SEVEN SECURITY GROUP

Payment Card Industry Security Standards

Pavel Kaminsky

PCI QSA, CISSP, CISA, CEH, Founder & CEO of 7Security GmbH
p.kaminsky@7sec.com

7Security GmbH

7Security GmbH - Vienna, Austria

PCI DSS, 3DS, PIN Security, SoftPOS in Europe and CEMEA

Assessor, Implementation and Penetration Testing Teams

90% entrusted us with their 1st PCI DSS

PCI QSA, 3DS, CISSP, CISA, CEH

VISA Innovation Program

Level39 London

Startupbootcamp Fintech & Cybersecurity Amsterdam

Impact Hub, Fintech Hive, NCA

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

Information Security Management System ISO 27001 Certified

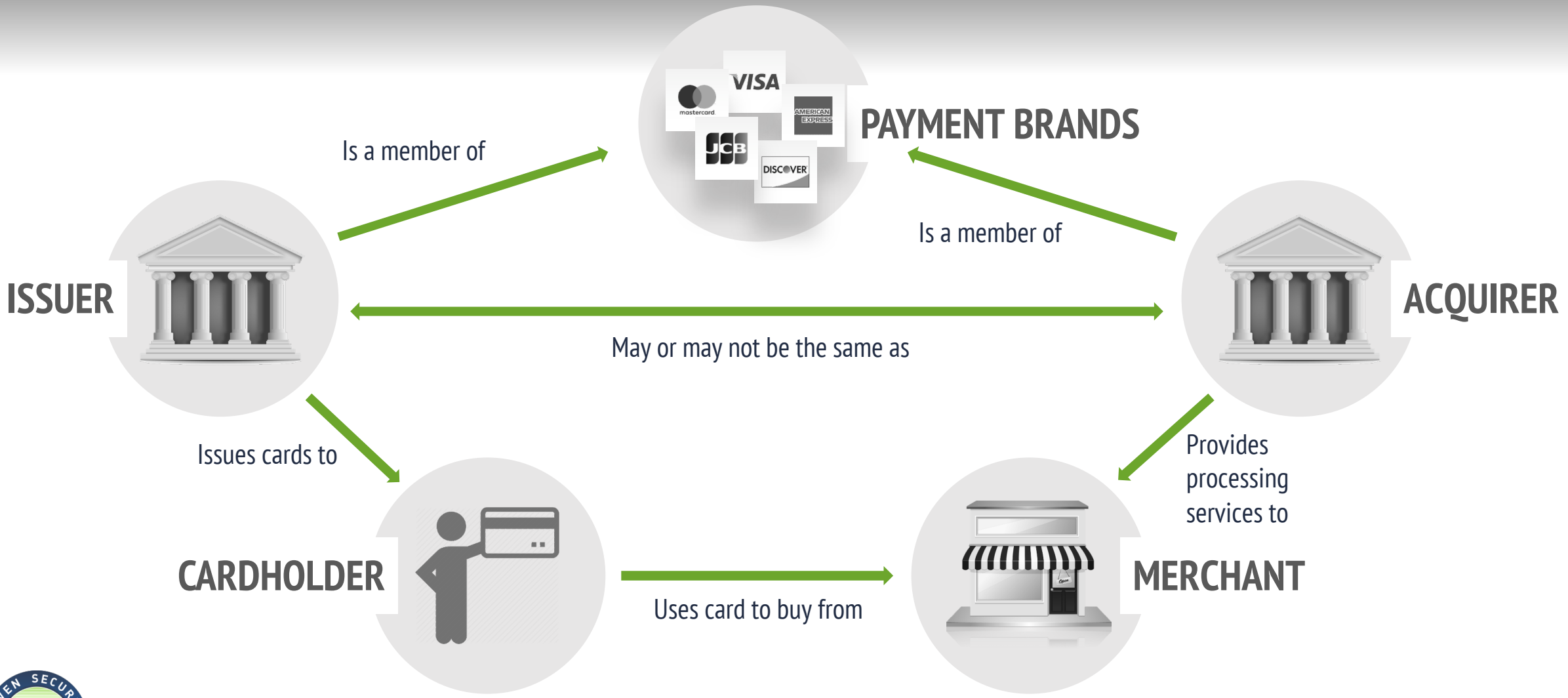
CISA Certified Information Systems Auditor® An ISACA® Certification

