PCI Compliance, Qualified Professionals, and Programs

John Elliott
Payments, Security, Privacy and Risk Specialist | PCIP

@withoutfire

Coming Up

Why comply with any of the PCI standards?

Who to get to help

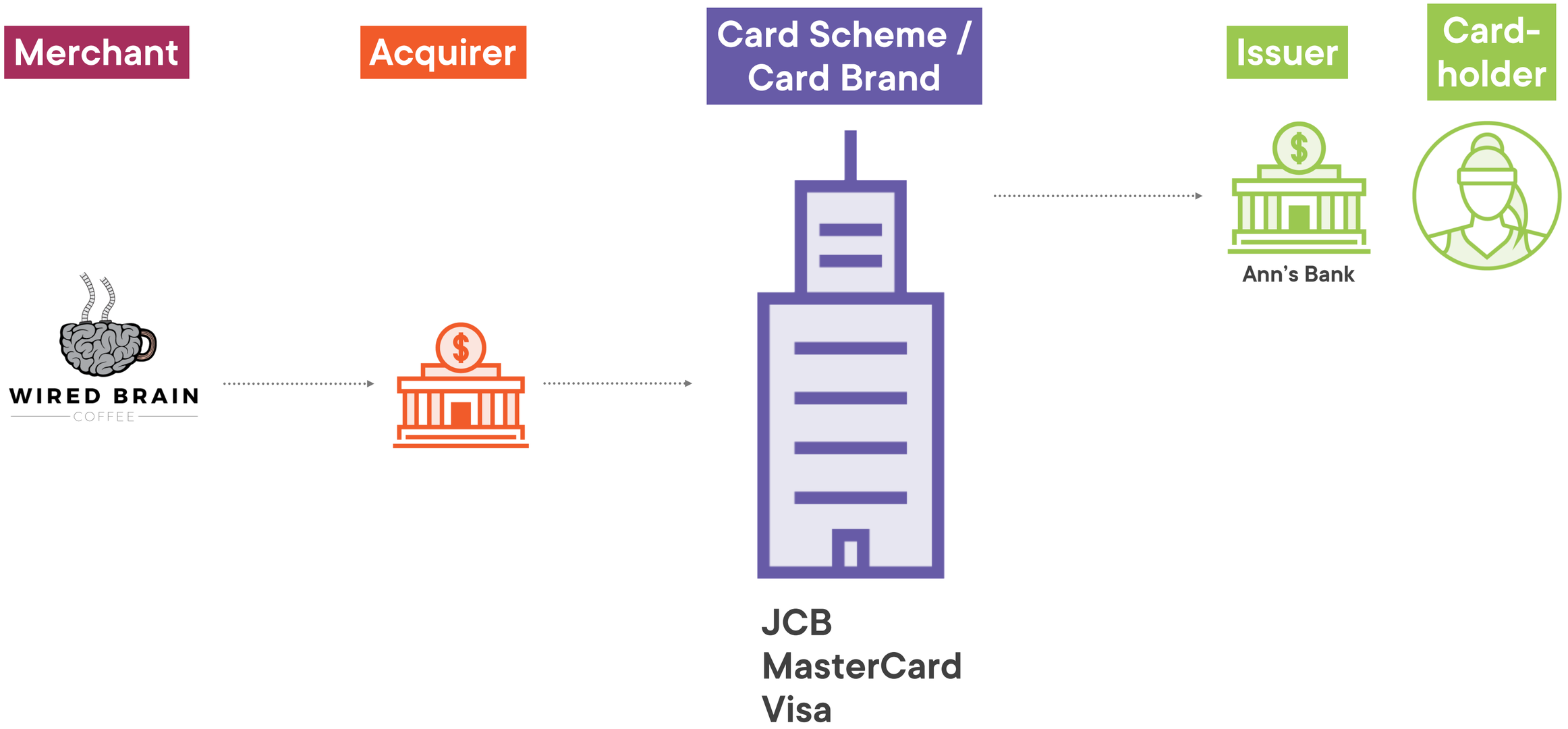
What the card schemes do, what acquirers do, and what the SSC does

PCI programs and qualifications

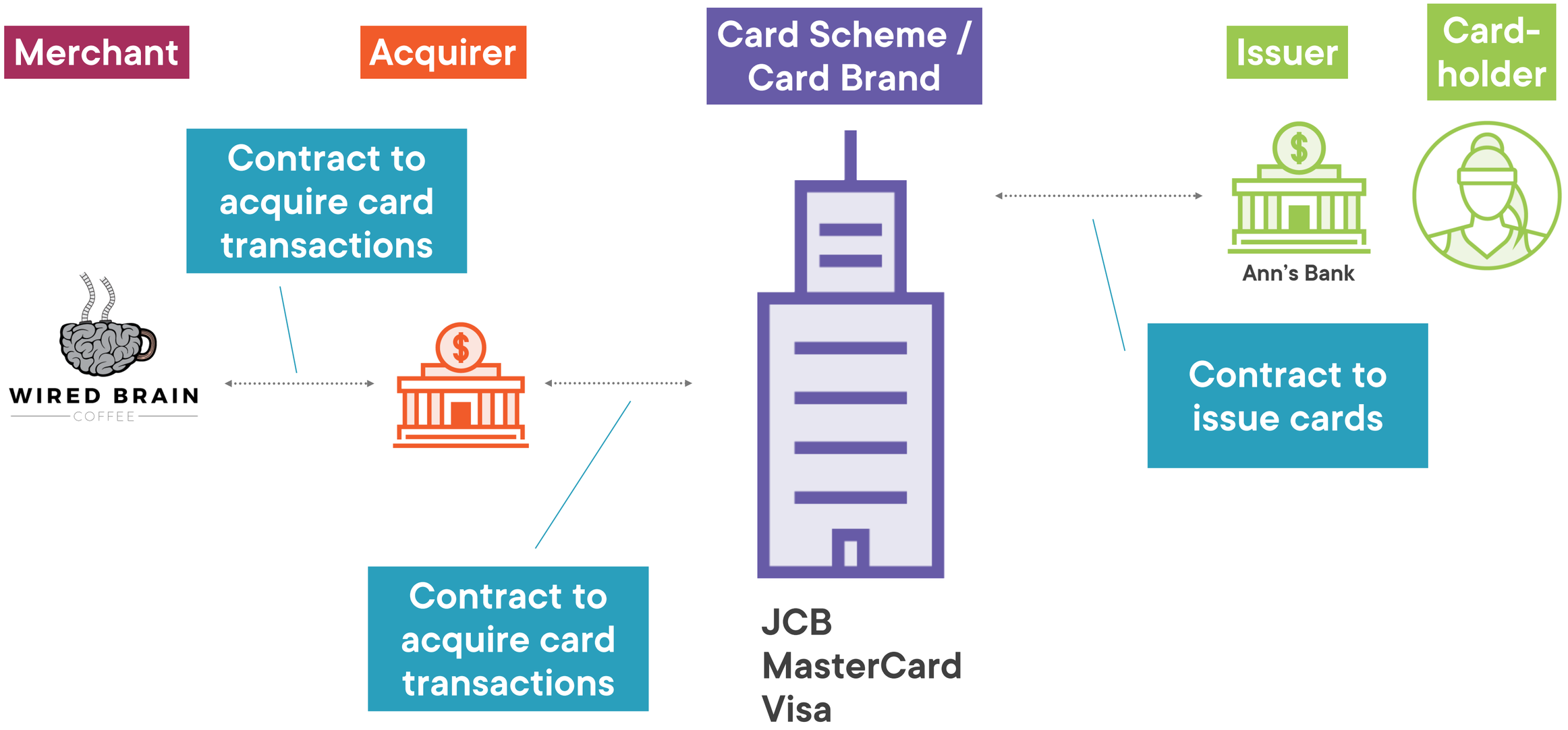
Compliance with the PCI standards is (generally) not a legal requirement

So why do companies have to comply?

