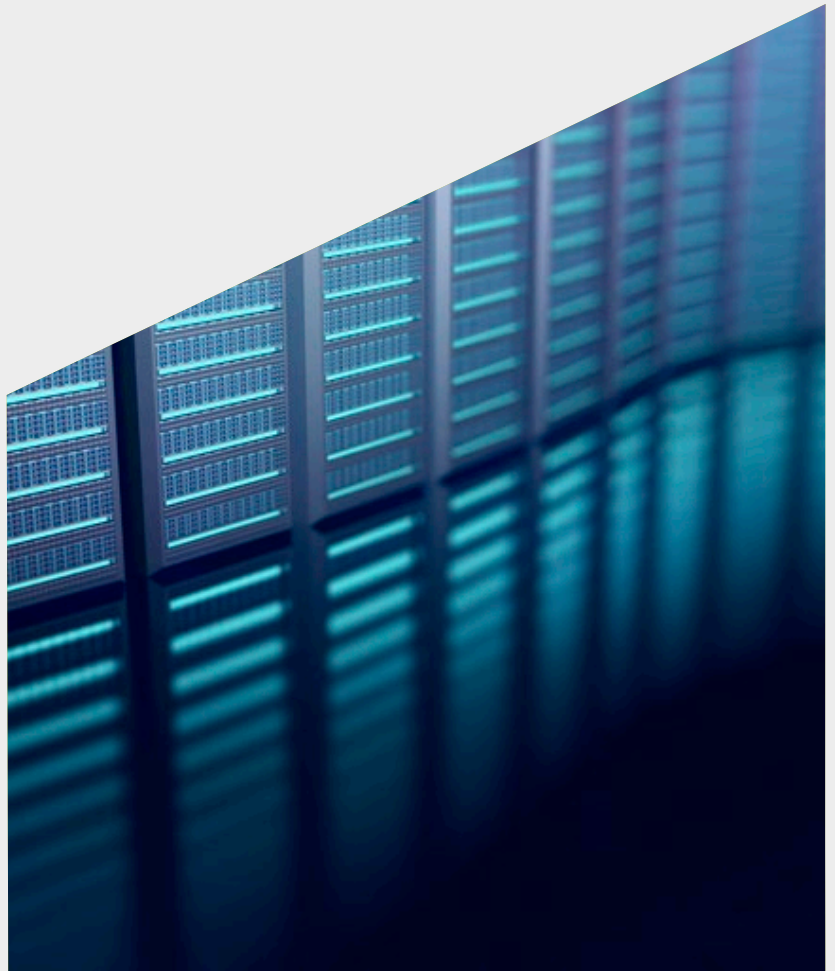
McDermott Will & Emery

PCI DSS 4.0

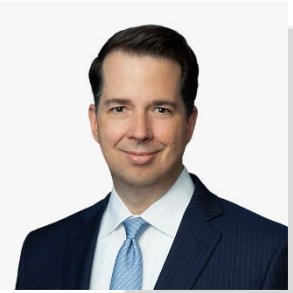
Everything You Need to Know About The Transformational Changes Required of Your Business



