PCI DSS v4.0 Highlights

Lauren Holloway, Director, Data Security Standards
PCI Security Standards Council

PCI Security Standards Council®

Inside PCI DSS v4.0

PCI Security Standards Council®

Goals For PCI DSS v4.0

- Ensure the standard continues to meet the security needs of the payments industry
- Add flexibility to support different methodologies being used to achieve security
- Promote security as a continuous process
- Enhance validation methods and procedures

PCI Security Standards Council®

PCI DSS – Introductory Sections

10 Testing Methods

1 Introduction and Overview

5 Best Practices for BAU

7 Descriptions of Timeframes

4 Scope of Requirements

9 Protecting Info about Entity's Security

14 PCI DSS Versions

6 Sampling

13 Additional References

2 Applicability Info

3 Relationship between PCI DSS and PCI SSF Standards

8 Approaches for Implementing and Validating PCI DSS

12 Assessment Process

11 ROC Info

PCI Security Standards Council

PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem

PCI Security Standards Council®

The 12 Requirements Remain

…but read carefully because the wording may have changed

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	1. Install and maintain **network security controls.** 2. **Apply secure configurations to all system components**.
Protect Account Data	3. Protect stored **account data.** 4. Protect cardholder data **with strong cryptography** during transmission over open, public networks.

The 12 Requirements Remain

…but read carefully because the wording may have changed

PCI Data Security Standard – High Level Overview	
Maintain a Vulnerability Management Program	5. Protect all systems **and networks** from malicious software. 6. Develop and maintain secure systems and **software**.
Implement Strong Access Control Measures	7. Restrict access to **system components** and cardholder data by business need to know. 8. Identify users and authenticate access to system components. 9. Restrict physical access to cardholder data.

PCI Security Standards Council ®

The 12 Requirements Remain

…but read carefully because the wording may have changed

PCI Data Security Standard – High Level Overview	
Regularly Monitor and Test Networks	**10.** Log and monitor all access to system components and cardholder data. 11. Test security of systems and networks regularly.
Maintain an Information Security Policy	**12.** Support information security with organizational policies and programs.

PCI Security Standards Council®

PCI DSS Applicability Information

Clarified that PCI DSS is intended for:

- Entities that store, process, or transmit cardholder data and/or sensitive authentication data

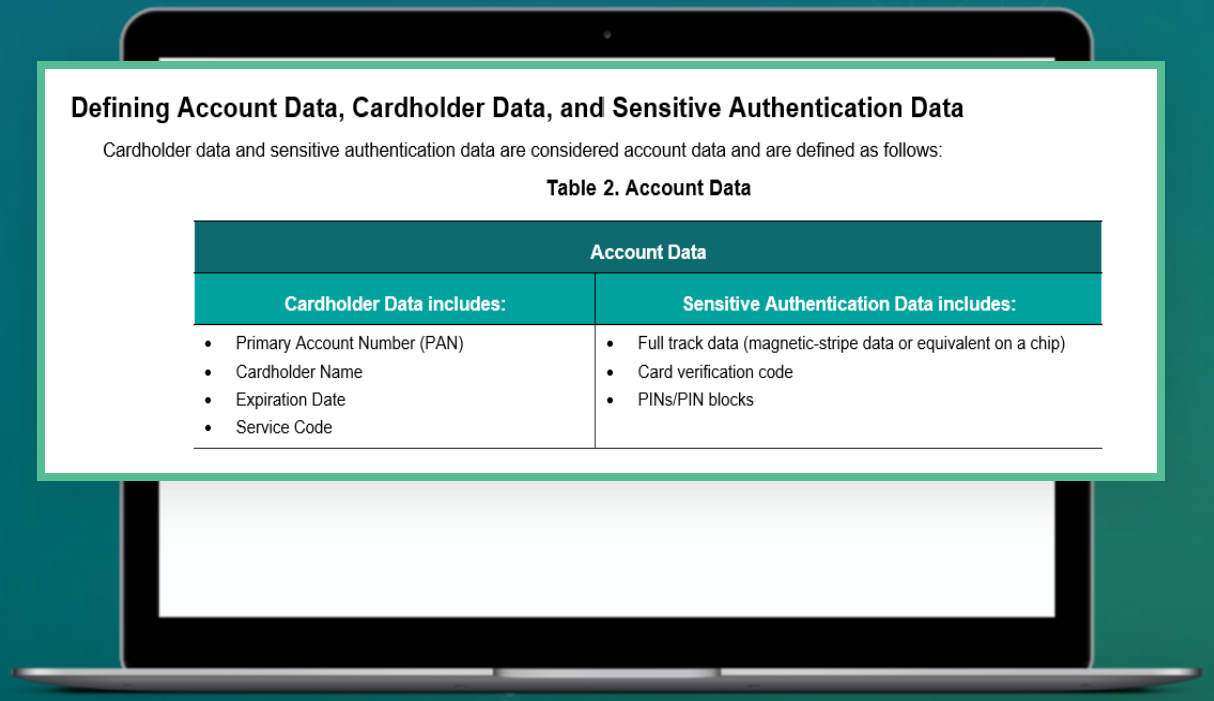
AND

- Entities that could impact the security of the cardholder data environment

PCI Security Standards Council

Does the Organization Store, Process, Or Transmit Primary Account Number?

