

What Is PCI DSS Compliance?



John Elliott

PAYMENTS, SECURITY, PRIVACY AND RISK SPECIALIST

@withoutfire www.withoutfire.com



Card Brand / Card Scheme

One of the five card companies that established the PCI Security Standards Council

American
Express



Discover



JCB

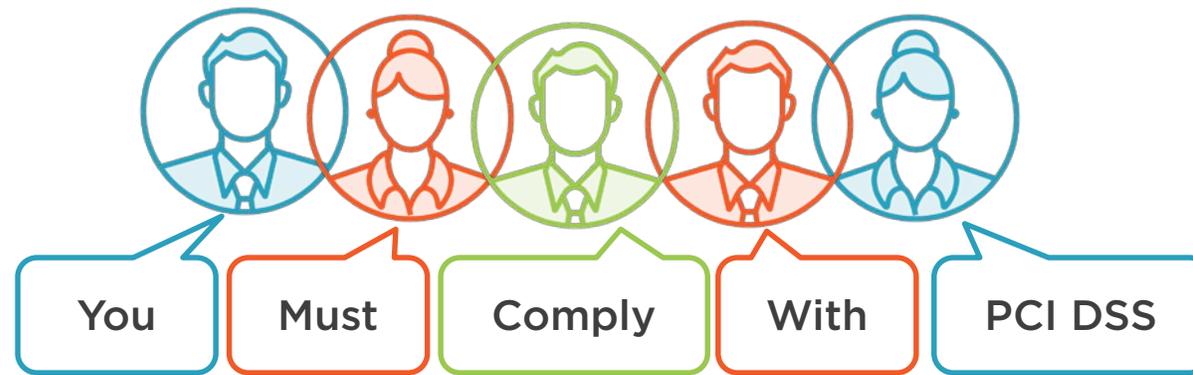


Mastercard



Visa





Compliance with the PCI standards is (generally) not a legal requirement

Because someone asked them to!

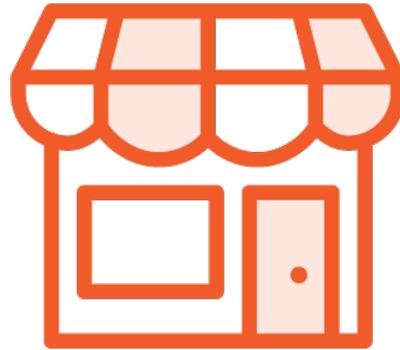
So why do organizations have to comply?

Who Can Be Compliant?