May 3, 2022

mwe.com

SPEAKERS



TODD MCCLELLAND

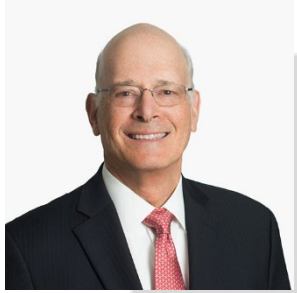
McDermott Will & Emery

Partner
tmcclelland@mwe.com

ALAN GUTIERREZ-ARANA

RSM US

Principal
Alan.gutierrezarana@rsmus.com



MARK SCHREIBER

McDermott Will & Emery

Senior Counsel
mschreiber@mwe.com

ROBERT DUFFY

McDermott Will & Emery

Counsel
reduffy@mwe.com

BRIAN LONG

McDermott Will & Emery

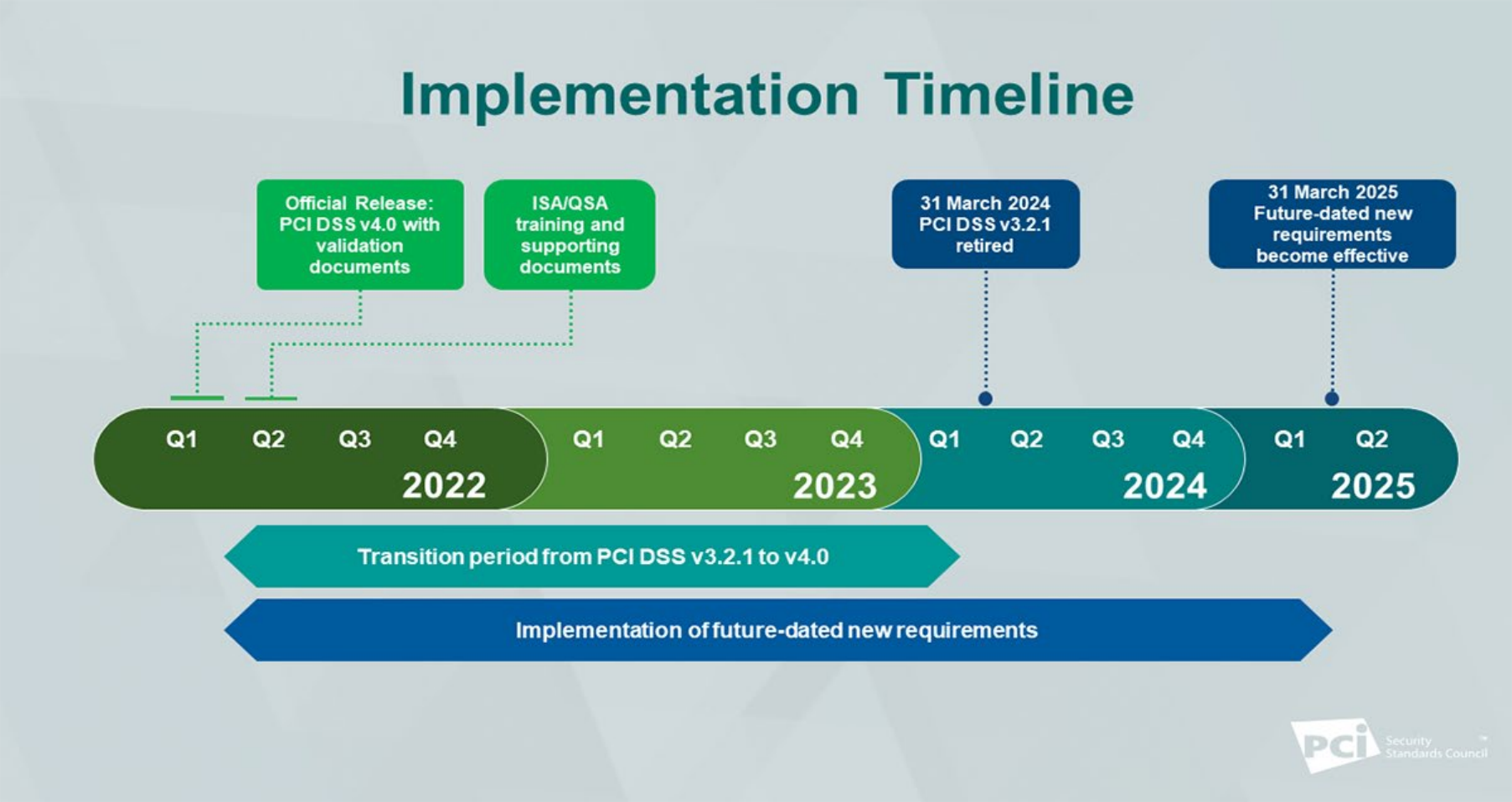
Associate
brlong@mwe.com

AGENDA

- Introduction / Overview
- Key Changes
- Legal Risks
- Closing Thoughts
- Q&A

KEY CHANGES IN PCI DSS 4.0

PCI DSS VERSION 4.0 TIMELINE

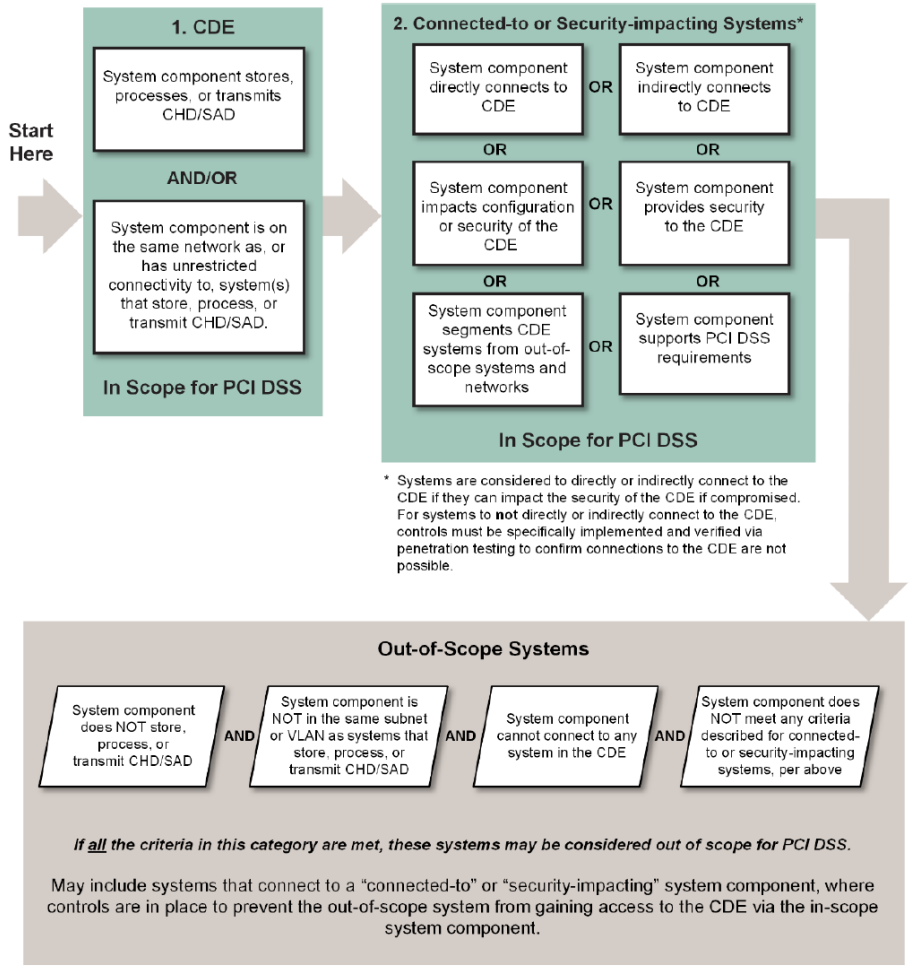