- **Yes** – A cardholder data environment exists, and PCI DSS requirements apply
- **No** – Some PCI DSS requirements may still apply



Defining Account Data, Cardholder Data, and Sensitive Authentication Data

Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Table 2. Account Data

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

PCI Security Standards Council®

PAN Means PAN…

Use of Account Data, Sensitive Authentication Data, Cardholder Data, and Primary Account Number in PCI DSS

Requirements apply specifically to the data referenced

PCI Security Standards Council®

Relationship Between PCI DSS and PCI SSC's Software Standards

Leveraging the PCI Software Security Framework

- Focuses on software developed and maintained according to the PCI SSF Standards
- Considerations for implementing Requirement 6
- Bespoke and custom software and PCI DSS scope

PCI Security Standards Council®

Scope of PCI DSS Requirements

1. The CDE, comprised of:
   - System components, people, processes that store, process, transmit CHD and/or SAD
   - System components that may not store, process, transmit CHD or SAD but have *unrestricted access* to system components that do store, process, transmit CHD or SAD
2. System components, people, or processes that could impact the security of the CDE

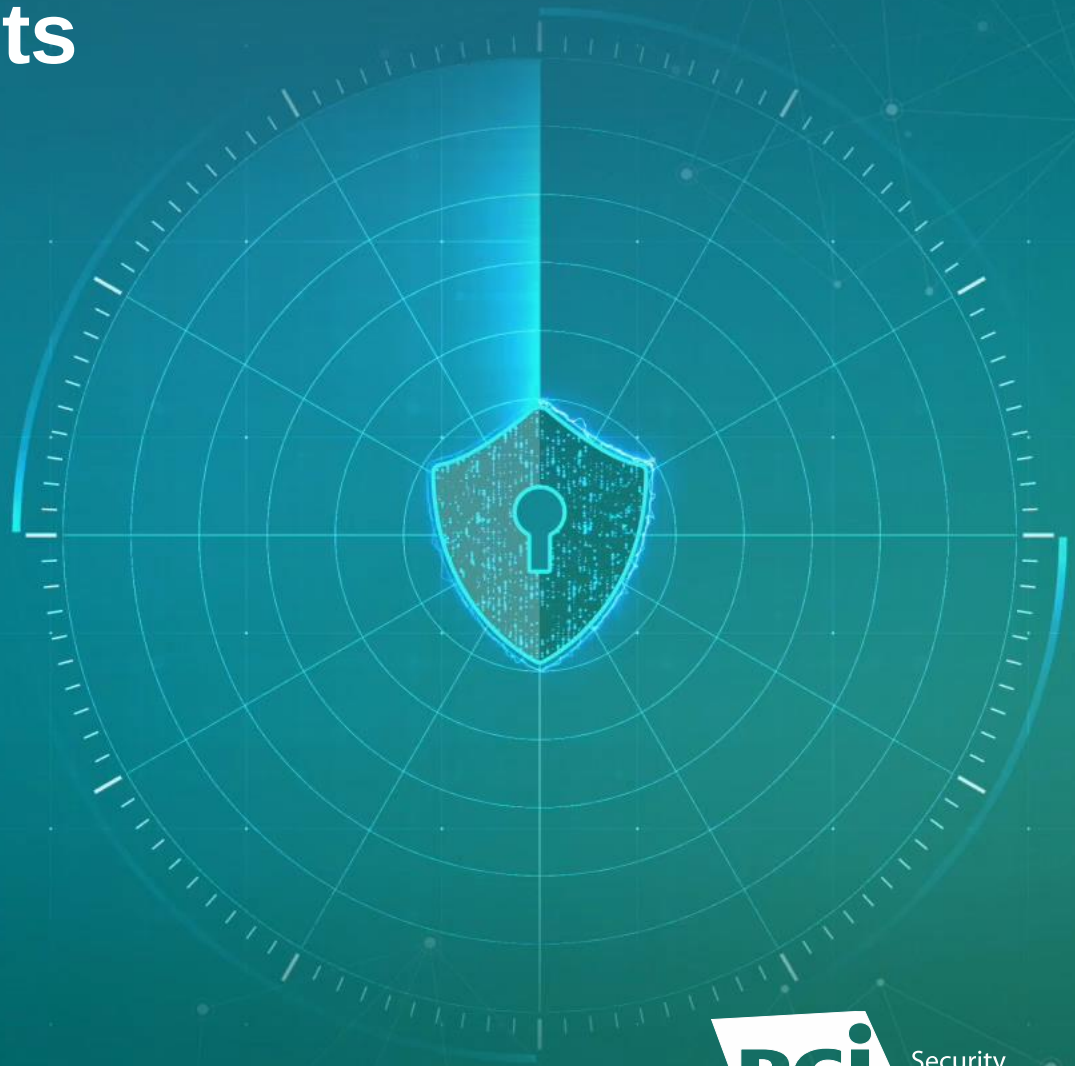
CDE = Cardholder data environment
CHD = Cardholder data
SAD = Sensitive authentication data

