

Securing Modern Payment Software: New Software Security Framework

Carlos Caetano

Associate Regional Director – Brazil

PCI Security Standards Council



Securing Payments is a Global Challenge

Understanding the Risk

World Economic Forum



2018

Extreme weather event

Natural disasters

No. 3 → Cyber-attacks

No. 4 →

Data fraud or theft

Failure of climate-change and adaptation

Top 5 Global Risks in terms of likelihood

Compromises in LAC

Criminals seeking data for monetization

HELP SECURE
PAYMENT
DATA



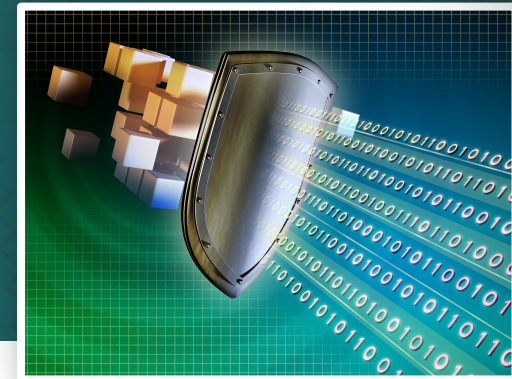
66%

E-commerce compromises
in Latin America



E-commerce compromise methods

- 53%** Code Injection
- 26%** Application Exploitation
- 11%** File upload
- 10%** SQL Injection