Authorization in Practice



Contracts

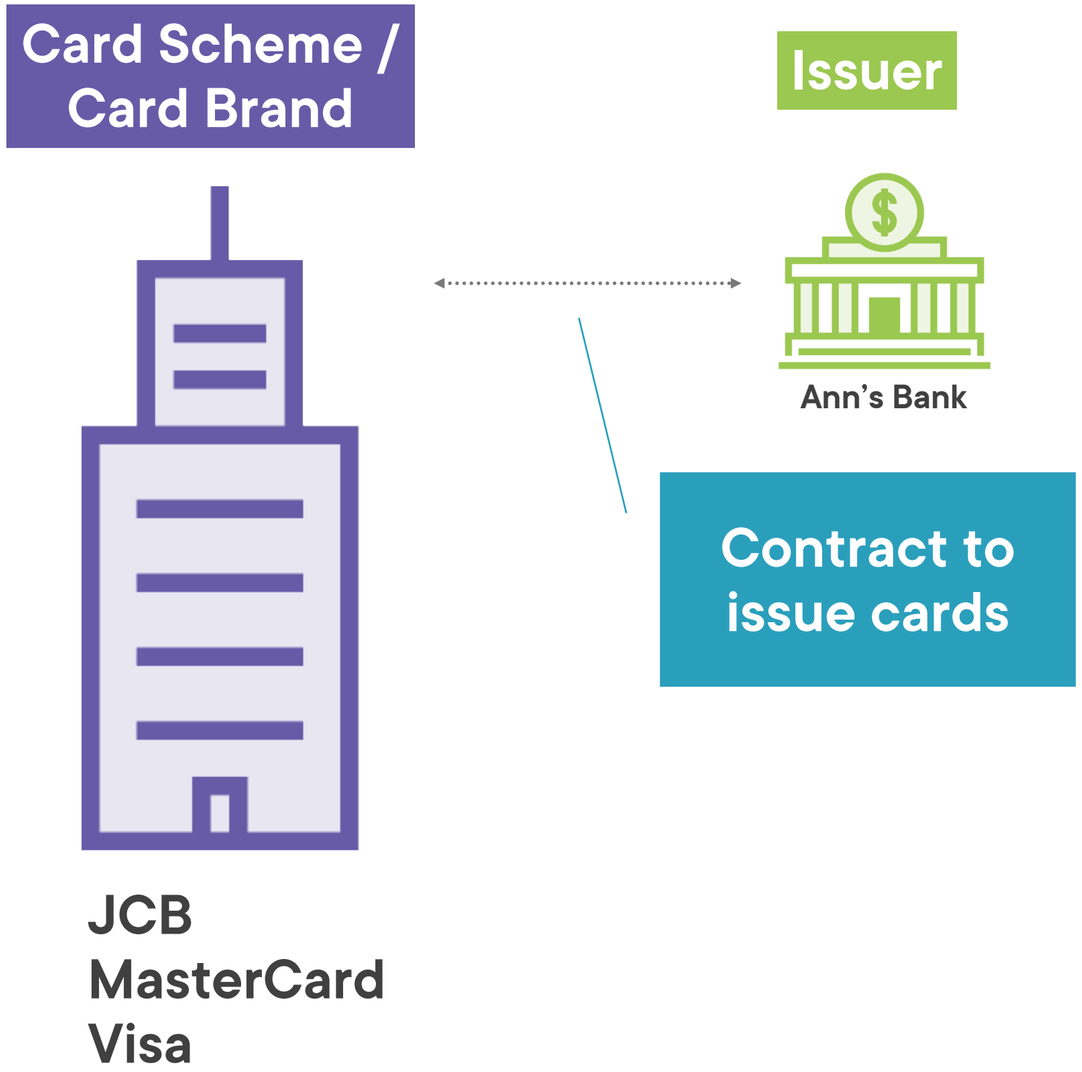

Merchant
Acquirer
Card Scheme / Card Brand
Issuer
Card-holder
Contract to acquire card transactions
WIRED BRAIN
COFFEE
Ann's Bank
Contract to issue cards
Contract to acquire card transactions
JCB
MasterCard
Visa

Scheme-issuer Contract

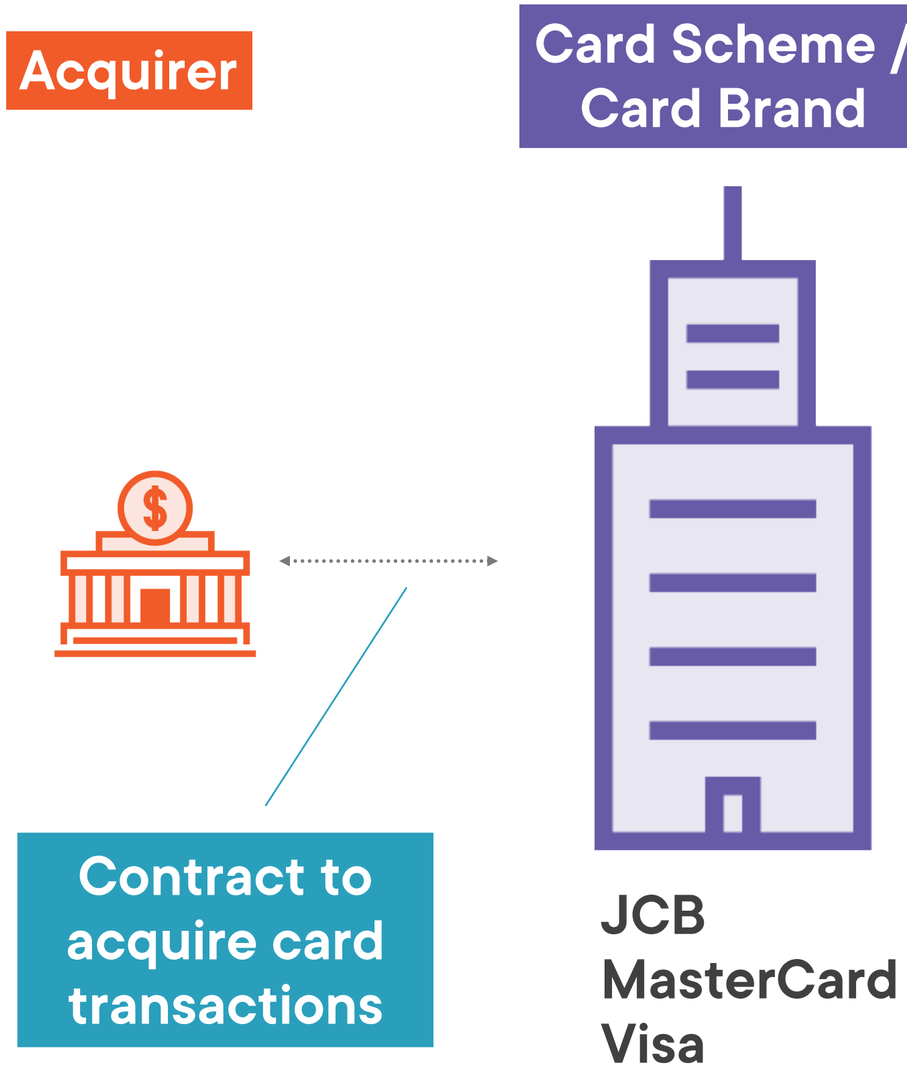
"Comply with all relevant PCI Standards"

- **Card Production**
- **PCI DSS**

- **3DS**
- **TSP**



Scheme-acquirer Contract



“Comply with all relevant PCI Standards”

- **PCI DSS**
- **PCI PIN**

“Ensure all your merchants..”

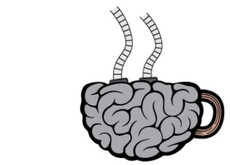
- **Comply with PCI DSS**
- **Only use SSS validated apps**
- **Only use PTS POI devices**

Acquirer-merchant Contract

Merchant

Acquirer

Contract to acquire card transactions



WIRED BRAIN
COFFEE

"You must"

- **Comply with PCI DSS**
- **Only use SSS validated apps**
- **Only use PTS POI devices**

Three-party Model

Merchant

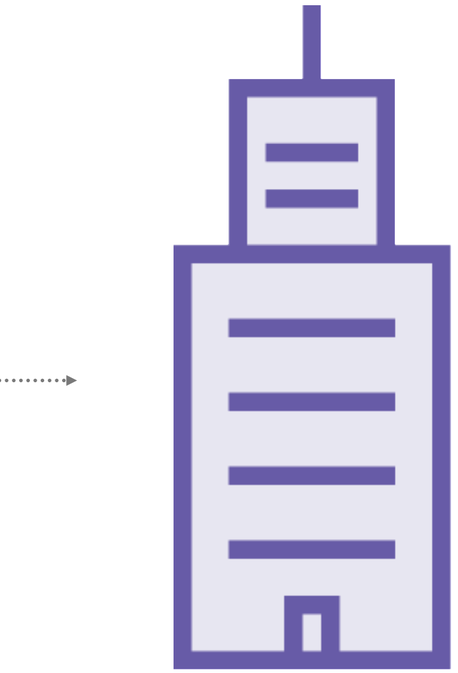
Acquirer

Card Scheme / Card Brand

Issuer

Card-holder

WIRED BRAIN COFFEE



American Express
Discover
JCB

Three-party Model

Merchant

WIRED BRAIN COFFEE

Contract to acquire card transactions

Card Scheme / Card Brand

American Express
Discover
JCB

"You must"

- **Comply with PCI DSS**
- **Only use SSS validated apps**
- **Only use PTS POI devices**

The Payment Card Industry Security Standards Council is a standards body

(the clue is in the name)

Who Does What?

PCI SSC

Writes and maintains the PCI security standards

Card brands / schemes

Makes organizations comply with the PCI security standards

Schemes vs. PCI SSC

Card Schemes	PCI Security Standards Council
Make merchants comply with PCI DSS	Write & maintain PCI Data Security Standard
Make merchants' third parties comply with PCI DSS	Write & maintain PCI Data Security Standard
Make acquirers comply with PCI PTS PIN	Write & maintain PCI PTS PIN standard
Make merchants only use PCI PTS POI devices to read cards	Write & maintain PCI PTS POI

Card Schemes vs. PCI SSC

Enforcement

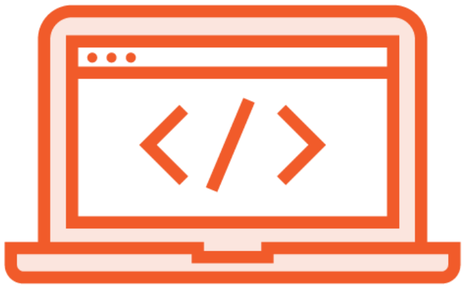
Standards Development

What Does the PCI SSC Do?