SUGGESTED PREPARATION

- Near Term: Perform a PCI DSS 4.0 Readiness Assessment
- Do a practice run:
  - Before March 31, 2023, perform an assessment of new/updated PCI DSS 4.0 controls along with PCI DSS 3.2.1 efforts
  - Remediate any deficiencies with PCI DSS 4.0 required practices
  - Develop any controls using a Customized Approach
- Before March 31, 2024: Perform first ROC/SAQ using PCI DSS 4.0 and perform additional gap assessment against Best Practice Controls
- Before March 31, 2025: Perform next ROC/SAQ using PCI DSS 4.0 and include PCI DSS Best Practice Controls

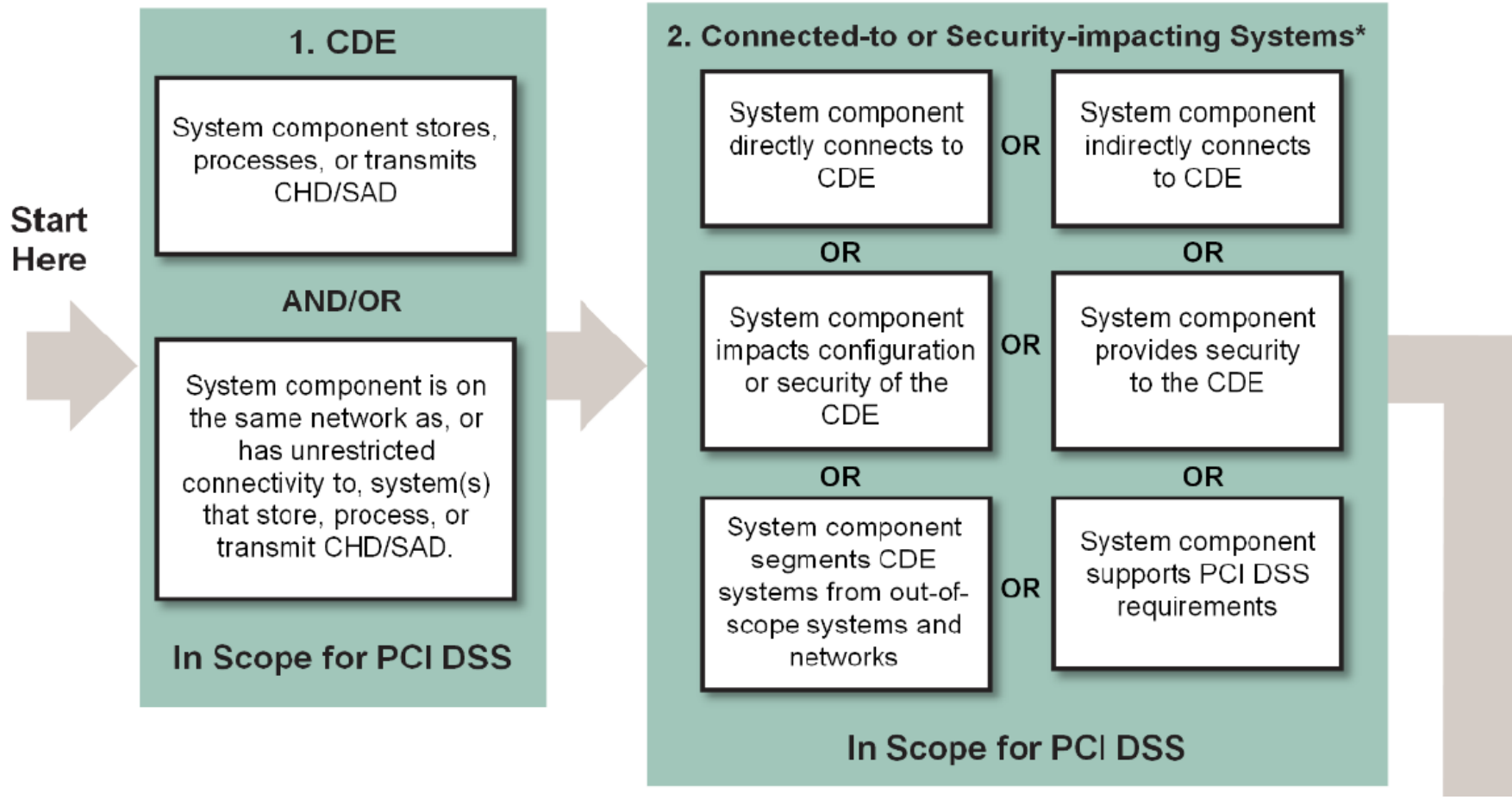
PCI APPLICABILITY AND SCOPE CLARIFICATIONS

