PCI Informational Update

Presented February 2026

NEBRASKA
OFFICE OF THE CIO

ISA Information

- OCIO since October 2022
- Internal Security Assessor (ISA) originally certified May 26, 2023

2025 Completed SAQs

- 32: SAQ A
- 11: SAQ P2PE
- 3: SAQ B-IP
- 2: SAQ D

SAQ: Self-Assessment Questionnaire

General Timeline

Agency SAQ(s) submissions: March 1 – July 1

- You can submit drafts of the SAQ(s), and I will review and let you know if I notice anything that you may want to consider before having it signed.

ISA PCI SAQ reviews: March 1 – September 1

ISA PCI Onsite reviews: July 1 – October 31

Unresponsive Email (ISA Supervisor): September 1-15

Unresponsive Email (Deputy CISO): October 1-15

ISA submit SAQ results to Treasurer: November 1 – November 10

PCI Resources

PCI Document Library

- PCI DSS Quick Reference Guide (38 page pdf, revised January 2025)
  - Introduction to PCI DSS, Understanding PCI DSS, and Resources
- SAQ Instructions and Guidelines (30-page pdf, revised October 2024)
  - Starting on Page 4-6 and page 9. Contains additional details for each SAQ
- PCI DSS Summary of Changes version 4.0 to 4.0.1
  - (11-page pdf, revised August 2024)
- PCI DSS Requirements and Testing Procedures
  - (397-page pdf, revised June 2024)
- Individual SAQs downloaded from the PCI Document Library
  - MS Word Version is fillable – PDF Version is not fillable
- TRA Guidance (6-page pdf, revised November 2023)
  - Page 6 on frequency guidance

PCI Resources (continued)

PCI FAQs

PCI Merchant Resources

PCI on YouTube

State PCI SharePoint Site

- Only available to @nebraska.gov email addresses
- Contains example SAQs and discussions.

State Treasurer PCI Site

- Contains items to be included in the Merchant Manual

Visa Global Registry of Services

- Checks the PCI DSS Validation Status of a Service Provider

State Treasurer PCI Site

Physical/Digital Merchant Manual

- Section 1: Responsibility Matrix(es)
- Section 2: Annual PCI Self-Assessment Questionnaire
- Section 3: Vulnerability Scans or Attestation Of Compliance (AOC)
- Section 4: Cardholder Data Flow Diagram
- Section 5: Agency Policies and Procedures
- Section 6: Agreements with Treasurer's Office/Employees/Third Party Providers

This is the current list of items as of 23 FEB 2026.

Which SAQ(s) to complete and submit

"Merchants should consult with their compliance-accepting entity - the entity to which the SAQ will be submitted (typically, an acquirer (merchant bank) or a payment brand) to determine if they are eligible or required to submit an SAQ, and if so, which SAQ is appropriate for their environment.

Additional guidance is also provided in *PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*, available in the Document Library." - From FAQ 1215 (What is a PCI DSS Self-Assessment Questionnaire?)

In the State's environment, the agency will want to reach out to either the State Treasurer or to Elavon to see which SAQ(s) to complete.

Third Party Service Providers (TPSPs)

“Per Requirement 12.9.2, TPSPs are required to support their customers’ requests for information about the TPSP’s PCI DSS compliance status related to the services provided to customers, and about which PCI DSS requirements are the responsibility of the TPSP, which are the responsibility of the customer, and any responsibilities shared between the customer and the TPSP.” This is sometimes referred to as a Responsibility Matrix.

PCI DSS Requirements and Testing Procedures (Page 17)

SAQ General Changes

- Will use the same version as last year PCI version 4.0.1

SAQ General Changes

- None since August 2024

General SAQ Completion Guidance

The next several slides will cover sections/parts of the SAQs that are similar in all SAQs.

Section 1: Assessment Information

- Part 1a., 1b., 2a., 2b., 2c., 2d., 2g. 2f.

Section 2

- Self-assessment completion date

Appendix C

Section 3

- Part 3., Part 3a, Part 3b

Section 1, Part 1a

Part 1. Contact Information	
Part 1a. Assessed Merchant	
Company name:	Department of Processing Payment Cards
DBA (doing business as):	DPPC
Company mailing address:	501 S. 14th St., Lincoln, NE 68508 - USA
Company main website:	cio.nebraska.gov
Company contact name:	Edward Hawkins
Company contact title:	Chief Administration Officer
Contact phone number:	402.471.3134
Contact e-mail address:	edward.hawkins@nebraska.gov

Section 1, Part 1b

Part 1b. Assessor	
Provide the following information for all assessors involved in the assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	Jason Seamann
Qualified Security Assessor	
Company name:	
Company mailing address:	
Company website:	
Lead Assessor Name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor certificate number:	

Section 1, Part 2a

Look to “Completing the Self-Assessment Questionnaire” on Page iii for a list of available payment channels for your SAQ. Should only include channels you currently use.

Part 2a. Merchant Business Payment Channels (select all that apply):	
Indicate all payment channels used by the business that are included in this assessment. ☐ Mail order/telephone order (MOTO) ☒ E-Commerce ☐ Card-present	
Are any payment channels not included in this assessment? If yes, indicate which channel(s) is not included in the assessment and provide a brief explanation about why the channel was excluded.	☐ Yes ☒ No
Note: *If the organization has a payment channel that is not covered by this SAQ, consult with the entity(ies) to which this AOC will be submitted about validation for the other channels.*	

Section 1, Part 2b

Similar to Section 1, Part 2a, you should only select the channels included in the “Completing the Self-Assessment Questionnaire” on Page iii. Each line should represent a ‘Channel’ selected in Part 2a.

Part 2b. Description of Role with Payment Cards	
For each payment channel included in this assessment as selected in Part 2a above, describe how the business stores, processes, and/or transmits account data.	
Channel	**How Business Stores, Processes, and/or Transmits Account Data**
E-Commerce	Department of Processing Payment Cards outsources payment card processing to validated third party provider. We use an e-commerce site hosted through a validated third party vendor. At no time is card holder data stored, processed, or transmitted to or from department managed machines.

Section 1, Part 2c

Make sure you provide a high-level description of the environment covered by the assessment.