CISSP® Certified Information Systems Security Professional

OFFENSIVE security OSCP

C|EH Certified Ethical Hacker

PCI Components Overview



SEVEN SECURITY GROUP

PCI Security Standards Council

The **PCI Security Standards Council (PCI SSC)** is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for card payment data protection.

The **PCI SSC** founding payment brands are:

PCI SSC Resources

- PCI DSS, 3DS, PIN, PA-DSS, SSS, SSLCS, P2PE, PTS (POI, HSM), Card Production and supporting documents
- Registry of QSAs, 3DS-QSAs, QPAs, PCIPs, ASVs, Validated Payment Applications, PTS Devices, P2PE Solutions
- PCI FAQ
- Education & Outreach Programs
- Participating Organization Membership, Community Meetings, Feedback

https://www.pcisecuritystandards.org

PCI Standards Overview

- **PCI DSS:** security of environments that store, process or transmit cardholder data
- **PCI 3DS Core and SDK:** security requirements for entities that perform to provide 3DS Components & security requirements for 3-D Secure Software Development Kits
- **PIN Security:** secure management, processing and transmission of personal identification number (PIN)
- **PCI PA-DSS, SSS, SSLCS:** secure payment software applications and development to support PCI compliance
- **PCI P2PE:** encryption, decryption and key management
- **PCI PTS – POI:** protection of sensitive data at point-of-interaction devices and their secure components
- **PCI PTS – HSM:** physical, logical and device security requirements for securing Hardware Security Modules (HSM)
- **PCI Card Production:** security requirements for systems and business processes involved in card production
- **PCI TSP:** additional requirements for Token Service Providers for EMV Payment Tokens

PCI DSS: Why it's important

SEVERE PENALTIES:

- Security breaches cost a lot
- You can be suspended from processing credit card transactions
- You can face higher processing fees

IN CASE OF A COMPROMISE, NON-COMPLIANT MEMBERS OR THEIR NON-COMPLIANT MERCHANTS OR AGENTS ARE LIABLE TO PAY:

- Non-compliance fine
- Forensic investigation costs
- Dispute resolution costs
- Card re-issuance penalties
- Breach notification costs

Payment Brands Compliance Programs

Payment Brands:

- Have their own compliance program
- Are responsible for the compliance program enforcement
- Define forensic investigations
- Respond to account data compromises

Compliance Programs include:

- Tracking and enforcement
- Penalties, fees, compliance deadlines
- Validation process and who needs to validate
- Approval and posting of compliant entities
- Definition of merchant and service provider levels

PCI DSS

The **Payment Card Industry Data Security Standard (PCI DSS)** was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data.

PCI DSS applies to **all** entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to **all** other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

PCI DSS: The 12 Requirements

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Protect all systems against malware and regularly update antivirus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

PCI DSS: Validation Levels

SERVICE PROVIDERS

ROC by QSA

SAQ (QSA opt.)