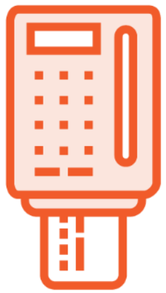
Standards

Assessors

Labs



Applications & P2PE Solutions



Card Reading & PIN Accepting Terminals

HSMs

What the PCI SSC Doesn't Do

Enforcement

Enforcement

Enforcement

Enforcement

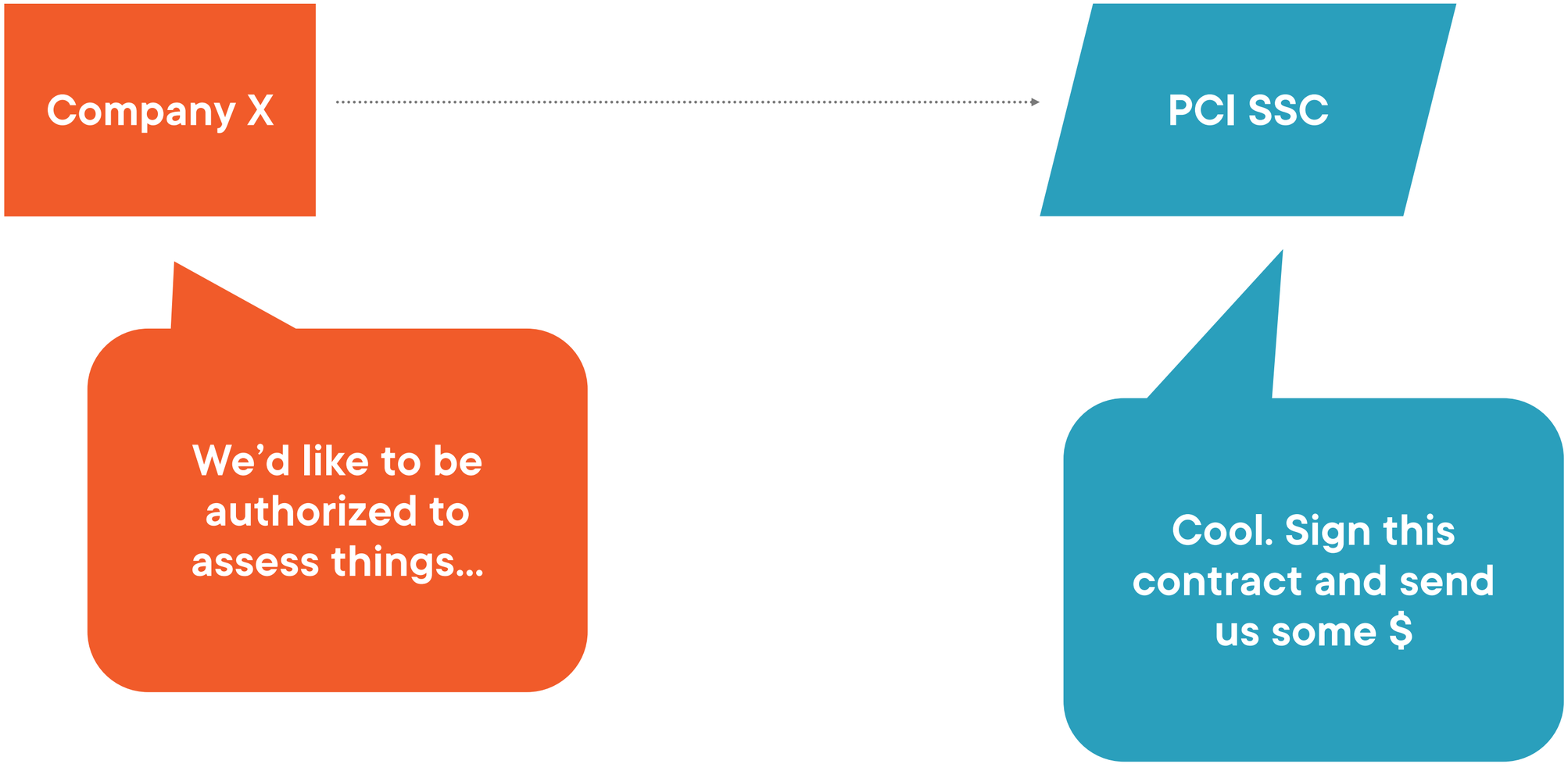
Enforcement

Enforcement

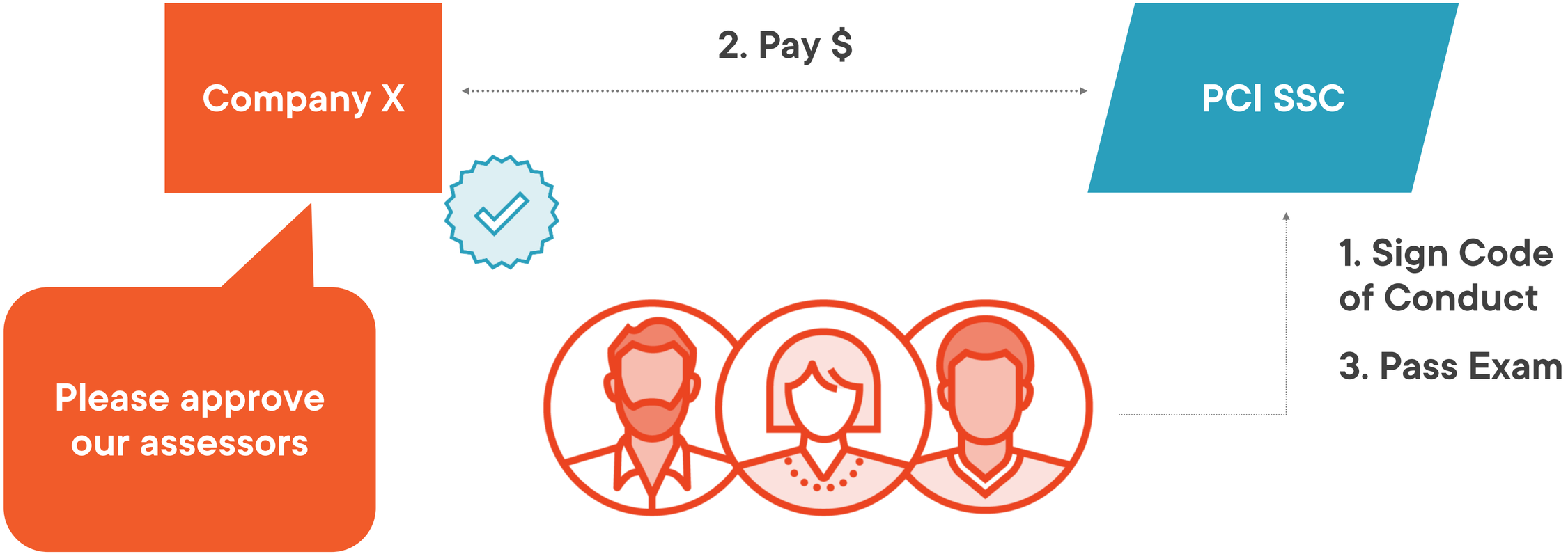
PCI SSC Assessor Accreditations

Standard	Assessor(s)
PCI DSS	Qualified Security Assessor - QSA Internal Security Assessor ISA
Software Security Standard	Secure Software Assessor
Secure Software Lifecycle	Secure Software Lifecycle (SLC) Assessor
Point to Point Encryption Standard	Qualified P2PE Assessor – QSA(P2PE)
3D Secure Core	3DS Assessor
PIN	Qualified PIN Assessor (QPA)
Card Production	Card Production Security Assessor (CPSA)

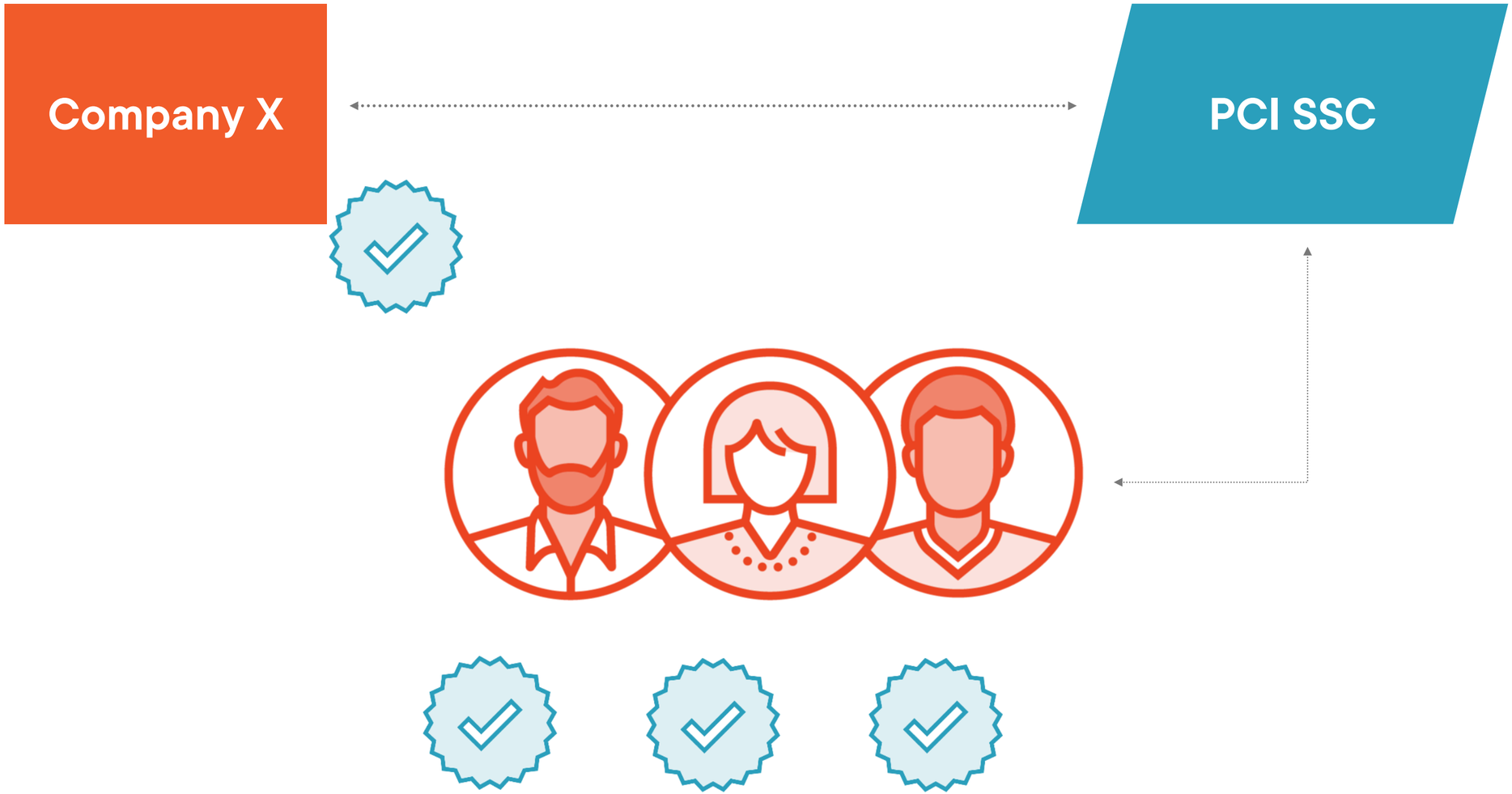
How SSC Programs Work



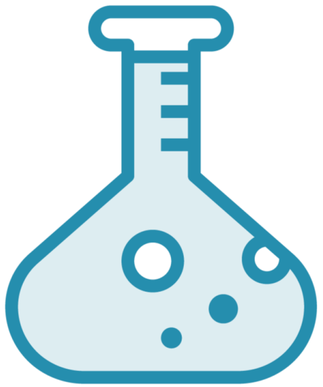
How SSC Programs Work



How SSC Programs Work



PCI SSC Lab Accreditations



Standard	Assessor(s)
PTS POI PTS HSM	PTS Labs
SPoC	SPoC Labs
CPoC	CPoC Labs
3D Software Development Kit	3DS SDK Labs