66%

Compromises detected by
regulators, card brands or
acquirers

PCI Security Standards Council

**We Help
Secure
Payment
Data**

Global, cross-industry effort to increase payment security

Industry-driven, flexible and effective standards and programs

Helping businesses detect, mitigate and prevent criminal attacks and breaches

PCI Security Standards

PCI Data Security Standard

PIN Security

Software-Based PIN Entry on COTS

Secure Software

Card Production -Physical

PCI 3-D Secure Core

PIN Transaction Security Hardware Module

PCI 3-D Secure Software Development Kit

Card Production - Logical

Payment Application Data Security Standard

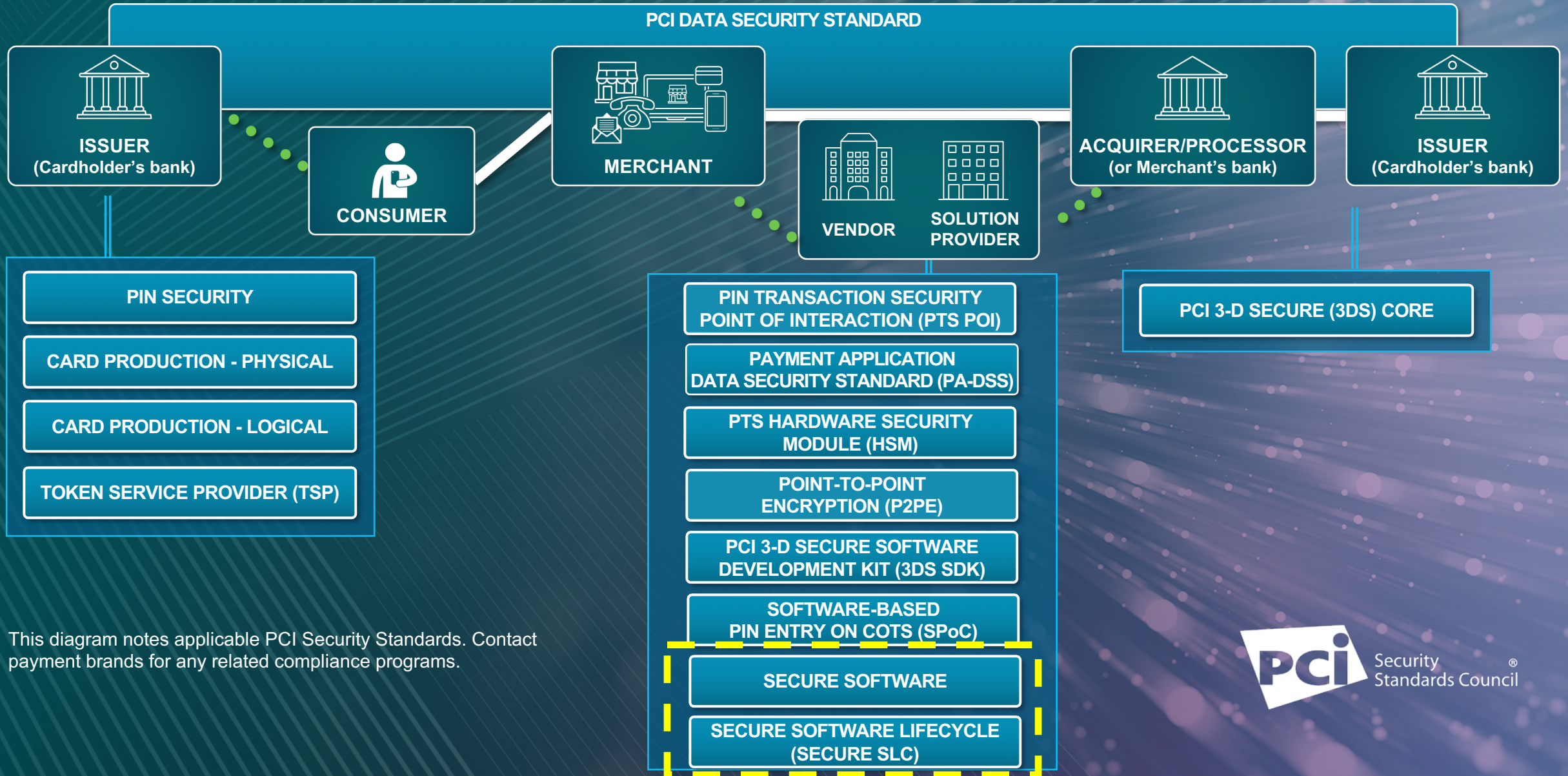
Point-to-Point Encryption

Token Service Provider

PIN Transaction Security Point of Interaction

Secure Software Lifecycle

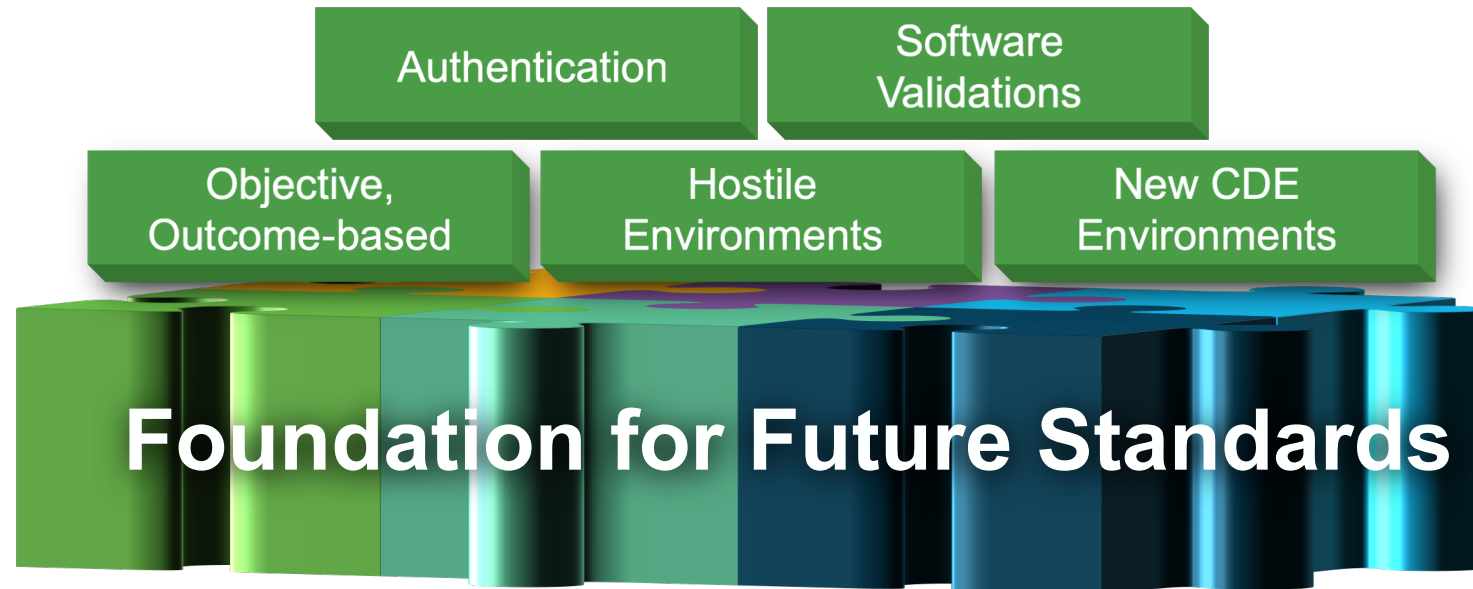
PCI Security Standards



This diagram notes applicable PCI Security Standards. Contact payment brands for any related compliance programs.

What Will the Next Generation of PCI Standards Provide?

Help Secure Payment Data





Software Security Framework

Software Security Framework



**Secure
Software
Standard**



**Secure Software
Lifecycle Standard**



**Validation
Programs**

Secure Software Standard

Minimizing the Attack Surface

Critical Asset Identification
Secure Defaults
Sensitive Data Retention

Activity Tracking
Attack Detection

Secure Software Operations

Software Protection Mechanisms

Critical Asset Protection
Authentication and Access Control
Sensitive Data Protection
Use of Cryptography

Threat and Vulnerability Management
Secure Software Updates
Vendor Security Guidance

Secure Software Lifecycle Management

Secure Software Standard

Module A – Account Data Protection

Sensitive Authentication Data
Cardholder Data Protection

Secure Software Standard

Control Objective 1: Critical Asset Identification

All software critical assets are identified and classified.

Control Objective 2: Secure Defaults

Default privileges, features, and functionality are restricted to only those necessary to provide a secure default configuration.

Control Objective 3: Sensitive Data Retention

Retention of sensitive data is minimized.

