

What Does Compliance Mean?



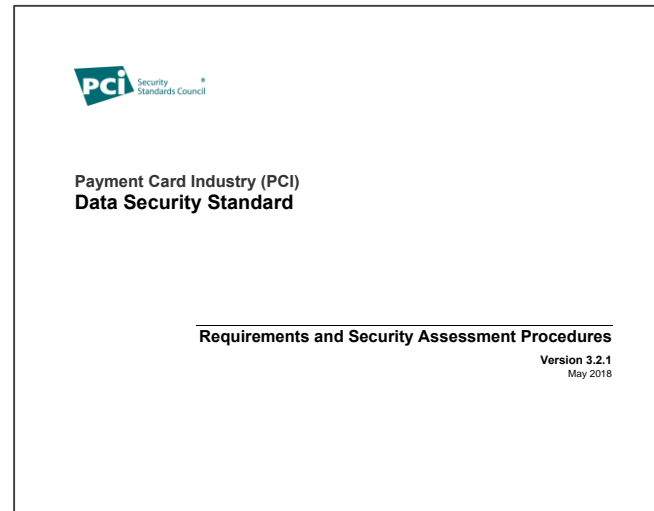
John Elliott

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

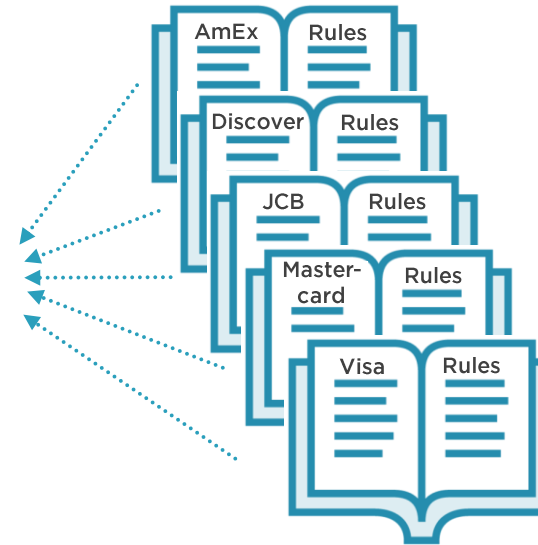
@withoutfire www.withoutfire.com



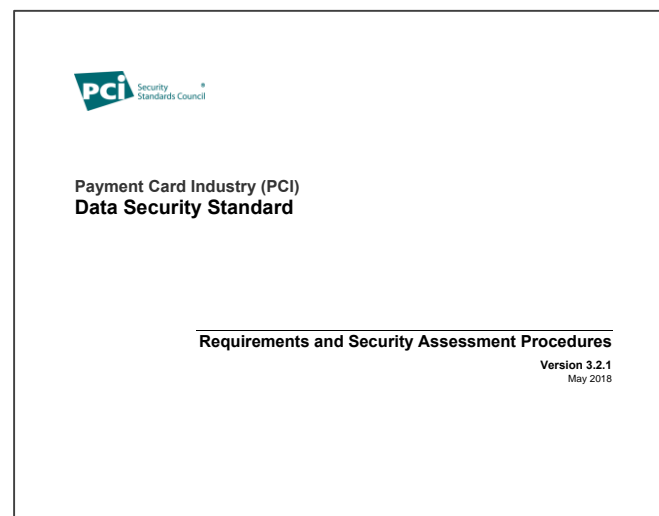
I see a data
security
standard



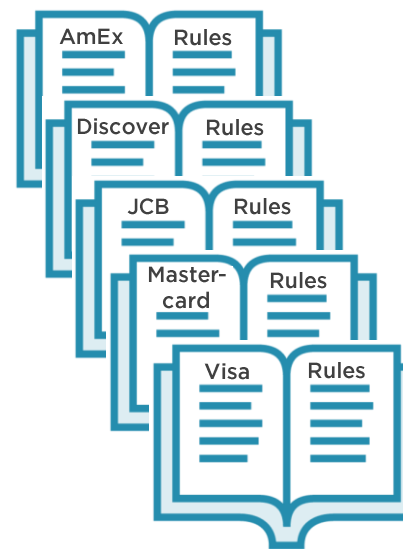
I see card brand rules
that each define
compliance with a data
security standard



I see a data
security
standard



I see card
brand rules



Questions to Ask



What does the end look like?

Why be compliant?

How will you validate compliance?



“If you don't know where you are going, you will probably end up somewhere else.”