The OCIO implements network segmentation.

Part 2c. Description of Payment Card Environment	
Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	Payments are accepted through a public web-server hosted by a validated third party vendor over a secure connection. The Department of Processing Payment Cards does not store, process or transmit cardholder data of any type.
Indicate whether the environment includes segmentation to reduce the scope of the assessment. *(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)*	☒ Yes ☐ No

Section 1, Part 2d

Include all the types of physical locations in scope for the PCI DSS assessment.

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities (for example, retail locations, corporate offices, data centers, call centers, and mail rooms) in scope for the PCI DSS assessment.

Facility Type	Total number of locations (How many locations of this type are in scope)	Location(s) of facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Main Office	1	Lincoln, NE, USA
Data Center	1	Lincoln, NE, USA

Section 1, Part 2f

Select the appropriate boxes and then provide a description of services provided. Requirement 12.8 applies to all the entities on the list.

Part 2f. Third-Party Service Providers	
Does the merchant have relationships with one or more third-party service providers that:	
• Store, process, or transmit account data on the merchant's behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)	☒ Yes ☐ No
• Manage system components included in the scope of the merchant's PCI DSS assessment—for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers.	☒ Yes ☐ No
• Could impact the security of the merchant's CDE (for example, vendors providing support via remote access, and/or bespoke software developers)	☐ Yes ☒ No
If Yes:	
Name of service provider:	**Description of service(s) provided:**
Third Party Service Provider (TPSP) name	Hosts webiste for handling all facets of DPPC payment processing.

Part 2g. Summary of Assessment

Complete Part 2g ***after you completed out Section 2*** of the SAQ. This will be a summary of the Required Responses. You can select more than one Requirement Response in Part 2g for each Requirement.

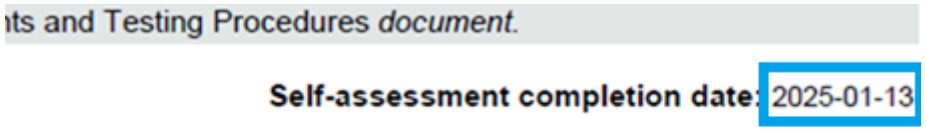
Part 2g. Summary of Assessment
(SAQ Section 2 and related appendices)

Indicate below all responses that were selected for each PCI DSS requirement.

PCI DSS Requirement *	Requirement Responses *More than one response may be selected for a given requirement. Indicate all responses that apply.*			
	In Place	In Place with CCW	Not Applicable	Not in Place
Requirement 1:	☒	☐	☐	☐
Requirement 2:	☒	☐	☒	☐
Requirement 3:	☒	☐	☒	☐

Section 2: Self-assessment completion date

Top right of the first page of Section 2 there is a date you need to enter for when you completed the Self-assessment. This should be the same date on Section, Part 3.



Section 2 Requirement responses

Select only one (1) response for each requirement in Section 2.

- *In Place*: The expected testing has been performed, and all elements of the requirement have been met as stated.
- *In Place with CCW* (Compensating Controls Worksheet): The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Controls Worksheet (CCW) in Appendix B of this SAQ. – *Not used on SAQ A, P2PE, B-IP*

From Page v of the SAQ.

Section 2 Requirement responses (continued)

Select only one (1) response for each requirement in Section 2.

- *Not Applicable*: The requirement does not apply to the merchant's environment. All responses in this column require a supporting explanation in Appendix C of this SAQ.
- *Not in Place*: Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before the merchant can confirm they are in place. Responses in this column may require the completion of Part 4, if requested by the entity to which this SAQ will be submitted.

From Page v of the SAQ.

Defining Account Data, Cardholder Data, and Sensitive Authentication Data

PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of cardholder data and/or sensitive authentication data. Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

Appendix C

Complete Appendix C ***after you completed all of Section 2***. If you want, you can group similar explanations onto a single line.

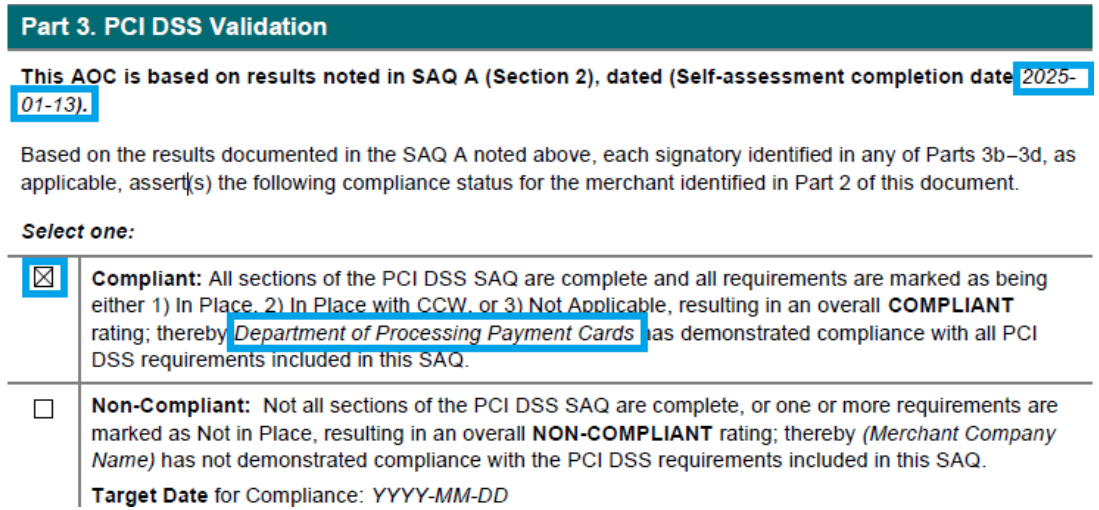
Appendix C: Explanation of Requirements Noted as Not Applicable

This Appendix must be completed for each requirement where Not Applicable was selected.

Requirement	Reason Requirement is Not Applicable
Example:	
Requirement 3.5.1	*Account data is never stored electronically*
3.1.1, 3.2.1, 9.4.1-9.4.6	Account data is never stored in paper records by the agency (merchant).

