Transitioning to PCI DSS v4.0 at a Large European Merchant

Tomás Perlines, Head of Payment Security,
Schwarz IT KG

PCI Security Standards Council®

SCHWARZ

LIDL

Kaufland

SCHWARZ Produktion

prezero

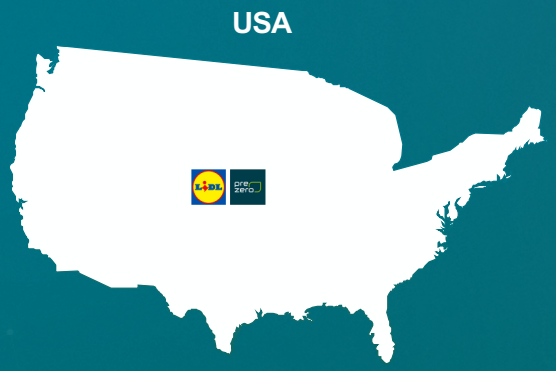
Agenda

1. Schwarz Group at a Glance
2. Transitioning to PCI DSS v4.0

PCI Security Standards Council®

Schwarz Group

Our Presence at a Glance



Represented in 32 countries, Lidl and Kaufland are counting more than

13,350 stores

Approx. 11,900 stores

Approx. 1,450 stores

PCI DSS @ Schwarz

Payment Security into ISMS

No storage of cardholder data

PCI DSS Compliance Process

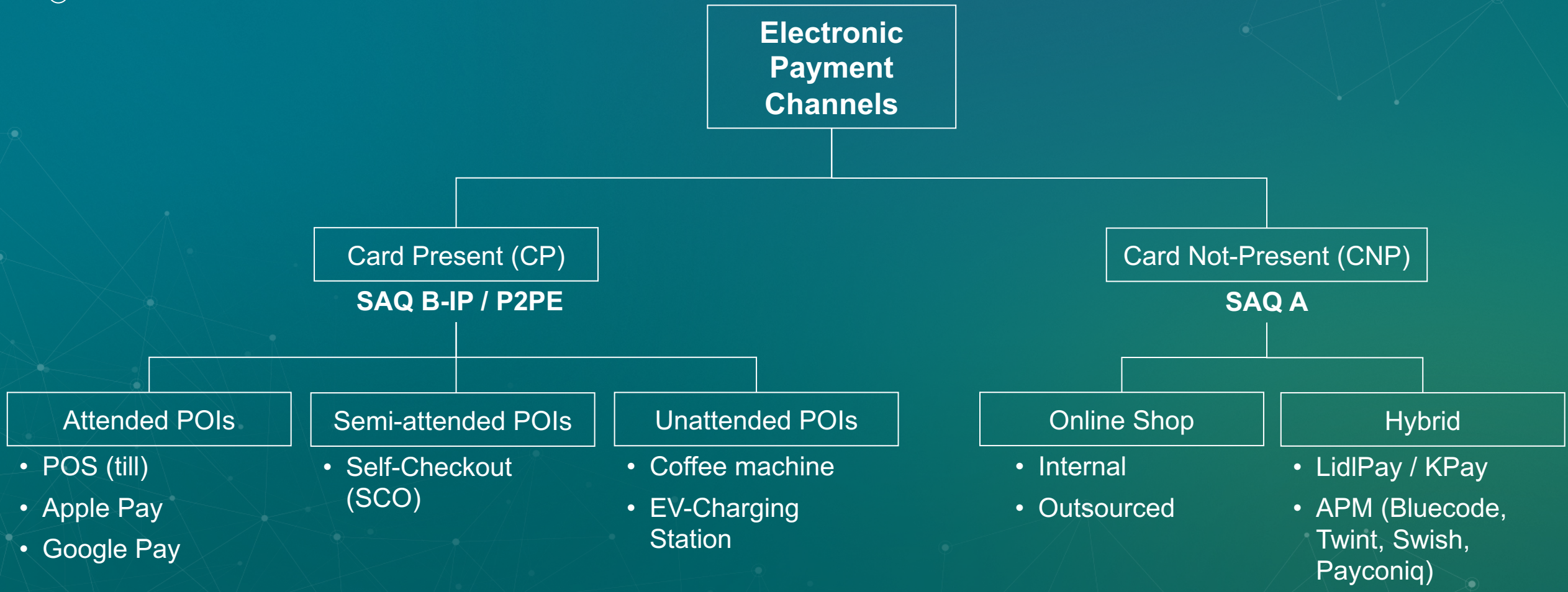
Card-Present Payment Channels