PCI SSC Services Program Accreditations

Program	Qualification
PCI Forensic Investigator (PFI)	PFI
Approved Scanning Vendor (ASV)	ASV
Qualified Integrator and Reseller (QIR)	QIR

Qualified Security Assessor (QSA)

Trained in:

- PCI DSS
- How payments work

Pass an examination

Authorized to conduct PCI DSS assessments

Internal Security Assessor (ISA)

Works for any company (typically large merchants and service providers)

Company must be a PCI Participating Organization

Understands PCI DSS

Authorized to conduct PCI DSS assessments

- If allowed by individual card schemes

Assessors for Other Standards

Secure Software Assessor

Qualified P2PE Assessor
QSA(P2PE)

3DS Assessor

Qualified PIN Assessor (QPA)

Card Production Security
Assessor (CPSA)

Will also be a normal QSA

Understands the specific standard

Specific in-depth technology knowledge:

- Cryptography and key management
- Physical security
- Software development

Qualified Integrator and Reseller (QIR)

Works for a QIR Company

Will understand Point-of-sale systems and how they need to be configured

Approved Scanning Vendor (ASV)

Provide external vulnerability scans to a quality specified by the PCI SSC

Look for vulnerabilities facing the internet

External scans are required:

- **By some card brands / schemes**
- **A requirement of PCI DSS**

Approved Scanning Vendor (ASV)

Provide external vulnerability scans to a quality specified by the PCI SSC

Look for vulnerabilities facing the internet

External scans are required:

- **By some card brands / schemes**
- **A requirement of PCI DSS**

Accreditation of scanning tool and personnel

PCI Forensic Investigator (PFI)

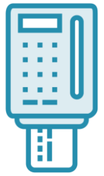
Will also be a normal QSA

Understands forensics and how criminals break into systems

Authorized to conduct post-breach forensic investigations

Products and Solutions

Secure Software



PTS POI – card reading devices

Point-to-point Encryption Solutions (P2PE)

Software Based PIN Entry on Commercial-off-the-shelf Devices (SPoC)

Contactless Payments on Commercial-off-the shelf Devices (CPoC)

Org ‘A’ Wants to Have Their ‘X’ Validated and Listed by the PCI SSC

Standard for ‘X’

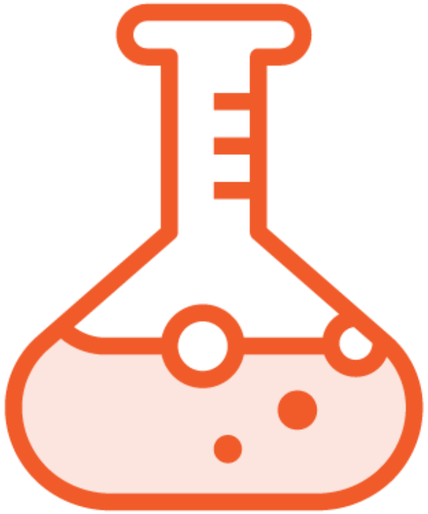
Assessor allowed to assess ‘X’

Report / evidence format for ‘X’

PCI SSC

Org ‘A’ Wants to Have Their Card Reading Terminal Validated by the PCI SSC

PCI PTS POI



PTS Lab

Evaluation Report

PCI SSC

Org ‘A’ Wants to Have Their Payment Application Validated by the PCI SSC

Secure Software Standard

Secure Software Assessor

RoV

PCI SSC

Org ‘A’ Wants to Have Their P2PE Solution Validated by the PCI SSC

PCI P2PE

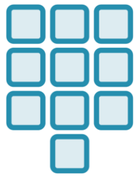
P2PE QSA

P-RoV

PCI SSC

Organizations

Data Security Standard



PIN

3DS Core

Token Service Provider

Card Production

Org ‘B’ Requires Org ‘A’ to Comply with Standard ‘X’

Standard for ‘X’

Assessor allowed to assess ‘X’

Validation document for ‘X’

Organization ‘B’

An Acquiring Bank Requires a Merchant to Comply with PCI DSS

PCI DSS

Qualified Security Assessor (QSA)

Report on Compliance (RoC)

Acquiring Bank

A Scheme Requires a Merchant to Comply with PCI DSS

PCI DSS

Qualified Security Assessor (QSA)

Report on Compliance (RoC)

Card Scheme

A Merchant Requires a Third-party Supplier to Comply with PCI DSS

PCI DSS

Qualified Security Assessor (QSA)

Report on Compliance (RoC)

Merchant

A Scheme Requires an Acquirer to Comply with PCI PIN

PCI PIN

Qualified PIN Assessor (QPA)

Report on Compliance (RoC)

Card Scheme

A Scheme Requires a Card Personalization Company to Comply with PCI Card Production

PCI Card Production

Card Production Security Assessor

Reports on Compliance (RoC)

Logical and Physical

Card Scheme

An Acquiring Bank Requires a Merchant to Undertake a Forensic Investigation

There is no standard. But there are rules.

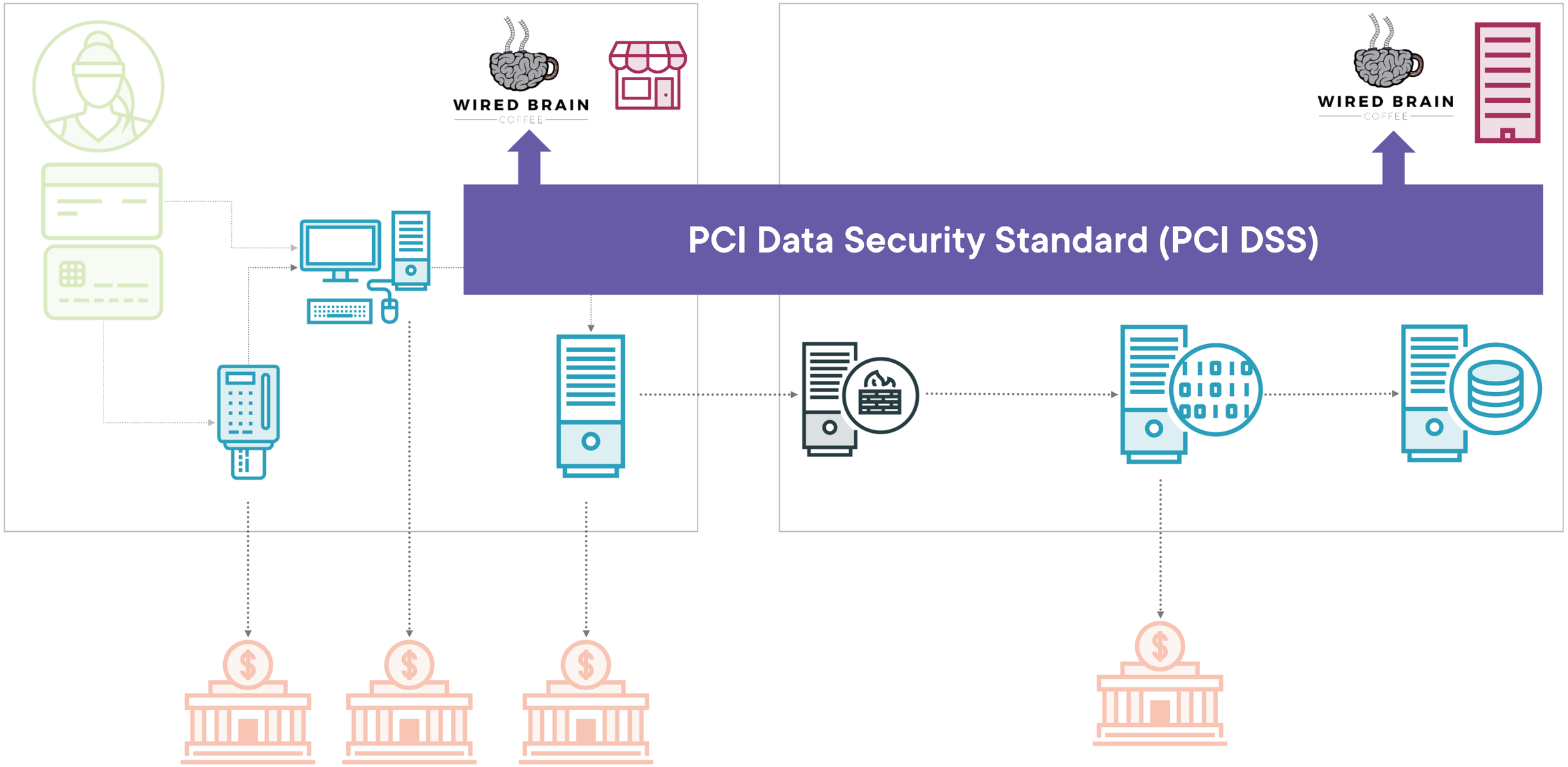
PCI Forensic Investigator (PFI)