Section 3, Part 3

At the top of the page enter the Self-assessment completion date (same date as top of Section 2). If you check any of the boxes other than Compliant, you will need to reach out to me. Also change the 'Merchant Company Name' to your organization name.



Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ A (Section 2), dated (Self-assessment completion date *2025-01-13).*

Based on the results documented in the SAQ A noted above, each signatory identified in any of Parts 3b–3d, as applicable, assert(s) the following compliance status for the merchant identified in Part 2 of this document.

Select one:

☒	**Compliant:** All sections of the PCI DSS SAQ are complete and all requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *Department of Processing Payment Cards* has demonstrated compliance with all PCI DSS requirements included in this SAQ.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Merchant Company Name)* has not demonstrated compliance with the PCI DSS requirements included in this SAQ. **Target Date** for Compliance: *YYYY-MM-DD*

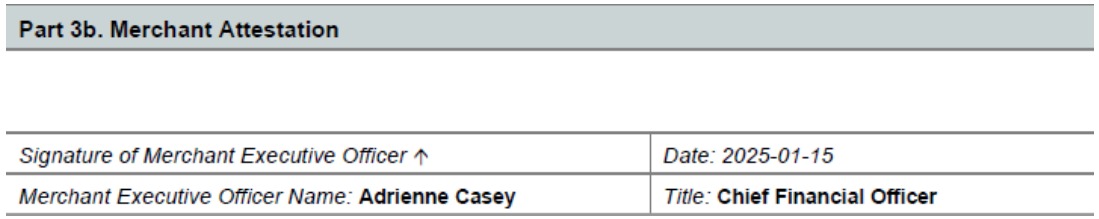
Section 3. Part 3a

If you do not select all the boxes, the SAQ will be returned. If you have questions on the boxes, please let me know.

Part 3a. Merchant Acknowledgement	
Signatory(s) confirms: *(Select all that apply)*	
☒	*PCI DSS Self-Assessment Questionnaire A, Version 4.0.1*, was completed according to the instructions therein.
☒	All information within the above-referenced SAQ and in this attestation fairly represents the results of the merchant's assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the merchant's environment.

Section 3. Part 3b

Once the SAQ is completed and finalized, you should have the Merchant Executive Officer* sign the form. Make sure you include their name, title, and date they signed the form. The signature date can be up to two (2) weeks after the SAQ is completed.



Part 3b. Merchant Attestation	
Signature of Merchant Executive Officer ↑	*Date:* 2025-01-15
Merchant Executive Officer Name: **Adrienne Casey**	*Title:* **Chief Financial Officer**

* https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-does-duly-authorized-officer-mean

Not In Place Requirements

- Section 2 Response marked “Not in Place”

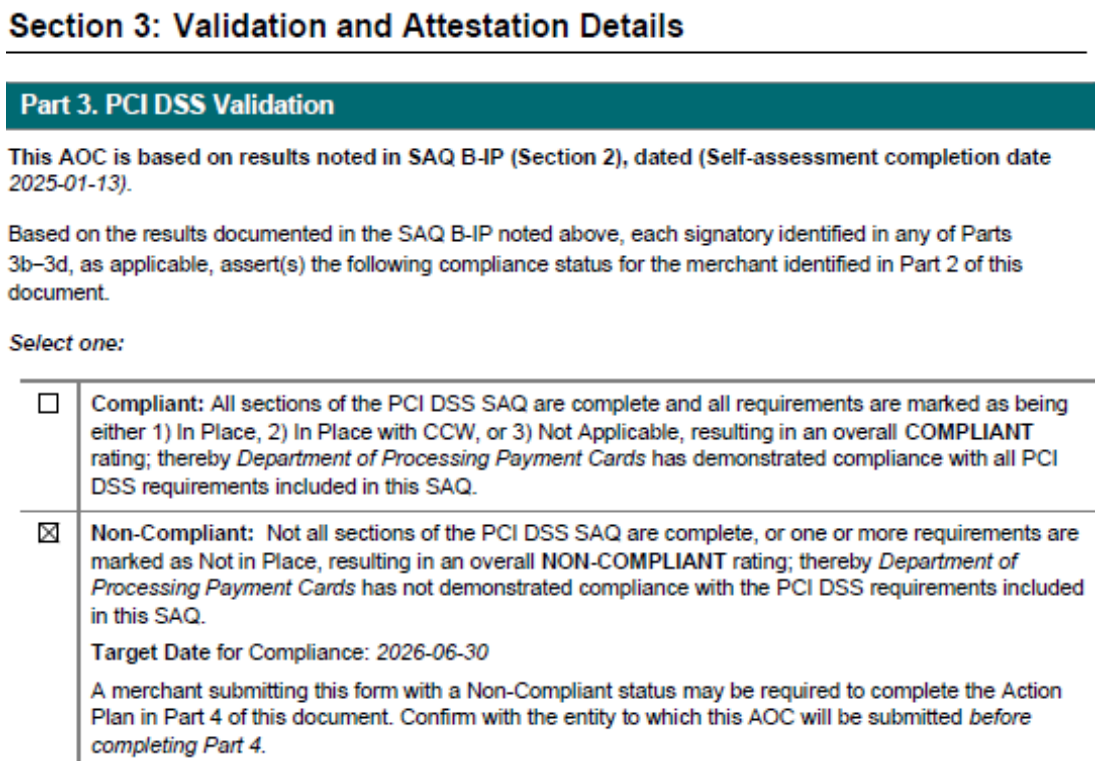
PCI DSS Requirement		Expected Testing	Response* (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.						
11.4.5	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods.	• Examine segmentation controls. • Review penetration-testing methodology. • Examine the results from the most recent penetration test.	☐	☐	☐	☒

Not In Place Requirements

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

- Mark ‘’Non-Compliant’’



Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ B-IP (Section 2), dated (Self-assessment completion date *2025-01-13).*

Based on the results documented in the SAQ B-IP noted above, each signatory identified in any of Parts 3b–3d, as applicable, assert(s) the following compliance status for the merchant identified in Part 2 of this document.