Control Objective 4: Critical Asset Protection

Critical assets are protected from attack scenarios.

Control Objective 5: Authentication and Access Control

The software implements strong authentication and access control to help protect the confidentiality and integrity of critical assets.

Control Objective 6: Sensitive Data Protection

Sensitive data is protected at rest and in transit.

Secure Software Standard

Control Objective 7: Use of Cryptography

Cryptography is used appropriately and correctly.

Control Objective 8: Activity Tracking

All software activity involving critical assets is tracked.

Control Objective 9: Attack Detection

Attacks are detected, and the impacts/effects of attacks are minimized.

Control Objective 10: Threat and Vulnerability Management

The software vendor identifies, assesses, and manages threats and vulnerabilities to its payment software.

Control Objective 11: Secure Software Updates

The software vendor facilitates secure software releases and updates.

Control Objective 12: Vendor Security Guidance

The software vendor provides stakeholders with clear and thorough guidance on the secure implementation, configuration, and operation of the software.

Secure Software Standard

Control Objective A.1: Sensitive Authentication Data

Sensitive authentication data is not retained after authorization.

Control Objective A.2: Cardholder Data Protection

Protect stored cardholder data.

Secure Software Lifecycle Standard

Software Security Governance

Security Responsibility and Resources
Software Security Policy and Strategy

Change Management
Software Integrity Protection
Sensitive Data Protection

Secure Software and Data Management

Secure Software Engineering

Threat Identification and Mitigation
Vulnerability Detection and Mitigation

Vendor Security Guidance
Stakeholder Communications
Software Update Information

Security Communications

Secure Software Lifecycle Standard

Control Objective 1: Security Responsibility and Resources

The vendor's senior leadership team establishes formal responsibility and authority for the security of the vendor's products and services. The vendor allocates resources to execute the strategy and ensure that personnel are appropriately skilled.