PCI Forensic Report

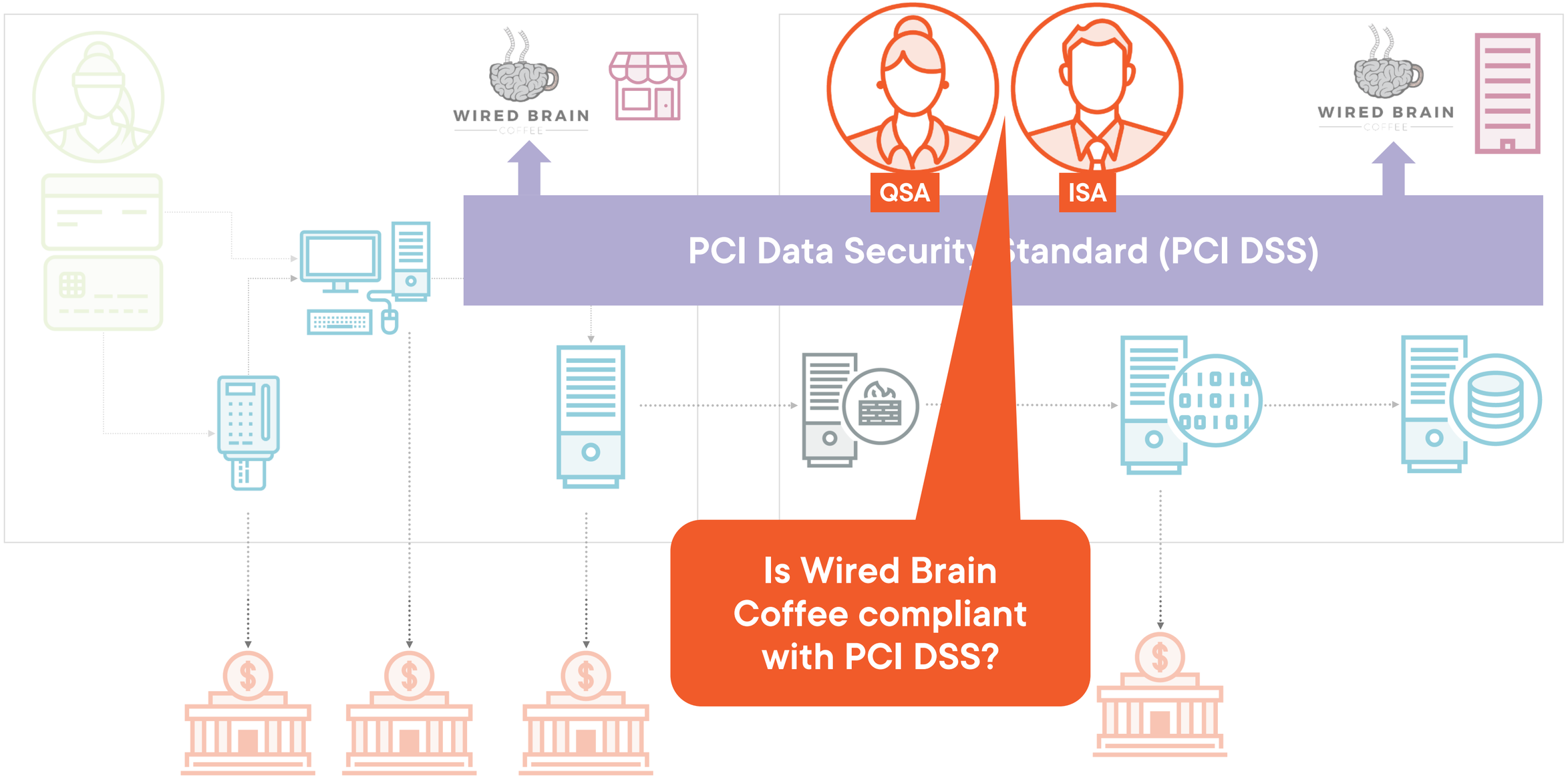
Acquiring Bank

Matching Assessor to Activity

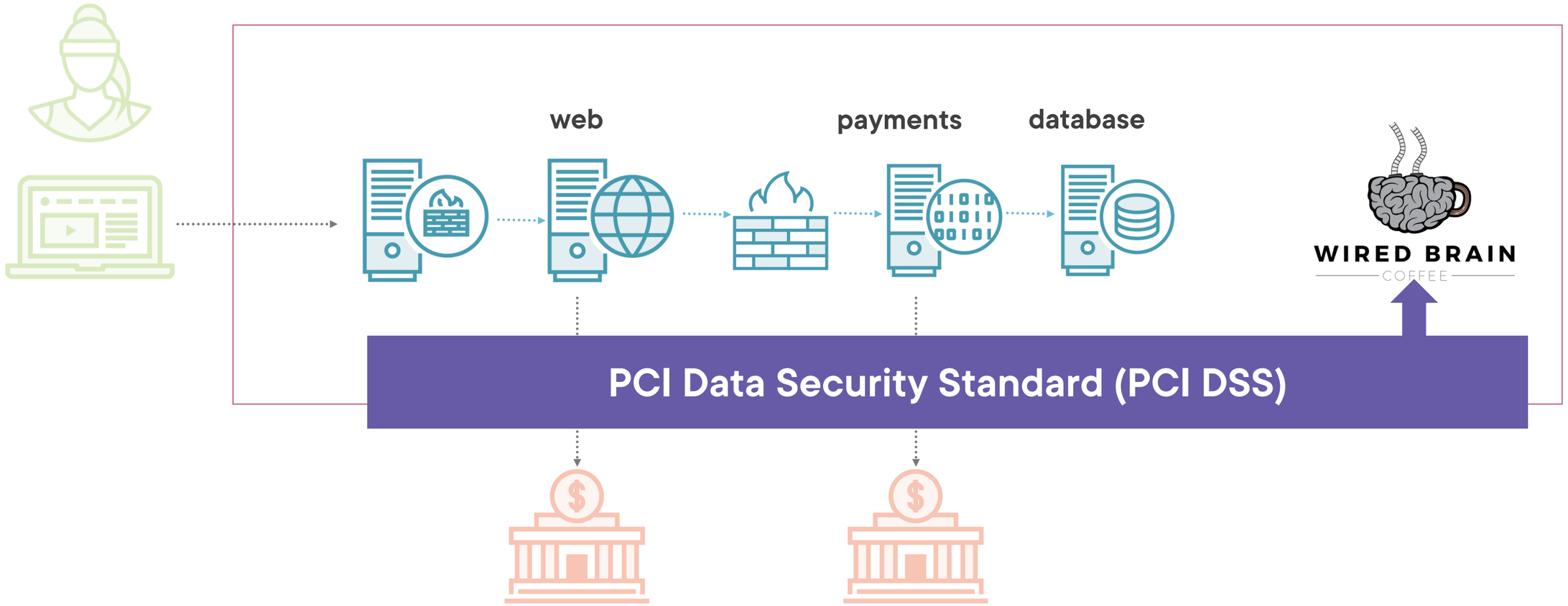
Which Standards Apply?



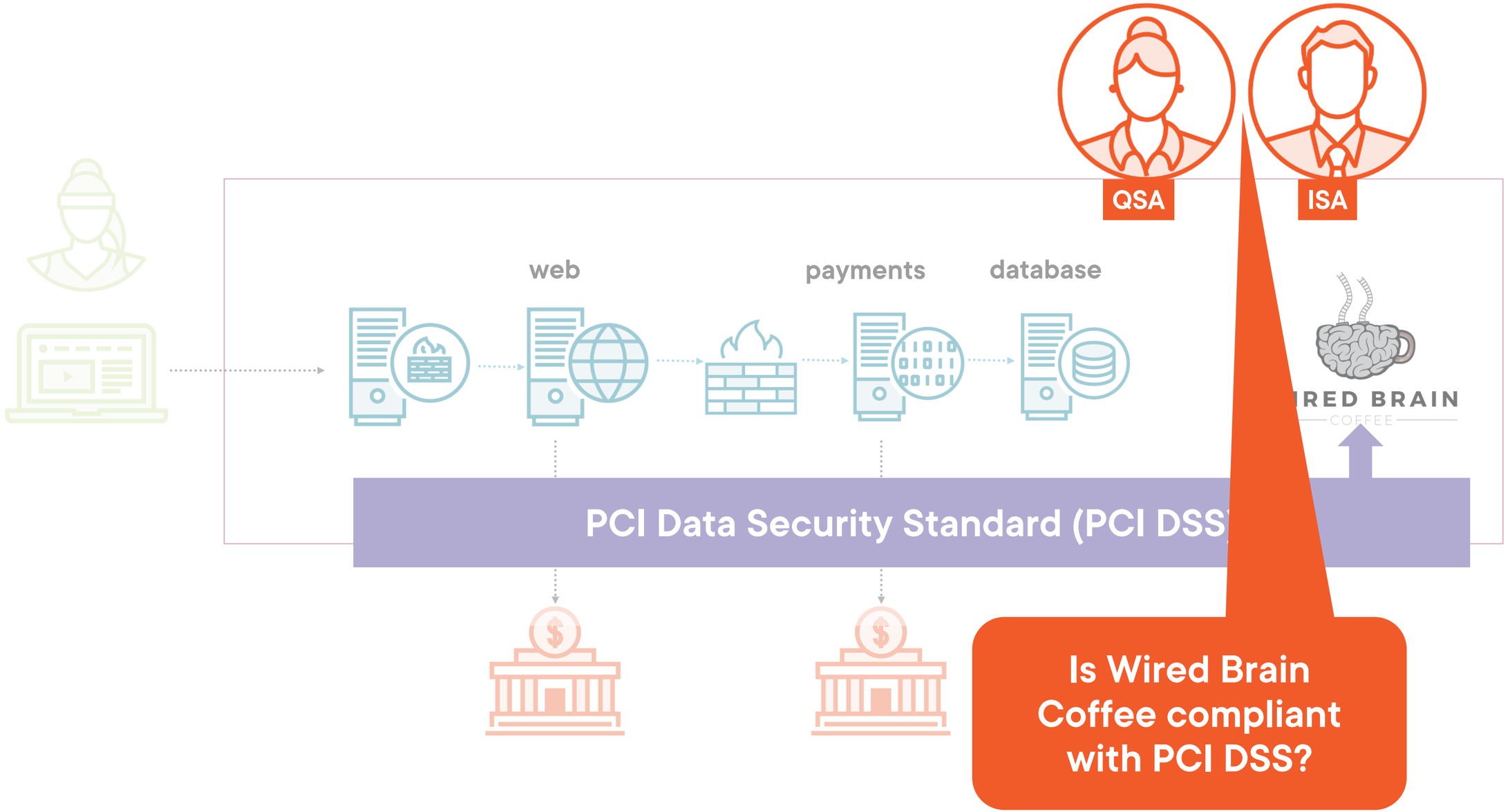
Which Assessors?