Yogi Berra



Determining Constraints



1. What type of assessment?
 2. Who you need to give it to?
 3. A rough timetable
- (There isn't really a finish line, because the PCI DSS race never ends)

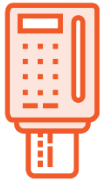


“Focus on security, not compliance”

Everyone I've ever met at a card brand, the PCI SSC and acquirers



Acceptance Channels



Face-to-face retail



e-Commerce



Mail Order / Telephone Order (MOTO)



How to Validate Compliance



On-site assessment

Report on Compliance (RoC)



Self assessment

**Self Assessment
Questionnaire (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



RoCs and SAQs



Report on Compliance

Completed by independent assessor

Assessor collects evidence that the requirement is “in place” by following defined testing procedures

6.4.3 Production data (live PANs) are not used for testing or development	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.
	6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.

All 300 requirements

Not Free



Self-assessment Questionnaire

Completed by the organization

Answer yes/no questions

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.4.3	Are production data (live PANs) not used for testing or development?	<input type="checkbox"/> Review change control processes and procedures. <input type="checkbox"/> Observe processes. <input type="checkbox"/> Interview personnel. <input type="checkbox"/> Examine test data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cut-down requirements based on methods of acceptance

Free



RoCs and SAQs



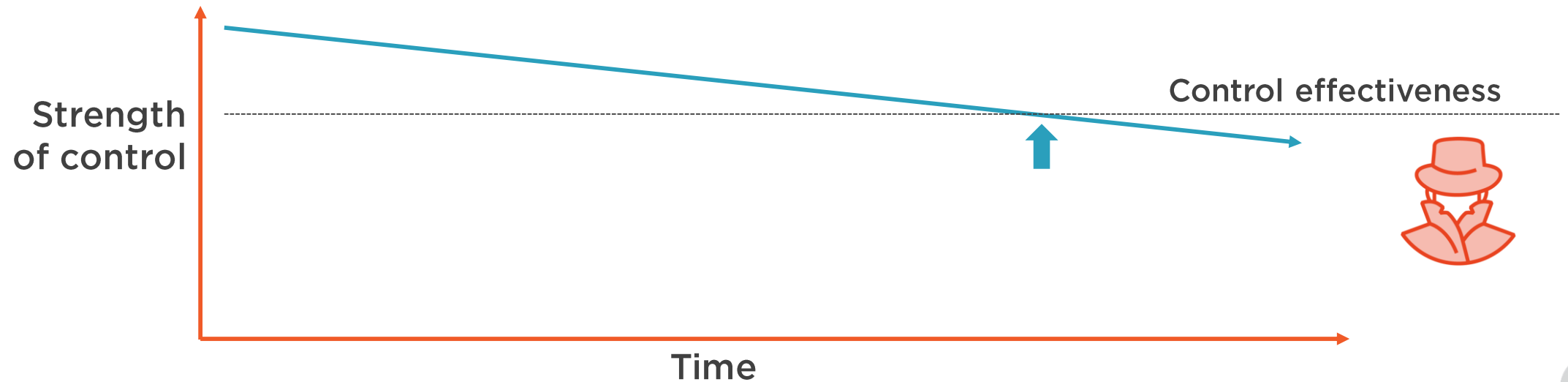
Report on Compliance

Can provide an independent assessment of the state of all 300 PCI DSS requirements



