The New Approach To Reporting

Brandy Cumberland, Director, Program Operations,
PCI Security Standards Council
Lauren Holloway, Director, Data Security Standards
PCI Security Standards Council

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

The New Approach to Reporting

Overview of Session

- PCI DSS v4.0 Changes that Impact Reporting
- Report on Compliance Updates
- Attestation of Compliance Updates

PCI Security Standards Council®

Flexibility for Different Methodologies

PCI Security Standards Council®

Validating to PCI DSS v4.0

Add flexibility for different methodologies used to achieve security

Defined Approach

Follows current PCI DSS requirements and testing procedures

Provides a defined method for meeting security objectives

PCI Security Standards Council®

Validating to PCI DSS v4.0

Add flexibility for different methodologies used to achieve security

Defined Approach

Follows current PCI DSS requirements and testing procedures

Provides a defined method for meeting security objectives

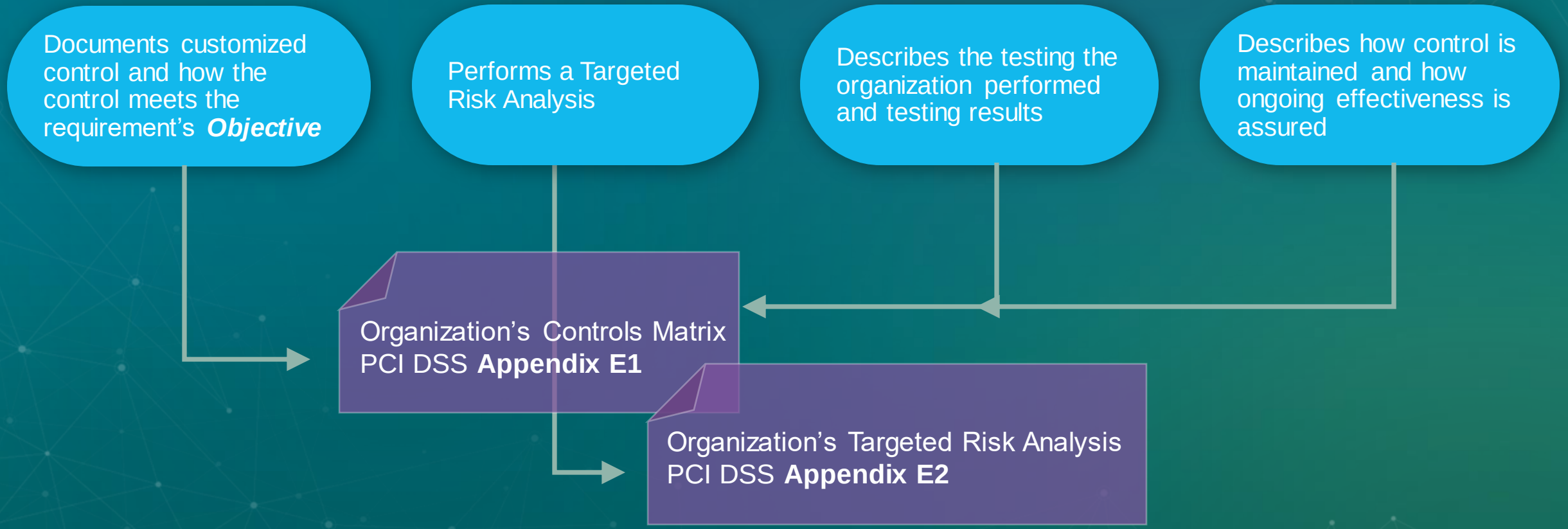
Customized Approach (NEW)

Focuses on the *objective* of each PCI DSS requirement

Provides greater flexibility for entities using different ways to achieve security

