

## ControlScan SAQ A Eligibility Walkthrough

(For merchants using Edge HostPay Partner Products only)

Merchants utilizing payment application software in a compliant manner without storage of cardholder data may be eligible to complete the less burdensome SAQ A questionnaire when validating PCI compliance. This walkthrough will guide a merchant within the ControlScan portal to qualify for the SAQ A questionnaire (for merchants Processing Using a Shopping Cart / ECommerce solution with a payment page outsourced to third-party provider).

### 1. Choose "Click here to complete Questionnaire".

The screenshot shows the ControlScan dashboard for Richard Rohena. It displays the merchant ID as 'Unknown'. Under 'Overall PCI Compliance Status', there is a red circle with the text 'Requires scan'. The 'Annual Questionnaire' section shows a green circle with 'Questionnaire passed as of 2015-10-28 SAQ Type B' and a 'Next Action: Click here to complete Questionnaire' button. The 'Quarterly Scan' section shows a red circle with 'Scan(s) required' and a 'Next Action: Click here to get started' button. Below this is a 'Questionnaire History' table:

Date of Completion	SAQ Type	SAQ Version	Attested By	Days until Expiration	SAQ	AOC
10-28-2015	B	3.0	Test	352		

### 2. Confirm your company info and choose **Next**.

The screenshot shows the 'Company Info' form. It includes fields for Country (United States), Company Name (Accelerated Payment Techno...), Address 1, Address 2, City, State (Georgia), ZIP (11111), Contact Name, Title, Contact Phone (999-999-9999), Contact Email (r.r@accelerated...), and Contact Website (www.controlscan.com). A 'Next' button is visible at the bottom right.

### 3. Choose No and choose Next.

The screenshot shows the 'Service Provider Collection' form. It contains two questions with radio button options for 'Yes' and 'No'. The first question asks if the merchant has a relationship with any other third-party agents. The second question asks if the merchant utilizes a Qualified Integrated Reseller (QIR) to implement, configure and/or support a Payment Application. A 'Next' button is visible at the bottom right.

4. Choose **No** and choose **Next**.

**Company Info**

Does your company have a relationship with one or more third-party agents (e.g. gateways (Authorize.net, Shift 4), web-hosting companies, affiliate booking agents, loyalty program agents, etc.)?

Yes

No

Reference: Relationship

[Back](#) [Next](#)

5. Choose your merchant type and choose **Next**.

**Enter Your Merchant Type**

Please use the selection tools below to describe the category and type of business that best describes your company.

Currently Selected Merchant Type(s):

Hardware, Equipment and Supplies

Select or start typing to search:

- Furniture, Home Furnishings, and Household Goods
- Furniture, Home Furnishings, and Equipment Stores, Except Appliances
- General Contractors - Residential and Commercial
- Glass, Paint, and Wallpaper Stores
- Hardware Stores
- Hardware, Equipment and Supplies
- Home Supply Warehouse Stores
- Household Appliance Stores
- Lumber and Building Materials Stores
- Miscellaneous House Furnishing Specialty Stores
- Nurseries and Lawn and Garden Supply Stores
- Print, Stationery and Copying

Check here if your organization provides payment related services, has access to credit card information for another company's customers, or provides services that could impact the security of credit card information for another organization.

Reference: C3MP-2

[Back](#) [Next](#)

6. Choose **Processing Using a Shopping Cart / ECommerce - (Payment page outsourced to third-party provider)** as the Processing Method and choose **Next**.

**Select your Processing Method**

If you use more than one processing method, select your first processing method and you can add another when complete. This helps determine the Questionnaire that is appropriate for your business.

- Device Capable of utilizing End-to-End Encryption (Examples: Ingenico® iPP320, iSC Touch 250, iSC Touch 400)**  
Select this method if you are using POS (Point of Sale) software in a retail environment utilizing an end-to-end encryption device (PP320, SC250, SC400) as the ONLY entry mode for cardholder data. This includes processing with OpenEdge PC (iCharge) or securely integrated hosted payment form using PP320, SC250, or SC400 devices.
- POS Application Using Hand-Keypad or Magnetic Stripe Devices (Examples: MagTek® Dynamag, or IPAD, HSR)**  
Select this method if you are using POS (Point-of-Sale) software in a retail environment using Dynamag, IPAD, standard MSR (Magnetic Stripe Readers), and/or hand-keyed cardholder data entry. This includes processing with OpenEdge PC (iCharge) or securely integrated hosted payment form in a POS application.
- Processing Using a Shopping Cart / ECommerce - (Payment page outsourced to third-party provider)**  
Select this method if your customers enter their credit card information into a website to make online purchases, payments, or donations, AND all payment acceptance and those processing services are delivered directly from a third-party PCI validated server provider such as OpenEdge. Choose this option if you have no administrative control over the checkout page.
- Processing Using a Shopping Cart / Merchant Pay Page (Self-Hosted Pay Page or Page Administratively Controlled by Merchant)**  
During the payment process, the consumer enters credit card information on a checkout/payment page that is part of the merchant website or a website to which the merchant has administrative control.
- Processing Using a Virtual Terminal**  
Select this method if you use a web browser on a computer or mobile device to access a merchant services site (Businessview / Merchant Portal / OpenEdge View, etc.) for entering and authorizing credit card purchases. You should have a username and password and be able to access the site from any computer connected to the Internet.
- Manual Processing Using Phone/Paper/Imprint Machine**  
Select this method if you use a manual imprint machine or call a phone number and use the telephone key pad to submit credit card information to your processor.

