A summary of the new requirements found in the PCI DSS 4.0 SAQ A and some guidance for what you can do now to prepare.

PCI DSS 4.0 Requirement	SAQ Completion Guidance (from the 4.0 SAQ A)	HALOCK Guidance
3.1.1 All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Selection of any of the In Place responses for Requirement 3.1.1 means that, if the merchant has paper storage of account data, the merchant has policies and procedures in place that govern merchant activities for Requirement 3. This helps to ensure personnel are aware of and following security policies and documented operational procedures for managing the secure storage of any paper records with account data. If merchant does not store paper records with account data, mark this requirement as Not Applicable and complete Appendix D: Explanation of Requirements Noted as Not Applicable.	1. Determine if this is applicable to your organization. 2. Work on developing security policies and procedures required.
3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	Selection of any of the In Place responses for Requirement 3.2.1 means that if a merchant stores any paper (for example, receipts or paper reports) that contain account data, the merchant only stores the paper as long as it is needed for business, legal, and/or regulatory reasons and destroys the paper once it is no longer needed. If a merchant never prints or stores any paper containing account data, mark this requirement as Not Applicable and complete Appendix D: Explanation of Requirements Noted as Not Applicable.	1. Based on applicability, update policies, procedures, and processes to account for the new bullet that will be a full requirement in 2025.
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Bullet intentionally left blank for this SAQ.	Note: For SAQ A, Requirement 6 applies to webservers that host the page(s) on the merchant's website(s) that provide the address (the URL) of the TPSP's payment page/form to the merchant's customers.	This requirement was added to this SAQ type for outsourced eCommerce environments to compliment the patching requirement. Ensure this process is in place on merchant webservers.
6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written justification as to why each is necessary. Applicability Notes: This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Note: For SAQ A, Requirement 6.4.3 applies to the page(s) on the merchant's website(s) that provides the address (the URL) of the TPSP's payment page/form to the merchant's customers.	1. In line with the SSC's guidance for best practices when outsourcing eCommerce to third party service providers from 2017, the DSS will now include requirements to ensure that payment pages are managed and protected from unauthorized changes. 2. This is something organizations should start planning and designing in preparation for this becoming a full requirement in 2025.

PCI DSS 4.0 Requirement	SAQ Completion Guidance (from the 4.0 SAQ A)	HALOCK Guidance
8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use	Note: For SAQ A, Requirement 8 applies to merchant webservers that host the page(s) that provides the address (the URL) of the TPSP's payment page/form to the merchant's customers.	1. Additional password complexity requirements are being added for merchant webservers. Ensure these servers are configured to support this password complexity requirement.
8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters. Applicability Notes: This requirement is not intended to apply to: • User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). • Application or system accounts, which are governed by requirements in section 8.6. ***This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*** Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3.		1. Additional password complexity requirements are being added for merchant webservers. Ensure these servers are configured to support this password complexity requirement and plan for increasing the length of these passwords by 2025.
8.3.7 Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used. • Applicability Notes: This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).		1. Additional password complexity requirements are being added for merchant webservers. Ensure these servers are configured to support this password complexity requirement.
8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real -time access to resources is automatically determined accordingly. Applicability Notes: This requirement applies to in-scope system components that are not in the CDE because these components are not subject to MFA requirements. This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). This requirement does not apply to service providers' customer accounts but does apply to accounts for service provider personnel.		1. Additional password complexity requirements are being added for merchant webservers. Ensure these servers are configured to support this password complexity requirement.

PCI DSS 4.0 Requirement	SAQ Completion Guidance (from the 4.0 SAQ A)	HALOCK Guidance
9.4.1.1 Offline media backups with cardholder data are stored in a secure location.	Note: For SAQ A, Requirements at 9.4 only apply to merchants with paper records (for example, receipts or printed reports) with account data, including primary account numbers (PANs). Selection of any of the In Place responses for Requirements at 9.4 means that the merchant securely stores any paper media with account data, for example by storing the paper in a locked drawer, cabinet, or safe, and that the merchant destroys such paper when no longer needed for business purposes. This includes a written document or policy for employees, so they know how to secure paper with account data and how to destroy the paper when no longer needed. If the merchant never stores any paper with account data, mark this requirement as Not Applicable and complete Appendix D: Explanation of Requirements Noted as Not Applicable.	1. Based on applicability, update policies, procedures, and processes to account for the new requirement.
11.3.2 External vulnerability scans are performed as follows: • At least once every three months. • By PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan. Applicability Notes: For initial PCI DSS compliance, it is not required that four passing scans be completed within 12 months if the assessor verifies: 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring scanning at least once every three months, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months must have occurred. ASV scanning tools can scan a vast array of network types and topologies. Any specifics about the target environment (for example, load balancers, third-party providers, ISPs, specific configurations, protocols in use, scan interference) should be worked out between the ASV and scan customer. Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.	No additional guidance was provided in the SAQ for this requirement.	1. Historically, merchants with outsourced eCommerce sites were not required to conduct external vulnerability scans. HALOCK recommends merchants discuss this new requirement with their third-party service provider to determine how the scanning and remediation process will work between the organizations. 2. Since this is not an emerging new requirement, this will need to be in place prior to a 4.0 validation. Therefore, organization should start working on this now.

PCI DSS 4.0 Requirement	SAQ Completion Guidance (from the 4.0 SAQ A)	HALOCK Guidance
11.3.2.1 External vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	No additional guidance was provided in the SAQ for this requirement.	1. Historically, merchants with outsourced eCommerce sites were not required to conduct significant change external vulnerability scans. Merchants will need to ensure their change management processes are identifying any significant changes to payment processing environments to ensure changes trigger a external vulnerability scan. 2. Since this is not an emerging new requirement, this will need to be in place prior to a 4.0 validation. Therefore, organization should start working on this now.
11.6.1 A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP header and payment page. • The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). • Applicability Notes: The intention of this requirement is not that an entity installs software in the systems or browsers of its consumers, but rather that the entity uses techniques such as those described under Examples in the PCI DSS Guidance column (of PCI DSS Requirements and Testing Procedures) to prevent and detect unexpected script activities. ***This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.***	Note: For SAQ A, Requirement 11.6.1 applies to merchants that include a TPSP's inline frame (iframe) payment form on the merchant's website. SAQ Completion Guidance: If a merchant uses URL redirects, where the merchant hosts the page(s) on their website(s) that provides the address (the URL) of the merchant's payment page/form to the merchant's customers, the merchant marks this requirement as Not Applicable and completes Appendix D: Explanation of Requirements Noted as Not Applicable.	1. In line with the SSC's guidance for best practices when outsourcing eCommerce to third party service providers from 2017, the DSS will now include requirements to ensure that payment pages are managed and protected from unauthorized changes. 2. This is something organizations should start planning and designing in preparation for this becoming a full requirement in 2025.

Do you have questions or need additional guidance? Reach out to the HALOCK QSA team for Subject Matter Expertise and 4.0 preparation work. 4.0 transition training for QSA will be released in the middle of July and HALOCK is already allocating time to complete that training ASAP, to ensure our guidance for 4.0 is aligned with the SCC's intent.

HALOCK®