Self-assessment Questionnaire

Does not



RoCs and SAQs



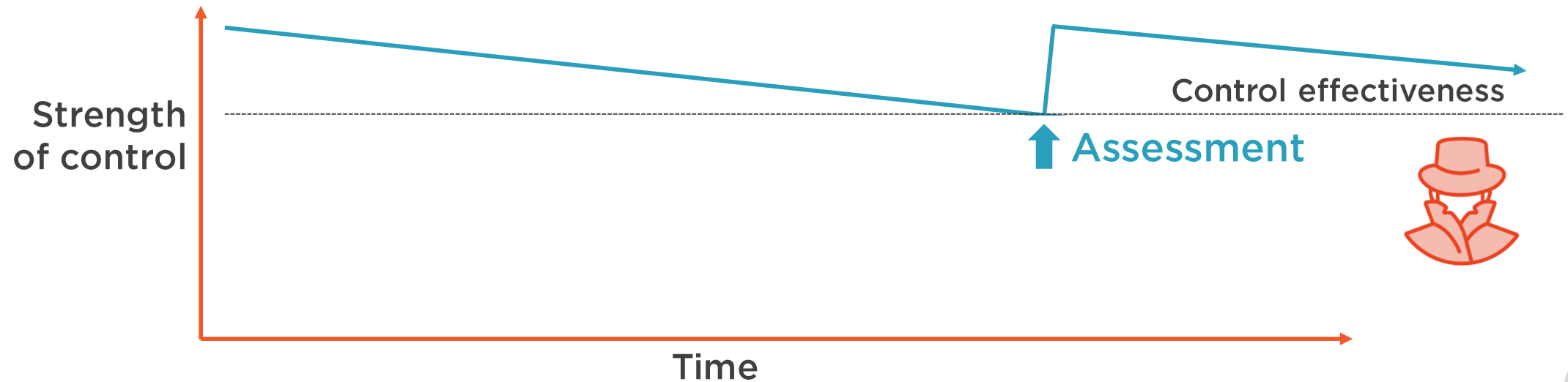
Report on Compliance

Can provide an independent assessment of the state of all 300 PCI DSS requirements



Self-assessment Questionnaire

Does not



PCI Roles (Qualifications)



Qualified Security
Assessor (QSA)

✓ RoC



Internal Security
Assessor (ISA)

✓ RoC*

*Depends on brand



PCI Professional
(PCIP)

✗ RoC



Who Can Complete an SAQ?



QSA



ISA



PCIP



Company CEO



Kevin the Janitor



Meghan the DBA





One

Report on Compliance



Eight

Self-assessment Questionnaires



SAQ
A

Card not present only

All payment processing outsourced

No electronic cardholder data anywhere

Some technical controls

Contracts with third parties



SAQ
A-EP

Partially outsourced electronic commerce

Where a compromise of the webserver can affect the security of the transaction

- Magecart

Controls around the webserver

Third-parties



SAQ B



Dial-up payment terminals

- Includes mobile 3G/4G

No other electronic processing

Less common



SAQ

B-IP



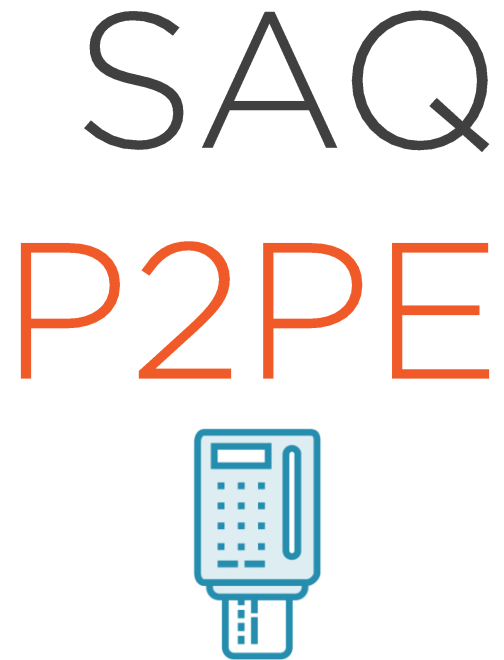
Internet (IP) connected payment terminals (POIs)

- POIs must be listed on the PCI SSC website

Not connected to any other systems

No electronic storage or receipt of cardholder data





Uses validated Point-to-point encryption solutions

- Listed on the PCI SSC website

F2F or MOTO

No electronic storage or receipt of cardholder data



SAQ
C

Payment systems – typically POS, cash registers etc, IP connection to payment processing

No electronic storage of cardholder data

Typically Face-to-face

- Could also be MOTO
- Never e-commerce



SAQ
C-VT

Virtual payment terminals

- Typically web browser connected to a payment processor website

MOTO

No storage of cardholder data

No electronic receipt of cardholder data



SAQ
D

Everything else

Same requirements as full RoC



There Are Eight SAQs

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



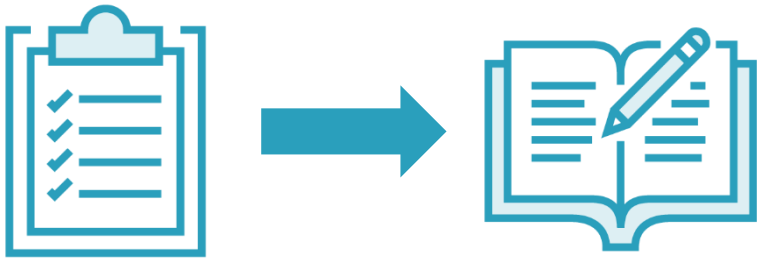
Multiple SAQs



It is possible for a merchant to use multiple SAQs if their payment channels are separate



SAQ to RoC



If an environment meets the eligibility criteria for a SAQ, the assessor can use the SAQ as the basis of an assessment

PCI SSC FAQ 1331



Critical Questions

Who

Why?

