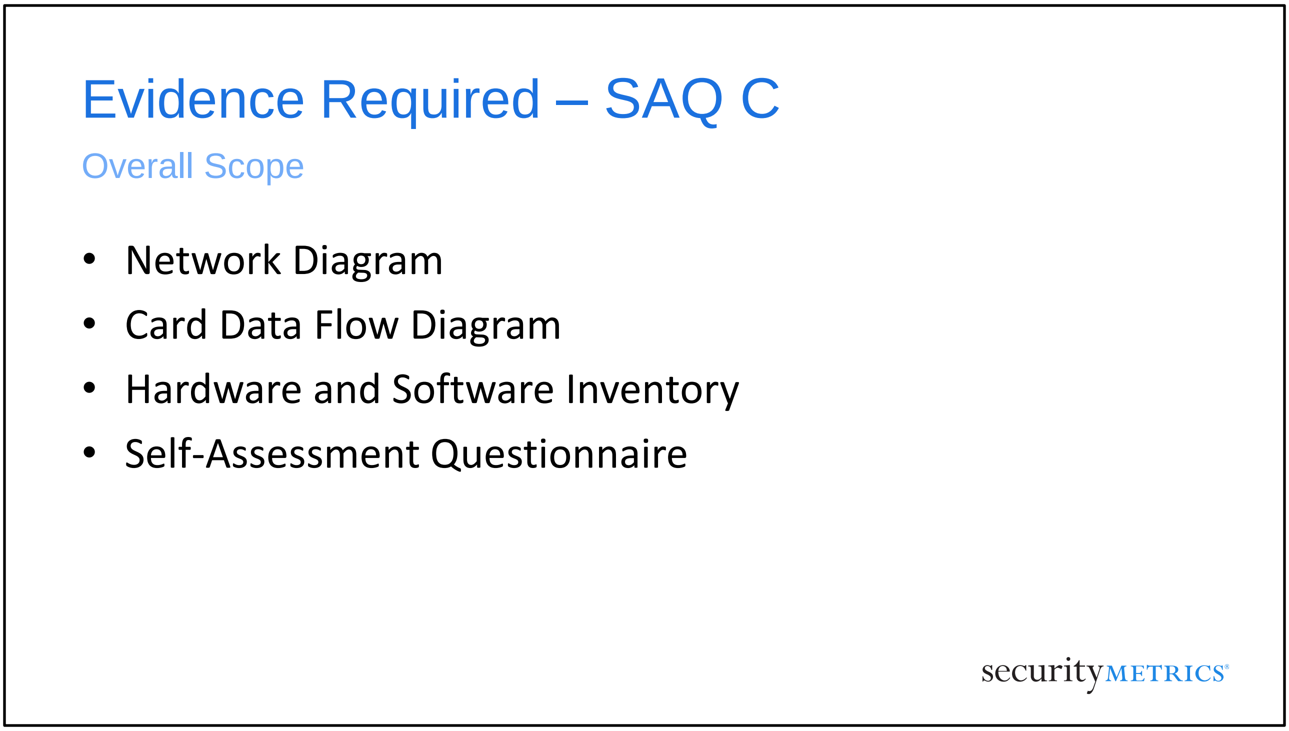
- □ Merchant has a payment application system and an Internet connection on the same device and/or same local area network (LAN);
- □ The payment application system/Internet device is not connected to any other system within the merchant environment;
- □ The physical location of the POS environment is not connected to other premises or locations, and any LAN is for a single location only;
- □ Merchant does not store cardholder data in electronic format; **and**
- □ If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically.

securityMETRICS

To determine if SAQ C is the right questionnaire for your merchant PCI DSS assessment, you'll find an eligibility checklist at its beginning. Let's understand these criteria in detail. I won't read what's already on the screen, but I'll go through them one at a time:

1. You process card data via payment applications that are connected to the internet.
2. The system should be purpose-built.
3. Your POS environment is segmented from all other networks.

4 and 5 - If the merchant retains any cardholder data, it's strictly in the form of physical records, such as paper receipts. This data must not have been received through electronic channels.



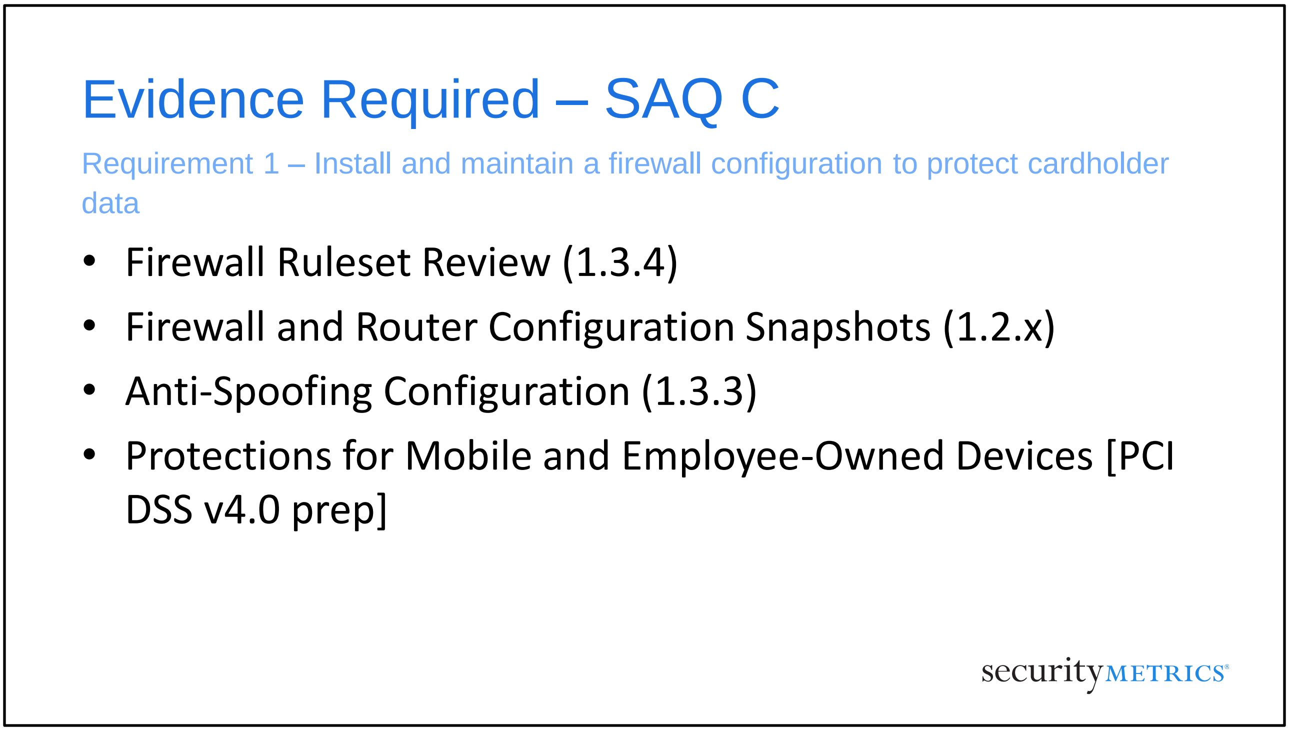
Evidence Required – SAQ C

Overall Scope

- Network Diagram
- Card Data Flow Diagram
- Hardware and Software Inventory
- Self-Assessment Questionnaire

securityMETRICS

1. **Network Diagram:** This is a visual representation of your organization's network infrastructure. It should detail all interconnected systems, devices, and any external connections. Ensure it's up-to-date and accurately reflects the current state of your network, showcasing both the logical and physical connections.
2. **Card Data Flow Diagram:** This diagram visually portrays how cardholder data moves within your organization - from the point of entry (like point-of-sale systems) to where it's processed, transmitted, and stored. Sometimes it’s helpful to have a numbered diagram with a description of each step along with how cardholder data is protected (i.e., TLS, etc.).
3. **Hardware and Software Inventory:** Provide a comprehensive list of all hardware devices and software applications in use within the cardholder data environment. This inventory helps in understanding the technology landscape, ensuring that all components are secure and compliant.
4. **Completed Self-Assessment Questionnaire (SAQ):** Ensure that the SAQ is thoroughly and accurately filled out, reflecting the security controls you have implemented.