PCI Security Standards Council®

Scope of PCI DSS Requirements

Includes numerous sub-sections with valuable information

- Wireless
- Encrypted Cardholder Data and Impact on PCI DSS Scope
- Encrypted Cardholder Data and Impact to PCI DSS Scope for TPSPs
- Use of Third-Party Service Providers



PCI Security Standards Council®

Third-Party Service Providers (TPSPs)

Use of Third-Party Service Providers

- Use of TPSPs and the Impact on Customers Meeting PCI DSS Requirement 12.8.
- Impact of Using TPSPs for Services that Meet Customers' PCI DSS Requirements.
- Options for TPSPs to Validate Compliance for TPSP Services that Meet Customers' PCI DSS Requirements.
- TPSPs Presence on a Payment Brand List(s) of PCI DSS Compliant Service Providers.

PCI Security Standards Council

Third-Party Service Providers (TPSPs)

Use of Third-Party Service Providers

- Use of TPSPs and the Impact on Customers Meeting PCI DSS Requirement 12.8.
- Impact of Using TPSPs for Services that Meet Customers' PCI DSS Requirements.
- Options for TPSPs to Validate Compliance for TPSP Services that Meet Customers' PCI DSS Requirements.
- TPSPs Presence on a Payment Brand List(s) of PCI DSS Compliant Service Providers.

PCI Security Standards Council®

Third-Party Service Providers (TPSPs)

Use of Third-Party Service Providers

- Use of TPSPs and the Impact on Customers Meeting PCI DSS Requirement 12.8.
- Impact of Using TPSPs for Services that Meet Customers' PCI DSS Requirements.
- Options for TPSPs to Validate Compliance for TPSP Services that Meet Customers' PCI DSS Requirements.
- TPSPs Presence on a Payment Brand List(s) of PCI DSS Compliant Service Providers.

PCI Security Standards Council

Third-Party Service Providers (TPSPs)

Use of Third-Party Service Providers

- Use of TPSPs and the Impact on Customers Meeting PCI DSS Requirement 12.8.
- Impact of Using TPSPs for Services that Meet Customers' PCI DSS Requirements.
- Options for TPSPs to Validate Compliance for TPSP Services that Meet Customers' PCI DSS Requirements.
- TPSPs Presence on a Payment Brand List(s) of PCI DSS Compliant Service Providers.

PCI Security Standards Council

For Assessors: Sampling for PCI DSS Assessments

Enhanced sampling guidance for assessors

- Sampling is an option if there are large numbers of items in a population to be tested
- Review 100% of a population if automated processes can quickly and effectively perform testing

Select the sample without undue influence from the assessed organization

PCI Security Standards Council®

Description of Timeframes Used in PCI DSS Requirements

Outlines the frequency expected for timeframes called out in PCI DSS requirements

- Perform activities as close to the specified interval without exceeding it
- Considerations for organizations when defining frequencies for periodic activities
- Describes processes for an organization to detect and address if a scheduled activity is missed

PCI Security Standards Council®

Approaches for Implementing and Validating PCI DSS

Two approaches for implementing and validating PCI DSS

Defined Approach

Follows current PCI DSS requirements and testing procedures

Provides a defined method for meeting security objectives

PCI Security Standards Council®

Section 8: Approaches for Implementing and Validating PCI DSS

Two approaches for implementing and validating PCI DSS

Defined Approach

Follows current PCI DSS requirements and testing procedures

Provides a defined method for meeting security objectives

Customized Approach (NEW)