Control Objective 2: Software Security Policy and Strategy

The vendor defines, maintains, and communicates a software security policy and a strategy for ensuring the secure design, development, and management of its products and services. Performance against the software security strategy is monitored and tracked.

Control Objective 3: Threat Identification and Mitigation

The vendor continuously identifies, assesses, and manages risk to its payment software and services.

Control Objective 4: Vulnerability Detection and Mitigation

The vendor detects and mitigates vulnerabilities in the software and its components to ensure that payment software remains resistant to attacks throughout its entire lifetime.

Control Objective 5: Change Management

Identify and manage payment software changes throughout the software lifecycle

Secure Software Lifecycle Standard

Control Objective 6: Software Integrity Protection

Protect the integrity of the payment software throughout the software lifecycle.

Control Objective 7: Sensitive Data Protection

The confidentiality of customers' sensitive production data on vendor systems is maintained.

Control Objective 8: Vendor Security Guidance

The vendor provides stakeholders with clear and thorough guidance on the secure implementation, configuration, and operation of its payment software applications.

Control Objective 9: Stakeholder Communications

The vendor maintains communication channels with stakeholders regarding potential security issues and mitigation options.

Control Objective 10: Software Update Information

The vendor provides stakeholders with detailed explanations of all software changes.

Industry Benefits



Application Vendors

Security to meet release demands

Flexibility in applied security

Awareness of payment security responsibilities



Application Users (e.g. merchants)

