PCI Scope Wizard

Getting Ready Workbook

PCI Security Standards Council®
ASSOCIATE PARTICIPATING ORGANIZATION

datatel
PAYMENT TECHNOLOGIES
(800) 831-6660
sales@datatel-systems.com
www.datatel-systems.com

Set Yourself Up for Success

Before beginning the PCI Scope Wizard, please take a few minutes to collect some information about your credit card collection and handling methods. We recommend gathering all these details before heading back to the PCI Scope Wizard.

The Wizard asks questions about your collection methods to determine which **Self-Assessment Questionnaires** (SAQs) your organization is eligible to complete to achieve PCI compliance.

If you have already collected this information, the process will be quick and easy!

Payment Processor General Information

Step 1. PCI Entity Type

Under PCI guidelines, businesses are either classified as being a Merchant or a Service Provider. This impacts your PCI security responsibilities and the reporting methods that you are eligible for:

- **Merchants:** You accept payment cards only from YOUR OWN CUSTOMERS.
- **Service Providers:** You process, store, transmit, handle or display payment card data in any way FOR OTHER BUSINESSES.

PCI Entity Type Declaration (check one applicable statement only):

☐ **We are considered a merchant.**
☐ **We are considered a service provider.**

Step 2. Name all Payment Processors Used

Name each credit card **Payment Processor** that you use to process credit card transactions:

Processor 1:	**Processor 2:**	**Processor 3:**	**Processor 4:**
Processor Name	Processor Name	Processor Name	Processor Name

Step 3. Total Annual Number of Payment Transactions

Enter the annual total number of all credit card transactions that you process. A close estimate is acceptable:

Total Annual Transactions

For each payment processor(s) that you use, enter the annual number of transactions processed:

Processor 1:	**Processor 2:**	**Processor 3:**	**Processor 4:**
Annual Transactions	Annual Transactions	Annual Transactions	Annual Transactions

Step 4. Electronic Storage of Payment Card data in Merchant Systems

Confirm that you do not store any credit card information electronically in any of the systems or applications that your business directly manages or that operate on infrastructure you directly control:

- **Example 1:** If you store any card information electronically in any applications, systems or infrastructure that your business either manages, hosts or leases, then you are storing cards electronically.
- **Example 2:** If you can retrieve or view the original stored card information, after electronically storing it in any application, whether it was stored encrypted or not, then you are storing cards electronically.
- **Example 3:** If you accept card information electronically by email or fax, whether it was encrypted or not, then you should also report this as storing cards electronically.

Card Data Storage Declaration (check the applicable statements):

☐ **We do not store any card data electronically.**
☐ **We only store card data on a service hosted by a PCI compliant service provider.**
☐ **We store card data using a system that we host or manage ourselves.**

- **Tip:** Include all storage of credit cards that are stored on your own servers, databases, or other electronic systems you directly manage or host. Do not include storage provided by a PCI compliant Service Provider (e.g., a payment processor, gateway, or other token service provider).

Card Present (In-Person) Payments

Step 1. Customer Card Entry in Terminals

List all types of card readers (terminals) that you are using in your business that allow your customers to enter/tap/swipe their own cards in person:

- **Example 1:** if your customers tap or swipe cards in person, using card terminals that are only connected to a payment processor by the internet, this is one payment method
- **Example 2:** if your customers tap or swipe cards in person, using card terminals that are connected to a point-of-sale system, this is another payment method

For any payment methods that you use below – enter the info for each payment processor(s) you use:

Payment Methods	Processor 1	Processor 2	Processor 3	Processor 4
Dial-up terminals Stand-alone terminals that are connected by dial-up telephone to a processor.	Brand/Model	Brand/Model	Brand/Model	Brand/Model
PTS terminals Stand-alone terminals that are connected by internet to a processor. PTS terminals also accept PIN code entry. Do not include terminals that are connected to a POS system.	Brand/Model	Brand/Model	Brand/Model	Brand/Model
POS terminals Integrated terminals that are connected to a POS system to exchange sales data with merchant records, including terminals that are connected to electronic cash drawers or self-serve check-out kiosks. Do not include terminals that are part of a PCI listed P2PE system.	Brand/Model	Brand/Model	Brand/Model	Brand/Model
P2PE systems Secure terminals that are P2PE certified. Contact your vendor to verify your solution is P2PE listed.	Brand/Model	Brand/Model	Brand/Model	Brand/Model
SPoC systems Secure terminals that are SPoC certified and which also use a separate merchant operated mobile device or tablet for PIN code entry. Contact your vendor to verify if your solution is SPoC listed.	Brand/Model	Brand/Model	Brand/Model	Brand/Model
Card Imprinters A mechanical device that takes a carbon paper copy of card.	☐	☐	☐	☐

- **Tip:** For each electronic method used above, state the **card reader Brand and Model**.
- **Tip:** If you're unsure of your terminal types (i.e. if your card reader is a PTS terminal or a POS terminal), contact your terminal vendor. You can also check your merchant agreement to confirm what equipment you purchased or leased.