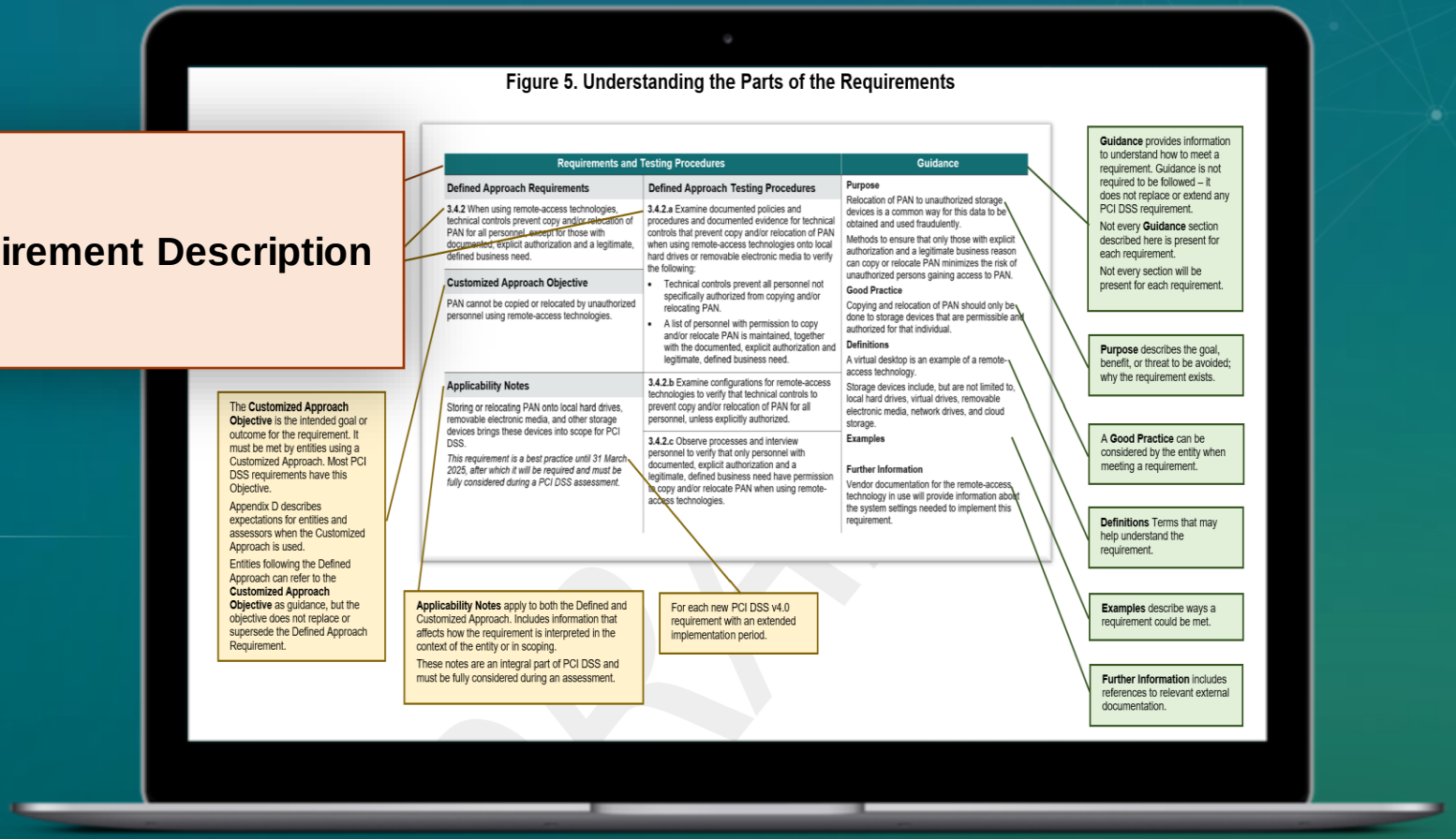
Focuses on the objective of each PCI DSS requirement

Provides greater flexibility for entities using different ways to achieve security

PCI Security Standards Council

The “Explainer”