- Applicability updated to explicitly include organizations who could impact the security of the CDE (even entities who are not processing) (p. 4)
- Scope of PCI DSS Requirements clarified (p. 9):
  - CDE, which includes:
    - System components, people, and processes that store, process, and transmit cardholder data or SAD; and
    - System components that may not store, process or transmit CHD/SAD but have unrestricted connectivity to system components that store process or transmit CHD/SAD; and
  - System components, people, and processes that could impact the security of the CDE
- Assessed entity must annually confirm PCI Scope (p. 12, req 12.5.2)



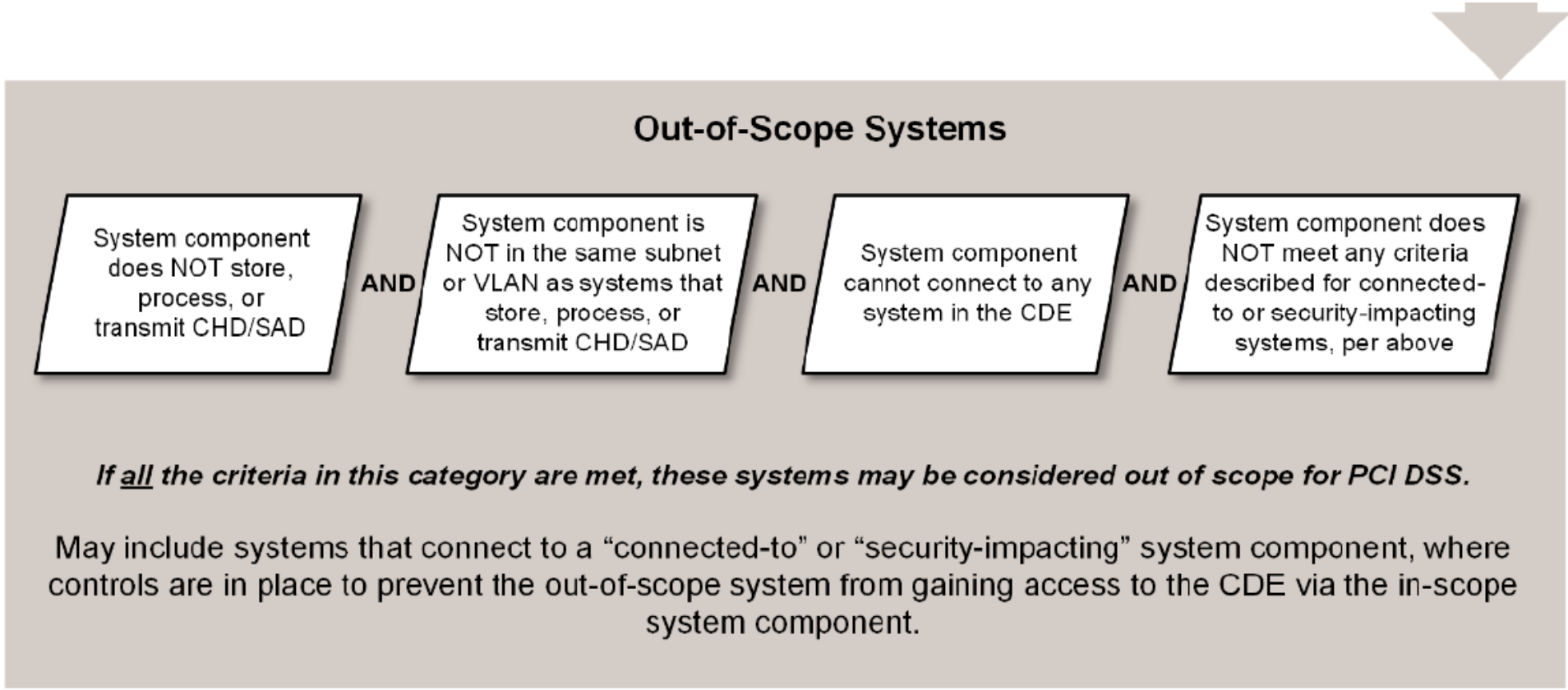
Graphic sourced from PCI DSS 4.0, page 11

PCI APPLICABILITY AND SCOPE CLARIFICATIONS (CONT.)



Graphic sourced from PCI DSS 4.0, page 11

PCI APPLICABILITY AND SCOPE CLARIFICATIONS (CONT.)



Graphic sourced from PCI DSS 4.0, page 11

PCI APPLICABILITY AND SCOPE CLARIFICATIONS (CONT.)

- Network segmentation clarified: out-of-scope systems cannot impact the security of any in scope system components (p. 13)
  - If this test fails, the entire network is in scope

- Wireless scans required "even when wireless is not used within the CDE and the entity has a policy that prohibits the use of wireless technology" (p. 14, req. 11.2.1)

PCI APPLICABILITY AND SCOPE CLARIFICATIONS (CONT.)