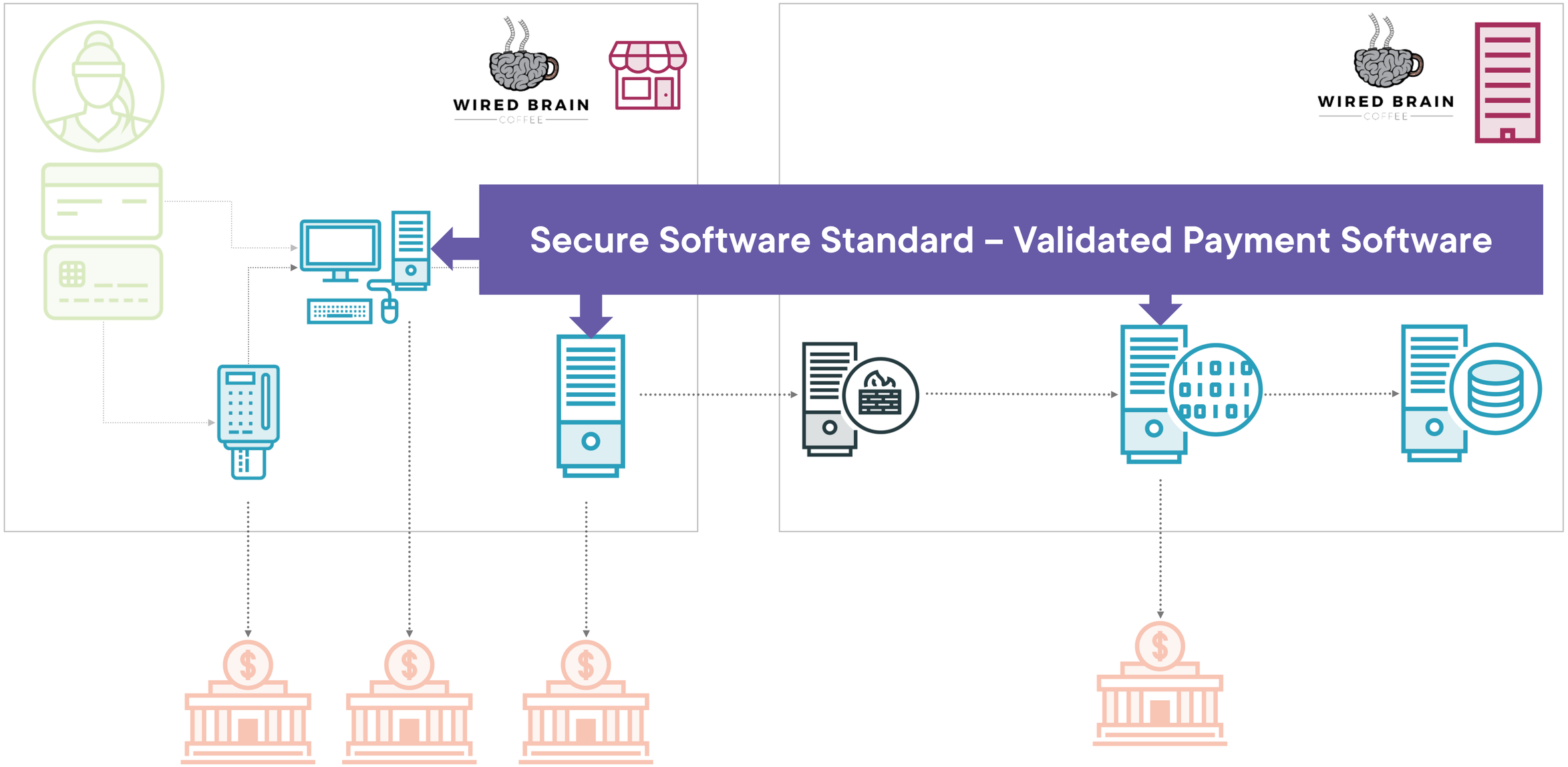
Which Standards Apply?



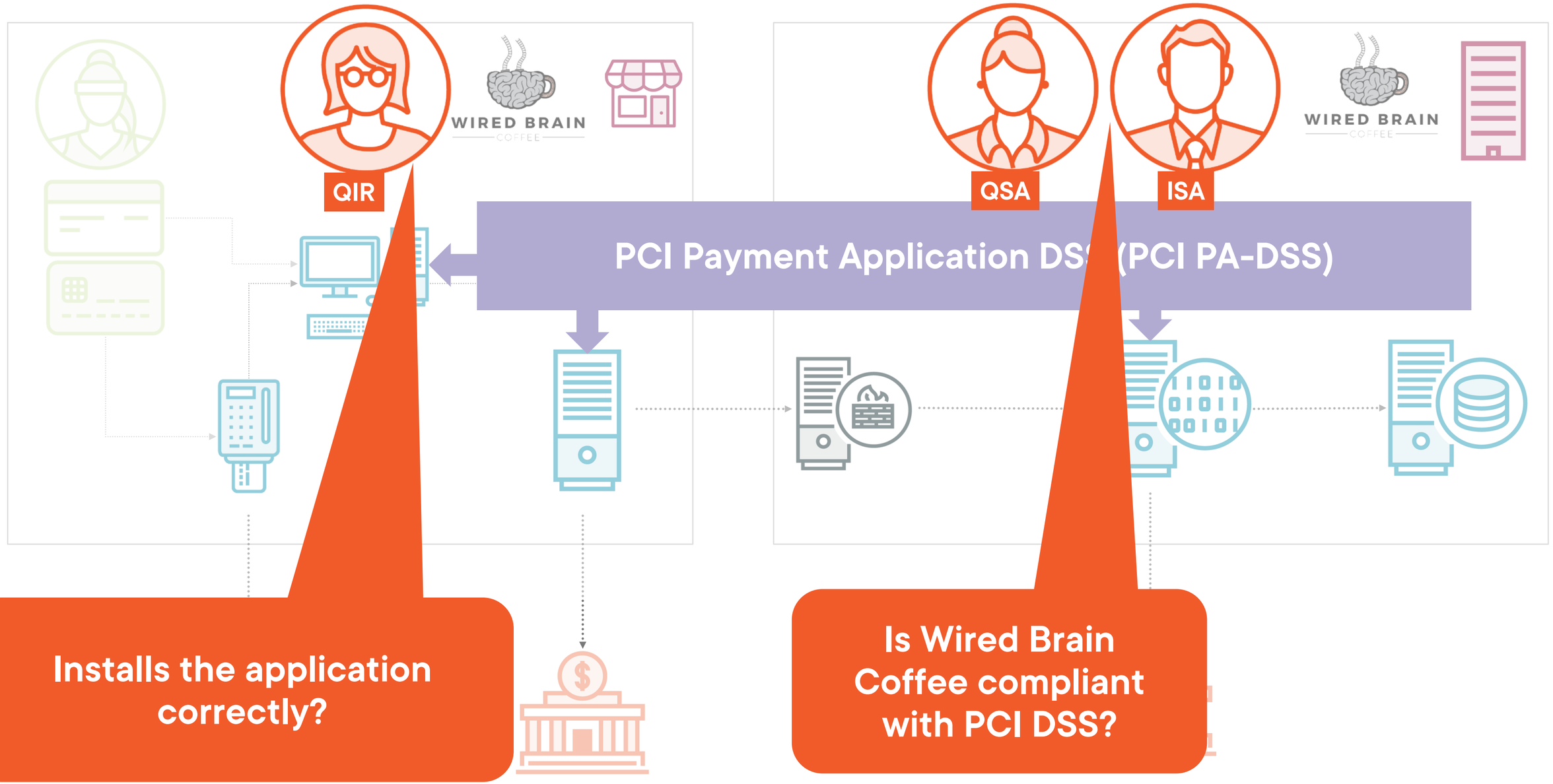
Which Assessors?



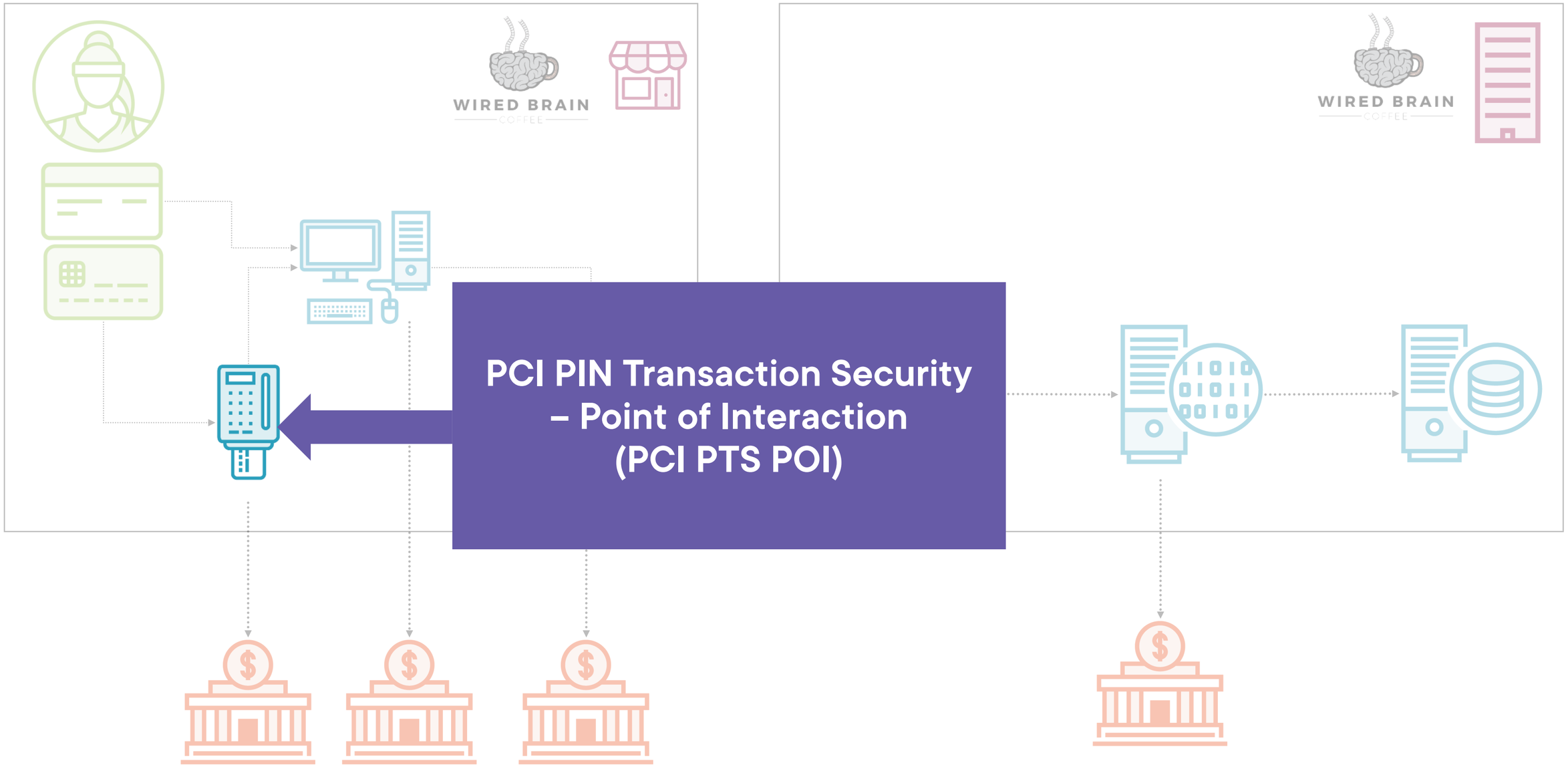
Which Standards Apply?