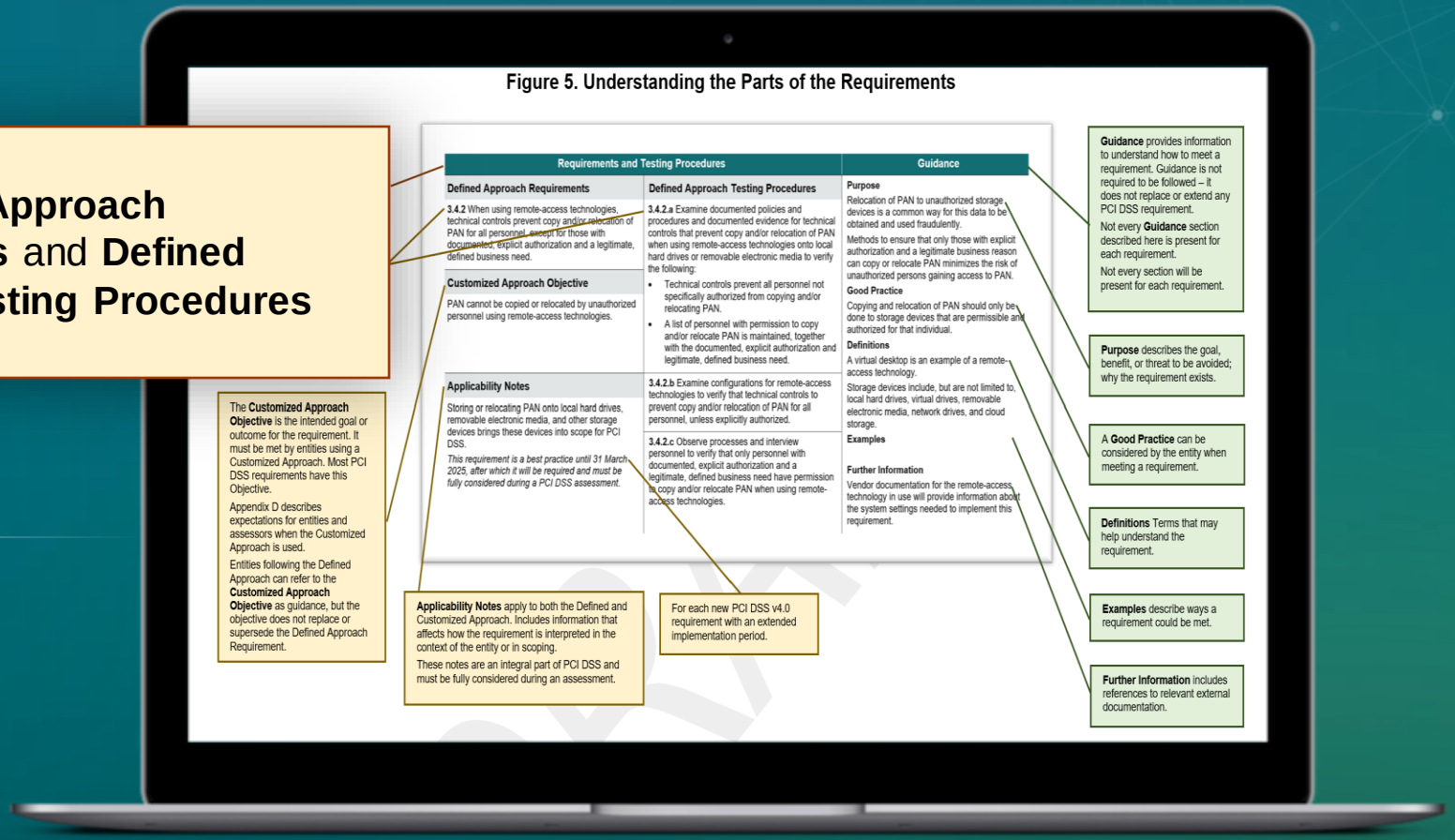
The **Requirement Description**



PCI Security Standards Council®

The “Explainer”