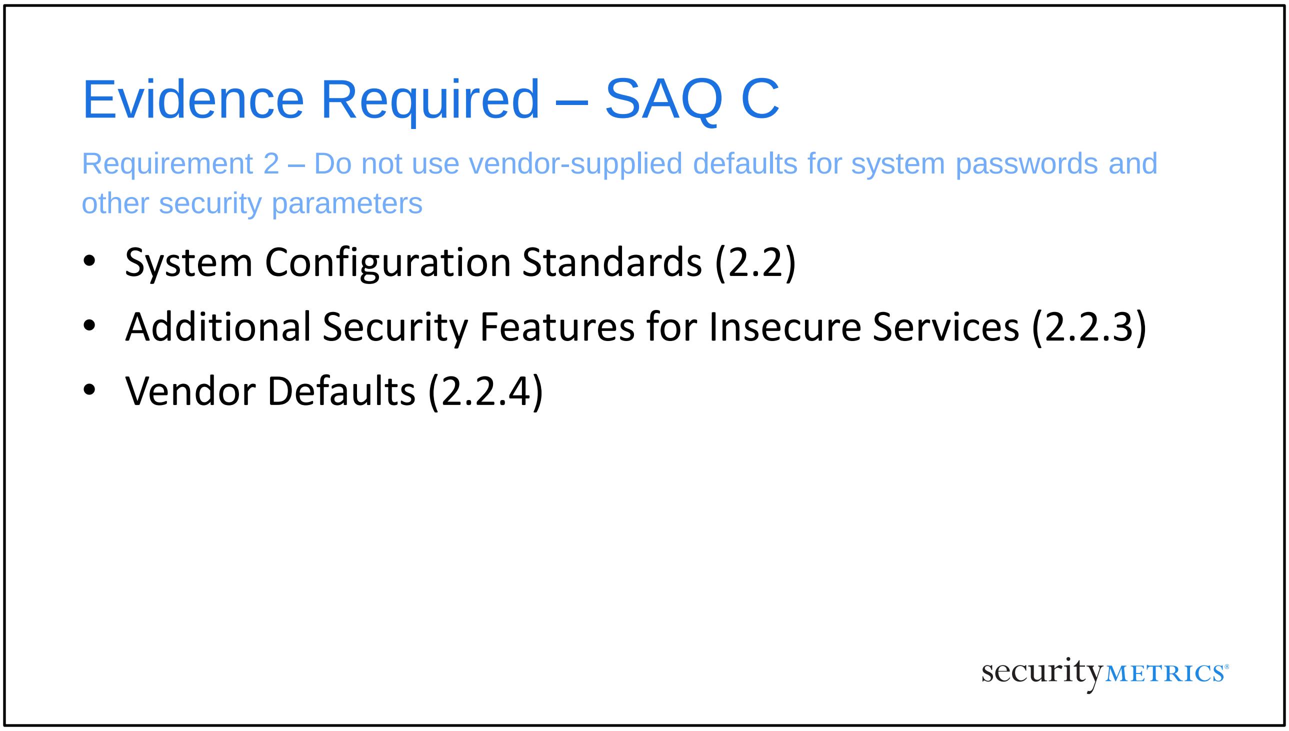
Evidence Required – SAQ C

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

- Firewall Ruleset Review (1.3.4)
- Firewall and Router Configuration Snapshots (1.2.x)
- Anti-Spoofing Configuration (1.3.3)
- Protections for Mobile and Employee-Owned Devices [PCI DSS v4.0 prep]

securityMETRICS

1. **Firewall Ruleset Review (1.3.4):** Submit evidence that your firewall configuration has been reviewed recently and was approved by a responsible party
2. **Firewall and Router Configuration Snapshots (1.2.x):** These are point-in-time captures of your current firewall and router configurations. They help in analyzing and verifying that the network devices are set up securely, ensuring no unintended access or vulnerabilities.
3. **Anti-Spoofing Configuration (1.3.3):** Provide documentation on how you've configured systems to detect and prevent spoofing attacks. This ensures that attackers cannot masquerade as legitimate entities within your network.
4. **Protections for Mobile and Employee-Owned Devices (PCI DSS v4.0 prep):** As PCI DSS evolves, it's crucial to be prepared for the new version's requirements. Submit details on how you safeguard both mobile and employee-owned devices that interact with cardholder data. This should include information on device management, access controls, and any other relevant security measures.



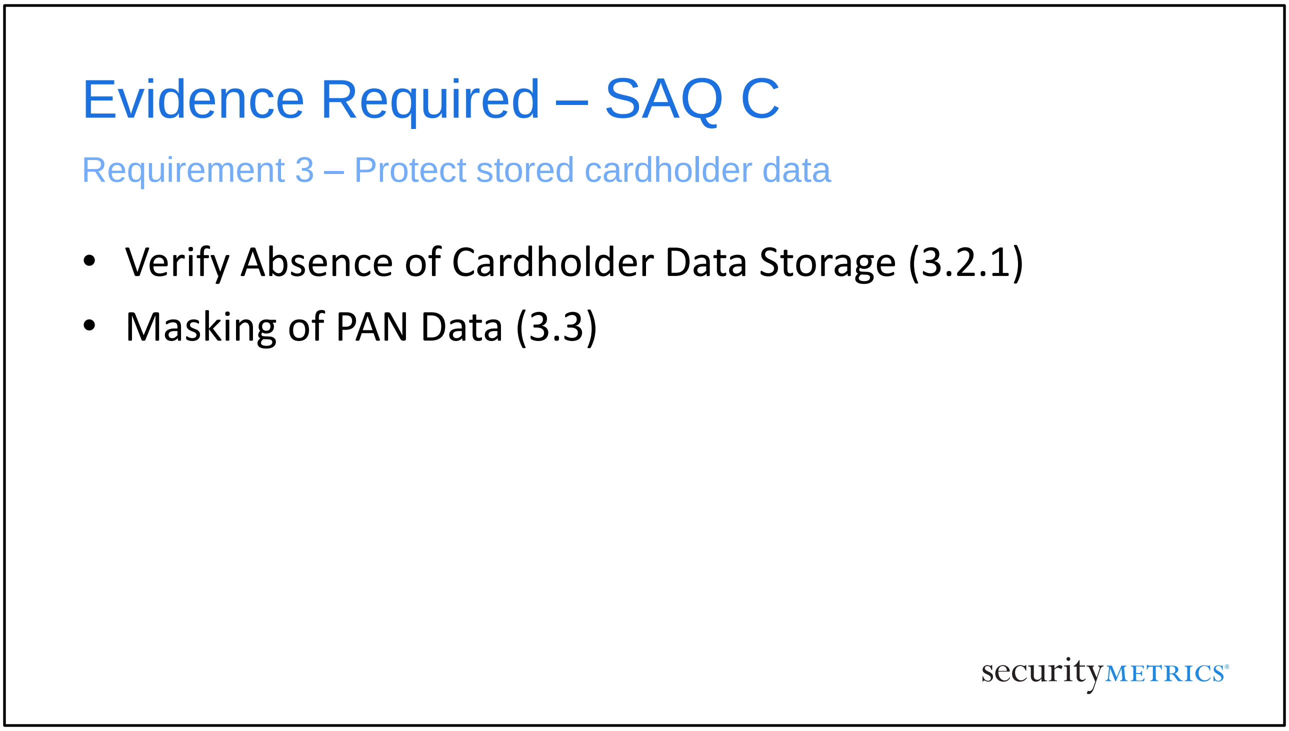
Evidence Required – SAQ C

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

- System Configuration Standards (2.2)
- Additional Security Features for Insecure Services (2.2.3)
- Vendor Defaults (2.2.4)

securityMETRICS

1. **System Configuration Standards (2.2):** Submit your organization's established standards for configuring systems within the cardholder data environment. These standards should detail the baseline security measures applied to various systems, ensuring they're hardened against potential threats and vulnerabilities.
2. **Additional Security Features for Insecure Services (2.2.3):** Provide documentation on the supplementary security measures you've implemented for services considered to be insecure or vulnerable. This might include services that are historically prone to attacks or those that operate using less secure protocols. The documentation should specify the controls in place to mitigate associated risks.
3. **Vendor Defaults (2.2.4):** Share information about any vendor-supplied defaults in your environment, including default usernames and passwords. Additionally, provide evidence of the steps taken to change these defaults upon system setup, ensuring that systems aren't left exposed with widely known credentials.