Organizations that store, process, or transmit cardholder data



**Financial institutions
(Banks)**



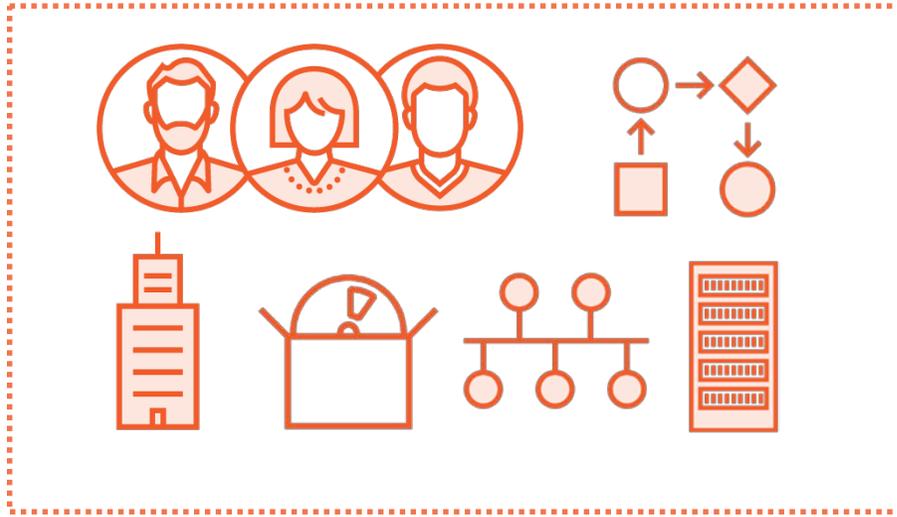
Merchants



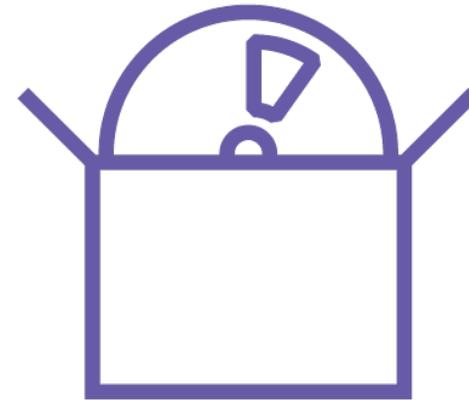
**Service
providers**



Things Can't Be Compliant, Only Organizations



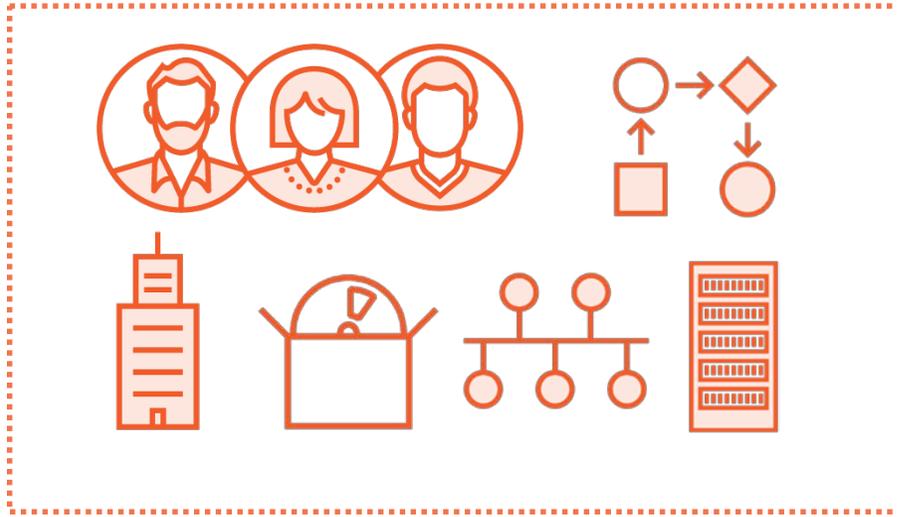
Organization ✓



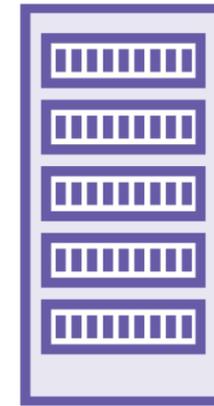
Software ✗



Things Can't Be Compliant, Only Organizations



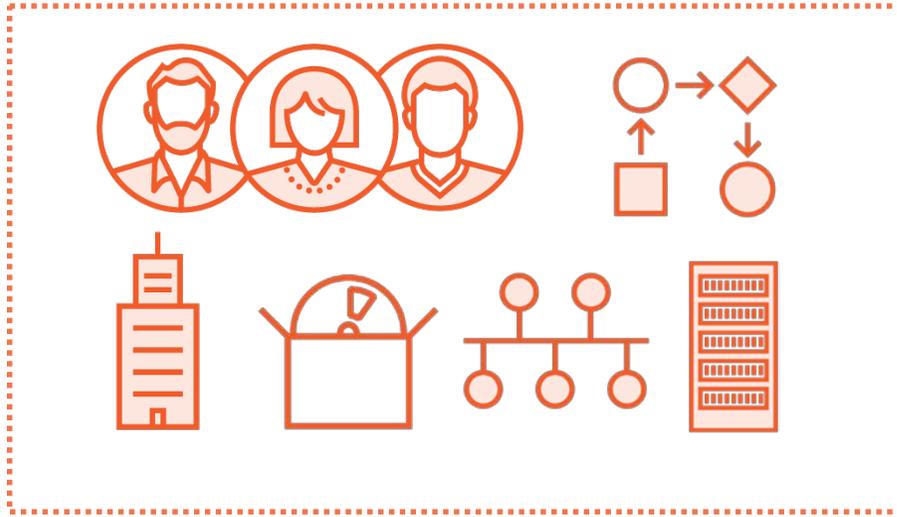
 **Organization** ✓



Software ✗
Hardware ✗



Things Can't Be Compliant, Only Organizations



   **Organization** ✓



Software ✗
Hardware ✗
People ✗



When You Need to Be PCI Compliant



Who is asking you to comply with PCI DSS



Why are they asking you to comply?



How do they want you to validate that you are compliant



How to Validate Compliance



External audit

Report On Compliance (RoC)



Self assessment

**Self Assessment
Questionnaire (SAQ)**



If You're a Merchant

Who?



Acquiring bank / merchant bank

Why?



It is part of your acquiring contract

How?



