PCI Security Standards Council

How to Balance Conflicting Acquiring Bank Objectives

Insights into the conflicting payments, risk and compliance management landscape in the small merchants' segment

Agenda

- Introductions
- Acquiring Bank Conflicting Objectives and Drivers
- Achieving Balance and Managing Risk
- Creating a Seamless and Integrated Merchant Experience
- What Can We Do to Better Serve the SME Merchant Business Community and Wider Payments Industry?
- Takeaways

Daniela Christoffel

Compliance Manager (PCI), Scheme Management
Nexi Group

Natasja Bolton

PCI Compliance and Security Specialist,
VikingCloud

PCI Security Standards Council

slido

Please download and install the
Slido app on all computers you use

Join at slido.com
#EUCM2024

ⓘ Start presenting to display the joining instructions on this slide.

slido

Please download and install the Slido app on all computers you use

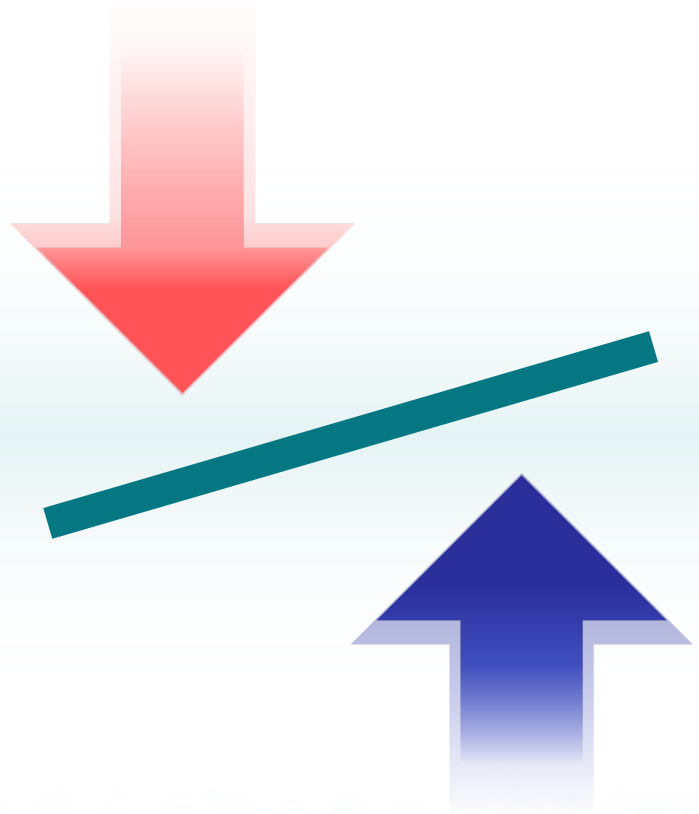
What type of business do you represent and what is your role??

ⓘ Start presenting to display the poll results on this slide.

Acquiring Bank Conflicting Objectives and Drivers

Acquirer obligations

- Require PCI DSS Compliance
- Payment Card Risk Programmes
- Merchant Compliance Management
- Time and Knowledge Gap: Between Technology Release to Market vs. PCI DSS Applicability