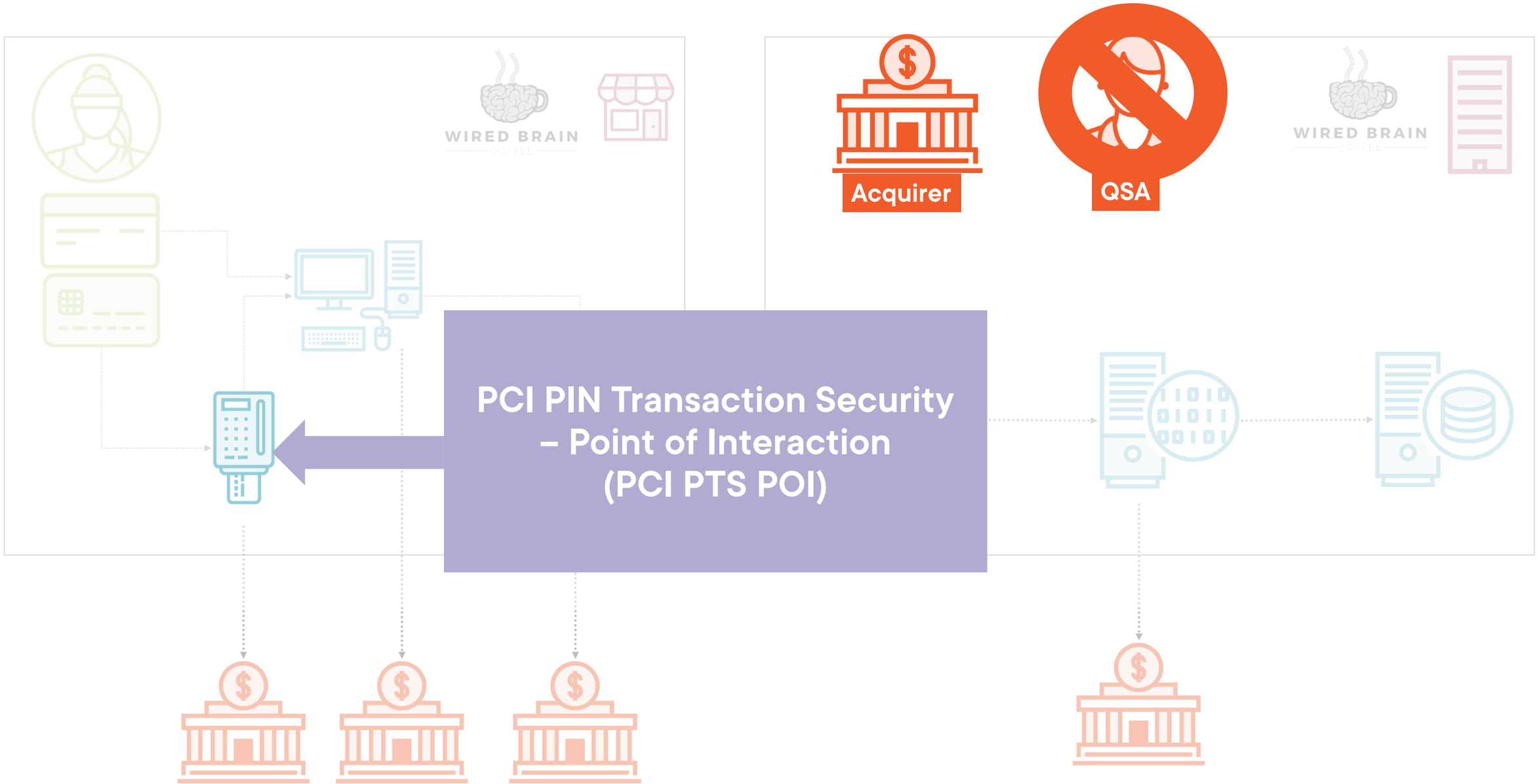
Which Assessors?