What authority?

So what ...?

How?
(SAQ or RoC)

By when ...?



Who Is Asking?

Acquirer or Brand
(You are a Merchant)

Merchant
(Service Provider)

Card Brand
(Financial Institution)

Financial Institution
(Service Provider)

**The Law or
Other Regulation**



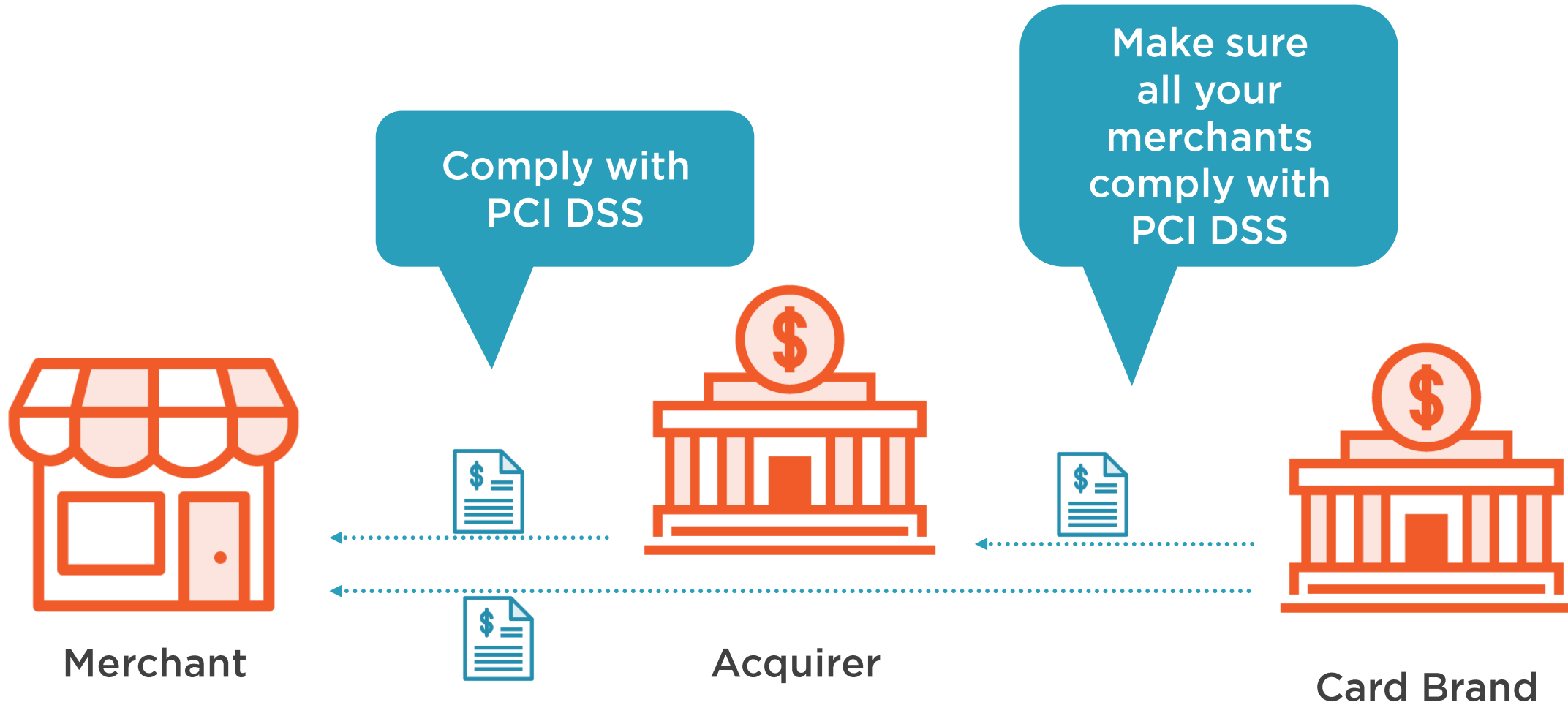


Contracts

PCI DSS Compliance is generally contractual



Merchant

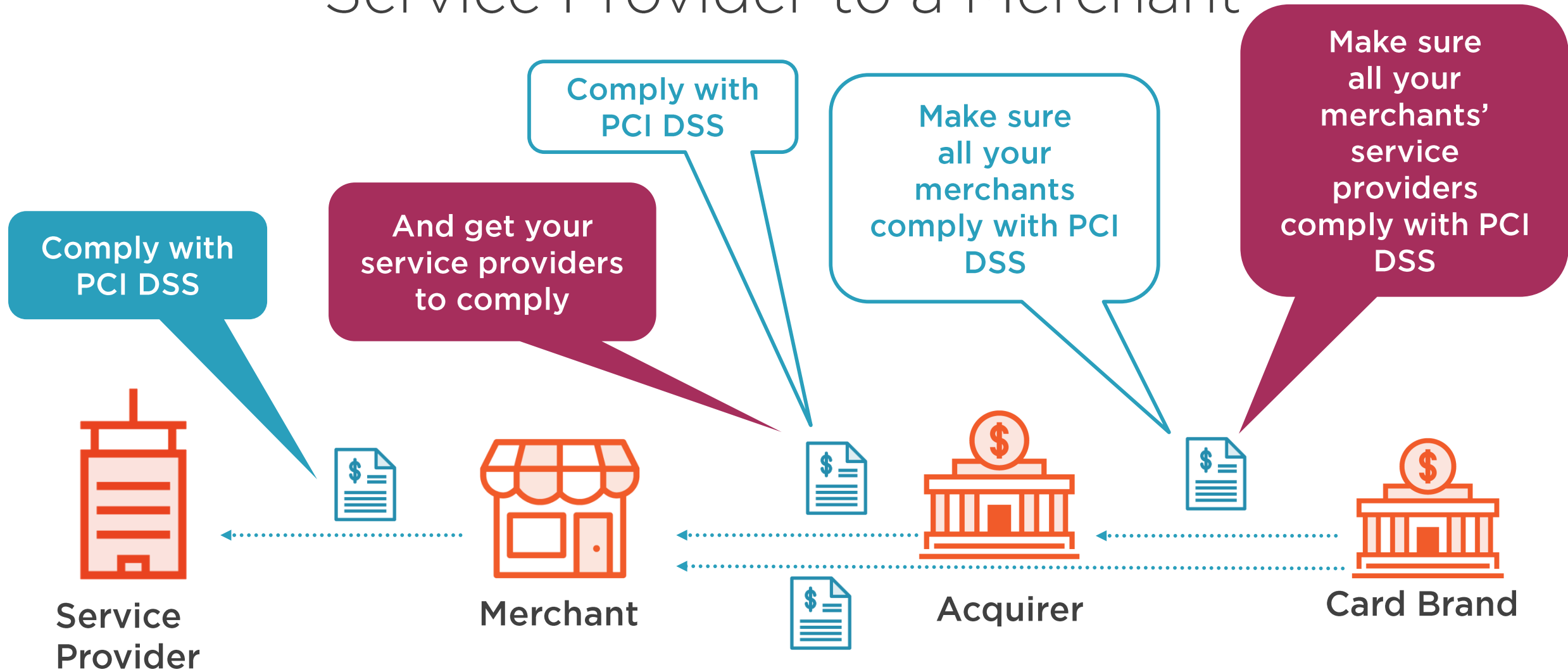


Merchant Compliance

Who is asking?	Acquirer (or Card Brand)
Why?	Card brand contract
Their authority?	Merchant's contract to accept cards
If you don't ...	Varies. Can be penalties. Theoretically can stop acceptance
Evidence	Depends on merchant size and which Card Brand. L1 > 6 million, L2 > 1 million : RoC L3, L4 - SAQ
Deadline	Usually 12 months (unless there's been a data compromise)
Can you negotiate?	Yes. Lots.