- Encrypted data scope clarifications: channels used to capture the data, encrypt the data and systems that are on the same network segment as the decryption key are all in scope (pp. 14-15)

- Service providers that can affect the security of the CDE, now explicitly in scope (p. 16)
  - For example, a loyalty provider who connects to a POS is in scope

UPDATED “SIGNIFICANT CHANGE” GUIDANCE

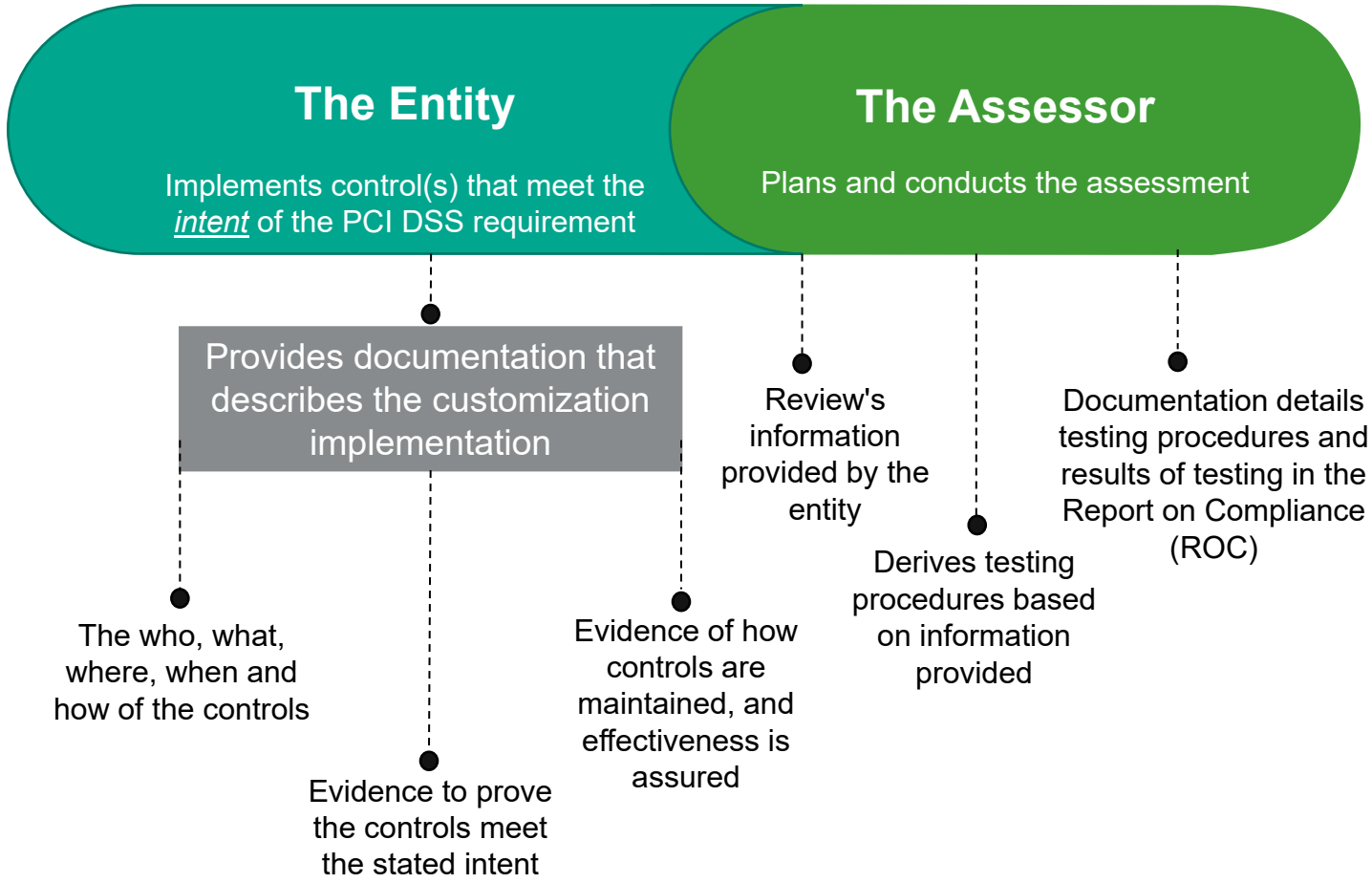
- “Significant Change” is not new; it is an important trigger for timing certain PCI DSS requirements, *e.g.*, perform new scope validation, vulnerability scans, confirm PCI controls. However, the term’s definition is dependent on the environment
- Significant Changes determine the timing of requirements such as vulnerability scanning, log review, and Targeted Risk Analyses
- Significant Change must now include all of the following:
  - New hardware, software, or networking equipment added to the CDE
  - Any replacement or major upgrades of hardware and software in the CDE
  - Any changes in the flow or storage of account data
  - Any changes to the boundary of the CDE and/or to the scope of the PCI DSS assessment
  - Any changes to the underlying supporting infrastructure of the CDE (including, but not limited to, changes to directory services, time servers, logging, and monitoring)
  - Any changes to third party vendors/service providers (or services provided) that support the CDE or meet PCI DSS requirements on behalf of the entity
- Significant Change is still “highly dependent” on an environment’s configuration, activities, and impacts on the CDE (p. 26)

IMPLEMENTATION AND VALIDATION APPROACHES (CUSTOMIZED APPROACH)