P2PE Solutions

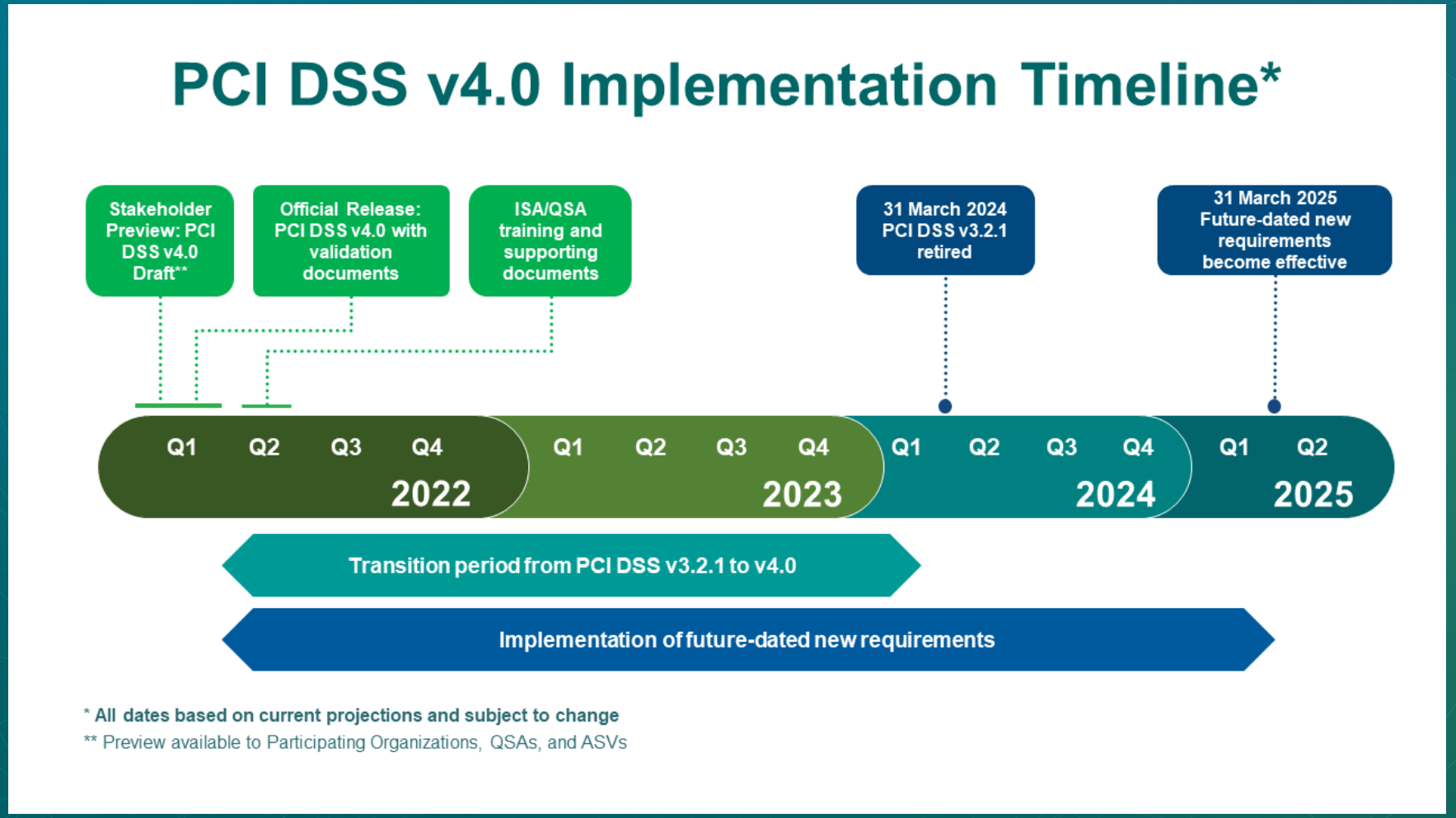
CCTV: No PIN-entry recording

Security Seal for Tethered POI

Payment Channels @ Schwarz



PCI DSS v4.0 Implementation Timeline



Source: PCI SSC

Transitioning to PCI DSS v4.0

Jun 22

Workshops with international QSACs

Jul 22

ISA Training

Taskletter to Local Entities with actions

Sep 22

Start PCI DSS v4.0 with selected payment channels

Mar 24

Transition to PCI DSS v4.0 completed

Support for all payment channels
Exception: Local QSACs

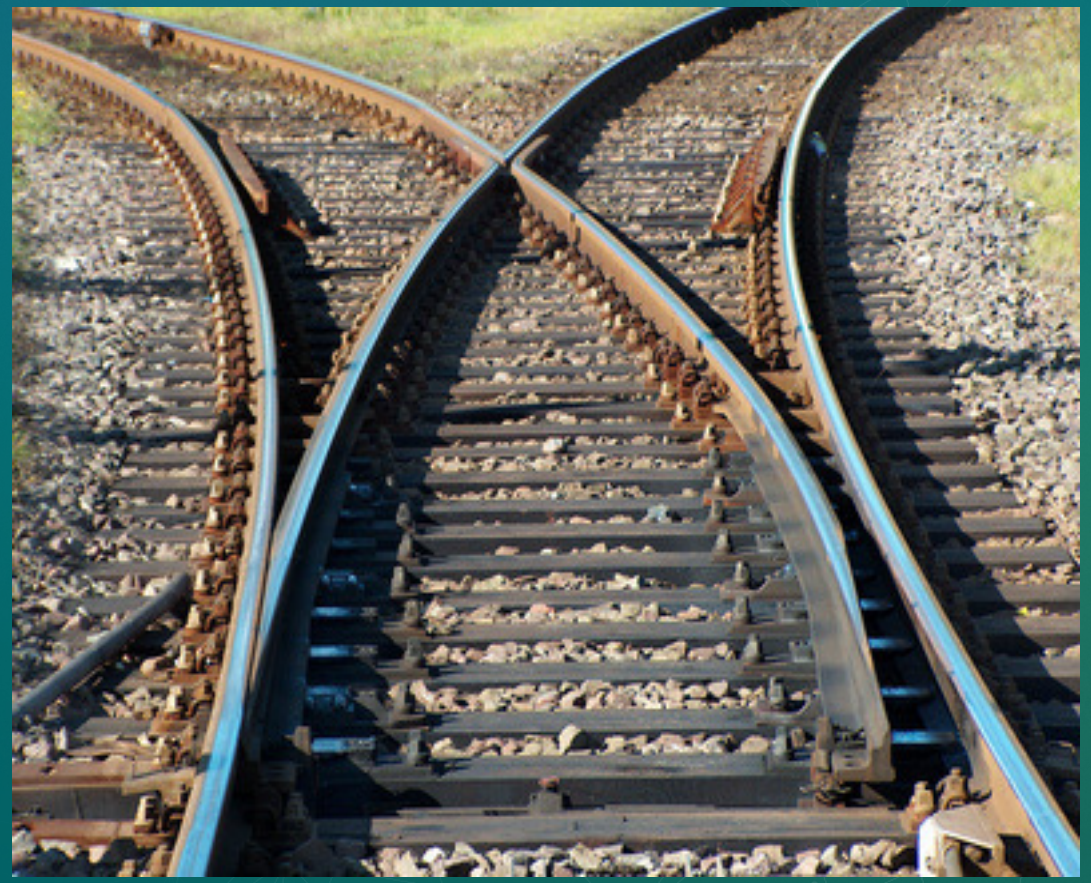
Mar 25

Completion Future Dated Requirements

PCI DSS v4.0 @Schwarz

Challenges

- Changes to Requirements
  - Proper understanding
  - Prioritazion
  - Impact evaluation
- Alignment of timeline
  - Communication to all relevant stakeholders
  - Impact to financial planning process
- Proper implementation according to given timeline



PCI DSS v4.0: What´s new

Validation Methodologies

Defined Validation	Customized Validation

• Assessor assesses according to „Defined Approach Testing Procedures“	• Focuses on the objective of each PCI DSS Requirement
	• Not supported to be used within SAQs, instead RoC shall be used
	• Procedure:
	  • Define and agree „Testing Procedures“ with QSA
	  • Perform „Testing Procedures“ by QSA
	+ Greater Flexibility for re-usage within existing internal control frameworks
	− Higher Costs