Service Provider to a Merchant

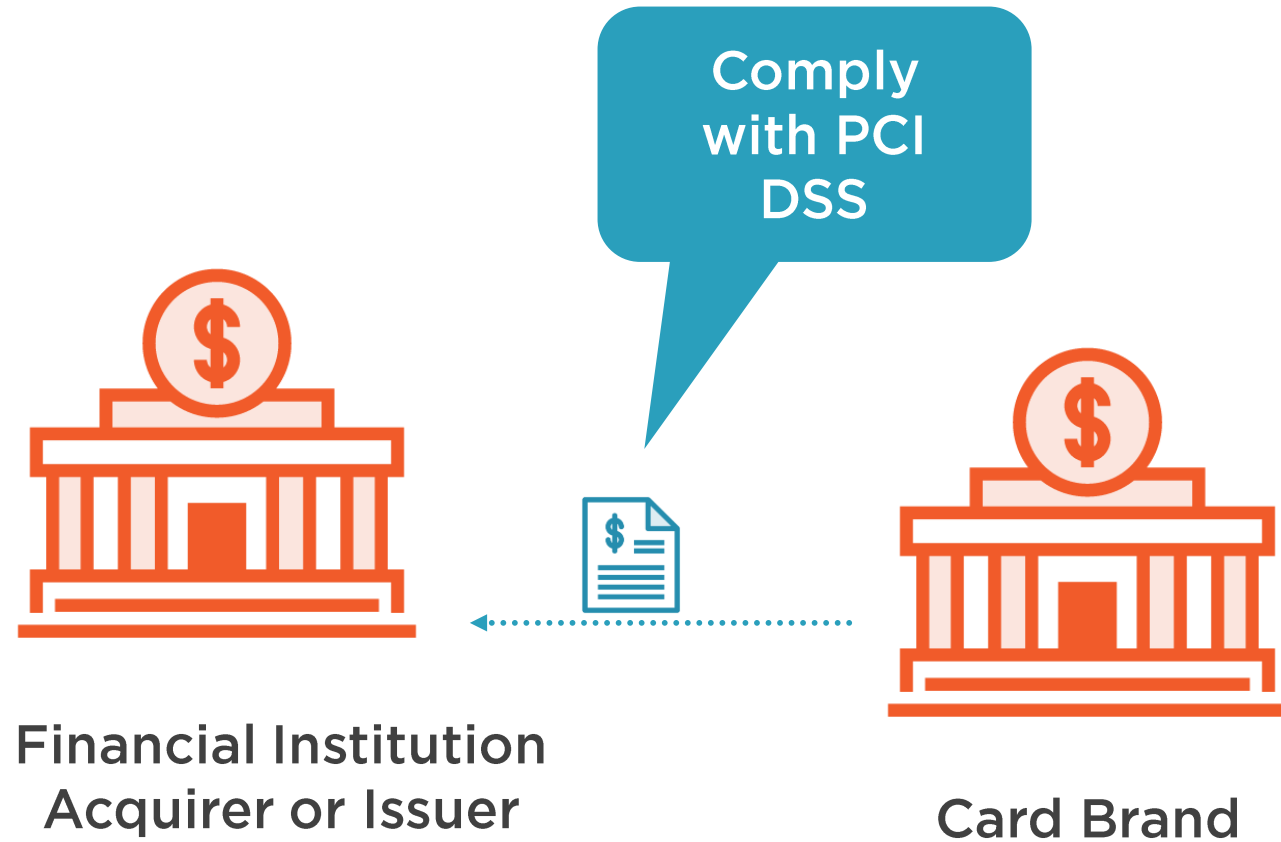


Service Provider to Merchant

Who is asking?	Merchant
Why?	Acquiring contract
Their authority?	Contract
If you don't ...	Limited
Evidence	Merchants want on-site assessment, may accept SAQ
Deadline	Merchant-dependent
Can you negotiate?	Yes. Lots. At the end of the day it is a risk decision for the merchant.