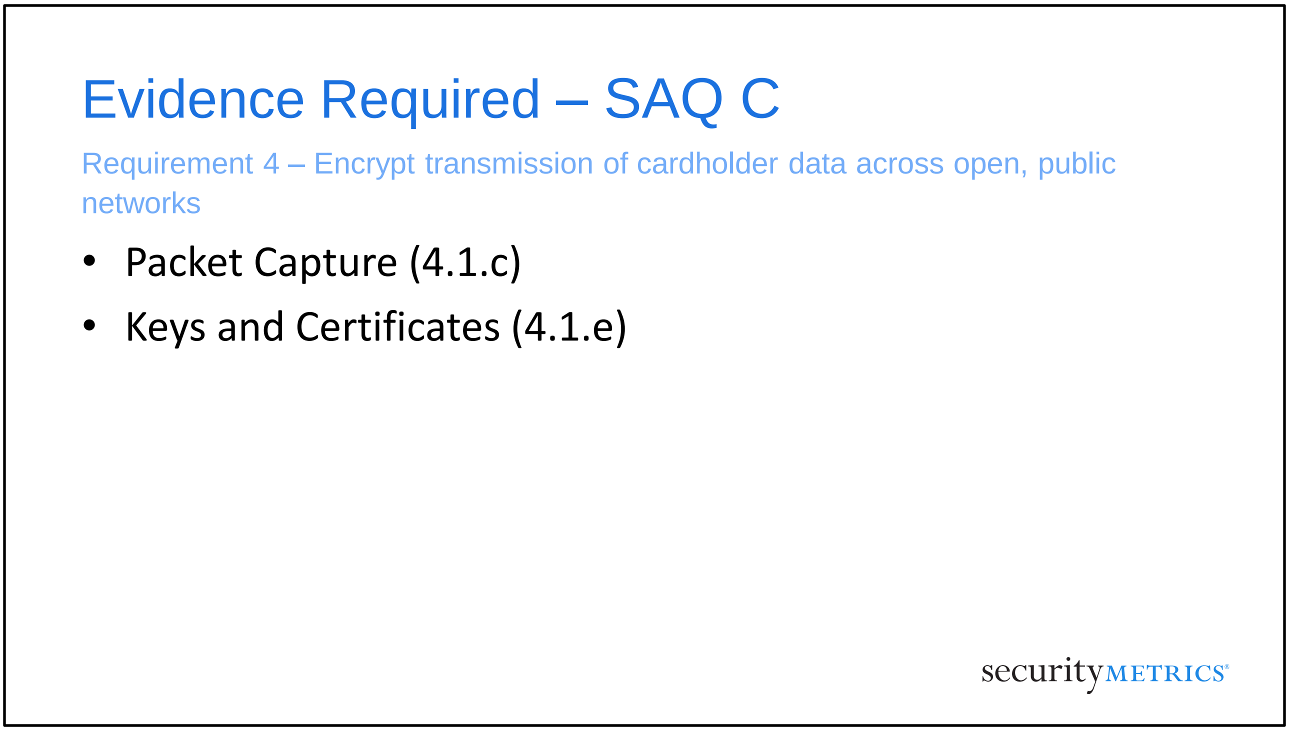
Evidence Required – SAQ C

Requirement 3 – Protect stored cardholder data

- Verify Absence of Cardholder Data Storage (3.2.1)
- Masking of PAN Data (3.3)

securityMETRICS

1. **Verify Absence of Cardholder Data Storage (3.2.1)**: Run PANscan, a tool provided by SecurityMetrics, on all servers and workstations in the cardholder data environment and upload the exported scan results. If PANscan identifies files that may contain cardholder data, investigate the findings to determine if it is a false-positive or an actual finding. If it is determined to be a false-positive, use the comment field to notate these findings. If it is not a false-positive, contact your assessor. If the data is legitimate and unexpected, you may want to initiate your incident response plan.
2. **Masking of PAN Data (3.3):** If PAN is visible electronically, it must be masked. If full PAN is visible on physical media (mailed-in forms, hand-written based, etc.), provide a document which details who has access to view these documents that includes business justification for such access.



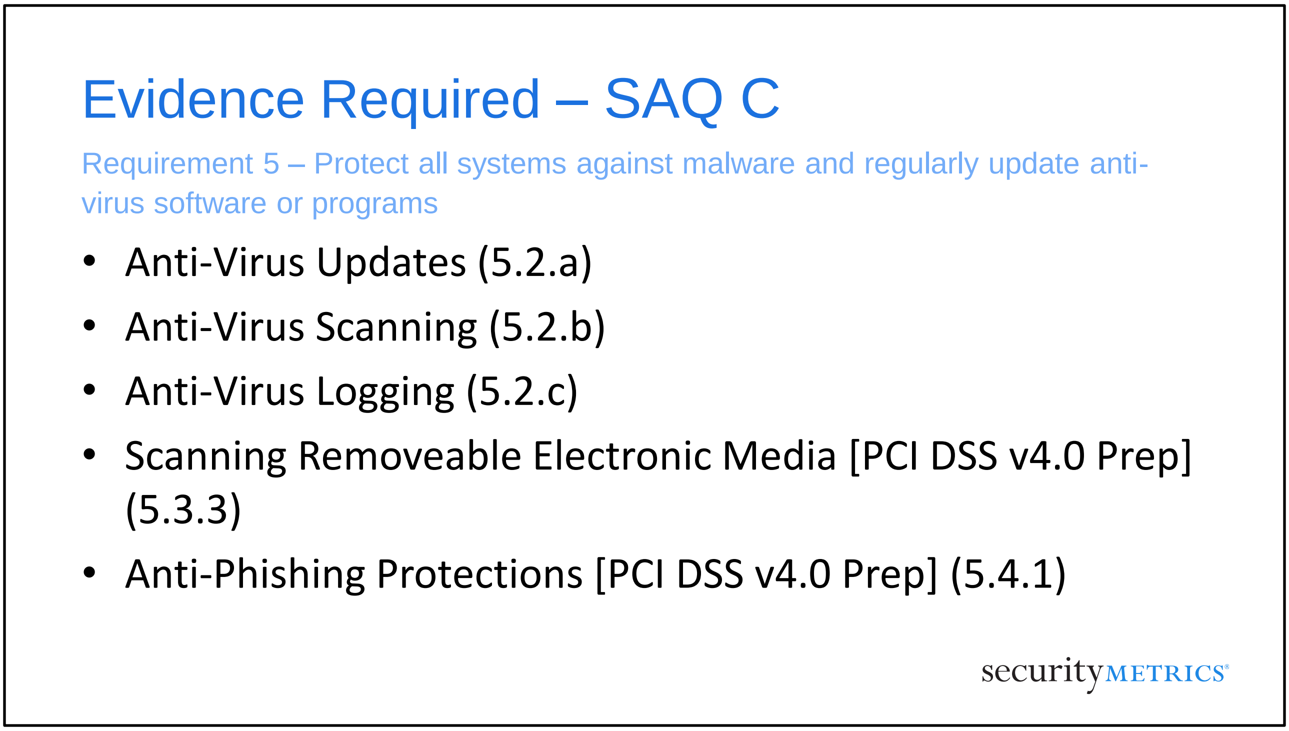
Evidence Required – SAQ C

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

- Packet Capture (4.1.c)
- Keys and Certificates (4.1.e)

securityMETRICS

1. **Packet Capture (4.1.c):** Provide a packet capture that showcases the encrypted transmissions of cardholder data across open, public networks. This capture will be instrumental in verifying that sensitive data isn't exposed during transit and that encryption measures are effectively implemented.
2. **Keys and Certificates (4.1.e):** Submit evidence showing the encryption details of all in-scope public transmissions of cardholder data in use. They should demonstrate that only trusted and secure keys and certificates are used. There are many popular online SSL scanning tools that you can use to gather this.