>6 million

Depends on how many transactions



<6 million



If You're a Merchant

Who?



AMEX
Discover

Why?



It is part of your
acquiring contract

How?



>6 million

Depends on how
many transactions



<6 million



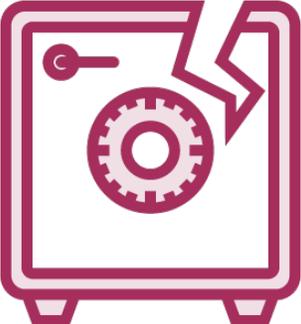
If You're a Merchant

Who?



All schemes

Why?



You've suffered a data breach

How?

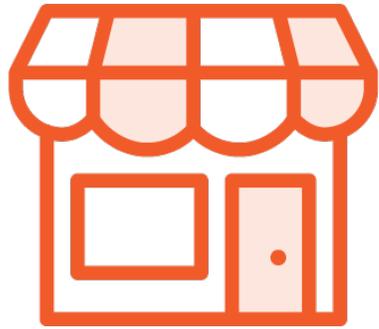


Report on compliance



If You're a Service Provider

Who?



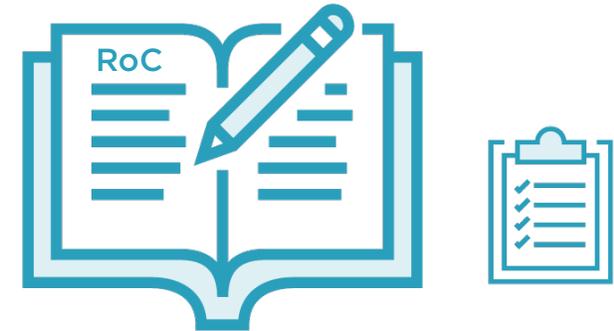
Your customer
(typically a merchant)

Why?



Usually contractual
Merchant has to be
compliant, so do all its
service providers

How?



Depends on how many
transactions and
contract negotiations



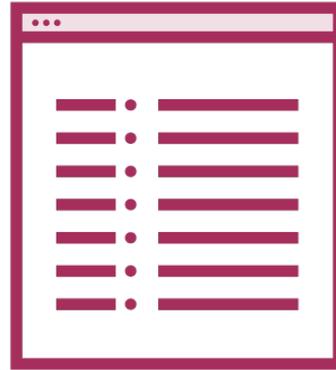
If You're a Service Provider

Who?



Card brands

Why?



You want to appear on
the card brand's
'approved' list

How?



Report on Compliance



If You're a Service Provider

Who?



Financial Institution:
Card issuer or acquirer

Why?



Their contract with the
card brands requires
all service providers to
be compliant

How?