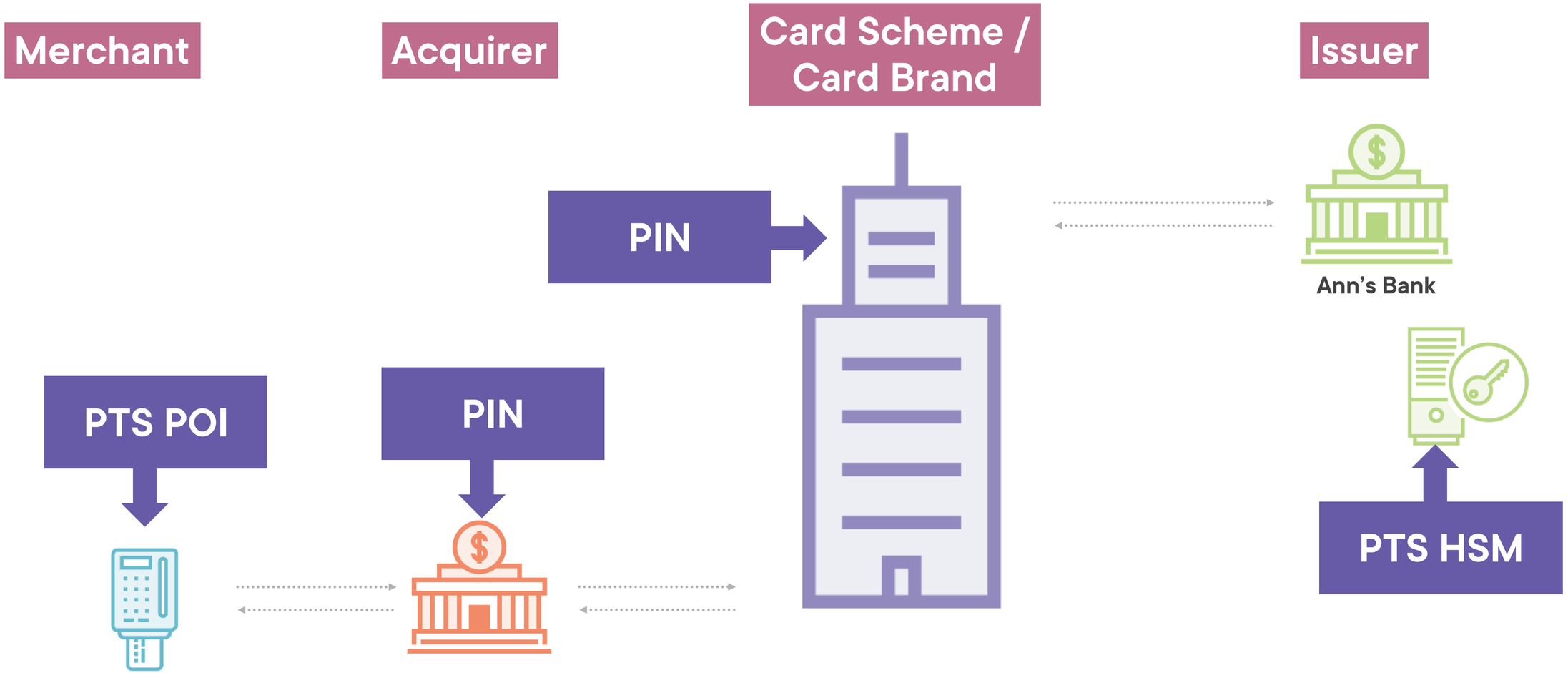
PTS POI at an F2F Merchant



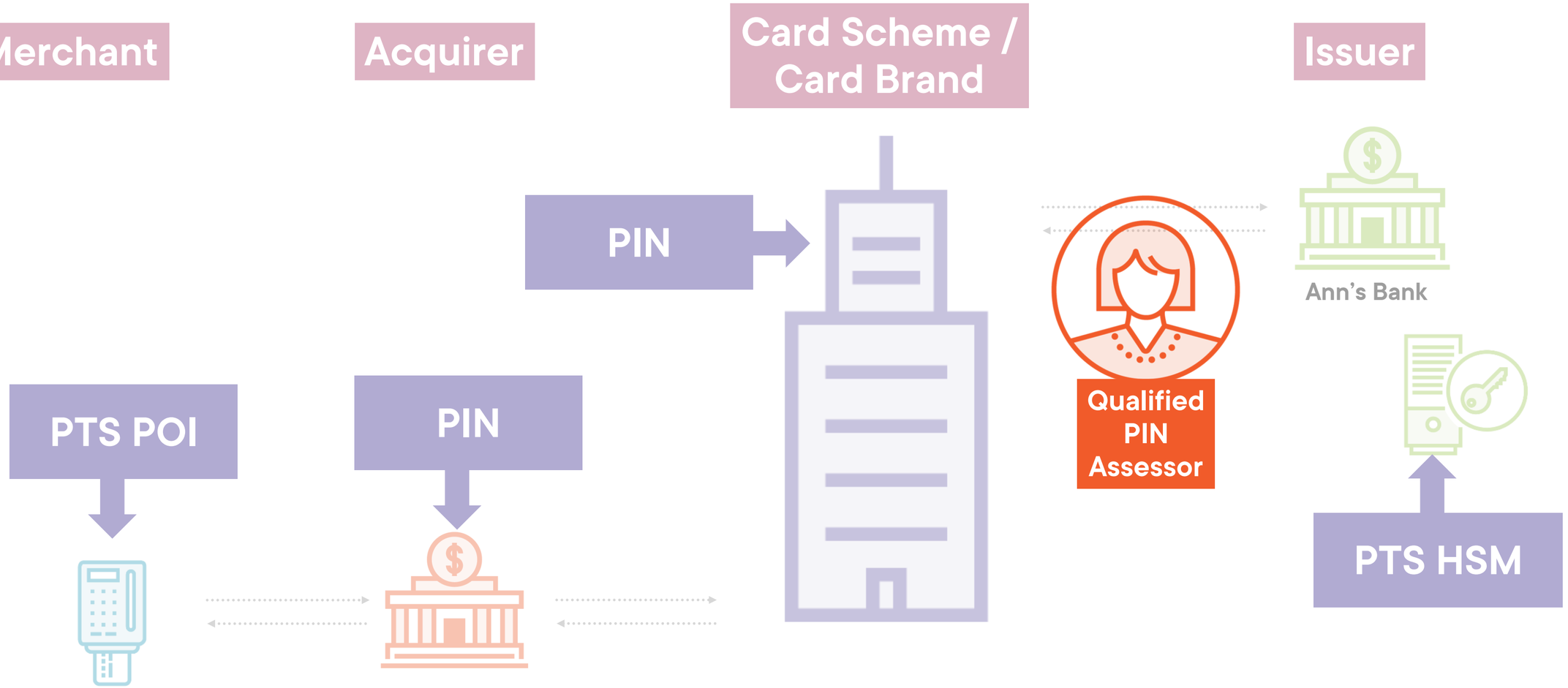
Which Assessor?



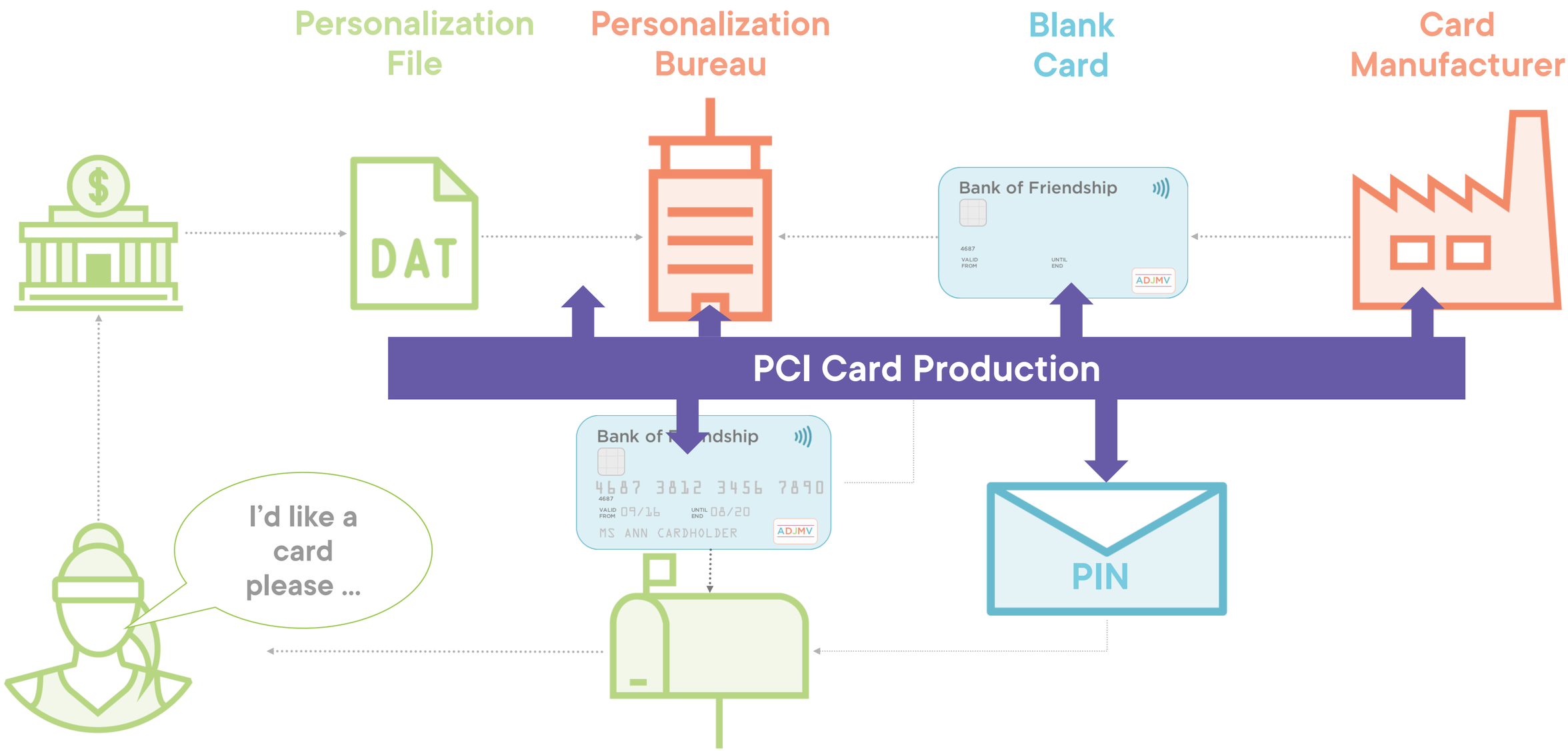
PTS in Practice



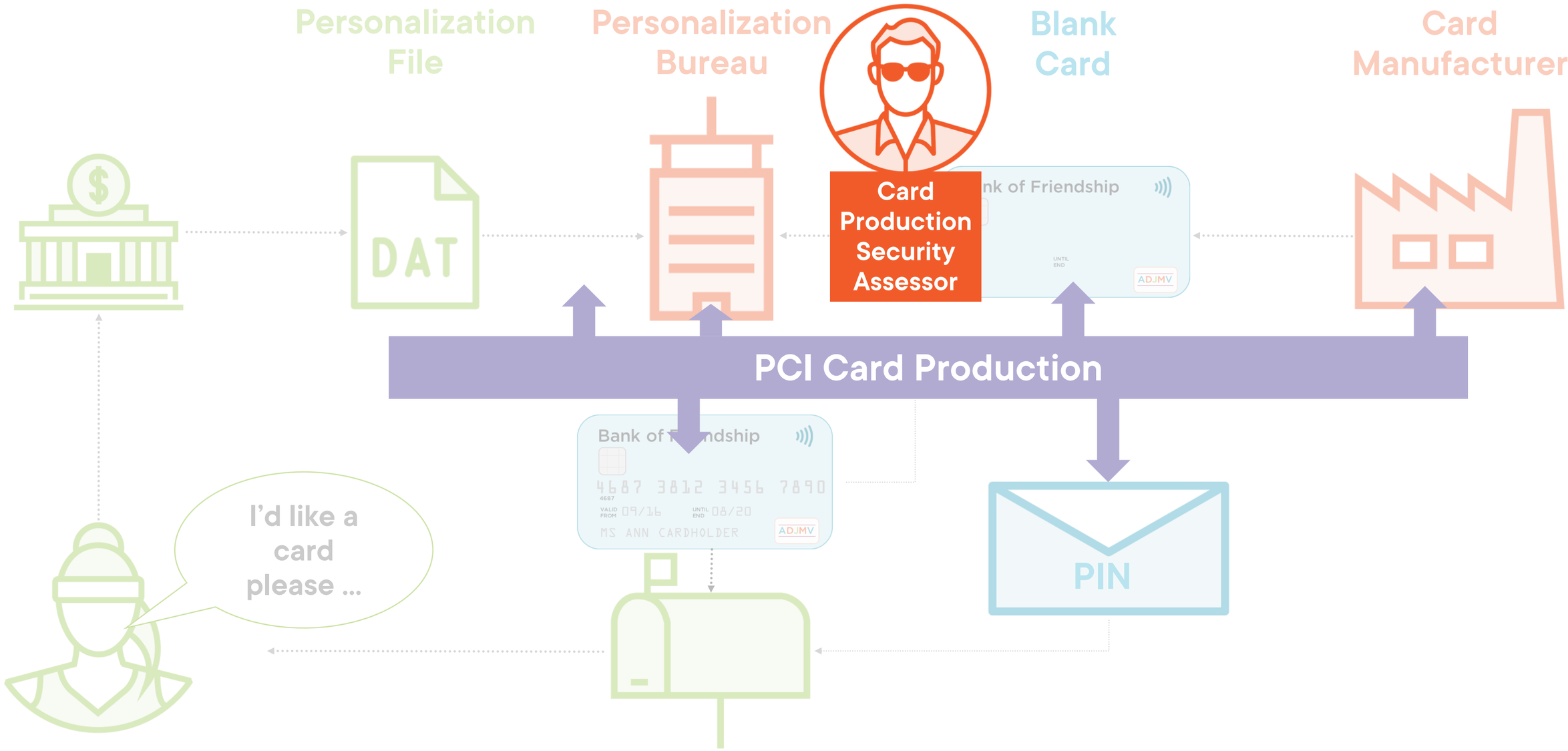
Which Assessor?



Card Production Standards



Which Assessor?



Round-up

The PCI SSC writes standards

Card brands/schemes say who has to comply with the standards

PCI compliance is not the law, compliance driven is driven by contracts

PCI SSC accredits assessors and labs provide independent assessments of products and services

- **PTS POI, PTS HSM, P2PE, SPoC, CPoC**

PCI SSC accredits assessors to provide independent assessments of organizations

- **PCI DSS, PCI PIN, 3DS Core, TSP, Card Production**

PCI Professional (PCIP)

The only PCI qualification that's not for assessors

Will understand payments, PCI standards, PCI DSS and security concepts

Could this be you?