PCI DSS v4.0: What´s new

Response Types

Response	When to use this response:
In Place	The expected testing has been performed, and all elements of the requirement have been met as stated.
In Place with CCW (Compensating Controls Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Controls Worksheet (CCW) in Appendix B of this SAQ. Information on the use of compensating controls and guidance on how to complete the worksheet is provided in PCI DSS in Appendices B and C.
In Place with Remediation	The requirement was Not in Place when the expected testing was initially performed, but the merchant addressed the situation and put processes in place to prevent re-occurrence prior to completion of the self-assessment. In all cases of In Place with Remediation, the merchant has identified and addressed the reason the control failed, has implemented the control, and has implemented ongoing processes to prevent re-occurrence of the control failure. All responses in this column require a supporting explanation in Appendix C of this SAQ.
Not Applicable	The merchantrequirement does not apply to the merchant's environment. (See "Guidance for Not Applicable Requirements" below for examples.) All responses in this column require a supporting explanation in Appendix D of this SAQ.
Not Tested	*This response is not applicable to, and not included as an option for, this SAQ.* *This SAQ was created for a specific type of environment based on how the merchant stores, processes, and/or transmits account data and defines the specific PCI DSS requirements that apply for this environment. Consequently, all requirements in this SAQ must be tested.*
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before the merchant can confirm they are in place. Responses in this column may require the completion of Part 4, if requested by the entity to which this SAQ will be submitted. This response is also used if a requirement cannot be met due to a legal restriction. (See "Legal Exception" below for more guidance).

Source: PCI SSC

PCI DSS v4.0 for Card-Present

SAQ B-IP / SAQ P2PE

- Elegibility Criteria: unchanged
- Requirements:
  - Changes without financial impact
  - Documentation must be updated to reflect the new Requirements

- Strategy confirmed to implement certified and listed “P2PE Solutions”