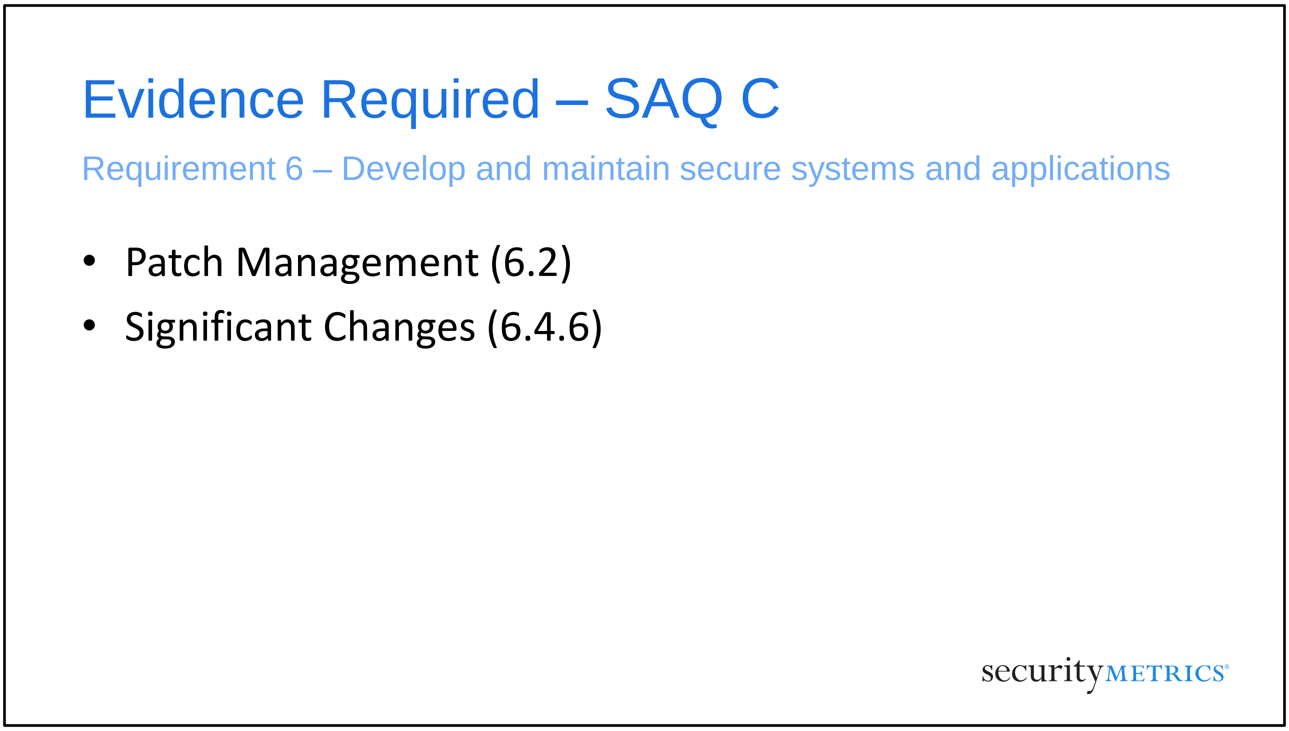
Evidence Required – SAQ C

Requirement 5 – Protect all systems against malware and regularly update anti-virus software or programs

- Anti-Virus Updates (5.2.a)
- Anti-Virus Scanning (5.2.b)
- Anti-Virus Logging (5.2.c)
- Scanning Removeable Electronic Media [PCI DSS v4.0 Prep] (5.3.3)
- Anti-Phishing Protections [PCI DSS v4.0 Prep] (5.4.1)

securityMETRICS

1. **Anti-Virus Updates (5.2.a):** Submit records showing the regular updates to your anti-virus software. These records should indicate that the software is always equipped with the latest virus definitions, ensuring optimal detection and protection against malware.
2. **Anti-Virus Scanning (5.2.b):** Provide evidence of periodic and on-demand anti-virus scanning activities. This should include scan schedules, the scope of scans, and any action taken on detected threats.
3. **Anti-Virus Logging (5.2.c):** Share logs related to anti-virus activities. These logs help verify that the software is actively monitoring and taking appropriate actions against potential threats, and that these activities are being properly recorded.
4. **Scanning Removable Electronic Media [PCI DSS v4.0 Prep] (5.3.3):** As part of preparation for PCI DSS v4.0, provide documentation on how removable electronic media (like USB drives) are scanned for potential threats when connected to systems in the cardholder data environment.
5. **Anti-Phishing Protections [PCI DSS v4.0 Prep] (5.4.1):** Outline the measures your organization has in place to protect against phishing attacks. This could include training programs, email filtering solutions, or other relevant protections.



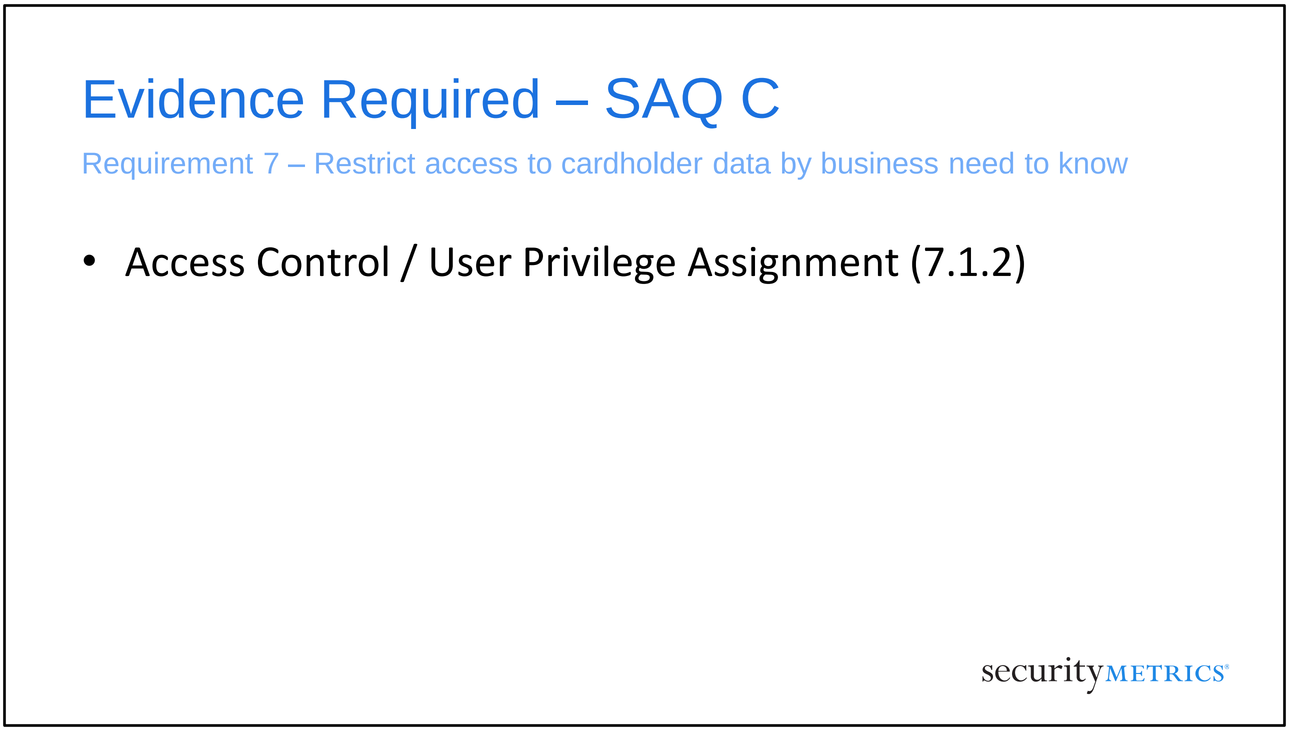
Evidence Required – SAQ C

Requirement 6 – Develop and maintain secure systems and applications

- Patch Management (6.2)
- Significant Changes (6.4.6)