Report on Compliance



Compliance Documents



**Report on Compliance
(RoC)**



**Self assessment Questionnaires
(SAQ)**



Validate a Requirement Is In-place

Requirement

6.4.3 Production data (live PANs) are not used for testing or development



RoCs and SAQs validate that a **requirement** is in place by confirming the **testing procedure** happened



Testing Procedure

- a) Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development
- b) Examine a sample of test data to verify production data (live PANs) is not used for testing or development



PCI Roles (Qualifications)



Qualified Security Assessor (QSA)



Internal Security Assessor (ISA)



*Depends on brand



PCI Professional (PCIP)



Who Can Complete an SAQ?



QSA



ISA



PCIP



Company CEO



Terry the Janitor



Sally the DBA



RoCs and SAQs: The Documents



PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.3 Production data (live PANs) are not used for testing or development.			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	Identify the responsible personnel interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development.	<Report Findings Here>					
6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	Describe how a sample of test data was examined to verify production data (live PANs) is not used for testing.	<Report Findings Here>					



PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.3 Production data (live PANs) are not used for testing or development.			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	Identify the responsible personnel interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development.	<Report Findings Here>					
6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	Describe how a sample of test data was examined to verify production data (live PANs) is not used for testing.	<Report Findings Here>					



PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.3 Production data (live PANs) are not used for testing or development.			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	Identify the responsible personnel interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development.	<Report Findings Here>					
6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	Describe how a sample of test data was examined to verify production data (live PANs) is not used for testing.	<Report Findings Here>					



PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.3 Production data (live PANs) are not used for testing or development.			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	Identify the responsible personnel interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development.	<Report Findings Here>					
6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	Describe how a sample of test data was examined to verify production data (live PANs) is not used for testing.	<Report Findings Here>					



PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
6.4.3 Production data (live PANs) are not used for testing or development.			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	Identify the responsible personnel interviewed who confirm that procedures are in place to ensure production data (live PANs) are not used for testing or development.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for testing.	<Report Findings Here>					
	Describe how testing processes were observed to verify procedures are in place to ensure production data (live PANs) are not used for development.	<Report Findings Here>					
6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	Describe how a sample of test data was examined to verify production data (live PANs) is not used for testing.	<Report Findings Here>					



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.4.2	Is there separation of duties between personnel assigned to the development/test environments and those assigned to the production environment?	<ul style="list-style-type: none"> ▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3	Are production data (live PANs) <i>not</i> used for testing or development?	<ul style="list-style-type: none"> ▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel ▪ Examine test data 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4	Are test data and accounts removed from system components before the system becomes active / goes into production?	<ul style="list-style-type: none"> ▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel ▪ Examine production systems 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.4.2	Is there separation of duties between personnel assigned to the development/test environments and those assigned to the production environment?	<ul style="list-style-type: none"> ▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3	Are production data (live PANs) <i>not</i> used for testing or development?	<ul style="list-style-type: none"> ▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel ▪ Examine test data 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4	Are test data and accounts removed from system components before the system becomes active / goes into production?	<ul style="list-style-type: none"> ▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel ▪ Examine production systems 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.4.2	Is there separation of duties between personnel assigned to the development/test environments and those assigned to the production environment?	<ul style="list-style-type: none"> ▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3	Are production data (live PANs) <i>not</i> used for testing or development?	<ul style="list-style-type: none"> ▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel ▪ Examine test data 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4	Are test data and accounts removed from system components before the system becomes active / goes into production?	<ul style="list-style-type: none"> ▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel ▪ Examine production systems 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.4.2	Is there separation of duties between personnel assigned to the development/test environments and those assigned to the production environment?	<ul style="list-style-type: none"> ▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3	Are production data (live PANs) <i>not</i> used for testing or development?	<ul style="list-style-type: none"> ▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel ▪ Examine test data 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4	Are test data and accounts removed from system components before the system becomes active / goes into production?	<ul style="list-style-type: none"> ▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel ▪ Examine production systems 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



When Can an SAQ be Used?