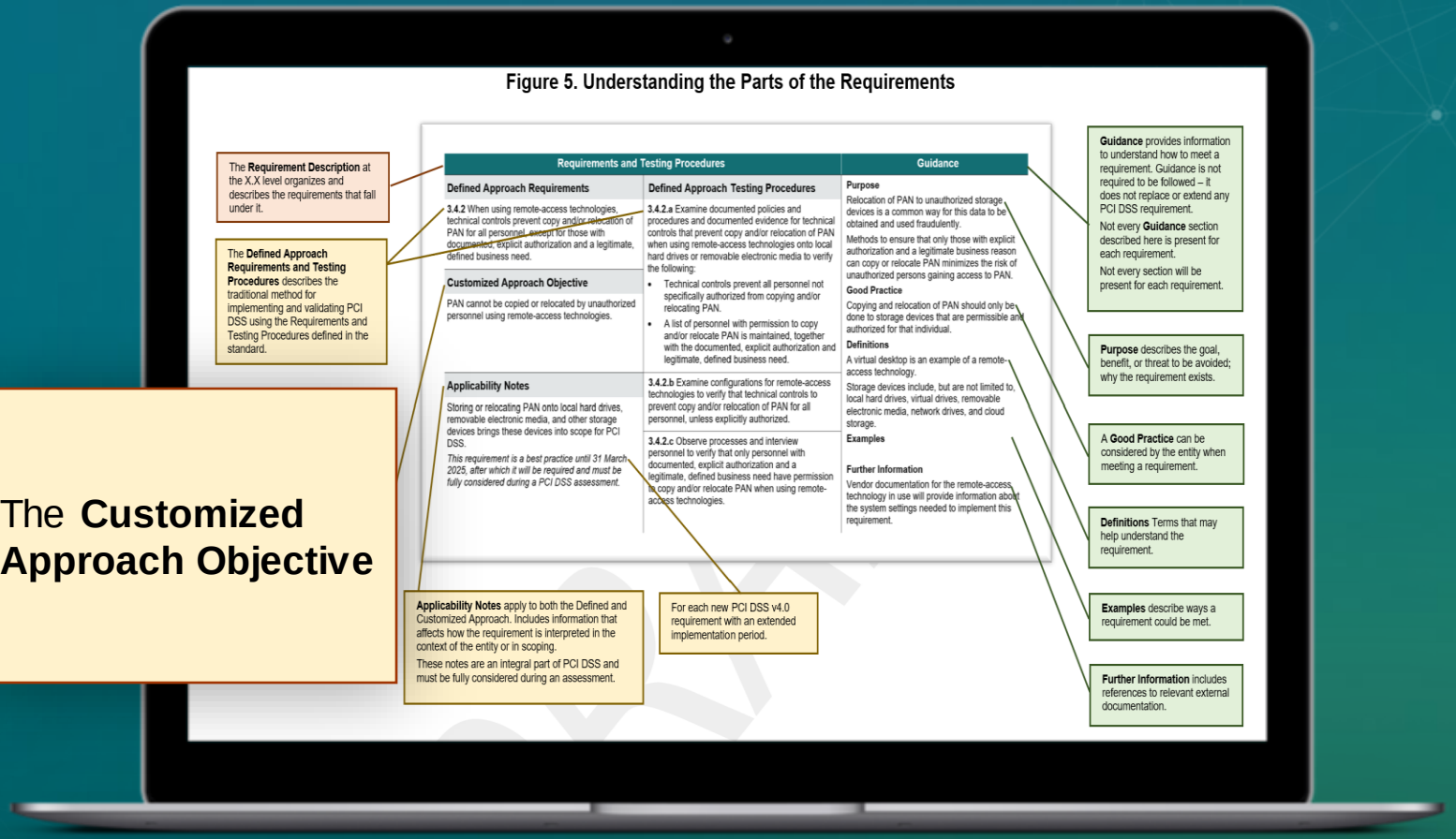
The **Defined Approach Requirements** and **Defined Approach Testing