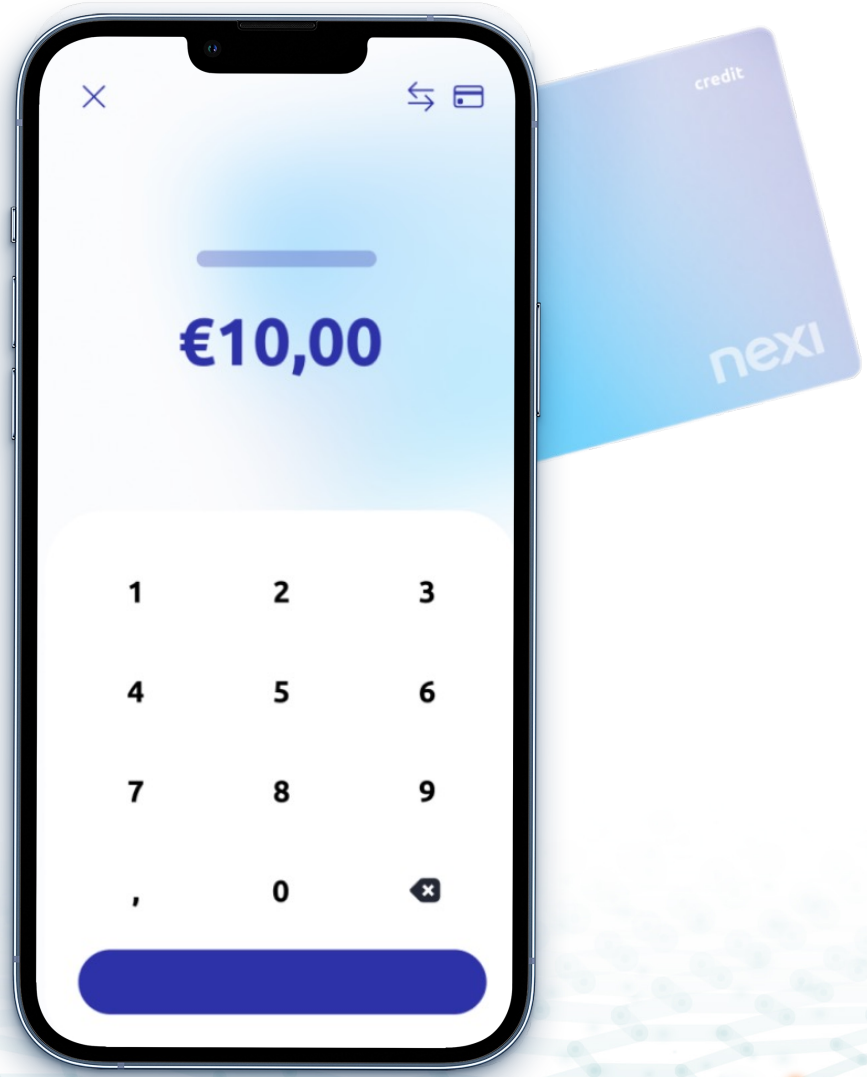


Business Needs / Requirements

- Evolving Technology and Markets
- Merchant and Consumer Expectations and Adoption
- Appropriate Small Merchant Compliance Approach
- Anticipate how PCI DSS applies to emerging technologies

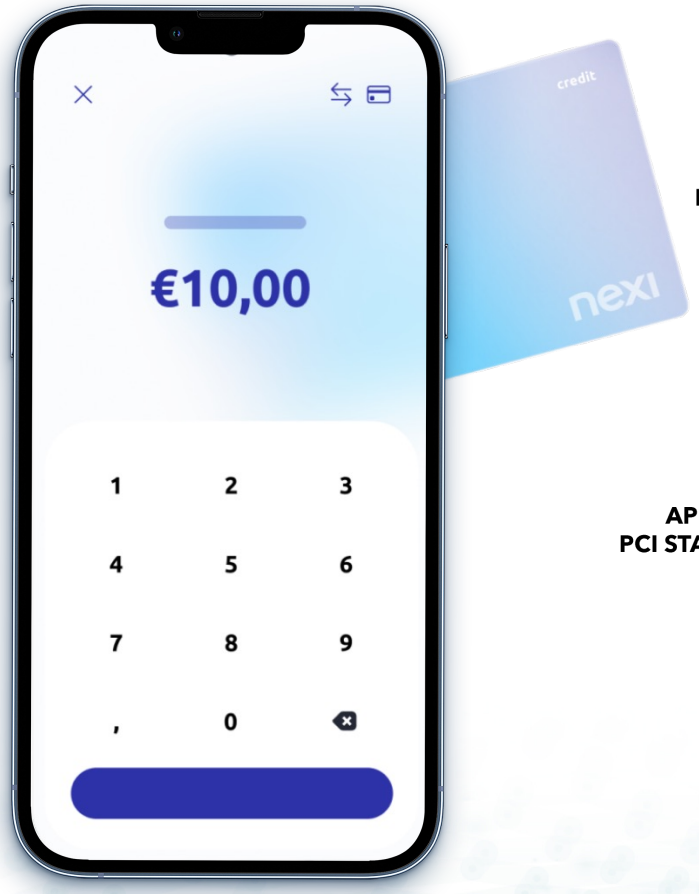
PCI Security Standards Council

Achieving Balance and Managing Risk



PCI Security Standards Council

Achieving Balance and Managing Risk



The PCI Security Standards Ecosystem

PAYMENT PROCESS

- PCI Data Security Standard — **ISSUER** (Cardholder's Bank)
- **CONSUMER**
- PCI Data Security Standard — **MERCHANT**
- PCI Data Security Standard — **ACQUIRER/PROCESSOR** (or Merchant's Bank)
- PCI Data Security Standard — **ISSUER** (Cardholder's Bank)
- **VENDOR**
- **SOLUTION PROVIDER**