Select one:

☐	**Compliant:** All sections of the PCI DSS SAQ are complete and all requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *Department of Processing Payment Cards* has demonstrated compliance with all PCI DSS requirements included in this SAQ.
☒	**Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *Department of Processing Payment Cards* has not demonstrated compliance with the PCI DSS requirements included in this SAQ. **Target Date** for Compliance: *2026-06-30* A merchant submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted *before completing Part 4.*

Not In Place Requirements

Part 4. Action Plan for Non-Compliant Requirements:

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has a Non-Compliant status noted in Section 3.

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has a Non-Compliant status noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the merchant expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement*	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
9	Restrict physical access to cardholder data	☐	☐	
11	Test security systems and networks regularly	☐	☒	Expects to be in compliance 2026-06-30. Working with the OCIO to have penetration testing done on the network.

SAQ A

27 FEB 2026

SAQ A

Self-Assessment Questionnaire (SAQ) A includes only those PCI DSS requirements applicable to merchants with account data functions completely outsourced to PCI DSS validated and compliant third parties, where the merchant retains only paper reports or receipts with account data. SAQ A merchants may be either ***e-commerce or mail/telephone-order merchants (card-not-present)*** and do not store, process, or transmit any account data in electronic format on their systems or premises.

This SAQ is not applicable to face-to-face channels.

SAQ A: Updates

- January 2025:
  - Removed Requirements 6.4.3 (page scripts), 11.6.1 (tamper-detection), and 12.3.1 (target risk analysis) and added an Eligibility Criteria for merchants to confirm that their site is not susceptible to attacks from scripts that could affect the merchant's e-commerce system(s).

https://blog.pcisecuritystandards.org/important-updates-announced-for-merchants-validating-to-self-assessment-questionnaire-a

Section 1. Part 2e

You should check ‘No’ and not enter additional validated products and solutions.

Part 2e. PCI SSC Validated Products and Solutions

Does the merchant use any item identified on any PCI SSC Lists of Validated Products and Solutions•?

☐ Yes ☒ No

Provide the following information regarding each item the merchant uses from PCI SSC’s Lists of Validated Products and Solutions.

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which product or solution was validated	PCI SSC listing reference number	Expiry date of listing (YYYY-MM-DD)
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD

Part 2h.

If you do not select all the boxes, then the SAQ will be returned.

Part 2h. Eligibility to Complete SAQ A	
Merchant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment channel:	
☒	The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transaction.
☒	All processing of account data is entirely outsourced to a PCI DSS compliant third-party service provider (TPSP)/payment processor.
☒	The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions.
☒	The merchant has confirmed that TPSP(s) are PCI DSS compliant for the services being used by the merchant.
☒	Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.
Additionally, for e-commerce channels, merchant certifies:	
☒	All elements of the payment page(s)/form(s) delivered to the customer's browser originate only and directly from a PCI DSS compliant TPSP/payment processor.
☒	The merchant has confirmed that their site is not susceptible to attacks from scripts that could affect the merchant's e-commerce system(s).

Section 2. Requirement 3

Make sure you read through the SAQ Completion Guidance as this will help to determine which response to check. See previous slide in presentation on what is defined as ‘account data.’

Requirement 3: Protect Stored Account Data

Note: *For SAQ A, Requirement 3 applies only to merchants with paper records that include account data (for example, receipts or printed reports).*

PCI DSS Requirement		Expected Testing	Response* (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
3.1 Processes and mechanisms for protecting stored account data are defined and understood.						
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.	• Examine documentation. • Interview personnel.	☐	☐	☒	☐

SAQ Completion Guidance:

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 C: Explanation of Requirements Noted as Not Applicable.

SAQ A: Requirements 6.3.1 & 6.3.3

- Note:
  - For SAQ A, Requirement 6 applies to merchant server(s) with a webpage that either 1) redirects customers from the merchant webpage to a TPSP/payment processor for payment processing (for example, with a URL redirect) or 2) includes a TPSP's/payment processor's embedded payment page/form (for example, one or more inline frames or iframes).
- Expected Testing:
  - Policies and procedures to identify new security vulnerabilities, vulnerabilities are assigned a risk ranking.
  - Patches/updates for critical vulnerabilities are installed within one month of release.
  - Compare list of security patches installed to recent vendor patch lists.

SAQ A: Requirement 11.3.2 (ASV)

There are two different scans mentioned for Requirement 11. They can be run at the same time. Requirement 11.3.2 needs to be performed by a PCI SSC Approved Scanning Vendor (ASV).

- The ASV scan can either be provided by the TPSP or by the OCIO (for a fee*)
  - If by the OCIO, if you have any vulnerability(ies) with a CVSS score of 4.0 or greater, you will need to either correct the vulnerability or dispute the failure before it can be submitted to Tenable (the ASV).
  - Passing scan at least once every three months.

* As of 09 FEB 2026, the OCIO did not charge for the scan(s) for the previous year(s) scans. If the OCIO starts charging for the scans, I will let you know prior to the charges.

SAQ A: Requirement 11.3.2.1

External vulnerability scans are performed after any significant change.

- Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved.
- Rescans are conducted as needed.
- Is not the same as the ASV scan.

SAQ B-IP vs SAQ P2PE

- Number of Primary Requirements
  - SAQ B-IP: *11* vs SAQ P2PE: *3*
- SAQ P2PE transfers more risk because of the software solution
  - If you do not have the solution, you will need to contact the Treasurer (Char Scott). As of the time of this presentation, the cost was $25 per month per device.

SAQ P2PE

27 FEB 2026

SAQ P2PE

Self-Assessment Questionnaire for Point-to-Point Encryption (SAQ P2PE) includes only those PCI DSS requirements applicable to merchants that process account data only via a validated PCI-listed P2PE solution. SAQ P2PE merchants do not have access to clear-text account data on any computer system, and only enter account data via payment terminals from a validated PCI-listed P2PE solution.

SAQ P2PE merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants. For example, a mail/telephone-order merchant could be eligible for SAQ P2PE if they receive account data on paper or over a telephone, and key it directly and only into payment terminal from a validated PCI-listed P2PE solution.

This SAQ is not applicable to e-commerce channels.