Financial Institution

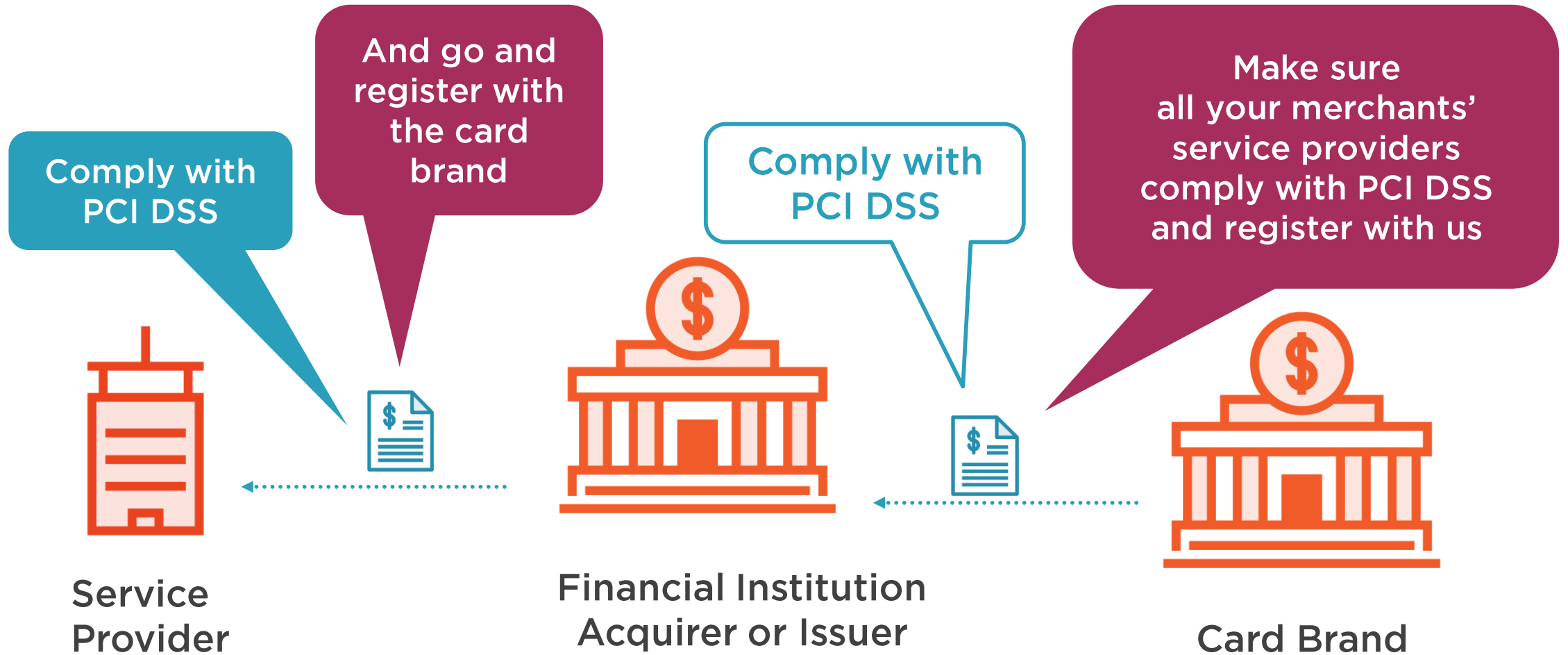


Financial Institution

Who is asking?	Card Brand
Why?	Card brand contract
Their authority?	Contract to acquirer or issue cards
If you don't ...	Can be penalties (if caught)
Evidence	None
Deadline	No. On signing the contract
Can you negotiate?	No



Service Provider to a Financial Institution



Service Provider to Financial Institution

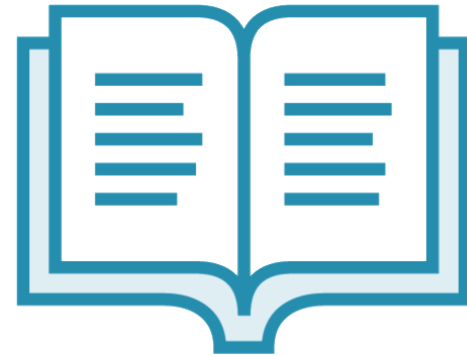
Who is asking?	Acquirer or issuer
Why?	Acquiring or issuing contract
Their authority?	Contract with SP
If you don't ...	They will struggle - card brands really enforce this
Evidence	L1 > 300K transactions - RoC L2 < 300K transactions - SAQ
Deadline	Depends - often 12 months
Can you negotiate?	Less so because ultimately you're negotiating with the card brand



Merchant



Merchant



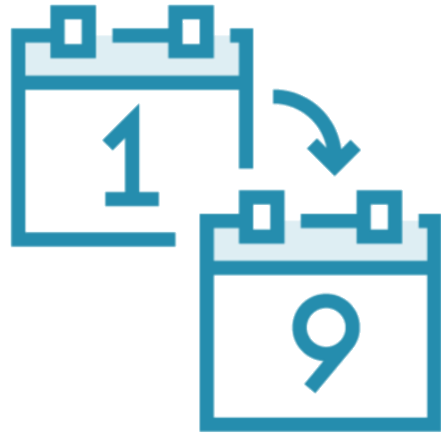
Law or Rules

Merchant

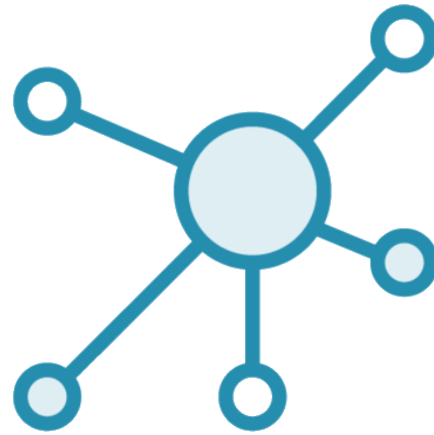
Who is asking?	No one
Why?	-
Their authority?	-
If you don't ...	-
Evidence	-
Deadline	-
Can you negotiate?	-