Allowed by compliance
program based on number of
transactions
(Typically <6 million)

How you accept transactions
(Meet the technical
eligibility criteria)



There Are Eight SAQs

Name	Number of requirements	Used for:		
		F2F	MOTO	E-Com
SAQ A	10	Y	Y	Y
SAQ A-EP	89	-	-	Y
SAQ B	43	Y	-	-
SAQ B-IP	77	Y	-	-
SAQ P2PE	56	Y	-	-
SAQ C	43	Y	Y	-
SAQ C-VT	56	-	Y	-
SAQ D	280+	Y	Y	Y



Understanding the SAQs for PCI DSS version 3

The PCI DSS self-assessment questionnaires (SAQs) are validation tools intended to assist merchants and service providers report the results of their PCI DSS self-assessment. The different SAQ types are shown in the table below to help you identify which SAQ best applies to your organization. Detailed descriptions for each SAQ are provided within the applicable SAQ.

Note: Entities should ensure they meet all the requirements for a particular SAQ before using the SAQ. Merchants are encouraged to contact their merchant bank (acquirer) or the applicable payment brand(s) to identify the appropriate SAQ based on their eligibility.

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. <i>Not applicable to face-to-face channels.</i>
A-EP*	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. <i>Applicable only to e-commerce channels.</i>
B	Merchants using only: <input type="checkbox"/> Imprint machines with no electronic cardholder data storage; and/or <input type="checkbox"/> Standalone, dial-out terminals with no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
B-IP*	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.

There's a useful document to help you find applicable SAQs

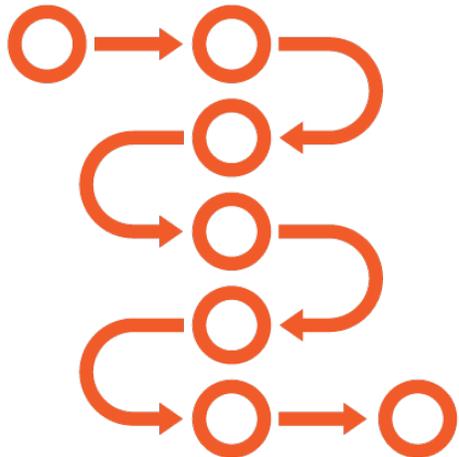
https://www.pcisecuritystandards.org/documents/Understanding_SAQs_PCI_DSS_v3.pdf

SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.

* New for PCI DSS v3.0



Prioritized Approach



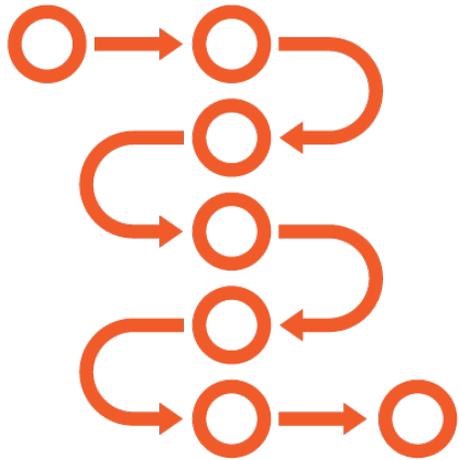
All PCI DSS requirements are divided into one of six milestones

Requirements in milestone one reduce most risk

Risk-based approach to becoming compliant



Prioritized Approach Milestones



Milestone 1

Remove sensitive authentication data and limit data retention

Milestone 2

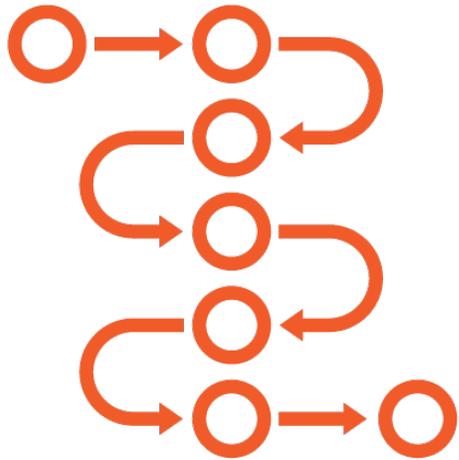
Protect systems and networks, and be prepared to respond to a system breach