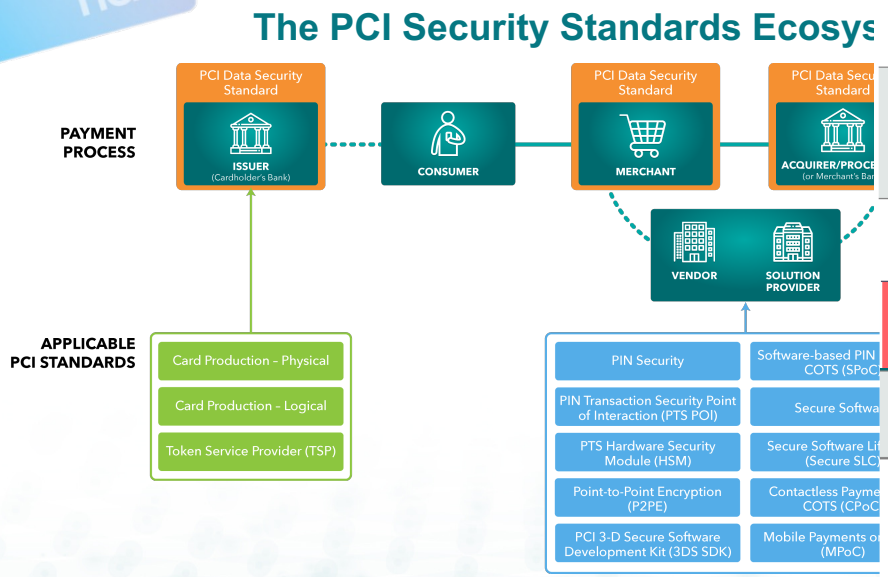
APPLICABLE PCI STANDARDS

- Card Production – Physical
- Card Production – Logical
- Token Service Provider (TSP)
- PIN Security
- Software-based PIN Entry on COTS (SPoC)
- PIN Transaction Security Point of Interaction (PTS POI)
- Secure Software
- PTS Hardware Security Module (HSM)
- Secure Software Lifecycle (Secure SLC)
- Point-to-Point Encryption (P2PE)
- Contactless Payments on COTS (CPoC)
- PCI 3-D Secure Software Development Kit (3DS SDK)
- Mobile Payments on COTS (MPoC)
- PCI 3-D Secure (3DS) Core

Source: https://www.pcisecuritystandards.org/standards/

PCI Security Standards Council®

Achieving Balance and Managing Risk



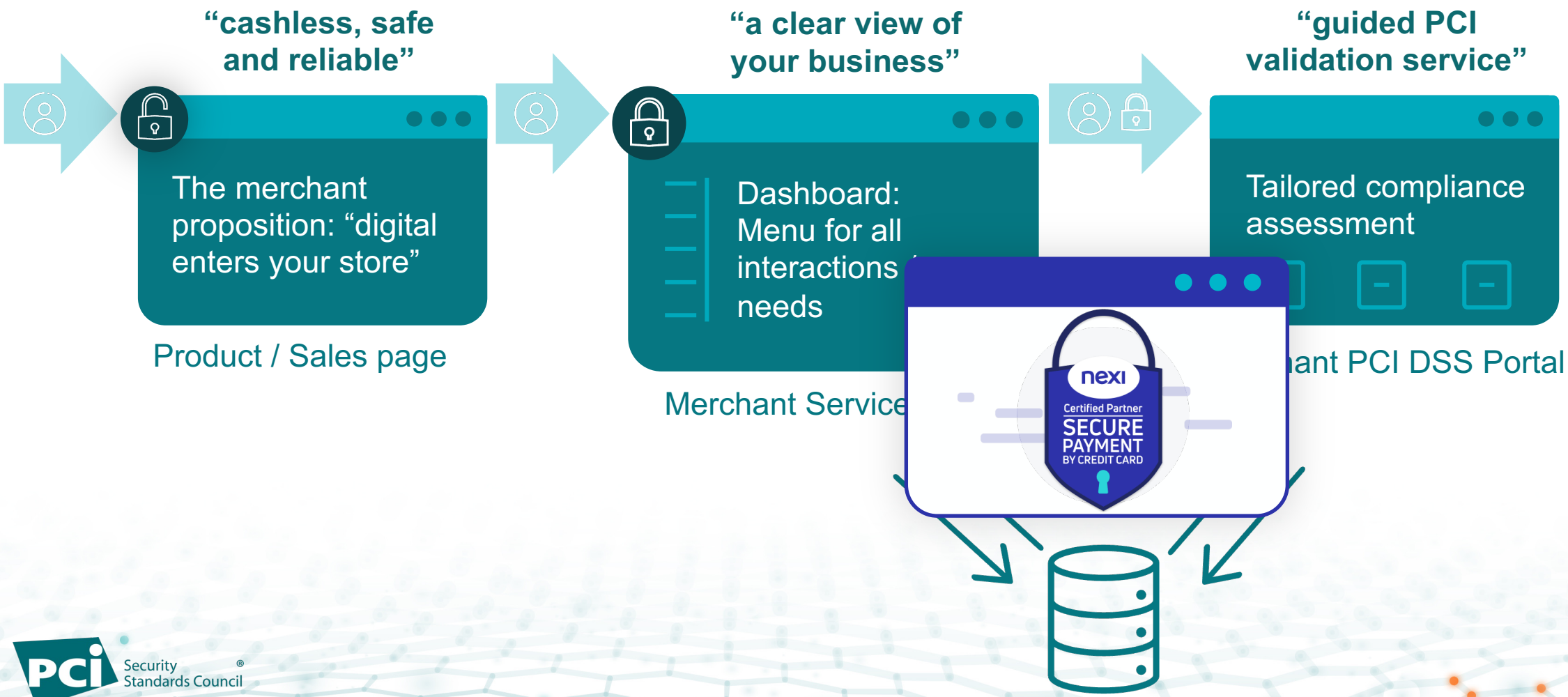
Source: https://www.pcisecuritystandards.org/standards/