- PCI DSS 4.0 introduces a new way to implement and validate its requirements: the Customized Approach

Defined Approach (Legacy Approach)	Customized Approach
• Implement requirements in a prescriptive manner as done in prior PCI DSS versions • Many controls (with some exceptions, such as SAD) can be met with a compensating control if prescriptive control cannot be implemented • Control validation uses defined testing steps or compensating control evaluation using the compensating control worksheet and risk assessments • Annual requirement to document and validate any compensating control and include in the ROC	• Implement requirements using a customized control that implements the Customized Control Objective listed with the requirement • No compensating controls allowed • Requires a targeted risk analysis for each control • Customized control defined by entity; testing procedure defined by assessor (*e.g.* QSA) • Intended for risk-mature organizations • Must meet or exceed the security provided by the requirement in the Defined Approach • Expected to be greater effort for documentation and validation

VALIDATION TO THE CUSTOMIZED APPROACH



TARGETED RISK ANALYSES

- Multiple targeted risk analyses required at various points
  - Definition: “For PCI DSS purposes, a risk analysis that focuses on a specific PCI DSS requirement(s) of interest, either because the requirement allows flexibility (for example, as to frequency) or, for the Customized Approach, to explain how the entity assessed the risk and determined the customized control meets the objective of a PCI DSS requirement”
- Replaces the organization-wide risk assessment in PCI DSS 3.2.1 (req. 12.2)

TARGETED RISK ANALYSES (CONT.)

- Targeted Risk Analyses do not have to have a specific format but must include all the information defined in the template provided in E2 Sample Targeted Risk Analysis Template, p. 337. These include:
  - PCI Requirement, Control Objective, and the “mischief” the requirement was designed to prevent
  - Proposed Solution, including what parts of the requirement change, and how the proposed solution solves the mischief
  - Likelihood analysis
  - Impact analysis
  - Risk approval and review

TARGETED RISK ANALYSES TEMPLATE

Sample Targeted Risk Analysis for PCI DSS Requirements met via the Customized Approach To be completed by the entity being assessed	
Item	**Details**
1. Identify the requirement	
1.1 Identify the PCI DSS requirement as written.	<Entity identifies the requirement>
1.2 Identify the objective of the PCI DSS requirement as written.	<Entity identifies the objective of the requirement>
1.3 Describe the mischief that the requirement was designed to prevent	<Entity describes the mischief> <Entity describes the effect on its security if the objective is not successfully met by the entity.> <Entity describes which security fundamentals would not be in place, or what a threat actor may be able to do if the objective is not successfully met by the entity.>
2. Describe the proposed solution	
2.1 Customized control name/identifier	<Entity identifies the customized control as documented in the Controls Matrix.>
2.2 What parts of the requirement as written will change in the proposed solution?	<Entity identifies what elements of the requirement will not be met by the defined approach and so will be covered by customized approach. This could be as small as changing the periodicity of a requirement, or the implementation of a completely different set of controls to meet the objective.>
2.3 How will the proposed solution prevent the mischief?	<Entity describes how the controls detailed in the Controls Matrix will prevent the mischief identified in 1.3.>

Graphic sourced from PCI DSS 4.0, page 338

TARGETED RISK ANALYSES TEMPLATE (CONT.)

Sample Targeted Risk Analysis for PCI DSS Requirements met via the Customized Approach To be completed by the entity being assessed						
Item	**Details**					
3. Analyze any changes to the LIKELIHOOD of the mischief occurring, leading to a breach in confidentiality of cardholder data						
3.1 Describe the factors detailed in the Control Matrix that affect the likelihood of the mischief occurring.	Entity describes: • How successful the controls will be at preventing the mischief • How the controls detailed in the Control Matrix reduce the likelihood of the mischief occurring					
3.2 Describe the reasons the mischief may still occur after the application of the customized control.	Entity describes: • The typical reasons for the control to fail, the likelihood of this, and how could it be prevented • How resilient the entity's processes and systems are for detecting that the control(s) are not operating normally? • How a threat actor could bypass this control – what steps would they need to take, how hard is it, would the threat actor be detected before the control failed? How has this been determined?					
3.3 To what extent do the controls detailed in the customized approach represent a change in the likelihood of the mischief occurring when compared with the defined approach requirement?	Mischief more likely to occur	☐	No change	☐	Mischief less likely to occur	☐
3.4 Provide the reasoning for your assessment of the change in likelihood that the mischief occurs once the customized controls are in place.	Entity provides: • The justification for the assessment documented at 3.3. • The criteria and values used for the assessment documented at 3.3.					

Graphic sourced from PCI DSS 4.0, page 338

TARGETED RISK ANALYSES TEMPLATE (CONT.)