[Back](#) [Next](#)

## 7. Choose "No, finished adding processing methods".

The screenshot shows a web application interface for selecting processing methods. The main heading is "Select your Processing Method". Below it, there is a section for "Currently Selected Processing Method(s)" which is empty. There is also a section for "Add Another Processing Method:" with four options: Payment Terminal, Virtual Terminal, POS Terminal, and Shopping Cart. A modal dialog box is open in the center, asking "Do you want to add another Processing Method?". The dialog has two radio buttons: "Yes, Add another Processing Method" and "No, finished adding processing methods". The "No" option is selected. The background is dimmed.

## 8. Choose No and choose Next.

The screenshot shows a question screen titled "Does your business electronically store credit card numbers?". The question text explains that electronic storage of credit card numbers is not allowed unless there is a compelling business reason. Below the question, there are two radio buttons: "Yes" and "No". The "No" option is selected. There is a "Reference: Q16.4" link below the radio buttons. At the bottom of the screen, there are "Back" and "Next" buttons.

## 9. Choose Yes and Next.

The screenshot shows an "Eligibility" screen. It states that based on previous answers, the user qualifies to complete a shortened version of the SAQ (SAQ A1) and asks to confirm the following statements:

- Your company accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
- All payment acceptance and processing are entirely outsourced to PCI DSS validated third-party service provider(s);
- Your company has no direct control of the manner in which cardholder data is captured, processed, transmitted, or stored;
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions;
- Your company has confirmed that all third party(s) handling acceptance, storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

Additionally, for e-commerce channels:

- The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s).

Below the statements, there is a question: "Do you agree with all of the above statements?". There are two radio buttons: "Yes" and "No". The "Yes" option is selected. There is a "Reference: Q16.5" link below the radio buttons. At the bottom of the screen, there are "Back" and "Next" buttons.

10. You are now ready to begin the less burdensome SAQ A questionnaire. This questionnaire is designed to provide merchants with insight into the security features already in place at their location, as well as possible security gaps and vulnerabilities. The wizard will allow you to return to any question to change an answer if you are unsure of your current state in regards to any specific question.

The screenshot displays a web-based questionnaire interface. At the top, a navigation bar includes tabs for 'Introduction', 'Company Info', 'Qualification', 'Questionnaire', and 'Confirmation'. A progress indicator shows '39%' completion. The main content area is divided into two sections. On the left, a sidebar lists various security topics, with 'Use and Update Anti-Virus Software' selected. The main panel displays a question: 'Anti-virus software is deployed on all systems commonly affected by malicious software.' Below the question are three radio button options: 'True', 'False', and 'Not Applicable'. A reference to 'SAQ C.5.1' and a note '(14) questions answered' are visible. At the bottom, there are 'Back' and 'Next' buttons, along with an 'Auto Advance' toggle set to 'OFF'.

Introduction Company Info Qualification **Questionnaire** Confirmation 39%

**Use and Update Anti-Virus Software**

Anti-virus software is deployed on all systems commonly affected by malicious software.

All anti-virus programs are capable of detecting, removing, and preventing the execution of malicious software. If your organization uses systems considered to be rarely affected by malicious software, you may not have anti-virus software installed on those systems. All anti-virus software and definitions are kept current.

**Security Maintenance**

- Restrict access to cardholder data
- Restrict Physical Access
- Assign Unique Access controls
- Protect Sensitive Authentication Data
- Install and Maintain a Firewall
- Do Not Use Vendor Defaults
- Encrypted Transmission of Data
- Track and Monitor Access
- Maintain a security policy
- Test Security Systems

Anti-virus software is deployed on all systems commonly affected by malicious software.

True

False

Not Applicable

References: SAQ C.5.1  
(14) questions answered

Back Auto Advance OFF Question Loaded Next