securityMETRICS

1. **Patch Management (6.2):** Provide an overview of your organization's patch management process. This should detail how you identify, test, and apply critical security patches in a timely manner. Ensure to include records of recent patch installations, emphasizing the patches related to the security of cardholder data systems.
2. **Significant Changes (6.4.6):** Submit documentation on significant changes made to the cardholder data environment. This could include system upgrades, network modifications, or major software installations. Highlight how these changes were reviewed and validated to ensure they did not inadvertently introduce vulnerabilities or compromise security controls.



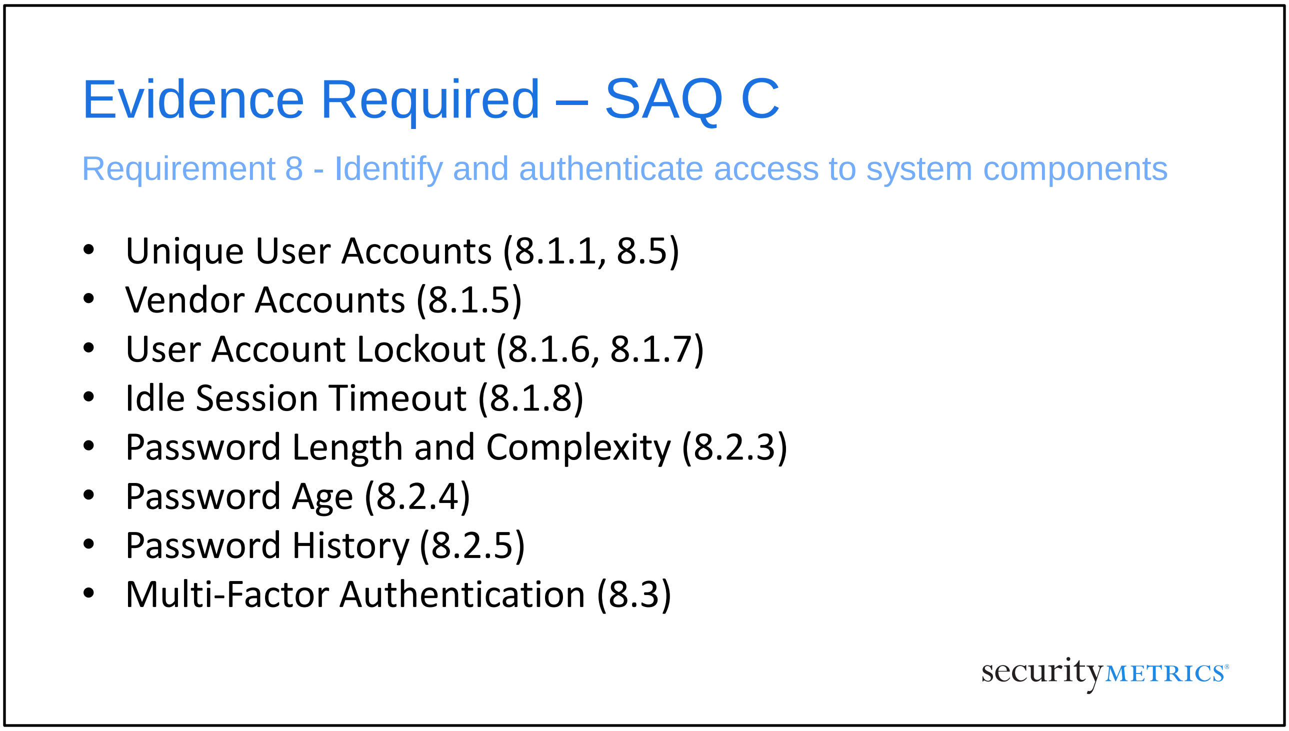
Evidence Required – SAQ C

Requirement 7 – Restrict access to cardholder data by business need to know

- Access Control / User Privilege Assignment (7.1.2)

securityMETRICS

1. **Access Control / User Privilege Assignment (7.1.2):** Please provide a list of user roles used within the cardholder data environment along with a list of users with privileged/administrative access.



Evidence Required – SAQ C

Requirement 8 - Identify and authenticate access to system components

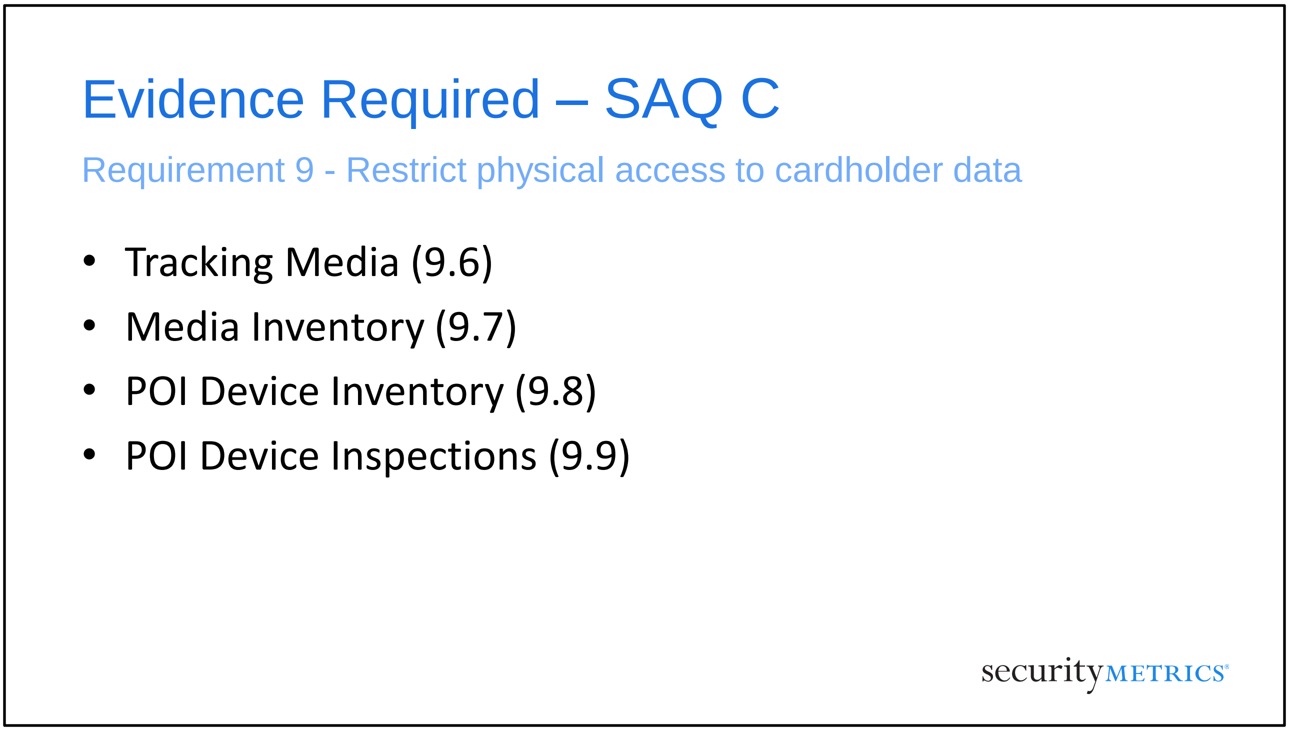
- Unique User Accounts (8.1.1, 8.5)
- Vendor Accounts (8.1.5)
- User Account Lockout (8.1.6, 8.1.7)
- Idle Session Timeout (8.1.8)
- Password Length and Complexity (8.2.3)
- Password Age (8.2.4)
- Password History (8.2.5)
- Multi-Factor Authentication (8.3)