Broader applicability of AppSec

More customization while maintaining security

Transparency in level of testing



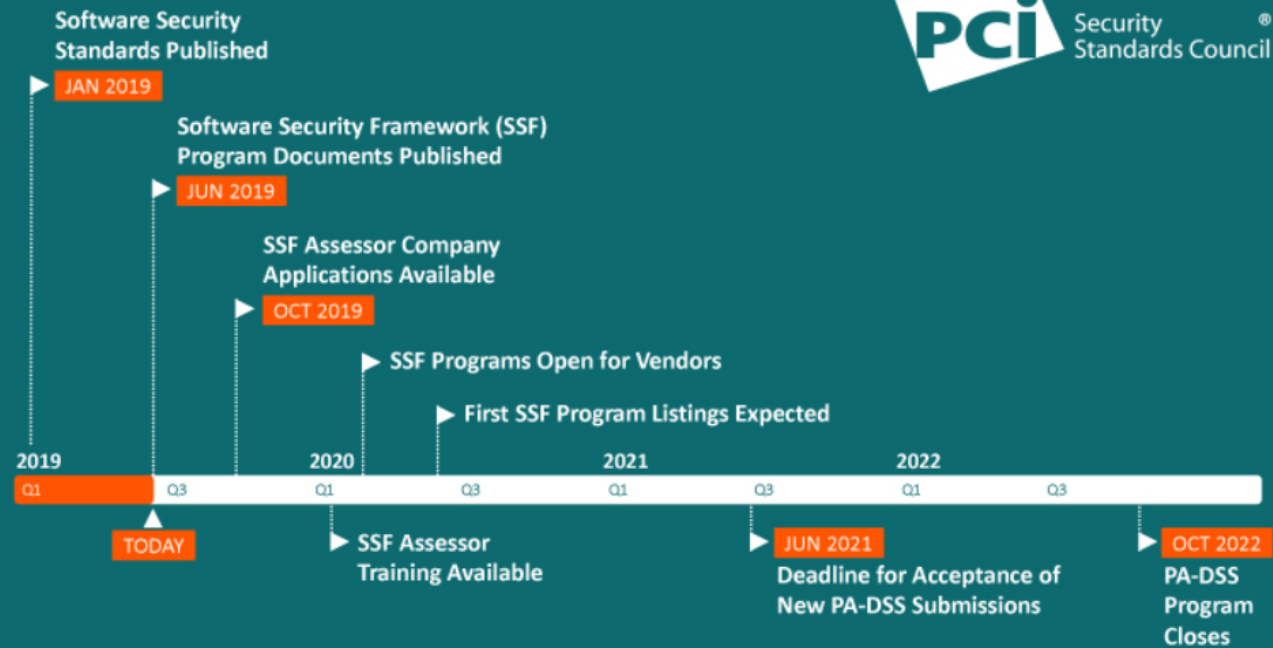
Payment Industry

Consistency in testing

Scalable framework

Improved quality and integrity

PCI Secure Software and Secure SLC Programs



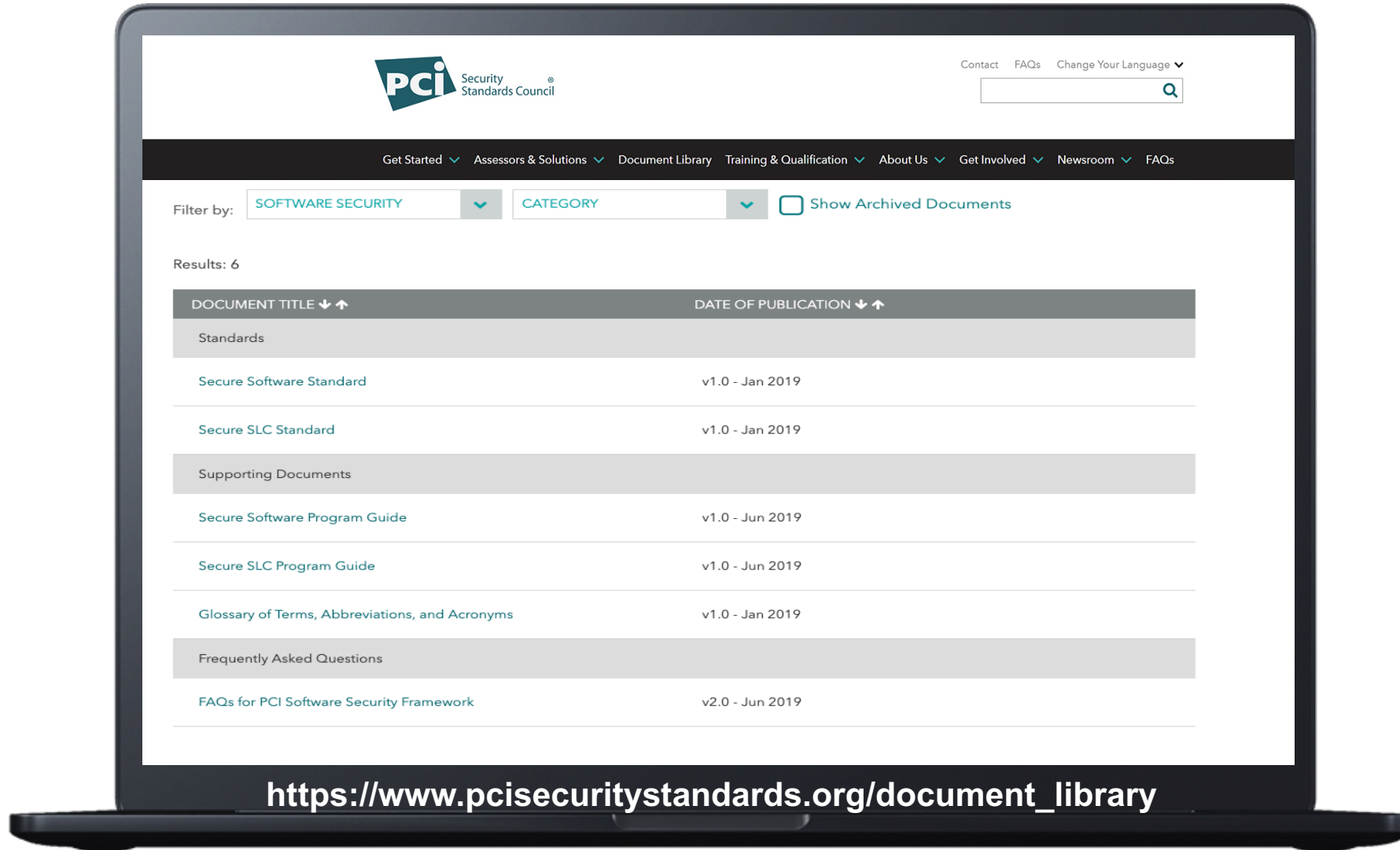
- For payment software vendors to demonstrate their software products and development practices meet Secure Software and Secure SLC Standards
- Qualification requirements for both assessor company and individual assessor
- Listing of PCI SSC validated software and qualified vendors
- Program documentation now available on PCI SSC website