Step 2. Staff Manual Card Entry in Person

If your staff accept card information physically in person, then list all methods your staff use to enter the card information for a transaction:

- **Example 1:** Your staff might use a virtual terminal (a software app) that was provided by your payment processor, to manually enter the card number for a transaction
- **Example 2:** Your staff might use a hardware terminal (such as POS card reader), to manually enter the card number for a transaction

For any payment methods that you use below – check which payment processor(s) you use with each:

Payment Methods	Processor 1	Processor 2	Processor 3	Processor
Virtual Terminal Software A third-party hosted software application that accepts manual card entry for payment processing. Most commonly this is the merchant terminal application hosted by your payment processor.	Brand	Brand	Brand	Brand
Dial-up terminals Stand-alone terminals that are connected by dial-up telephone to a processor.	Brand/Model	Brand/Model	Brand/Model	Brand/Model
PTS terminals Stand-alone terminals are connected by internet to a processor. PTS terminals also accept PIN code entry. Do not include terminals that are connected to a POS system.	Brand/Model	Brand/Model	Brand/Model	Brand/Model
POS terminals Integrated terminals that are connected to a POS system to exchange sales data with merchant records, including terminals that are connected to electronic cash drawers or self-serve check-out kiosks. Do not include terminals that are part of a PCI listed P2PE system.	Brand/Model	Brand/Model	Brand/Model	Brand/Model
Card Imprinters A mechanical device that takes a carbon paper copy of card.	☐	☐	☐	☐

- **Tip:** Include any cases where staff "physically" enter card details into either a virtual terminal (payment software) or into a hardware terminal (card readers).
- **Tip:** For each electronic method used above, state the **card reader Brand and Model or the virtual terminal vendor,** as may be applicable.

Mail Order & Telephone Order Payments

Step 1. Customer Card Entry in third-party hosted IVR Payments systems

If your customers can directly enter their own card info by phone keypad in IVR Payment applications that are fully hosted by PCI compliant third-party service providers, then check each payment processor(s) you use below:

Payment Methods	Processor 1	Processor 2	Processor 3	Processor 4
IVR Phone Payments Software	☐	☐	☐	☐

(A third-party hosted IVR software application that accepts customer card entry over the phone. Do not Include systems that your business hosts on your infrastructure or on leased cloud infrastructure.)

- **Tip:** If you host your own IVR solution on your own infrastructure, speak to your QSA about the reporting requirements. Treat this as a self-hosted ecommerce solution for this scope evaluation.

Step 2. Staff Manual Card Entry from Phone or Mail Orders

If your staff accept card information verbally over the phone, or by mail, then for any payment methods that your staff use for this below – check each payment processor(s) you use below:

Payment Methods	Processor 1	Processor 2	Processor 3	Processor
Virtual Terminal Software A third-party hosted software application that accepts manual card entry for payment processing. Most commonly, this is the merchant terminal application hosted by your payment processor.	Brand	Brand	Brand	Brand
Dial-up terminals Stand-alone terminals that are connected by dial-up telephone to a processor.	Brand/Model	Brand/Model	Brand/Model	Brand/Model
PTS terminals Stand-alone terminals are connected by internet to a processor. PTS terminals also accept PIN code entry. Do not include terminals that are connected to a POS system.	Brand/Model	Brand/Model	Brand/Model	Brand/Model
POS terminals Integrated terminals that are connected to a POS system to exchange sales data with merchant records, including terminals that are connected to electronic cash drawers or self-serve check-out kiosks. Do not include terminals that are part of a PCI listed P2PE system.	Brand/Model	Brand/Model	Brand/Model	Brand/Model
Card Imprinters (A mechanical device that takes a carbon paper copy of card)	☐	☐	☐	☐

- **Tip:** Include any cases where staff “physically” enter card details into either a virtual terminal (payment software) or into a hardware terminal (card readers).