Sample Targeted Risk Analysis for PCI DSS Requirements met via the Customized Approach To be completed by the entity being assessed				
Item	**Details**			
4. Analyze any changes to the IMPACT of unauthorized access to account data				
4.1 For the scope of system components that this solution covers what volume of account data would be at risk of unauthorized access if the solution failed?	**4.1.1** Number of stored PANs	*Maximum at any one time*	**4.1.2** Number of PANs processed or transmitted over a 12-month period	*Total*
4.2 Description of how the customized controls will directly: • Reduce the number of individual PANs compromised if a threat actor is successful, and/or • Allow quicker notification of the PANs compromised to the card brands.	Impact to the payment ecosystem is directly related to the number of accounts compromised and how quickly any compromised PANs can be blocked by the card issuer. Entity describes how the customized controls achieve the following if any of the customized controls: • Reduce the volume of cardholder data that is stored, processed, or transmitted and therefore reduce what is available to a successful threat actor, and/or • Decrease the time to detection, notification of compromised accounts, and containment of the threat actor.			
5. Risk approval and review				
5.1 I have reviewed the above risk analysis and I agree that the use of the proposed customized approach as detailed provides at least an equivalent level of protection as the defined approach for the applicable PCI DSS requirement.	A member of executive management must review and agree to the proposed customized approach. <Member of entity's executive management signs that it reviewed and agreed to the customized approach documented herein.>			
5.2 This risk analysis must be reviewed and updated no later than:	The risk analysis should be reviewed at least every twelve months and more frequently if the customized approach itself is time limited (for example, because there is a planned change in technology) or if other factors dictate a needed change. In the event of an unscheduled risk review, detail the reason the review occurred. <Entity indicates date the targeted risk analysis was reviewed and updated.>			

Graphic sourced from PCI DSS 4.0, page 338

THIRD PARTY SERVICE PROVIDERS

Entity's Management of TPSP

- 12.8.1 Maintain a list and description of all TPSPs
- 12.8.2 Maintain written agreements with TPSPs where account data is shared or security of CDE could be affected
- 12.8.3 Establish a process including due diligence prior to engagement for all TSPS
- 12.8.4 Implement a program to monitor TPSPs' PCI DSS compliance status at least once every 12 months
- 12.8.5 Maintain information about which PCI DSS requirements are
  - managed by each TPSP,
  - managed by the entity, and
  - that are shared between the TPSP and the entity

TPSP's Responsibilities to Entity

- 12.9.1 TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's CDE
- 12.9.2 TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request:
  - PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4)
  - Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5)

PCI DSS VERSION 4.0 CHANGES

- PCI DSS v4.0 includes 53 new requirements for all entities and 11 new requires for TPSPs. These requirements are either:

- Effective immediately for all PCI DSS v4.0 assessments (13 requirements)

- Best practices until 31 March 2025, after which these requirements will be required and must be fully considered during a PCI DSS assessment (51 requirements)

NOTABLE REQUIREMENT CHANGES

High Level Requirement	PCI DSS 3.2.1	PCI DSS 4.0	Notable Changes and Updates
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data	1. Install and Maintain Network Security Controls.	• Focus on a broader range of security controls beyond firewalls and routers using new term “Network Security Controls (NSC)” • Greater clarity on placement of NSCs between trusted and untrusted networks • Clarifications regarding devices that connect to the CDE and other untrusted networks.
	2. Do not use vendor-supplied defaults for system passwords and other security parameters	2. Apply Secure Configurations to All System Components.	• Document roles and responsibilities^ • Business justification is now required for any insecure protocol used • Clarifications on wireless security requirements

^Designates new requirement
**Designates best practice until March 31, 2025*

NOTABLE REQUIREMENT CHANGES (CONT.)

High Level Requirement	PCI DSS 3.2.1	PCI DSS 4.0	Notable Changes and Updates
Protect Cardholder Data [3.2.1] **Protect Account Data** [4.0]	3. Protect stored cardholder data	3. Protect Stored Account Data.	• Document roles and responsibilities^ • Protect SAD prior to authorization^* • Added issuer requirements for storage of SAD • Clarifications for PAN masking • Protect PAN from remote access^* • Keyed cryptographic hashes for PAN^* • Disk-level or partition-level encryption only used for on removable media; additional encryption needed for non-removable media^* • Service providers must document the use of the same cryptographic keys in production and test is prevented^*
	4. Encrypt transmission of cardholder data across open, public networks	4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.	• Document roles and responsibilities^ • Confirm certificates used for PAN transmission are valid and not expired or revoked^* • Maintain an inventory of trusted keys and certificates^*

^Designates new requirement
**Designates best practice until March 31, 2025*

NOTABLE REQUIREMENT CHANGES (CONT.)

High Level Requirement	PCI DSS 3.2.1	PCI DSS 4.0	Notable Changes and Updates
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs	5. Protect All Systems and Networks from Malicious Software.	• Document roles and responsibilities^ • Replaced anti-virus with anti-malware • Clarifications regarding documentation required for systems not at risk for malware and period review based on risk^* • Frequency of periodic malware scans based on risk^* • Malware solution required for electronic media^* • Detect and protect personnel against phishing^*
	6. Develop and maintain secure systems and applications	6. Develop and Maintain Secure Systems and Software.	• Document roles and responsibilities^ • Clarification that requirement applies to bespoke and custom software and not third-party software • Maintain and inventory of bespoke and custom software^* • Protect public-facing web apps through automated solutions only (no more manual checks allows) ^* • New controls for scripts loaded on consumer's browser^* • Development and testing renamed "pre-production" • Clarifications around "segregation of duties" - focus is now on accountability that only approved changes occur • Shift from documented processes and procedures to specific requirements for testing procedures to verify policies and procedures of each requirement

^Designates new requirement
**Designates best practice until March 31, 2025*

NOTABLE REQUIREMENT CHANGES (CONT.)