MERCHANTS

ROC by QSA

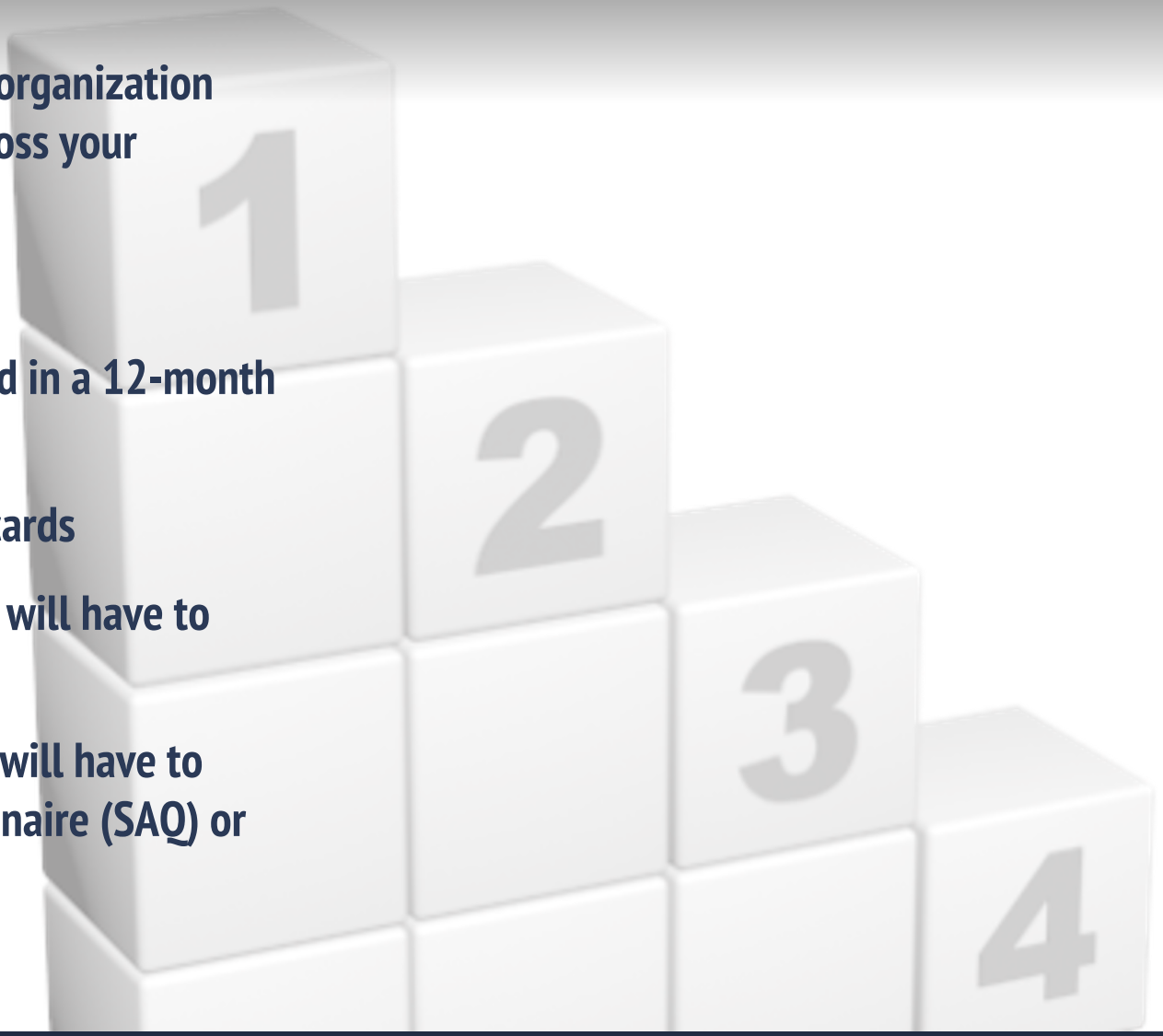
SAQ (QSA opt.)

SAQ

SAQ

PCI DSS

- PCI DSS Compliance is determined based on how your organization stores, processes, and/or transmits cardholder data across your infrastructure
- Compliance is based on "Level" and "Type"
- Level is based on the number of transactions performed in a 12-month period
- Type is defined by how your organization takes credit cards
- Depending on what "Type" of organization you are, you will have to address anywhere from 20 to 360 controls
- Depending on what "Level" of compliance you are, you will have to report your compliance with Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC) by QSA



PCI 3DS Core

The **PCI 3DS Core** security standard defines physical and logical security requirements and assessment procedures for entities that perform or provide the following functions, as defined in the EMV® 3-D Secure Protocol and Core Functions Specification:

- **3DS Server (3DSS)**
- **3DS Directory Server (DS)**
- **3DS Access Control Server (ACS)**

PCI 3DS Core Requirements

Part 1: Baseline Security Requirements:

1. Maintain security policies for all personnel
2. Secure network connectivity
3. Develop and maintain secure systems
4. Vulnerability management
5. Manage access
6. Physical security
7. Incident response preparedness

Part 2: 3DS Security Requirements:

1. Validate scope
2. Security governance
3. Protect 3DS systems and applications
4. Secure logical access to 3DS systems
5. Protect 3DS data
6. Cryptography and key management
7. Physically secure 3DS systems

PCI PIN Security

The **PCI PIN Security** standard contains a complete set of requirements for the secure management, processing, and transmission of personal identification number (PIN) data during online and offline payment card transaction processing at ATMs and point-of-sale (POS) terminals.

- **Identifies minimum security requirements for PIN-based interchange transactions**
- **Outlines the minimum acceptable requirements for securing PINs and encryption keys**
- **Assists all retail electronic payment system participants in establishing assurances that cardholder PINs will not be compromised**

PCI PIN Security Requirements

1. Transaction Processing Operations
2. Normative Annex A – Symmetric Key Distribution using Asymmetric Techniques
3. Normative Annex B – Key-Injection Facilities
4. Normative Annex C – Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms

Reporting Documents

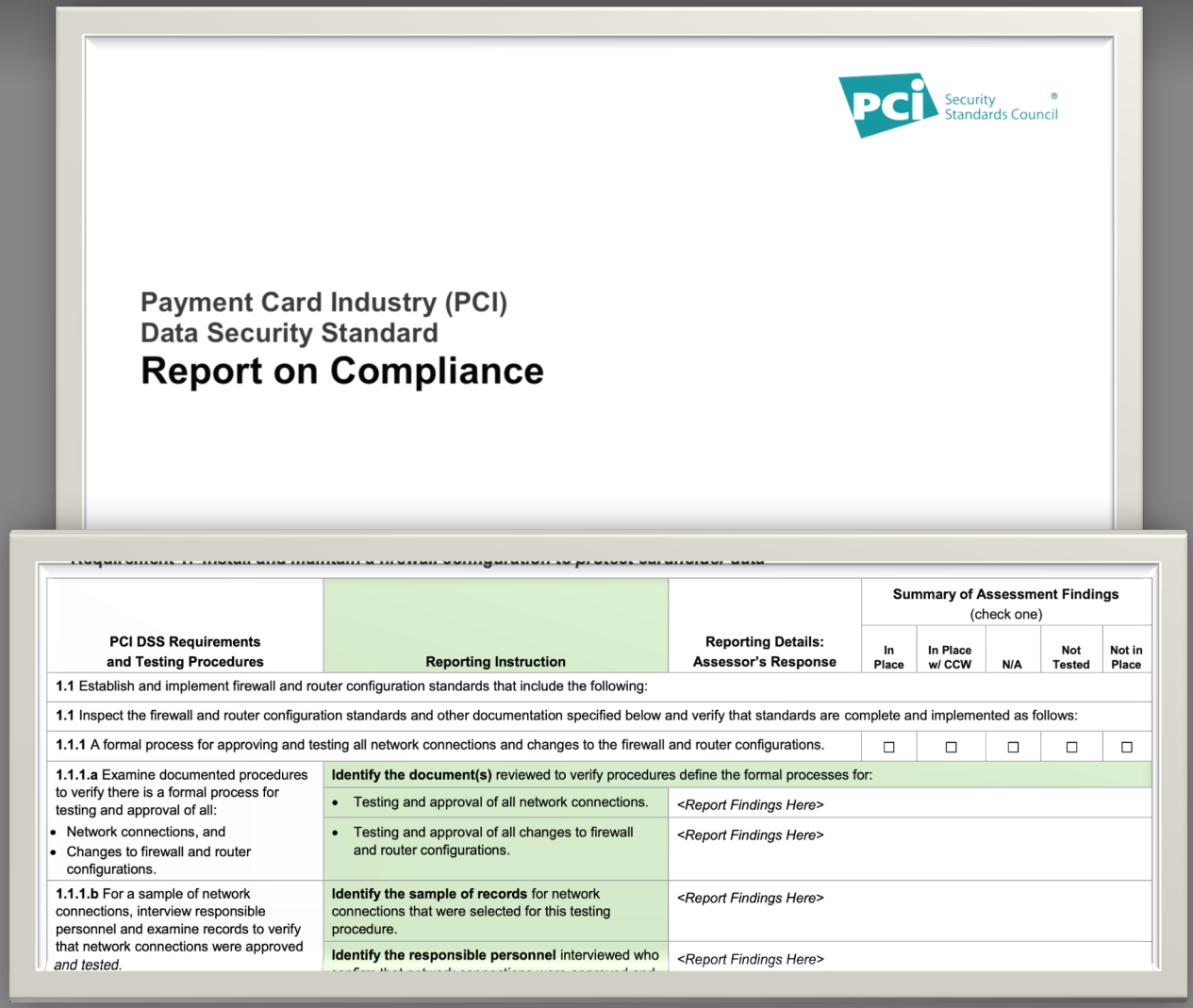
- **Report on Compliance (ROC)**
  Report documenting detailed results from an entity's onsite PCI assessment by QSA, 3DS-QSA or QPA.