securityMETRICS®

1. **Unique User Accounts (8.1.1, 8.5):** Provide evidence that each individual with access to cardholder data has a unique identification. This ensures individual accountability and traceability in all actions involving sensitive data.
2. **Vendor Accounts (8.1.5):** Share information regarding accounts provided to vendors or third parties. It's crucial to demonstrate that these accounts are monitored, given limited access, and disabled when not in use.
3. **User Account Lockout (8.1.6, 8.1.7):** Document your procedures for locking out user accounts after a certain number of failed login attempts. This should include lockout duration and the process for unlocking accounts, ensuring protection against brute-force attacks.
4. **Idle Session Timeout (8.1.8):** Submit details on how idle sessions are managed, specifically the duration after which an inactive session is automatically terminated, safeguarding against potential unauthorized access.
5. **Password Length and Complexity (8.2.3):** Provide your organization's password policies, emphasizing the requirements for password length and the mix of characters (e.g., uppercase, lowercase, numbers, special characters) for strong password creation.
6. **Password Age (8.2.4):** Share policies related to how often passwords must be changed, ensuring that potentially compromised passwords are regularly updated.
7. **Password History (8.2.5):** Document the system's capability to remember past passwords used by users, preventing them from reusing old passwords and thus

enhancing security.

8. **Multi-Factor Authentication (8.3):** Detail the implementation and use of multi-factor authentication for accessing the cardholder data environment. Highlight the different factors used (e.g., something you know, something you have, something you are) to ensure robust access controls.

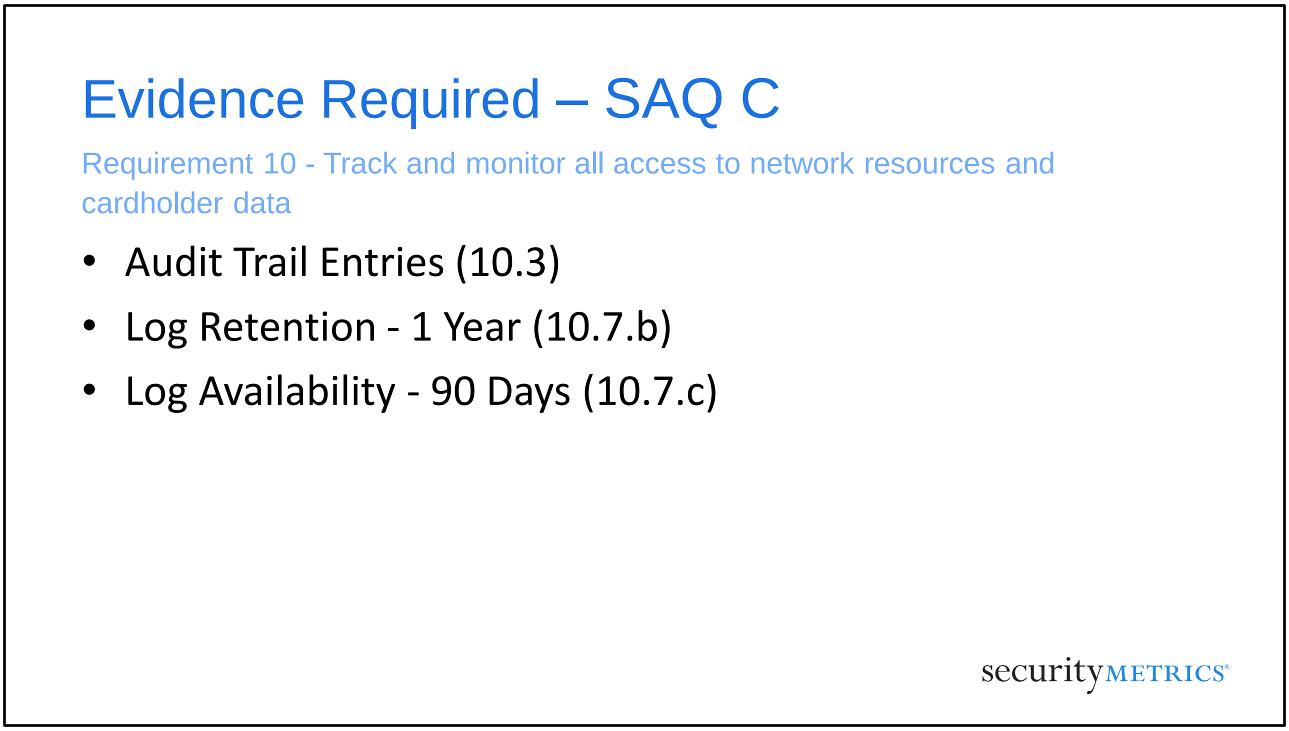


Evidence Required – SAQ C

Requirement 9 - Restrict physical access to cardholder data

- Tracking Media (9.6)
- Media Inventory (9.7)
- POI Device Inventory (9.8)
- POI Device Inspections (9.9)

1. **Tracking Media (9.6):** Submit evidence of your procedures for tracking the physical movement of media containing cardholder data, both within and outside the secure environment. This ensures that sensitive media is always accounted for and its whereabouts known.
2. **Media Inventory (9.7):** Provide a comprehensive inventory list of all media – be it hard drives, USBs, CDs, paper receipts, etc. – that store cardholder data. Regularly updated inventories ensure that all such media is known, traceable, and secured.
3. **POI Device Inventory (9.8):** Share a detailed inventory of all Point-of-Interaction (POI) devices. This list should include device make, model, location, and a unique identifier to help track and manage these critical components within the payment process.
4. **POI Device Inspections (9.9):** Document your regular inspection procedures for POI devices. These inspections are crucial to detect any tampering or substitution, ensuring the security and integrity of the transaction process.