Milestone 3

Secure payment card applications



Prioritized Approach Milestones



Milestone 4

Monitor and control access to your systems

Milestone 5

Protect stored cardholder data

Milestone 6

Finalize remaining compliance efforts, and ensure all controls are in place



Prioritized approach document shows which requirements fall into each milestone

https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf

ment to the Internet.	2
1.3.5 Permit only "established" connections into the network.	2





Prioritized Approach Tool (PAT)

Excel spreadsheet

Tracking compliance

Reporting compliance status

https://www.pcisecuritystandards.org/documents/Prioritized-Approach-v3_2.xlsx

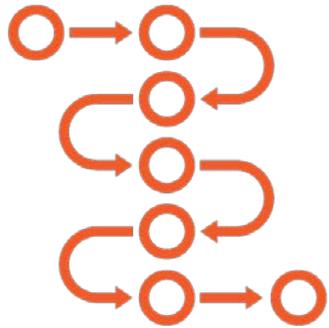


DEMO Placeholder
Using the Prioritized Approach
Spreadsheet Tool



Compliance Lifecycle

Prioritized Approach



Assessment



RoC or SAQ

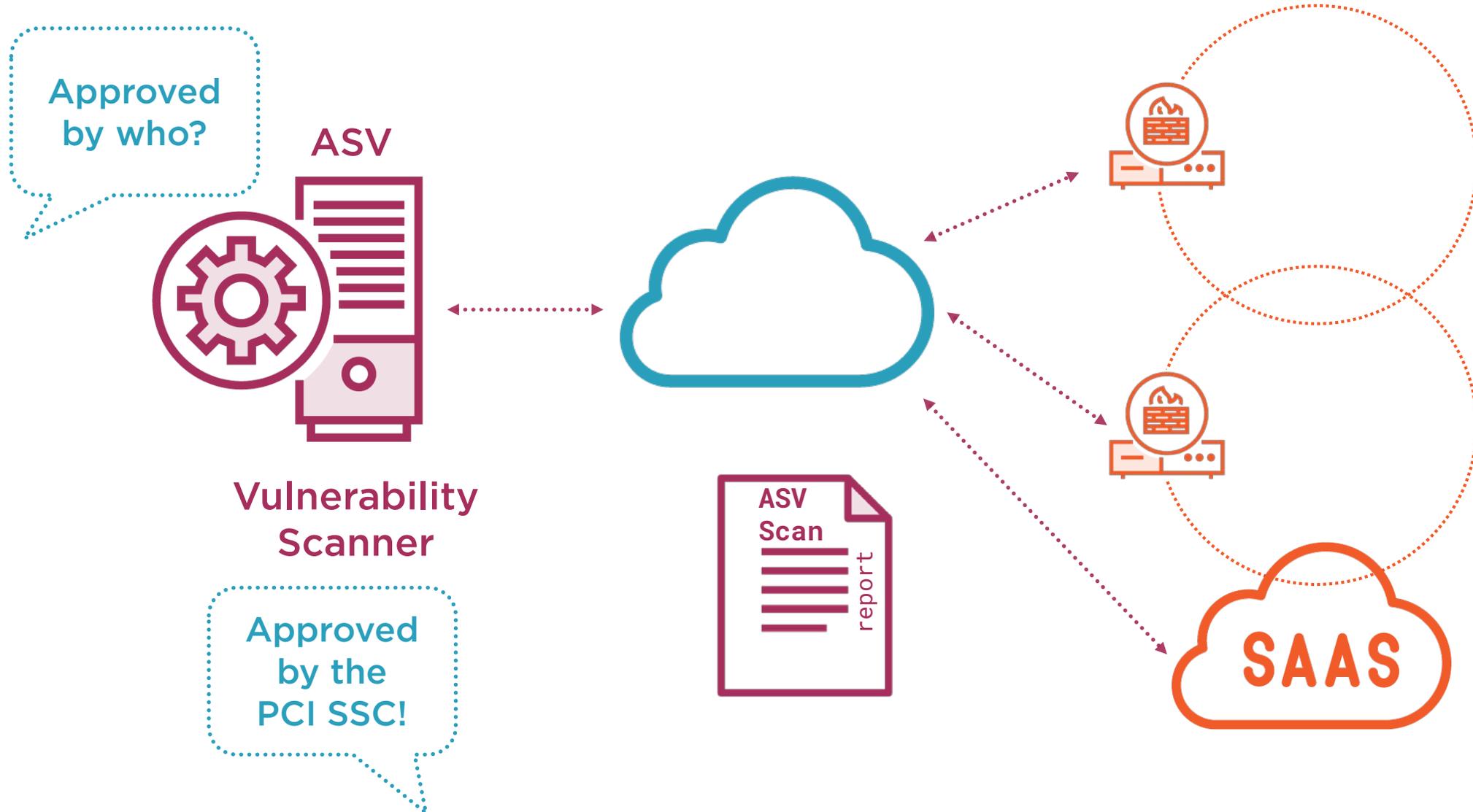


Continuous compliance

Assessment every  12 months



Approved Scanning Vendor (ASV) Scans



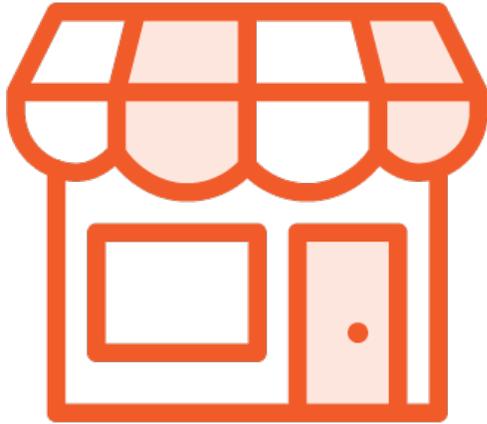


A quarterly ASV scan is also a PCI DSS requirement

11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved



Not Compliant: Merchant



In breach of contract

- Could receive monetary penalties