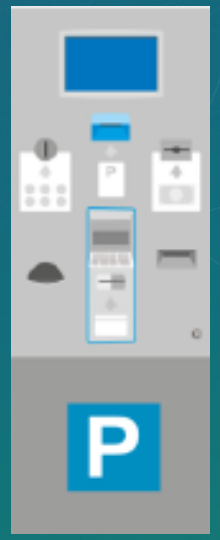
PCI DSS v4.0 for Card-Present

"P2PE Solutions" for the unattended use-case

Various Use Cases

Challenges

P2PE Solutions

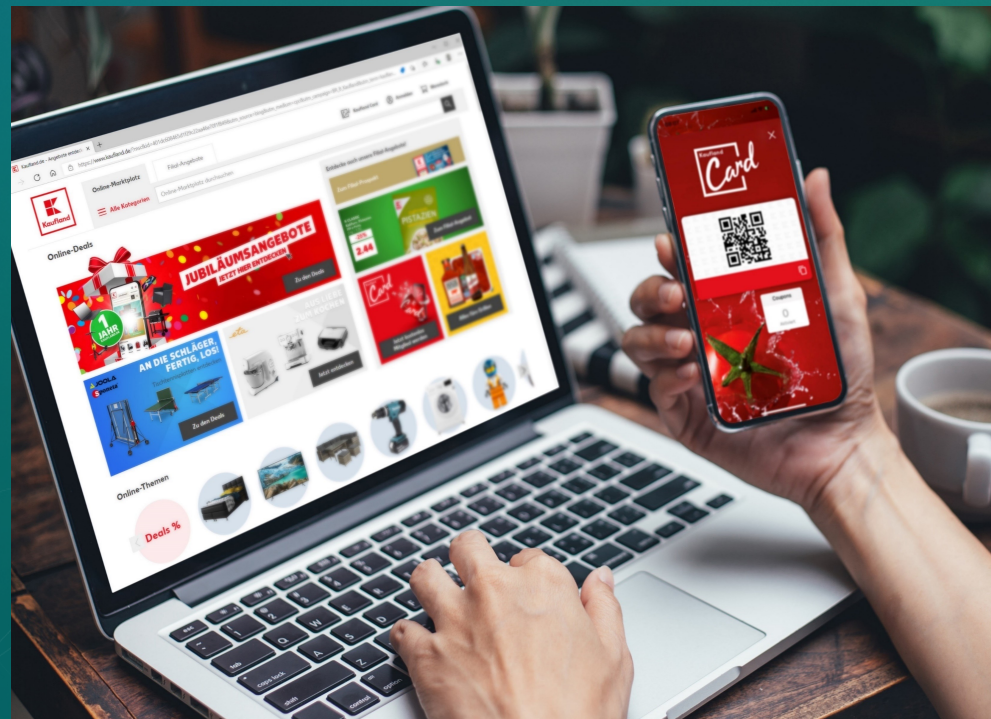


PCI DSS v4.0 for Card-Not-Present

SAQ A

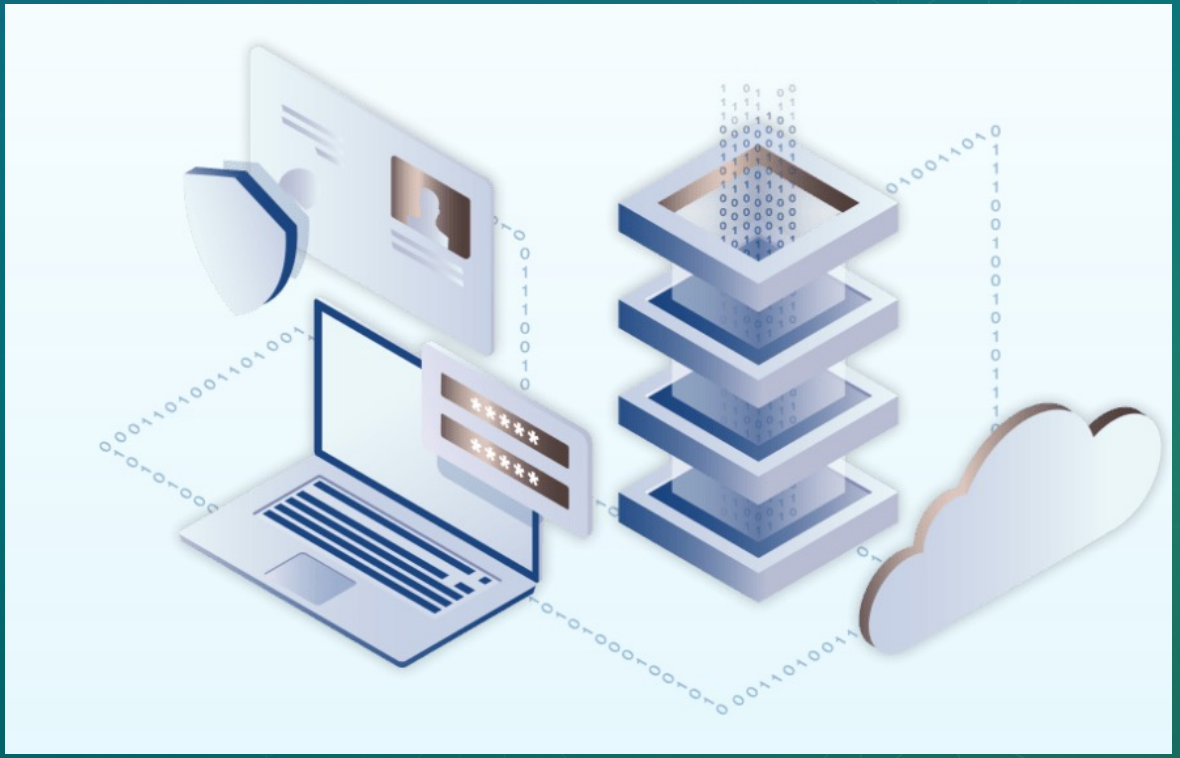
- Elegibility Criteria: unchanged
- Requirements:
  - Future-dated Requirements to be discussed with QSACs and Online-Shops subject-matter experts

- Strategy confirmed to implement entirely outsourced payment processing to PCI DSS compliant third-party service provider (TPSP) / payment processor



Cardholder Data Discovery Scan

- Objective: Provide evidence of no storage of cardholder data
- Initial Scope:
  - POS
  - Supporting systems
- Central scan infrastructure
- Local scan agents



PCI DSS v4.0

Communication

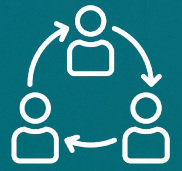
- ✓ Internal communication to be performed regularly
- ✓ External communication to involved parties to be performed regularly
- ✓ Track status of transition to PCI DSS v4.0 by service providers to be performed regularly

Key Takeaways

1

Standardised procedures guarantee the transitioning to PCI DSS v4.0 with optimised effort

2



Strong collaboration between merchant and assessor is key to an efficient assessment procedure

3

Implementation of innovative technologies help reduce the impact to transition to PCI DSS v4.0