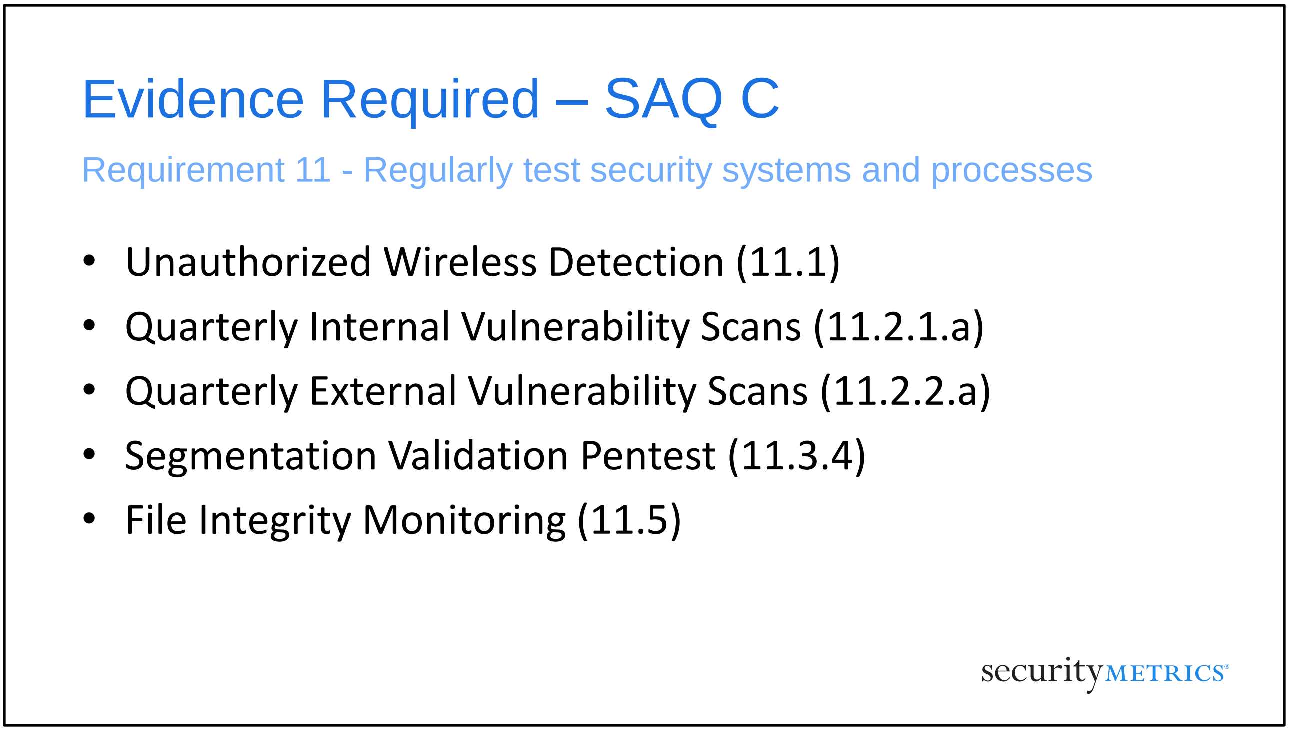
Evidence Required – SAQ C

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

- Audit Trail Entries (10.3)
- Log Retention - 1 Year (10.7.b)
- Log Availability - 90 Days (10.7.c)

securityMETRICS

1. **Audit Trail Entries (10.3):** Provide samples or templates of your audit trail entries. These entries should capture critical details such as the event type, date and time, success or failure indication, and the identity of the event initiator. This documentation ensures that all actions in the cardholder data environment are traceable and accountable.
2. **Log Retention - 1 Year (10.7.b):** Confirm and detail your log retention policies, highlighting that logs with cardholder data are stored for a minimum of one year. This ensures a robust historical record, vital for investigations or reviews.
3. **Log Availability - 90 Days (10.7.c):** Document your procedures to ensure that the most recent three months of logs (90 days) are immediately available for analysis. This ensures rapid response capabilities in the face of potential security incidents or breaches.



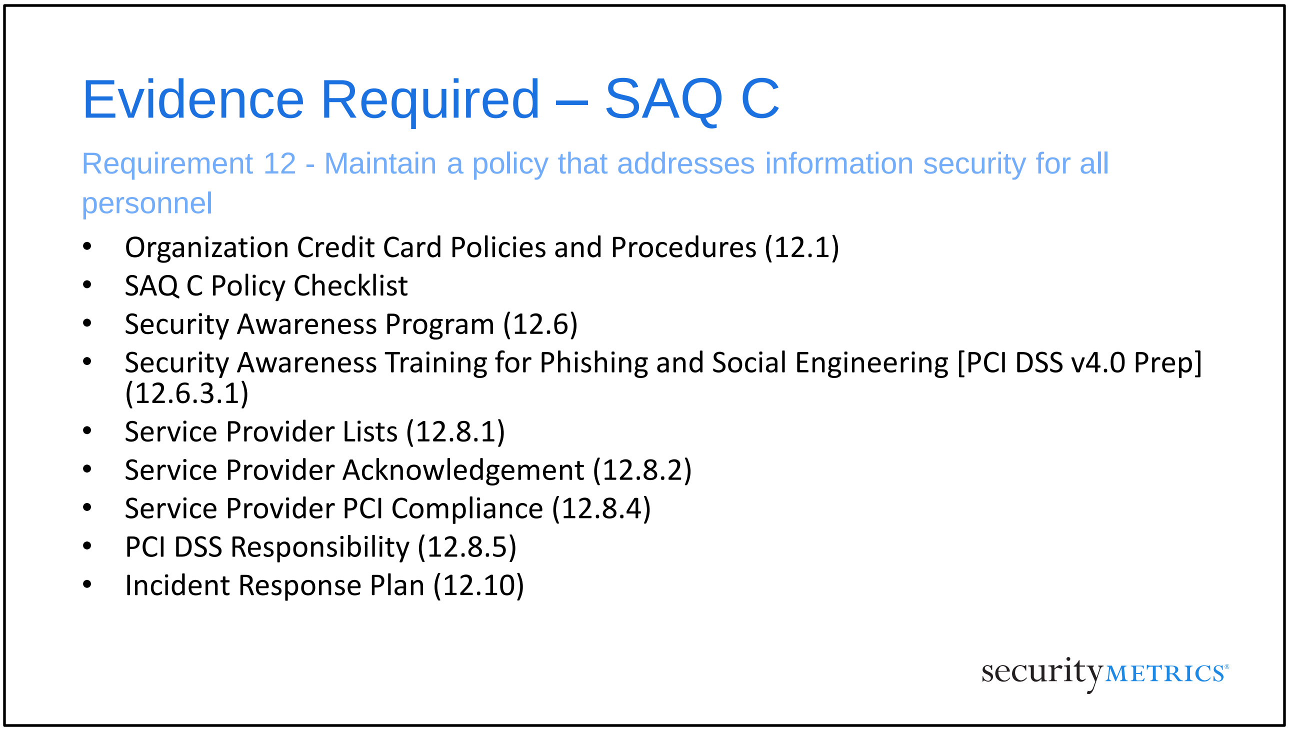
Evidence Required – SAQ C

Requirement 11 - Regularly test security systems and processes

- Unauthorized Wireless Detection (11.1)
- Quarterly Internal Vulnerability Scans (11.2.1.a)
- Quarterly External Vulnerability Scans (11.2.2.a)
- Segmentation Validation Pentest (11.3.4)
- File Integrity Monitoring (11.5)

securityMETRICS

1. **Unauthorized Wireless Detection (11.1):** Share evidence of your procedures and tools in place to detect unauthorized wireless access points in your environment. This ensures that rogue devices aren't covertly siphoning or compromising cardholder data.
2. **Quarterly Internal Vulnerability Scans (11.2.1.a):** Document your schedule and results for the regular internal vulnerability scans performed on your network. These scans should be conducted at least quarterly and after any significant change in the network.
3. **Quarterly External Vulnerability Scans (11.2.2.a):** Provide evidence of external vulnerability scans conducted by an Approved Scanning Vendor (ASV). These scans, targeting your external-facing systems, should also be done quarterly to identify potential vulnerabilities.
4. **Segmentation Validation Pentest (11.3.4):** Detail the penetration testing procedures carried out to validate the efficacy of your network segmentation. This ensures that systems outside of the cardholder data environment cannot adversely impact the security of that environment.
5. **File Integrity Monitoring (11.5):** Submit documentation on the tools and processes in place for monitoring critical system files. Highlight how they detect unauthorized modifications, ensuring the integrity and security of your systems.