Procedures**



PCI Security Standards Council®

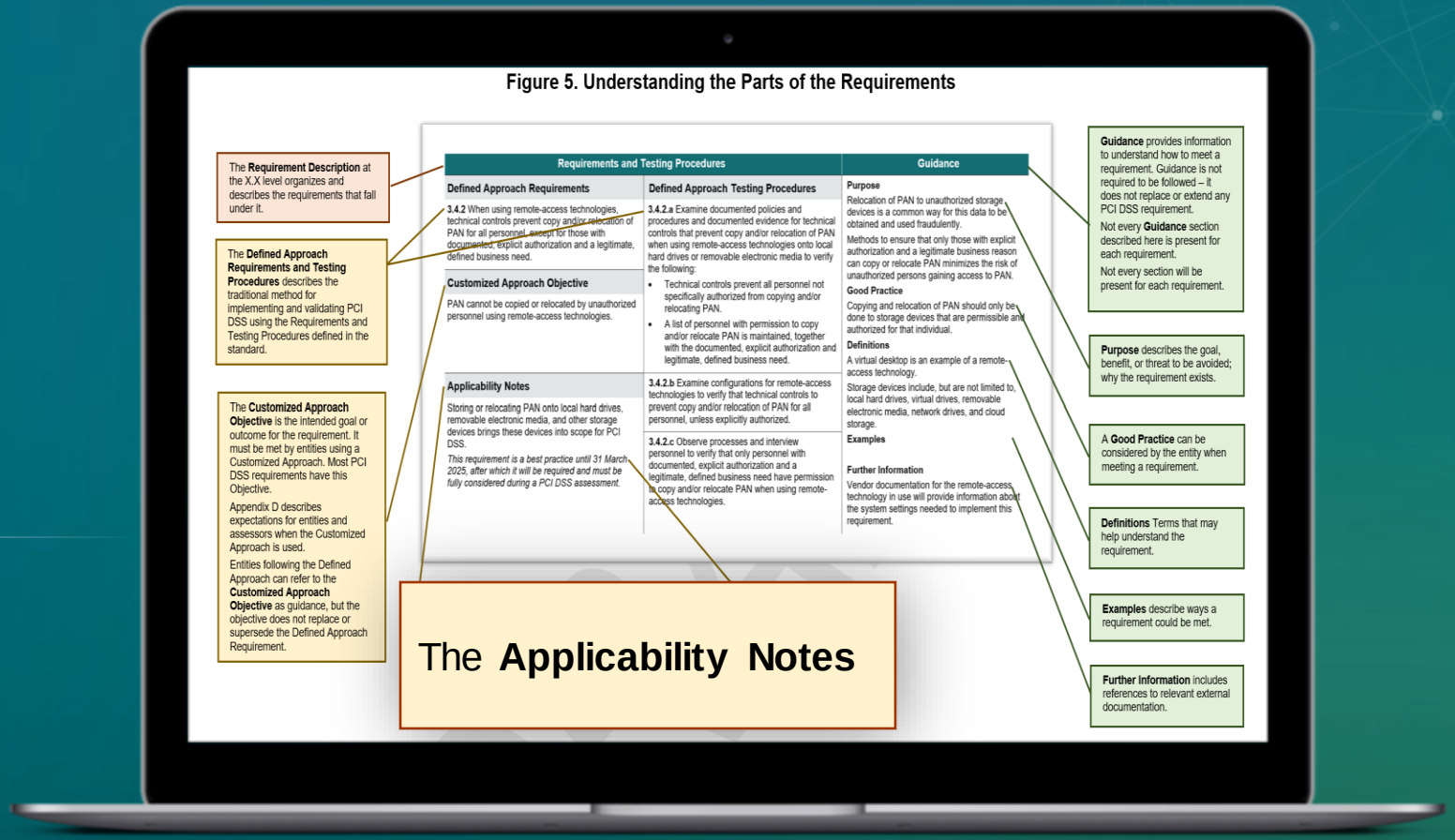
The “Explainer”