High Level Requirement	PCI DSS 3.2.1	PCI DSS 4.0	Notable Changes and Updates
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know	7. Restrict Access to System Components and Cardholder Data by Business Need to Know.	• Document roles and responsibilities^ • Expanded guidance on least privilege principles • Review all user accounts and related access privileges^* • Management of application and system accounts^* • Review of all application and system accounts^*
	8. Identify and authenticate access to system components	8. Identify Users and Authenticate Access to System Components.	• Document roles and responsibilities^ • Clarification: this requirement does not apply to consumers • Increased password length to 12 characters^* • Service providers provide guidance on password changes^* • MFA required for all access to the CDE^* • Requirements for MFA and interactive logins^* • No hard-coding of passwords into scripts^* • Password change / complexity requirements for system and application accounts^*
	9. Restrict physical access to cardholder data	9. Restrict Physical Access to Cardholder Data.	• Document roles and responsibilities^ • Clarified requirement to lock consoles in sensitive areas • Restructured requirements for procedures in this requirement • POI device inspections based on targeted risk analysis^*

^Designates new requirement
**Designates best practice until March 31, 2025*

NOTABLE REQUIREMENT CHANGES (CONT.)

High Level Requirement	PCI DSS 3.2.1	PCI DSS 4.0	Notable Changes and Updates
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data	10. Log and Monitor All Access to System Components and Cardholder Data.	• Document roles and responsibilities^ • Automated log reviews^ • Frequency of log reviews determined by risk analysis^* • Alerting requirement for all failures of critical security control systems^* • Prompt response required for failure of critical security controls (newly added for non-service providers) ^*
	11. Regularly test security systems and processes	11. Test Security of Systems and Networks Regularly.	• Document roles and responsibilities^ • Must scan for wireless even when wireless not used and policy against wireless^* • Internal vulnerability scans via authenticated scanning^* • Clarifications regarding penetration testing requirements • Multi-tenant service providers must support customers for external penetration testing^* • Service Providers must use intrusion-detection or intrusion-prevention techniques to address covert malware communication channels^* • Change-and-tamper-detection mechanism deployed to alert for modifications to HTTP headers and content of payment pages received by consumer browser^*

^Designates new requirement
**Designates best practice until March 31, 2025*

NOTABLE REQUIREMENT CHANGES (CONT.)

High Level Requirement	PCI DSS 3.2.1	PCI DSS 4.0	Notable Changes and Updates
Maintain an Information Security Policy **(which includes many more requirements about managing the security program and third-party vendors)**	12. Maintain a policy that addresses information security for all personnel	12. Support Information Security with Organizational Policies **and Programs**.	• **Clarified that use of a PCI DSS compliant TPSP does not make an entity compliant or remove responsibility for compliance from entity.** • Formal organization-wide risk assessment changed to targeted risk analyses^ • Personnel must formally acknowledge responsibilities^ • Targeted risk analysis required for any requirement that has flexibility in frequency of performance^* • Targeted risk analysis for any customized approach control^ • Review cryptographic cypher suites and protocols at least every 12 months^* • Review hardware and software technologies at least every 12 months^* • **Document and confirm PCI Scope at least every 12 months and after significant change^** • **Service Provider document and confirm scope at least every 6 months and on significant change^*** • **Service Providers must review impact to PCI of every significant change^*** • Review and update security awareness program at least every 12 months^* • Security Awareness training includes threats and vulnerabilities that could impact CDE^* • **TPSPs must support entity's requirements for PCI compliance for tasks they perform or share with entity^** • Targeted risk analysis to determine frequency of training^*

^Designates new requirement
**Designates best practice until March 31, 2025*

LEGAL RISKS

LEGAL RISKS

- What constitutes "reasonable security?" Has the bar (now) been raised?
  - FTC's unfair and deceptive practices standard
  - US state incorporation of or safe harbor for PCI DSS (Nevada, Washington, Minnesota, Ohio, Utah, Connecticut)
  - Implications of 4.0's "clarifications" on existing 3.2.1 compliance

- Conducting readiness exercises under attorney-client privilege

LEGAL RISKS (CONT.)

- Risk Analyses and Management
  - Who performs (in-house / third party vendor)?
  - Drafts of Targeted Risk Analyses and readiness exercises may be discoverable outside of attorney-client privilege
  - Final Targeted Risk Analyses are likely discoverable

- Decision making / acceptance of risk identified in course of Targeted Risk Analyses

LEGAL RISKS (CONT.)

- Contracting with or as Third-Party Service Providers (TPSPs)
  - Need to evaluate which third parties are in scope
  - Need requisite terms in place that complies with PCI DSS Req. 12

- Assessing responsibilities as a TPSP (including existing contracts)

- Disputes with TPSPs arising under PCI DSS 4.0

LEGAL RISKS (CONT.)

- Risk considerations between the prescriptive and customized approaches

- Governance issues
  - Board reporting
  - Roles and responsibilities
  - Policies

CLOSING THOUGHTS

THANK YOU / QUESTIONS