Negotiation



1. Time



2. Scope



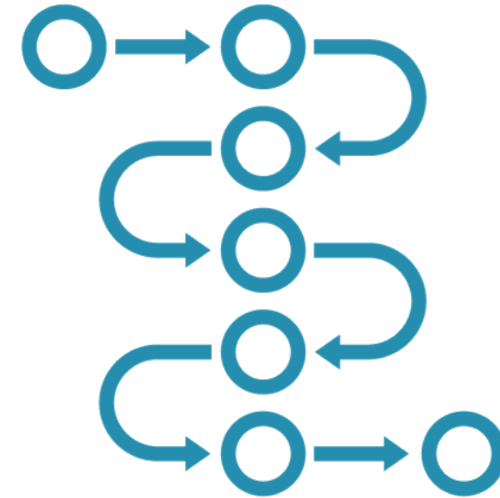
3. How



Not Just RoCs and SAQs



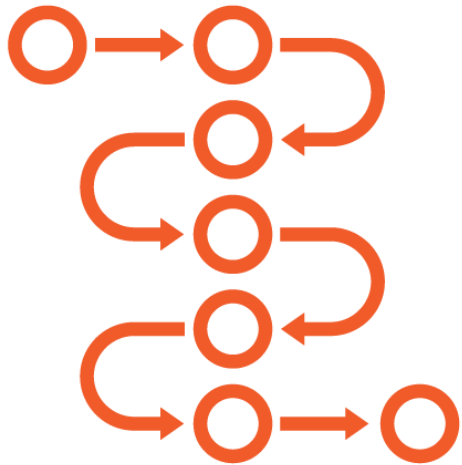
Project Plan



Prioritized Approach



Prioritized Approach



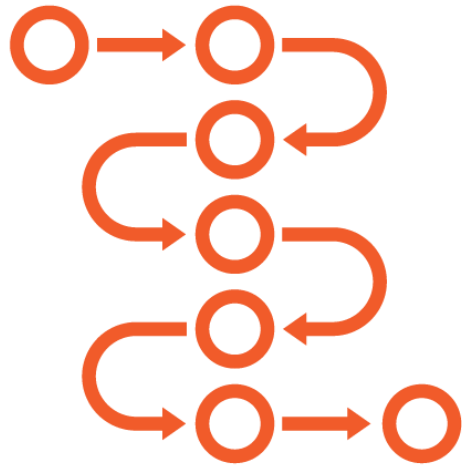
All PCI DSS requirements are divided into one of six milestones

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

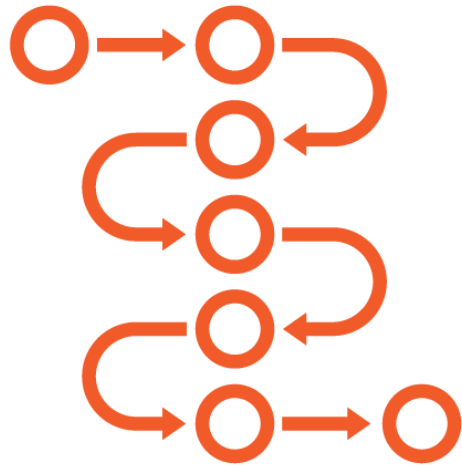
Protect systems and networks, and be prepared to respond to a system breach

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



PCI DSS Requirements v3.2	Milestone					
	1	2	3	4	5	6
Requirement 1: Install and maintain a firewall configuration to protect cardholder data						
1.1 Establish and implement firewall and router configuration standards that include the following:						
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations						6
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1					
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	1					
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone		2				
1.1.5 Description of groups, roles, and responsibilities for management of network components						6
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.		2				
1.1.7 Requirement to review firewall and router rule sets at least every six months						6
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.						
<i>Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.</i>						
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.		2				
1.2.2 Secure and synchronize router configuration files.		2				
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.		2				
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.						

Prioritized approach document shows which requirements fall into each milestone

https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2_1.pdf

1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	2
1.3.5 Permit only "established" connections into the network.	2



Negotiation



Sometimes PCI DSS is not cost-logical

In the meantime accept the risk of a compromise from this environment

Perhaps meet prioritized approach milestones 1 and 2?

Provide plan and status reports

Stick to project, be realistic





You are not the PCI Police

- Not everything is objective

Talk with whoever is asking you to comply with PCI DSS

Be secure first

- Compliant second



Next: The Compliance Journey