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that completely outsource all account data functions to PCI DSS validated and compliant third parties. No electronic storage, processing, or transmission of account data on their systems or premises. *Not applicable to face-to-face channels. Not applicable to service providers.*
A-EP	E-commerce merchants that partially outsource payment processing to PCI DSS validated and compliant third parties, and with a website(s) that does not itself receive account data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the customer's account data. No electronic storage, processing, or transmission of account data on the merchant's systems or premises. *Applicable only to e-commerce channels. Not applicable to service providers.*
B	Merchants using only: ▪ Imprint machines with no electronic account data storage, and/or ▪ Standalone, dial-out terminals with no electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*
B-IP	Merchants using only standalone, PCI-listed approved PIN Transaction Security (PTS) point-of-interaction (POI) devices with an IP connection to the payment processor. No electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*
C-VT	Merchants that manually enter payment account data a single transaction at a time via a keyboard into a PCI DSS validated and compliant third-party virtual payment terminal solution, with an isolated computing device and a securely connected web browser. No electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*
C	Merchants with payment application systems connected to the Internet, no electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*
	No applicable merchant SAQ
P2PE	Merchants using only a validated, PCI-listed Point-to-Point Encryption (P2PE) solution. No access to clear-text account data and no electronic account data storage. *Not applicable to e-commerce channels. Not applicable to service providers.*
SPoC*	Merchants using a commercial off-the-shelf mobile device (for example, a phone or tablet) with a secure card reader included on PCI SSC's list of validated SPoC Solutions. No access to clear-text account data and no electronic account data storage. *Not applicable to unattended card-present, mail-order/telephone order (MOTO), or e-commerce channels.* *Not applicable to service providers.*
D	***SAQ D for Merchants:*** All merchants not included in descriptions for the above SAQ types. *Not applicable to service providers.*

Source: PCI DSS Self-Assessment Questionnaire Instructions and Guidelines, v4.0

PCI Security Standards Council

Creating a Seamless and Integrated Merchant Experience



PCI Security Standards Council

slido

Please download and install the Slido app on all computers you use

What Can We Do to Better Serve the SME Merchant Business Community and Wider Payments Industry?

ⓘ Start presenting to display the poll results on this slide.

Takeaways

Is There a Right Way to ‘Keep Up’?

- **We need to ALL be on the same page**
- **Risk-based approach to small merchant PCI DSS Compliance**
  - Focus on remaining ‘gaps’ instead of secured payment channels
  - Merchant dependencies on TPSPs that can and do impact security of account data but don’t know or accept their PCI DSS obligations
- **Objective-based PCI DSS focused on helping small merchants**
  - Understand **where** and **why** risks need to be managed
  - Recognize the **value** and wider business benefits
  - Enables and supports SME engagement with their TPSPs
- **But…it is an ever-evolving landscape**

PCI Security Standards Council®

nexi

VIKINGCLOUD™

Thank You – Questions?

Daniela Christoffel

Compliance Manager (PCI), Scheme Management
Nexi Group
daniela.christoffel@nexigroup.com

Natasja Bolton

PCI Compliance and Security Specialist,
VikingCloud
natasjabolton@vikingcloud.com