Solution to Week 2 Assignment

Scenario 1: A small online retail store that only accepts card-not-present transactions and outsources all card processing functions to a third-party service provider.

Response: The right type of Self Assessment Questionnaire (SAQ) for this business is SAQ A.

Justification: SAQ A is the assessment that covers e-commerce merchants who outsource all cardholder data functions. Just as stated above the business in purview has transferred the responsibility of storing, processing or transmitting cardholder data with a third-party service provider.

The PCI DSS has identified a set of requirements that apply to SAQ A merchants as follows:

- If your organization only accepts card-not-present transactions (e-commerce or phone/mail order)
- If the processing of cardholder data is entirely outsourced to third-party service providers approved by PCI DSS
- Your organization does not electronically store, process, or transmit any cardholder data across your networks or facilities, but only rely on a third party to perform all these functions.
- If your organization indicates that any third party that performs the storage, processing or transmission of cardholder data is PCI DSS compliant.
- If the cardholder information kept by the organization is on paper and the documents are not received electronically

For SAQ A, you must never see a customer's physical card and accept payments by phone, traditional mail, or an e-commerce website. Seeing that the business in purview meets these requirements, SAQ A is the right assessment.

Scenario 2: A restaurant that accepts card-present transactions using a point-of-sale (POS) system connected to a wireless network. The restaurant also stores cardholder data for recurring billing purposes.

Response: The right type of Self Assessment Questionnaire (SAQ) for this business is SAQ D.

Justification: SAQ D caters to merchants or businesses who handle all aspect of payment processing themselves without relying on any external parties or service providers. These entities have direct control over cardholder data and are responsible for its storage, processing ands transmission. Seeing that the restaurant stores cardholder data, the right form for it is the SAQ D form.

Scenario 3: An e-commerce website that accepts card-present and card-not-present transactions. The website uses a third- party shopping cart service to handle payment processing, and cardholder data is encrypted before it reaches the merchant's systems.

Response: The right SAQ for this e-commerce website is SAQ D ass there is no other SAQ that meets the dynamics of the website. Although the SAQ P2PE seemed close, the SAQ is not eligible for e-commerce website and its suitable for hardware payment terminals (card-present).

Scenario 4: A medical clinic that accepts card-present transactions using an integrated payment system connected to their electronic health records (EHR) system. The clinic stores patient payment information for billing purposes.

Response: Given the peculiarity of the medical clinic, the right SAQ to be used is SAQ D.

Justification: The medical clinic uses an integrated payment system which is also connected to their electronic health records- legacy data (which implies that this is managed by them and not outsourced to a PCI DSS compliant service provider). The medical clinic stores patient payment information which further reiterated the need for SAQ D to be used. It is also important to note that no other SAQ fits the medical clinic characteristics better than SAQ D.

Scenario 5: A software development company that provides payment processing software to merchants. The company does not store, process, or transmit cardholder data on behalf of its clients but provides software that facilitates payment transactions.

Response: The right SAQ to be used by this software development company is SAQ D as it is a service provider.

Justification: PCI DSS defines a service provider as a third-party entity storing, processing and/or transmitting cardholder data (CHD) on behalf of a merchant, or that can impact upon the security of the merchant's cardholder data. Companies such as data centers, managed services providers, Software as a Service (SaaS) entities – and others – are looked upon in the world of PCI as service providers. While the software company is not directly involved in storage, processing, and/or transmitting of cardholder data, its affiliation with it is enough to identify it as such. So, while the software company may not have any direct access to cardholder data, they may still have indirect access to these information which further translates to the need for them to comply with the requirements of PCI DSS. This is not a straightforward scenario, and I am of the opinion that for the company to be on the safer side they should get assessed.

Also, the software company does not meet any additional SAQ questionnaire requirements, so it should complete SAQ D.

References

PCI DSS SAQ: Details you'll want to know - PCI DSS GUIDE

PCI SAQ A - PCI DSS GUIDE

Choosing the Right PCI DSS SAQ - PCI DSS GUIDE

PCI Service Providers Levels 1 and 2 Compliance Requirements (pcipolicyportal.com)

Service providers and PCI DSS Compliance – PCI Ramblings (Blog)