SAQ P2PE Updates

- None since October 2024

Section 1, Part 2e

P2PE solutions on the PCI list of Point-to-Point Solutions with Expired Validations are no longer considered “validated” per the P2PE Program Guide. Merchants using an expired P2PE solution should check with their acquirer or individual payment brands about acceptability of this SAQ.

Next several slides show how to find the information on the PCI website.

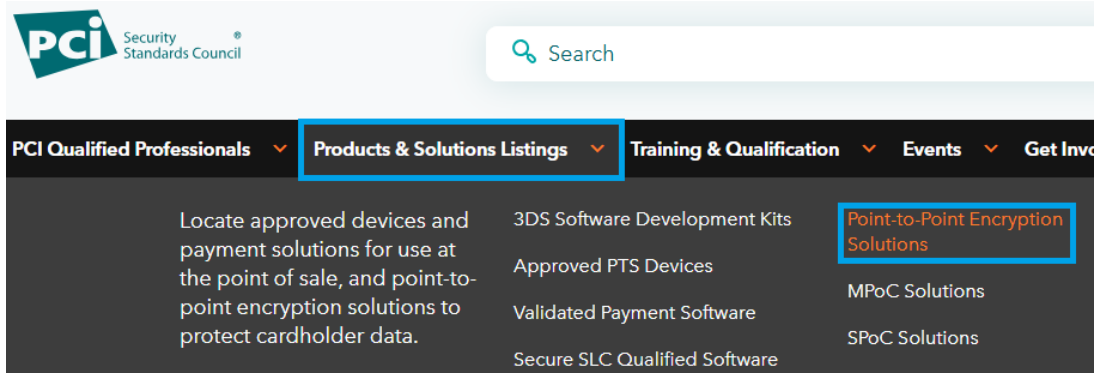
Part 2e. PCI Validated P2PE Solution	
Provide the following information regarding the validated• PCI-listed P2PE solution used by the merchant:	
Name of P2PE Solution Provider:	Elavon
Name of P2PE Solution:	Safe-T Link(TM) with P2PE Protect
P2PE Solution listing (“Reference #”:	2024-00679.007
Listed POI Devices used by Merchant (found under “PTS POI Devices Supported”):	Ingenico Desk 3500
P2PE Solution “Reassessment Date”:	21 November 2027

How To Find P2PE Solution

- https://www.pcisecuritystandards.org/
- Products & Solutions Listings
- Point-to-Point Encryption Solutions
  - Search for Elavon or Safe-T Link or the solution you are using
  - If search for Elavon, may need to select the different Elavon's until you find your solution. For example the Safe-T Link (TM) with P2PE Protect is under "Elavon, Inc."

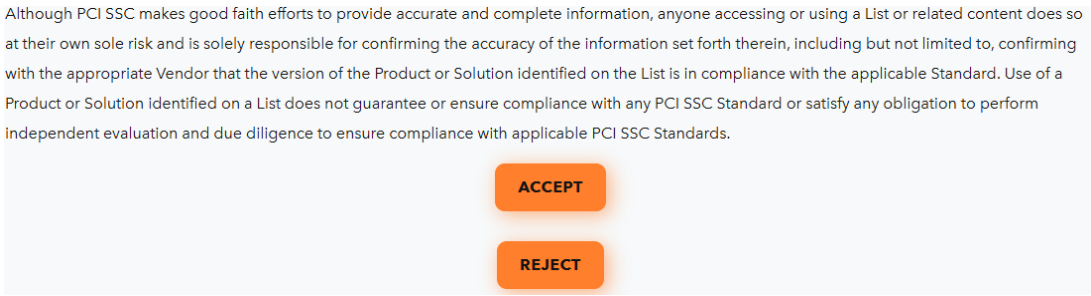
PCI Website: Find P2PE Solution

On PCI website click on Products & Solutions Listings. Then click on Point-to-Point Encryption Solutions.



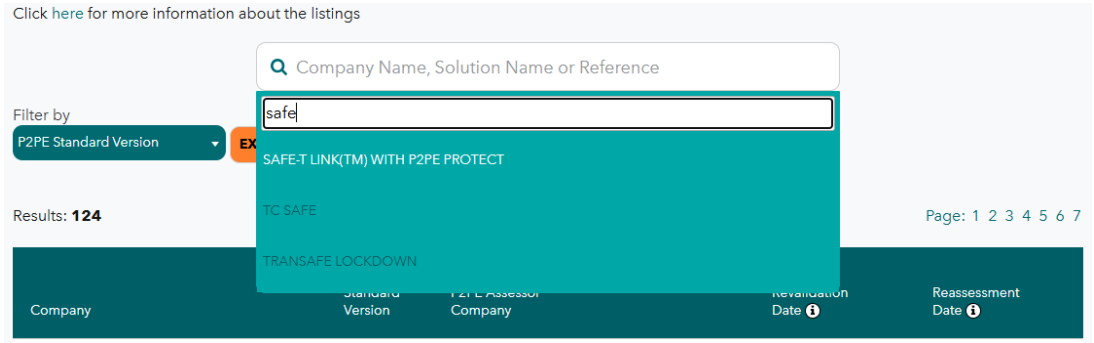
PCI Website: Find P2PE Solution

If the page opens up asking you to accept the terms on the page.



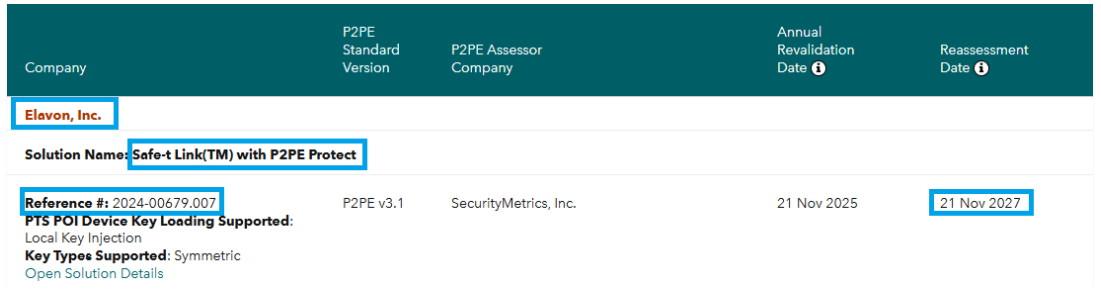
PCI Website: Find P2PE Solution

Click on the search box and type in the same of the solution. In this example it is SAFE-T. Click on the solution, once it comes up.



