Summary of the PCI-DSS Essentials - Merchant Assessment Document

This document provides guidance on how merchants can assess their compliance with PCI-DSS. It outlines the different levels of merchants based on transaction volume, the types of Self-Assessment Questionnaires (SAQs), and when a full Report on Compliance (ROC) is required.

Key Points:

1. Merchant Levels

Merchants are categorized into four levels based on the number of transactions processed annually:

- **Level 1**: >6 million transactions per year.
- **Level 2**: Between 1 million and 6 million transactions.
- **Level 3**: Between 20,000 and 1 million transactions.
- **Level 4**: <20,000 transactions per year.

Example: A large e-commerce retailer processing more than 6 million transactions per year would be a Level 1 merchant.

2. Self-Assessment Questionnaire (SAQ) vs. Report on Compliance (ROC)

- **SAQ**: A simplified self-assessment completed by merchants of Levels 2 to 4. It involves answering a set of questions based on how the merchant handles cardholder data (CHD).
- **ROC**: Required for Level 1 merchants. It must be performed by a Qualified Security Assessor (QSA) and involves an in-depth review of the merchant's PCI-DSS compliance.

Example: A small local retail store that processes 10,000 card transactions annually would complete an SAQ, while a global retailer with millions of transactions would require a ROC by a QSA.

3. SAQ Types

There are 8 types of SAQs, which vary based on how the merchant handles CHD. Each SAQ requires compliance with a different set of the 12 PCI-DSS requirements.

- **SAQ A**: For e-commerce merchants that fully outsource all card processing to third parties (e.g., using iFrames or redirects).
- **SAQ A-EP**: E-commerce merchants that partially outsource payment processing but still transmit CHD.
- **SAQ B**: For merchants using standalone terminals (e.g., dial-out chip/PIN devices).
- **SAQ B-IP**: For merchants using PTS-approved devices connected via IP.
- **SAQ C**: For merchants using internet-connected payment applications.
- **SAQ C-VT**: For merchants using isolated virtual terminals (e.g., call centers).
- **SAQ D**: The most comprehensive, covering all merchants that store CHD.
- **SAQ P2PE-HW**: For merchants using only PCI-validated hardware terminals that use Point-to-Point Encryption (P2PE).

Example: An e-commerce site using a third-party payment processor with a redirect might complete SAQ A, while a call center manually entering payment details into a web-based virtual terminal would complete SAQ C-VT.

4. Number of Questions Based on SAQ Type

Each SAQ includes a specific number of questions depending on the merchant's environment and how CHD is processed:

- **SAQ A**: 22 questions (only Reqs 2, 8, 9, 12).
- **SAQ A-EP**: 193 questions (covers all requirements).
- **SAQ B**: 41 questions (Reqs 3, 4, 7, 9, 12).
- **SAQ D**: 332 questions (covers all requirements).

Example: A Level 3 e-commerce business that stores no cardholder data would likely complete SAQ A, with only 22 questions to answer.

5. Selecting the Correct SAQ

Selecting the correct SAQ is essential to avoid non-compliance. Merchants must determine their SAQ type based on the way they handle CHD, and they may need to complete multiple SAQs if they meet different criteria.

Example: A business that processes both card-not-present (CNP) and card-present (CP) transactions may need to complete multiple SAQs, such as SAQ A for e-commerce and SAQ B for in-store transactions.

6. Merchant Assessment Consequences

Filling out the wrong SAQ or failing to comply with the correct SAQ requirements can result in fines, penalties, or loss of payment processing capabilities.

Example: A Level 2 merchant that selects the wrong SAQ type and fails to meet compliance standards may face fines from their acquiring bank or be required to implement compensating controls.

7. Validation Requirements

Sometimes, banks may require merchants to have their SAQ validated by a QSA, especially if there are concerns about the merchant’s compliance or security practices.

Example: A Level 4 merchant suspected of weak security practices may be asked by their bank to validate their SAQ with the assistance of a QSA to ensure accuracy.

***

Self-Assessment Questionnaire (SAQ) Breakdown

PCI-DSS allows merchants to complete different types of SAQs depending on their environment and how they handle CHD. Here is a detailed look at each SAQ type, including the number of questions and typical examples of use.

1. SAQ A (22 questions)

- **Who It's For**: E-commerce merchants who outsource all card processing to third parties (e.g., payment gateway via iFrame or redirect).
- **Requirements Covered**: 2, 8, 9, 12.
  Do Not Use Vendor-Supplied Defaults, Identify and Authenticate Access to System Components, Restrict Physical Access to Cardholder Data, Maintain a Policy that Addresses Information Security.
- **Example**: An online store that uses PayPal as its payment processor, where PayPal handles all transactions and the store itself does not store or process CHD.