- Could be “turned off”
- Could pay higher charges

Automatically “at fault” in the event of a breach of cardholder data



Not Compliant: Service Provider



Merchants might not want to use you

You can't be listed as compliant by the card brands (Visa, Mastercard)



What if You Can't Comply?



PCI DSS
The Standard



PCI DSS
The Compliance Program



When You Need to Be PCI Compliant



Who is asking you to
comply with PCI DSS



Why are they asking
you to comply?



How do they want you
to validate that you
are compliant



When You Can't Comply



Who is asking you to
comply with PCI DSS

Explain why you can't comply

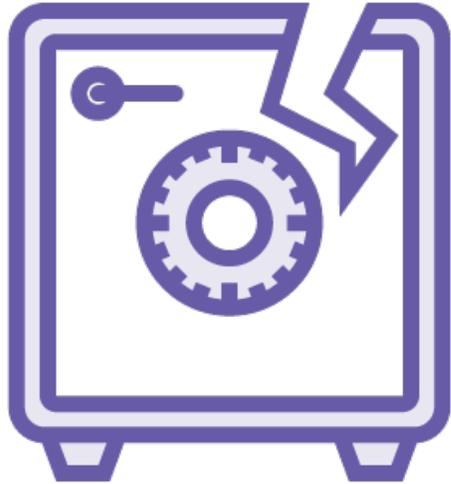
Describe your path to compliance

Quantify the risk of non-compliance

Get their written agreement



Data Breach



Don't panic

Tell your acquiring bank / card scheme

Formal PCI Forensic Investigator (PFI)

- Breach closed
- Window of compromise
- What happened?

There may be penalties



Summary



Compliance is generally a contractual requirement

You can validate you are compliant with a RoC or an SAQ

Each card brand has its own rules

- Mostly based on number of transactions

A QSA, ISA or PCIP can help you

Compliance questions follow contracts