PCI Website: Find P2PE Solution

You will be able to gather the Company, Solution Name, Reference #, and Reassessment Date to be inserted into Section 1 Part 2e.



Company	P2PE Standard Version	P2PE Assessor Company	Annual Revalidation Date	Reassessment Date
Elavon, Inc.				
Solution Name: Safe-t Link(TM) with P2PE Protect				
Reference #: 2024-00679.007 PTS POI Device Key Loading Supported: Local Key Injection Key Types Supported: Symmetric Open Solution Details	P2PE v3.1	SecurityMetrics, Inc.	21 Nov 2025	21 Nov 2027

Part 2e. PCI Validated P2PE Solution	
Provide the following information regarding the validated* PCI-listed P2PE solution used by the merchant:	
Name of P2PE Solution Provider:	Elavon
Name of P2PE Solution:	Safe-T Link(TM) with P2PE Protect
P2PE Solution listing ("Reference #":	2024-00679.007
Listed POI Devices used by Merchant (found under "PTS POI Devices Supported"):	Ingenico Desk 3500
P2PE Solution "Reassessment Date":	21 November 2027

How To Find POI Device

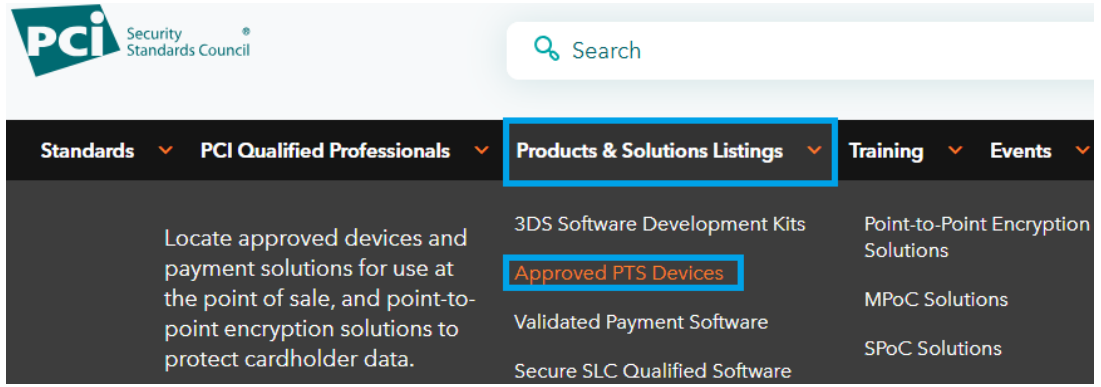
- https://www.pcisecuritystandards.org/
- Products & Solutions Listings
- Approved PTS Devices
  - Search for either Ingenico or DESK3500 or the device you are using

POI: Point-of-Interaction

PTS: PIN Transaction Security

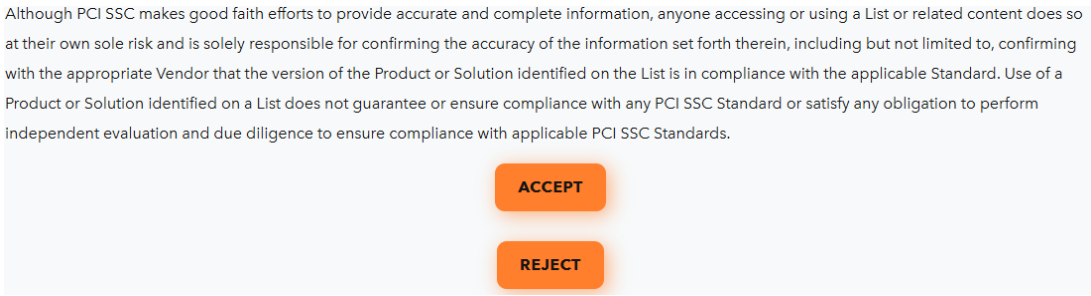
PCI Website: Find POI Device

On PCI website click on Products & Solutions Listings. Then click on Approved PTS Devices.



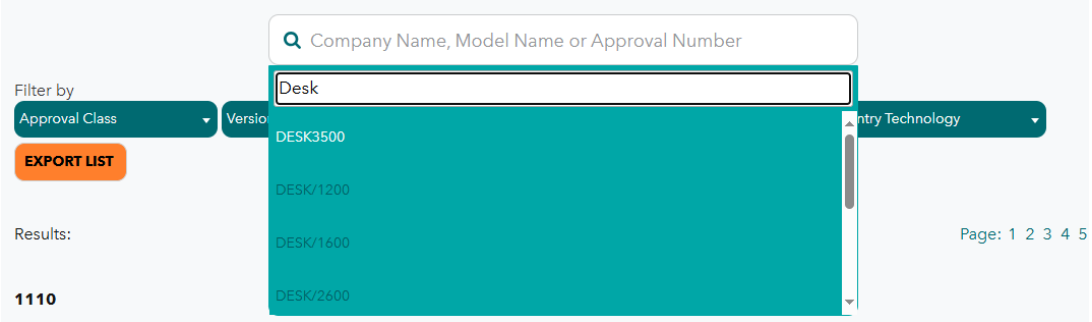
PCI Website: Find POI Device

If the page opens up asking you to accept the terms on the page.



PCI Website: Find POI Device

Click on the search box and type in the name of the device. In this example it is DESK3500. Click on the POI device, once it comes up.



PCI Website: Find POI Device

You will be able to verify the device is approved by PCI and you can insert the name into Section 1 Part 2e.