Evidence Required – SAQ C

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

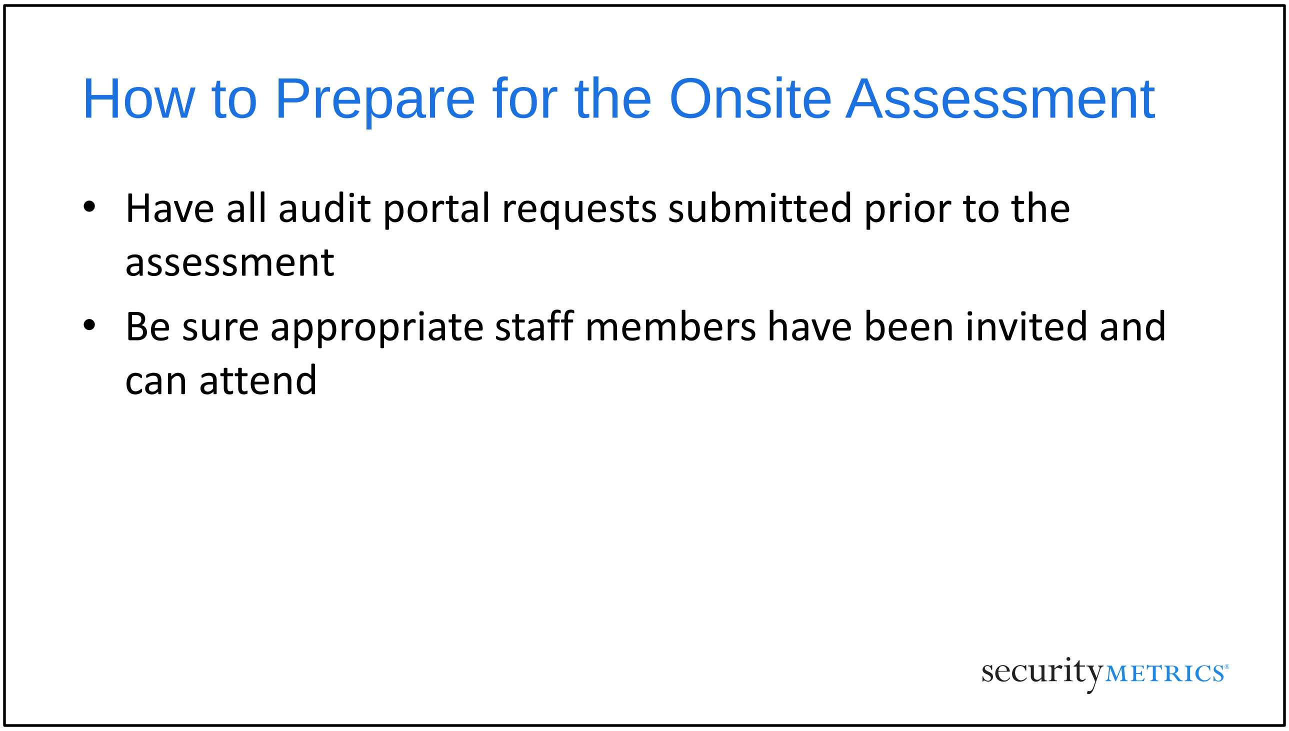
- Organization Credit Card Policies and Procedures (12.1)
- SAQ C Policy Checklist
- Security Awareness Program (12.6)
- Security Awareness Training for Phishing and Social Engineering [PCI DSS v4.0 Prep] (12.6.3.1)
- Service Provider Lists (12.8.1)
- Service Provider Acknowledgement (12.8.2)
- Service Provider PCI Compliance (12.8.4)
- PCI DSS Responsibility (12.8.5)
- Incident Response Plan (12.10)

1. **Organization Credit Card Policies and Procedures (12.1):** Share your comprehensive policy document detailing how credit card data is handled, processed, stored, and transmitted within the organization, ensuring a clear governance structure.
2. **SAQ C Policy Checklist:** Provide the checklist corresponding to SAQ C, confirming that all necessary policies related to this specific SAQ are in place and adhered to.
3. **Security Awareness Program (12.6):** Document the ongoing program established to educate staff on the importance of cardholder data security, showcasing content, frequency, and participation metrics.
4. **Security Awareness Training for Phishing and Social Engineering [PCI DSS v4.0 Prep] (12.6.3.1):** Highlight the training modules or sessions focusing on the threats of phishing and social engineering. As part of the PCI DSS v4.0 preparation, this ensures that employees are well-equipped to recognize and counteract these specific threats.
5. **Service Provider Lists (12.8.1):** Submit a detailed inventory of all third-party service providers that handle, process, or could affect the security of cardholder data.
6. **Service Provider Acknowledgement (12.8.2):** Provide acknowledgments from service providers confirming their understanding and commitment to maintaining the security of cardholder data they handle or affect.
7. **Service Provider PCI Compliance (12.8.4):** Share evidence, such as Attestations of Compliance (AOCs), that your service providers are PCI DSS compliant.

8. **PCI DSS Responsibility (12.8.5):** Document the delineation of responsibility between your organization and service providers regarding PCI DSS requirements, ensuring clarity in accountability.
9. **Incident Response Plan (12.10):** Submit your established plan detailing how to respond in the event of a security incident. This plan should outline roles, communication protocols, and steps for containment, eradication, and recovery.

Preparing for the Onsite Assessment

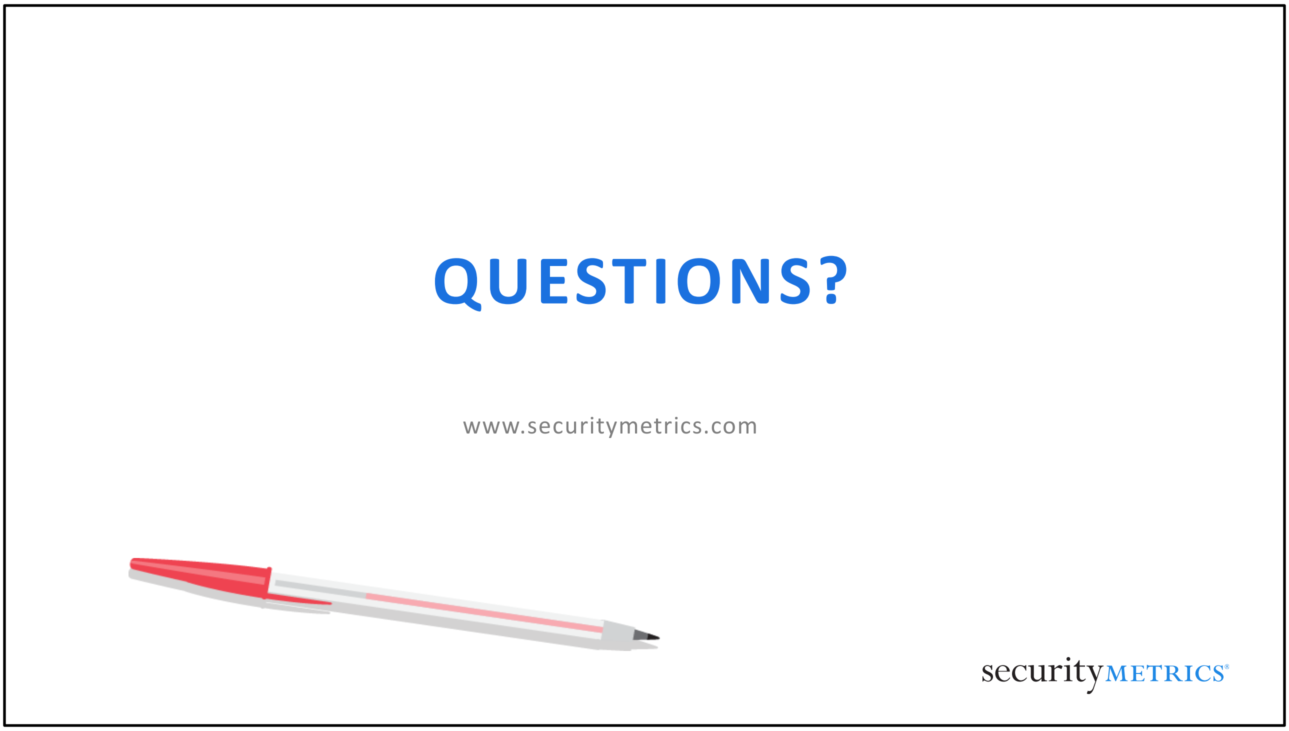
Now let’s discuss how you can be the most prepared for the onsite assessment.



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

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