- **Self-Assessment Questionnaire (SAQ)**
  Reporting tool used to document self-assessment results from an entity's PCI DSS assessment, QSA can participate.

- **Attestation of Compliance (AOC)**
  Form for merchants and service providers to attest to the results of a PCI assessment, as documented in the Self-Assessment Questionnaire or Report on Compliance.

Reporting Documents: ROC

- Predefined formats
- Produced by QSA, 3DS-QSA or QPA
- Descriptive responses on controls testing
- Involves mandatory on-site assessment
- ROC templates are available in PCI SSC Document Library

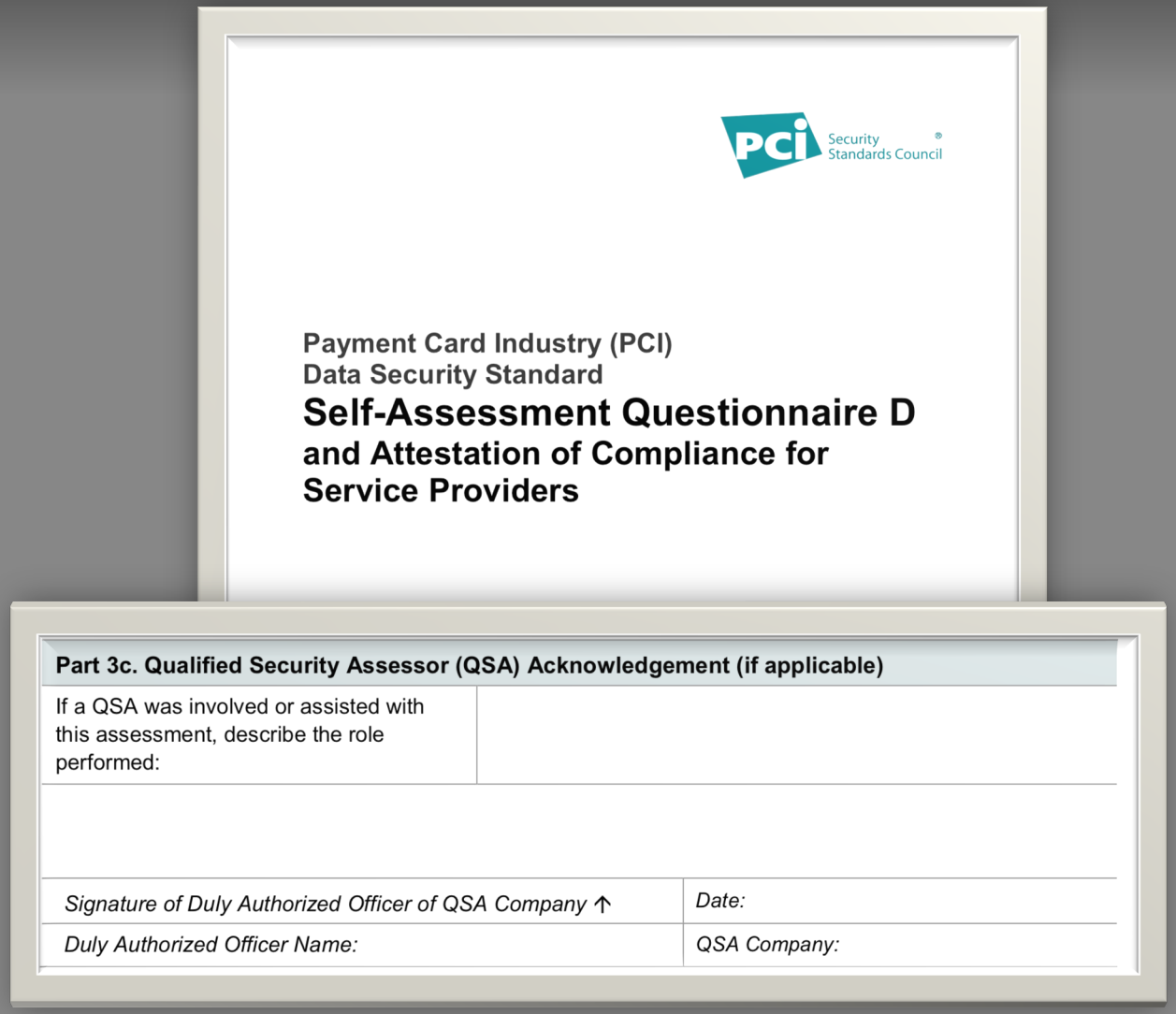


PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.1 Establish and implement firewall and router configuration standards that include the following:							
1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:							
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.			☐	☐	☐	☐	☐
1.1.1.a Examine documented procedures to verify there is a formal process for testing and approval of all: • Network connections, and • Changes to firewall and router configurations.	**Identify the document(s)** reviewed to verify procedures define the formal processes for: • Testing and approval of all network connections.	<*Report Findings Here*>					
	• Testing and approval of all changes to firewall and router configurations.	<*Report Findings Here*>					
1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved *and tested.*	**Identify the sample of records** for network connections that were selected for this testing procedure.	<*Report Findings Here*>					
	Identify the responsible personnel interviewed who	<*Report Findings Here*>					