Company	Approval Number	Version	Approval Class	Expiry Date
Ingenico **http://www.ingenico.com**				
DESK3500				
	4-100001	3.x	KLD	30 Apr 2026

Hardware #: DES35BB
DES35AB

Firmware #: 820380V01.xx (Scheme Pack)
820380V02.xx (Scheme Pack)
820380V04.xx (Scheme Pack)
820380V05.xx (Scheme Pack)
820380V06.xx (Scheme Pack)
820380V07.xx (Scheme Pack)
820380V08.xx (Security Services)
820563V02.xx 820380V03.xx (Scheme Pack)
820563V03.xx
820380V09.xx (Security Services)
820563V01.xx

Applic #:

View Security Policy

Part 2e. PCI Validated P2PE Solution	
Provide the following information regarding the validated* PCI-listed P2PE solution used by the merchant:	
Name of P2PE Solution Provider:	Elavon
Name of P2PE Solution:	Safe-T Link(TM) with P2PE Protect
P2PE Solution listing "Reference #":	2024-00679.007
Listed POI Devices used by Merchant (found under "PTS POI Devices Supported"):	Ingenico Desk 3500
P2PE Solution "Reassessment Date":	21 November 2027

Part 2h.

If you do not select all the boxes, then the SAQ will be returned.

Part 2h. Eligibility to Complete SAQ P2PE	
Merchant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment channel:	
☒	All payment processing is via a validated PCI-listed P2PE solution (per Part 2e above).
☒	The only systems in the merchant environment that store, process, or transmit account data are the payment terminals from a validated PCI-listed P2PE solution.
☒	The merchant does not otherwise receive, transmit, or store account data electronically.
☒	Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.
☒	The merchant has implemented all controls in the *P2PE Instruction Manual (PIM)* provided by the P2PE Solution Provider.

Section 2. Requirement 3

Make sure you read through the SAQ Completion Guidance as this will help to determine which response to check. See previous slide in presentation on what is defined as ‘account data.’

PCI DSS Requirement		Expected Testing	Response* (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 3.2.1 means that the merchant has data disposal policies that govern account data storage and if a merchant stores any paper (for example, receipts or paper reports) that contain account data, the merchant stores the paper per that policy (for example, only 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 C: Explanation of Requirements Noted as Not Applicable.*						
3.3 Sensitive authentication data (SAD) is not stored after authorization.						
3.3.1.2	The card verification code is not stored upon completion of the authorization process.	• Examine data sources.	☐	☐	☒	☐
	Applicability Notes					
	The card verification code is the three- or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions.					
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 3.3.1.2 means that if the merchant writes down the card verification code while a transaction is being conducted, the merchant either securely destroys the paper (for example, with a shredder) immediately after the transaction is complete, or obscures the code (for example, by “blacking it out” with a marker) before the paper is stored.* *If the merchant never requests the three-digit or four-digit number printed on the front or back of a payment card (“card verification code”), mark this requirement as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.*						

Section 2. Requirement 9.4.1 – 9.4.6

Make sure you read through the SAQ Completion Guidance as this will help to determine which response to check. See previous slide in presentation on what is defined as ‘account data.’

PCI DSS Requirement		Expected Testing	Response* (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
9.4.6	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction.	• Examine the media destruction policy. • Observe processes. • Interview personnel. • Observe storage containers.	☐	☐	☐	☐
	Applicability Notes					
	These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.					

SAQ Completion Guidance:

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 C: Explanation of Requirements Noted as Not Applicable.

Section 2. Requirement 9.5

Make sure you have policies/documents for Requirements 9.5.1 – 9.5.1.3.

- POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution.
- An up-to-date list of POI devices is maintained.
- POI device surfaces are periodically inspected to detect tampering and unauthorized substitution
- Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices

SAQ B-IP

27 FEB 2026

SAQ B-IP

- Self-Assessment Questionnaire (SAQ) B-IP includes only those PCI DSS requirements applicable to merchants that process account data only via standalone, PCI-listed approved PIN Transaction Security (PTS) point-of-interaction (POI) devices with an IP connection to the payment processor. An exception applies for PTS POI devices classified as Secure Card Readers (SCR) and Secure Card Readers for PIN (SCRPs); merchants using SCRs or SCRPs are not eligible for this SAQ.
- SAQ B-IP merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not present) merchants, and do not store account data on any computer system.
- This SAQ is not applicable to e-commerce channels.

SAQ B-IP Updates

- None since October 2024

Section 1. Part 2e

You will need to complete Part 2e with the PCI SCC validated Product.

Part 2e. PCI SSC Validated Products and Solutions

Does the merchant use any item identified on any PCI SSC Lists of Validated Products and Solutions*?

☒ Yes ☐ No

Provide the following information regarding each item the merchant uses from PCI SSC's Lists of Validated Products and Solutions.

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which product or solution was validated	PCI SSC listing reference number	Expiry date of listing (YYYY-MM-DD)
Ingenico Desk3500	DES35BB / DES35AB	3.x	4-100001	2026-04-30

SAQ B-IP – How To Find POI Device

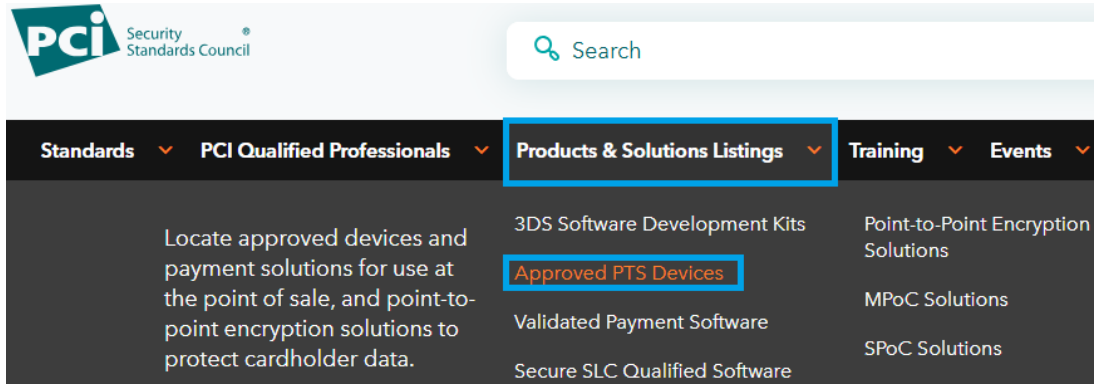
- https://www.pcisecuritystandards.org/
- Products & Solutions Listings
- Approved PTS Devices
  - Search for either Ingenico or DESK3500 or the device you are using