2. SAQ A-EP (193 questions)

- **Who It's For**: E-commerce merchants partially outsourcing payment processing but still handling the transmission of card data (e.g., accepting payments via API but not storing data).
- **Requirements Covered**: All 12 PCI-DSS requirements.
- **Example**: A website that integrates a third-party API to process payments but does not store CHD locally. This SAQ ensures encryption and secure transmission of CHD.

3. SAQ B (41 questions)

- **Who It's For**: Merchants using standalone, dial-out payment terminals with no electronic CHD storage.
- **Requirements Covered**: 3, 4, 7, 9, 12.
  Protect Stored Cardholder Data, Encrypt Transmission of Cardholder Data Across Open, Public Networks, Restrict Access to Cardholder Data by Business Need to Know, Restrict Physical Access to Cardholder Data, Maintain a Policy that Addresses Information Security.
- **Example**: A small brick-and-mortar retail shop that uses standalone payment terminals to process payments and does not store cardholder data.

4. SAQ B-IP (82 questions)

- **Who It's For**: Merchants using standalone IP-connected payment terminals with no CHD storage.
- **Requirements Covered**: 2, 4, 5, 9, 12.
  Do Not Use Vendor-Supplied Defaults, Encrypt Transmission of Cardholder Data Across Open, Public Networks, Protect All Systems Against Malware and Regularly Update Anti-virus Software or Programs, Restrict Physical Access to Cardholder Data, Maintain a Policy that Addresses Information Security.
- **Example**: A restaurant using an IP-connected terminal to process payments, without storing or transmitting CHD over the internet.

5. SAQ C (160 questions)

- **Who It's For**: Merchants using internet-connected payment applications (e.g., point-of-sale systems) to process payments.
- **Requirements Covered**: All 12 PCI-DSS requirements, excluding those related to physical security.

- **Example**: A retail store using an internet-based point-of-sale system, with no CHD storage but transmitting data securely.

6. SAQ C-VT (73 questions)

- **Who It's For**: Merchants using virtual terminals to manually enter CHD (e.g., call centers).
- **Requirements Covered**: 1, 2, 7, 8, 9, 12.
  Install and Maintain a Firewall Configuration, Do Not Use Vendor-Supplied Defaults, Restrict Access to Cardholder Data by Business Need to Know, Identify and Authenticate Access to System Components, Restrict Physical Access to Cardholder Data, Maintain a Policy that Addresses Information Security.
- **Example**: A call center manually entering customer card details into a virtual terminal via a web browser.

7. SAQ D - Merchants (332 questions)

- **Who It's For**: Merchants who store, process, or transmit cardholder data not covered by any other SAQ types.
- **Requirements Covered**: All 12 PCI-DSS requirements.
- **Example**: An e-commerce business that stores CHD in its database or a retailer managing its own payment infrastructure and systems.

8. SAQ P2PE-HW (33 questions)

- **Who It's For**: Merchants using PCI-validated Point-to-Point Encryption (P2PE) hardware terminals that ensure secure card data transmission.
- **Requirements Covered**: 2, 9, 12.
  Do Not Use Vendor-Supplied Defaults, Restrict Physical Access to Cardholder Data, Maintain a Policy that Addresses Information Security.
- **Example**: A retailer using P2PE terminals where CHD is encrypted at the point of capture and never decrypted within the merchant's environment.

Additional Information on Merchant Levels and SAQs

1. Merchant Levels

- **Level 1**: >6 million transactions per year, requiring a **Report on Compliance (ROC)** by a Qualified Security Assessor (QSA).
- **Level 2**: 1 million to 6 million transactions per year, can often use an SAQ but may also require QSA validation.
- **Level 3**: 20,000 to 1 million e-commerce transactions per year.
- **Level 4**: Less than 20,000 e-commerce or up to 1 million transactions, typically completing a simplified SAQ.

Why Merchant Assessment Is Important

Selecting the correct SAQ is critical for a merchant's compliance with PCI-DSS. This process ensures that all security measures align with the merchant's operations and the level of risk they present based on their handling of CHD.

Consequences of Non-Compliance:

- Fines and penalties from acquiring banks.
- Increased transaction fees.
- Potential revocation of payment processing capabilities.

Example of Merchant Assessment Process

1. **Evaluate the Environment**: A merchant reviews their business model and CHD flow to determine which SAQ type applies.
2. **Complete the SAQ**: The merchant answers questions relevant to their operations (e.g., web-based business completes SAQ A or A-EP).
3. **Submit to Acquirer**: Once completed, the SAQ is submitted to the acquiring bank, which reviews the merchant's compliance.
4. **Maintain Compliance**: The merchant continues to follow PCI-DSS rules and periodically reviews their systems to ensure compliance.