SEVEN SECURITY GROUP

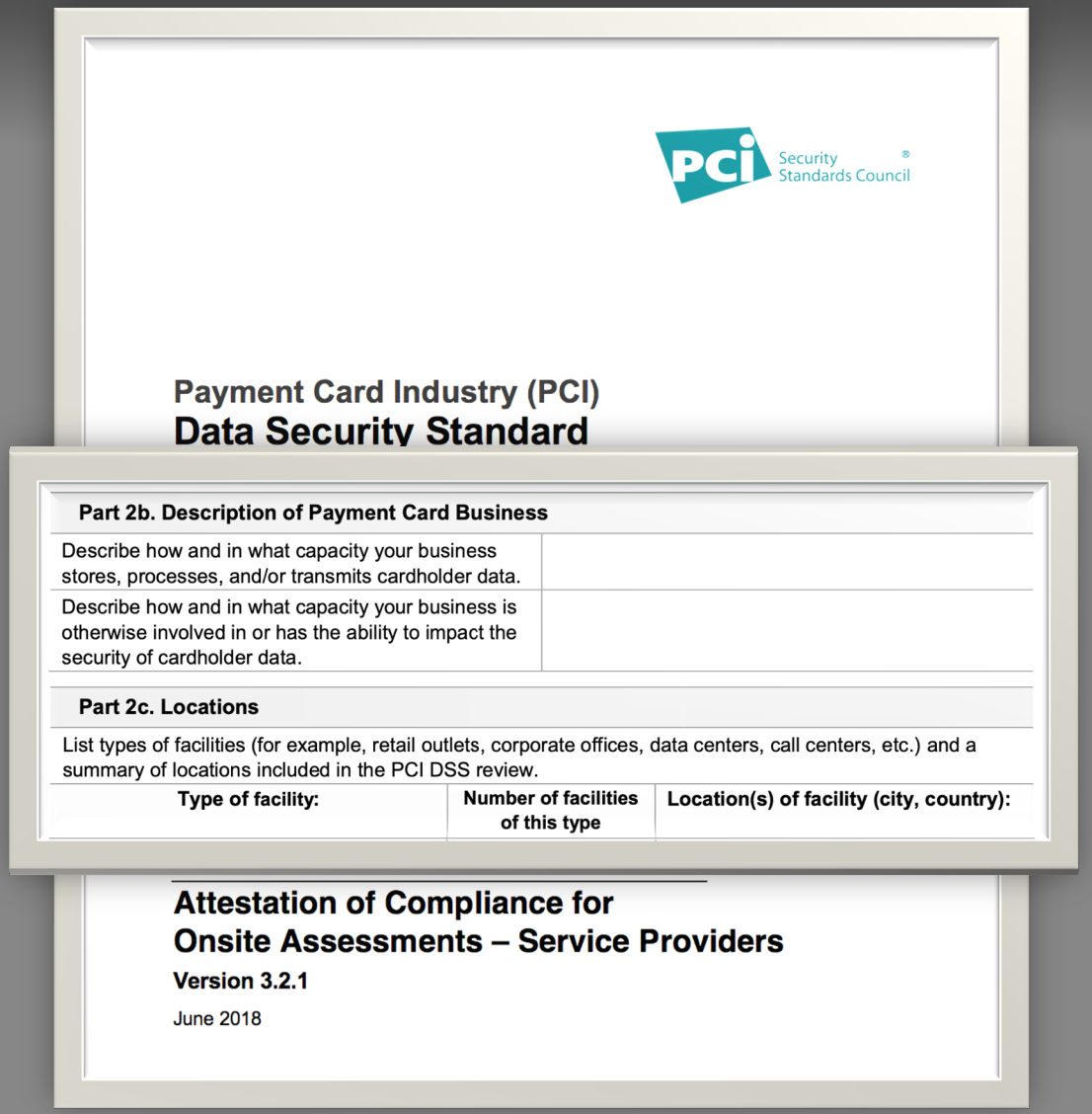
Reporting Documents: SAQ

- SAQ structured in three sections:
  - Section 1: Assessment Information and Executive Summary
  - Section 2: PCI DSS self-assessment questions
  - Section 3: Validation and Attestation Details
- Contains QSA Acknowledgement (if applicable)



Reporting Documents: AOC

- The AOC provides a declaration of the results of a PCI DSS self-assessment or QSA/3DS-QSA/QPA onsite assessment
- An executive officer of the entity signs the AOC, attesting that the information provided in the AOC and the accompanying ROC or SAQ is true and accurate
- The QSA (if used) signs the AOC
- AOC is submitted according to payment brand scheme rules to the requesting entities along with any supporting documentation
- Required for all onsite assessments and SAQs



Reporting Documents: Certificates

SEVEN SECURITY GROUP

PCI DSS: Common Myths

We don't have enough card transactions to require compliance

We outsource card processing so we are compliant

PCI is an IT issue

PCI is unreasonable / difficult

PCI certificate allows us to store card data

We are not a target

SEVEN SECURITY GROUP

SEVEN SECURITY GROUP

Thank you!

Pavel Kaminsky, PCI QSA, CISSP, CISA, CEH

Fintech IT Mentor, the guy Fintech founders call
when they need to implement secure and cost-efficient payment environments
p.kaminsky@7sec.com