The **Customized Approach Objective**



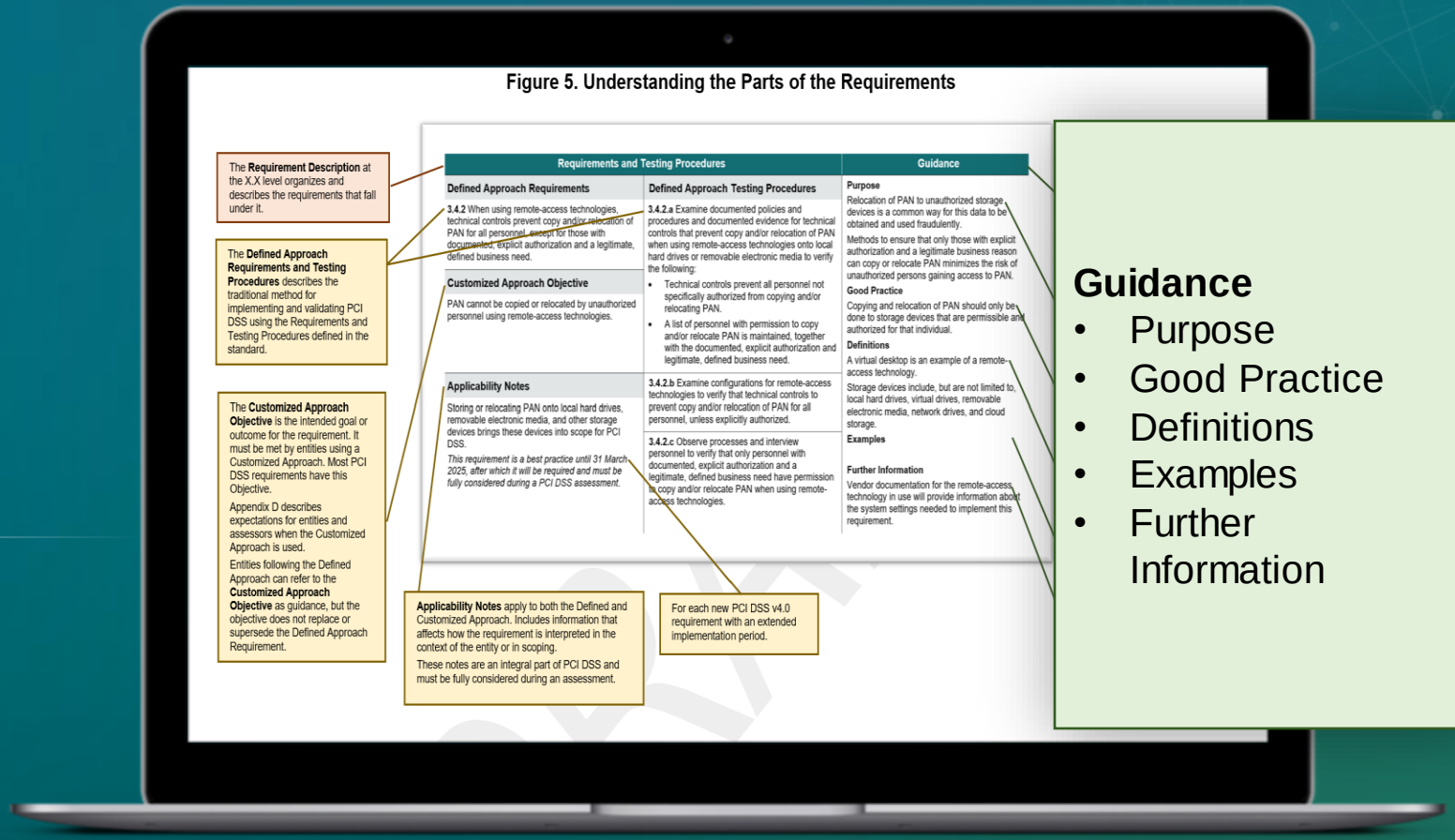
PCI Security Standards Council®

The “Explainer”



PCI Security Standards Council®

The “Explainer”

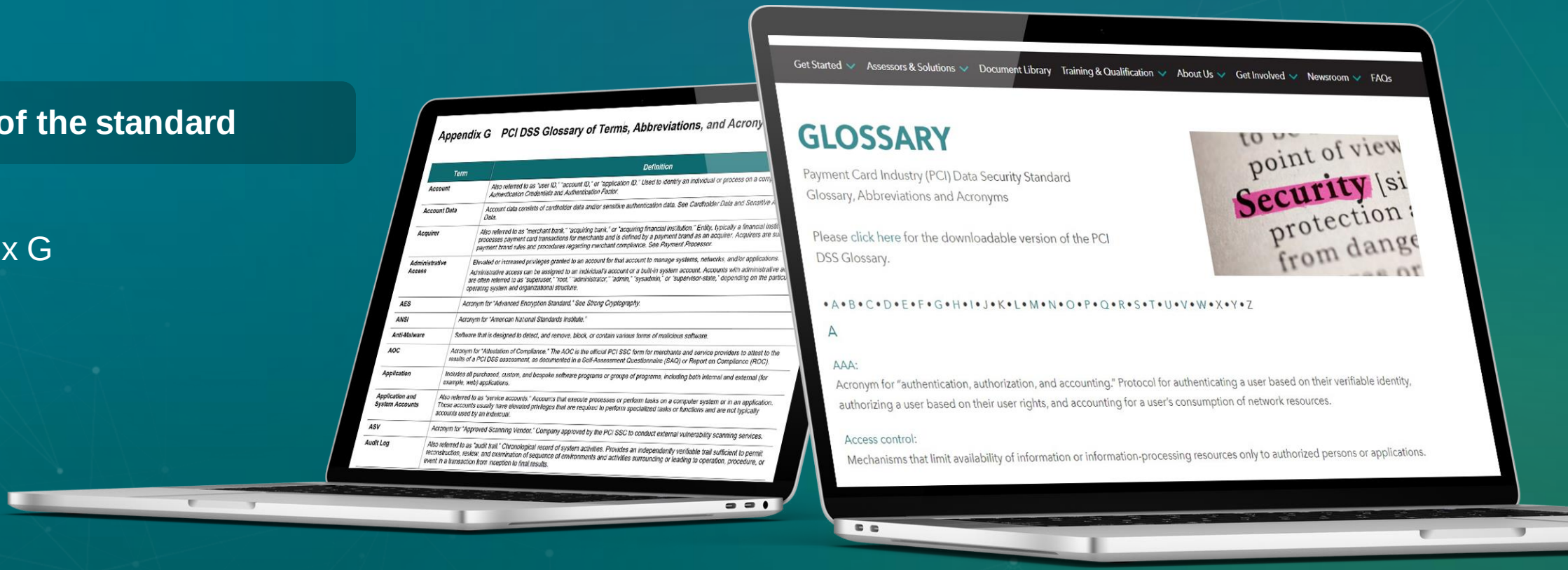


Security Standards Council®

The PCI DSS Glossary

Now part of the standard

In Appendix G



PCI Security Standards Council®

Requirements: What's New and Exciting?

Joel Weisz, Manager, Emerging Standards,
PCI Security Standards Council
Kandyce Young, Standards Manager, Data Security Standards,
PCI Security Standards Council

PCI Security Standards Council®