- **Tip:** For each electronic method used above, state the **card reader Brand and Model or the virtual terminal vendor,** as may be applicable.

Online (Ecommerce / Bill Pay) Payments

Step 1. Customer Card Entry in fully third-party hosted Online Payment Forms

If your customers can directly enter their own card info online in Payment Form applications that are fully hosted by PCI compliant third-party service providers, then check each payment processor(s) you use:

Payment Methods	Processor 1	Processor 2	Processor 3	Processor 4
Hosted Payment Forms	☐	☐	☐	☐

A fully third-party hosted online payment application that accepts customer card entry. Your website may use a redirect URL to link customers to this payment page. Do not include if your business hosts these payment forms or directly transmits card data.

- **Tip:** If you partly host your third -party Payment Form solution, i.e. this means by using Direct Post, Java Script, or an iframe to embed the payment form on your own webpage or shopping cart, then report this as a partly hosted ecommerce solution below in step 2.

Step 2. Customer Card Entry in partly third-party hosted Online Payment Forms

If your customers can directly enter their own card info online in Payment Form applications that is partly hosted by PCI compliant third-party service providers, then check each payment processor(s) you use:

Payment Methods	Processor 1	Processor 2	Processor 3	Processor 4
Partly Hosted Payment Forms	☐	☐	☐	☐

A partly third-party hosted online payment application that accepts customer card entry. Your website may use Direct Post, Java Script, or an iframe to embed the payment form on your own webpage or shopping cart. Do not include if your business hosts these payment forms or directly transmits card data.

- **Tip:** If you self-host your Payment Form solution, i.e. by directly transmitting card information to the payment processor using an API connection to your own webpage, shopping cart, or other applications that you host, then report this as a self-hosted ecommerce solution below in step 3.

Step 3. Customer Card Entry in self-hosted Online Payment Forms

If your customers can directly enter their own card info online in Payment Form applications that are self-hosted, then check each payment processor(s) you use:

Payment Methods	Processor 1	Processor 2	Processor 3	Processor 4
Self-Hosted Payment Forms	☐	☐	☐	☐

A self-hosted online payment application that accepts customer card entry and directly transmits card information to the payment processor using an API connection with your own webpage, shopping cart, or other applications that you host.

- **Tip:** If you are unclear whether your Payment Form solution is self-hosted, i.e., if it is directly integrated into your payment processor, speak to your IT team that manages this solution for you.

LETS START !

About Datatel

At Datatel, we help businesses, organizations, and government agencies modernize and secure how they accept and manage payments, making every transaction faster, safer, and smarter. We empower leaders to make the right decisions with confidence. For over 27 years, healthcare, government, education, utilities, and financial services organizations have trusted us to deliver secure, scalable solutions that improve efficiency and elevate the customer experience.

Payment Modernization

From our beginnings in interactive voice response to today's advanced IVR Payments, WebPay, and Token Migration services, Datatel has consistently helped businesses transform outdated payment processes into modern, automated systems. Our technologies enable organizations to reduce manual work, accelerate revenue collection, and deliver a seamless payment experience across every channel.

Risk & Compliance

As a PCI Level 1 Service Provider and a PCI SSC Associate Participating Organization, we are deeply committed to protecting our customers' payment ecosystems. Our solutions are designed to de-risk how organizations handle sensitive cardholder data ensuring they not only meet PCI DSS requirements but also reduce exposure to security, legal, and financial risks. With Datatel, compliance is not just a checkbox it's built into the way payments are processed and protected.

Advisory & Insights

Beyond technology, we provide the insights and expertise leaders need to make confident decisions about their payment operations. From PCI advisory services to Payment Flow Analysis, we equip organizations with the intelligence to align payment security with broader business goals, helping them stay agile, profitable, and future-ready.

Our Commitment

Datatel's success comes from investing in people, partnerships, and innovation. We believe in building technology that strengthens businesses and supporting communities that shape our shared future. Through initiatives like our work with Covenant House and Businesses GiveBack, we contribute to creating brighter opportunities for the most vulnerable members of society.

At Datatel, we're more than a payment technology provider. We are a partner in modernization, compliance, and long-term growth.

Contact Us – We're Here to Help

800-831-6660
www.datatel-systems.com
sales@datatel-systems.com

PCI Scope Wizard

datatel PAYMENT TECHNOLOGIES