POI: Point-of-Interaction

PTS: PIN Transaction Security

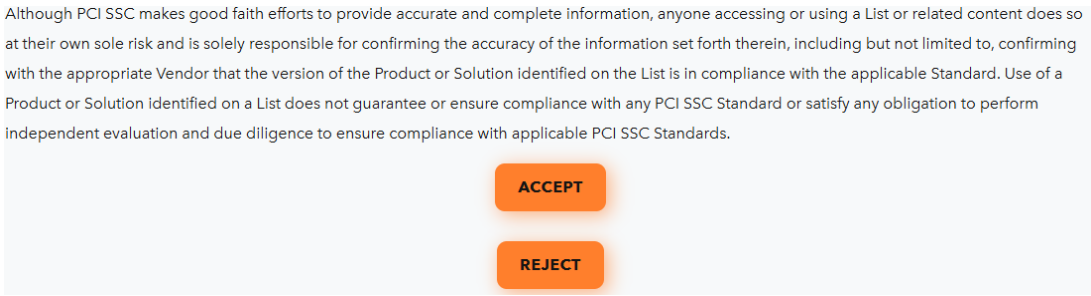
PCI Website: Find POI Device

On PCI website click on Products & Solutions Listings. Then click on Approved PTS Devices.



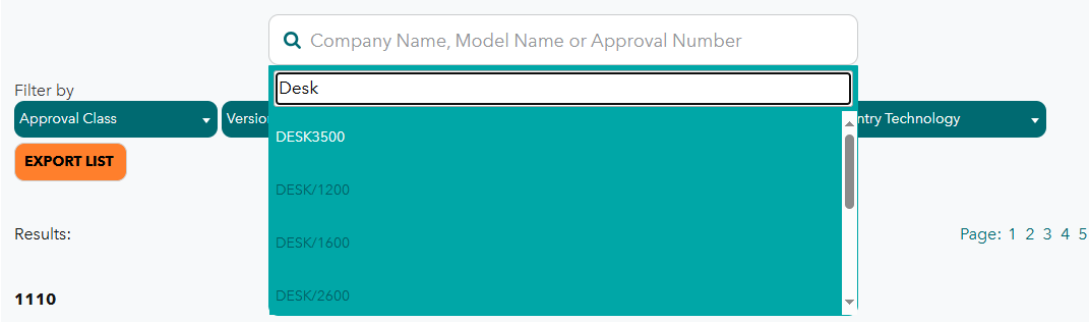
PCI Website: Find POI Device

If the page opens up asking you to accept the terms on the page.



PCI Website: Find POI Device

Click on the search box and type in the name of the device. In this example it is DESK3500. Click on the POI device, once it comes up.



PCI Website: Find POI Device

You will be able to verify the device is approved by PCI and you can insert the information into Section 1 Part 2e.

Company	Approval Number	Version	Approval Class	Expiry Date
Ingenico http://www.ingenico.com				
DESK3500				
	4-100001	3.x	KLD	30 Apr 2026

Hardware #: DES35BB
DES35AB

Firmware #: 820380V01.xx (Scheme Pack)
820380V02.xx (Scheme Pack)
820380V04.xx (Scheme Pack)
820380V05.xx (Scheme Pack)
820380V06.xx (Scheme Pack)
820380V07.xx (Scheme Pack)
820380V08.xx (Security Services)
820563V02.xx 820380V03.xx (Scheme Pack)
820563V03.xx
820380V09.xx (Security Services)
820563V01.xx

Applic #:

View Security Policy

Part 2e. PCI SSC Validated Products and Solutions

Does the merchant use any item identified on any PCI SSC Lists of Validated Products and Solutions*?

☒ Yes ☐ No

Provide the following information regarding each item the merchant uses from PCI SSC's Lists of Validated Products and Solutions.

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which product or solution was validated	PCI SSC listing reference number	Expiry date of listing (YYYY-MM-DD)
Ingenico Desk3500	DES35BB / DES35AB	3.x	4-100001	2026-04-30

Section 2: Requirements 1 and 2

Refer to you TPSP Responsibility Matrix as the primary source.
You can mark these items in place because the OCIO does

- Restrict inbound/outbound traffic to/from the CDE
- NCS are installed
- Anti-spoofing measures are implemented
- Vendor default accounts are managed
- All non-console administrative access is encrypted.
- Not Applicable for 2.3.1 and 2.3.2
    - The wireless environments should not be connected to the CDE

Section 2: Requirements 6.3.1 & 6.3.3

- Requirement 6.3.1: Security vulnerabilities are identified and managed.
- Requirement 6.3.3: All system components are protected from known vulnerabilities by installing applicable security patches/updates

Section 2. Requirement 9.5

Make sure you have policies/documents for Requirements 9.5.1 – 9.5.1.3.

- POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution.
- An up-to-date list of POI devices is maintained.
- POI device surfaces are periodically inspected to detect tampering and unauthorized substitution
- Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices

Section 2: Requirements 11.3.2 and 11.4.5

- Requirement 11.3.2: External vulnerability scans are performed at least once every three months, by a PCI SSC Approved Scanning Vendor (ASV), and Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met.
- Requirement 11.4.5: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls at least once every 12 months and after any changes to segmentation controls/methods, confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems, and confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).

Glossary

- AOC: Attestation of Compliance
- ASV: Approved Scanning Vendor
- CCW: Compensating Controls Worksheet
- CDE: Cardholder Data Environment
- CHD: Cardholder Data
- ISA: Internal Security Assessor
- OCIO: Office of Chief Information Office
- P2PE: Point-to-Point Encryption
- PCI DSS: Payment Card Industry Data Security Standard
- PCI SSC: Payment Card Industry Security Standards Council
- POI: Point-of-Interaction
- PTS: PIN Transaction Security
- QSA: Qualified Security Assessor
- SAD: Sensitive Authentication Data
- SAQ: Self-Assessment Questionnaire
- SCR: Secure Card Reader
- TPSP: Third Party Service Provider
- TRA: Targeted Risk Analysis

PCI DSS Requirements and Testing Procedures (page 379-393)

Thank you for attending

- Any questions?
- *The sooner you can submit the SAQ, the sooner they can be reviewed.*