PA-DSS Impact

- Transition path into SSF Assessor Programs for PA-QSAs and QSAs
- New PA-DSS submissions permitted until mid-2021
- Upon PA-DSS v3.2 expiry in 2022
 - PA-DSS program retired
 - Payment software assessments occur under Software Security Framework

See PCI Perspectives Blog: <https://blog.pcisecuritystandards.org/pci-software-security-framework-update-on-assessor-qualification>

Where Do I Find the SSF?



The screenshot shows the PCI Security Standards Council Document Library website. The page features a search bar at the top right with a magnifying glass icon. Below the search bar is a navigation menu with links for 'Get Started', 'Assessors & Solutions', 'Document Library', 'Training & Qualification', 'About Us', 'Get Involved', 'Newsroom', and 'FAQs'. The main content area has a filter section with 'Filter by:' followed by two dropdown menus: 'SOFTWARE SECURITY' and 'CATEGORY'. There is also a checkbox labeled 'Show Archived Documents'. Below the filters, it says 'Results: 6'. A table lists the documents with columns for 'DOCUMENT TITLE' and 'DATE OF PUBLICATION'. The table is divided into sections: 'Standards', 'Supporting Documents', and 'Frequently Asked Questions'.

DOCUMENT TITLE	DATE OF PUBLICATION
Standards	
Secure Software Standard	v1.0 - Jan 2019
Secure SLC Standard	v1.0 - Jan 2019
Supporting Documents	
Secure Software Program Guide	v1.0 - Jun 2019
Secure SLC Program Guide	v1.0 - Jun 2019
Glossary of Terms, Abbreviations, and Acronyms	v1.0 - Jan 2019
Frequently Asked Questions	
FAQs for PCI Software Security Framework	v2.0 - Jun 2019

https://www.pcisecuritystandards.org/document_library



HOW You Can Help Secure Payment Data



Participate



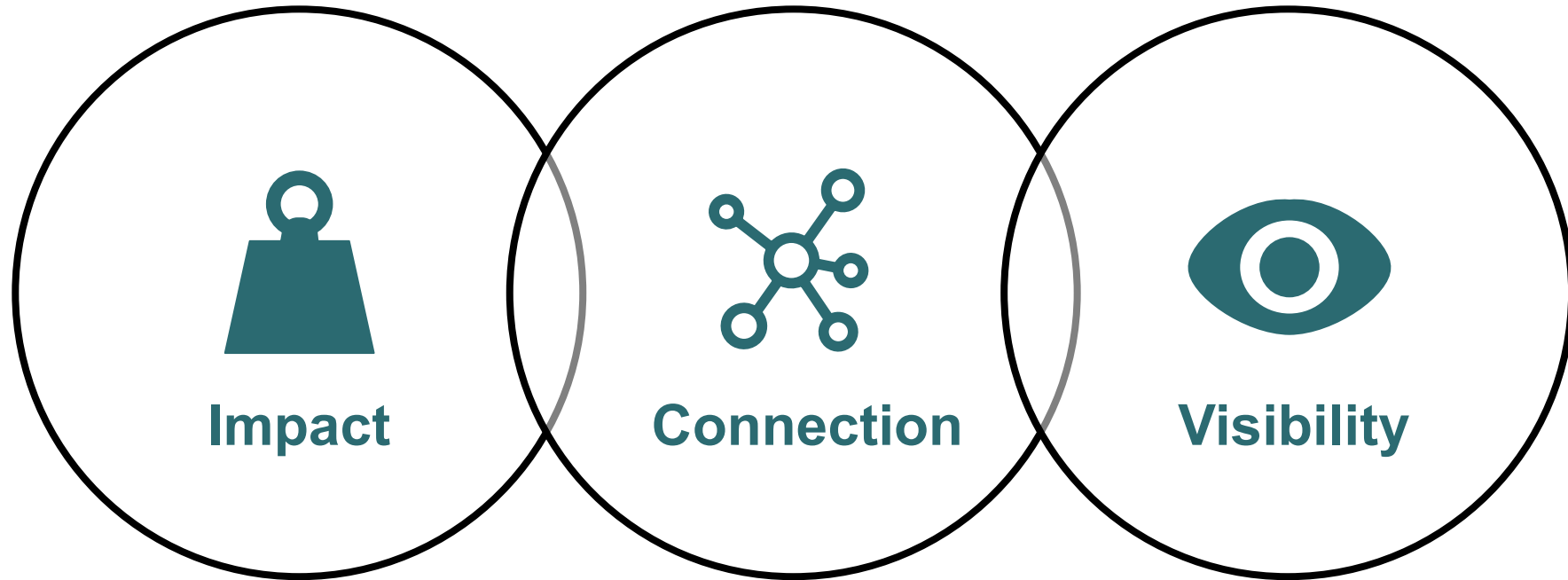
Learn



Share

Participate

Become a PCI SSC Participating Organization



Benefits and Opportunities

Demonstrate
your commitment
to payment
security



Provide Feedback

Request for
Comments (RFC)

PCI Data
Security
Standard

PIN
Security

Software-
Based PIN
Entry on COTS

Secure
Software

Card
Production
-Physical

PCI 3-D
Secure Core

PIN
Transaction
Security
Hardware
Module

PCI 3-D
Secure
Software
Development
Kit

Card
Production
- Logical

Payment
Application
Data Security
Standard

Point-to-Point
Encryption

Token
Service
Provider

PIN
Transaction
Security
Point of
Interaction

Secure
Software
Lifecycle

Nominate and Represent

Brazil Regional Engagement
Board

AirTkt

braspag

camara-e.net
Câmara Brasileira de Comércio Eletrônico
COMITÊ DE INSURTECHS

cielo

conductor
Tecnologia em Meios de Pagamento

CSU

despegar.com
EL MEJOR PRECIO PARA TU VIAJE!

celo

FIS

First Data

FOREGNIX

Gertec

getnet

Itaú

PayPal

TIVIT

VTEX

worldpay

The new regional Engagement Board brings together leaders in the Brazilian payment card industry to share their knowledge and local understanding of the payments space in Brazil. The formation of this outstanding group highlights the significance of the Brazilian market in the world of payments security.

Carlos Caetano
Associate Regional Director – Brazil
PCI Security Standards Council

Nominate and Serve

Brazil Regional Engagement Board

Provide advice, feedback, and guidance to PCI SSC on payment data security issues in Brazil.

Nomination Period: 1 – 29 November
Notification Period: 10 – 17 December
New Board Announcement : 2020 January

Learn Training

Substantial discounts for POs
Instructor-led, Hands-on
eLearning

If you haven't suffered a data breach, you've either been incredibly well prepared, or very, very lucky. Are you incredibly prepared?

2017 Verizon Data Breach Investigation
Report Executive Summary

Share Resources





Security[®]
Standards Council

Get Involved Today!

participation@pcisecuritystandards.org