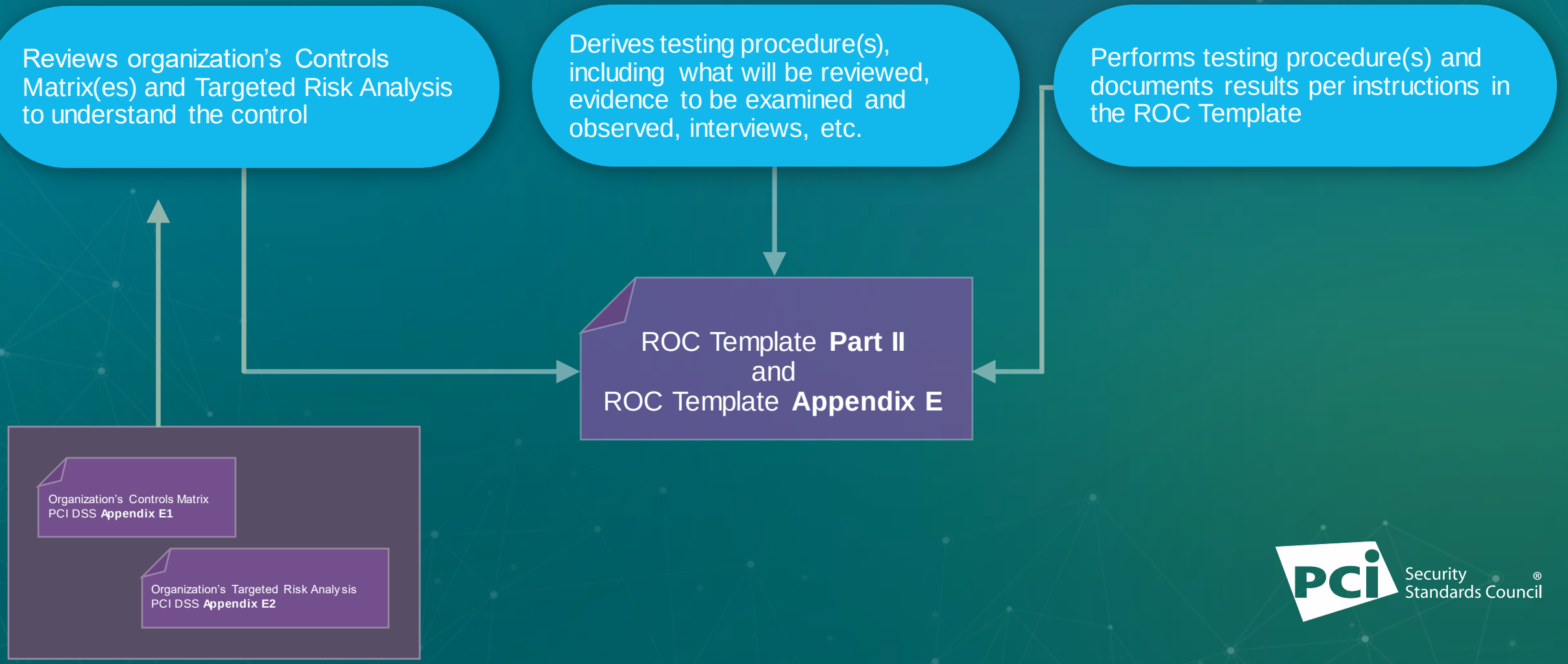
PCI Security Standards Council®

The Organization's Role



PCI Security Standards Council

The Assessor's Role



PCI Security Standards Council

Working Together is Key

PCI Security Standards Council®

Which Entities Can Use The Customized Approach?

PCI Security Standards Council

Compensating Controls and the Customized Approach

Compensating Controls

The organization cannot meet the requirement as stated *due to documented technical or business constraints* but has implemented alternative controls to mitigate the risk.

PCI Security Standards Council®

Compensating Controls and the Customized Approach

Compensating Controls

The organization cannot meet the requirement as stated *due to documented technical or business constraints* but has implemented alternative controls to mitigate the risk.

Customized Approach

The organization has mature risk-management practices and chooses to implement different controls that *meet the Customized Approach Objective* in a different way than the defined requirement.

PCI Security Standards Council®

Security as a Continuous Process

PCI Security Standards Council®

PCI DSS Requirement Responses

Responses *at the individual requirement* to indicate the entity's status

- In Place
- In Place with Remediation
- Not Applicable
- Not Tested
- Not in Place

PCI Security Standards Council®

New Reporting Options

In Place with Remediation

PCI Security Standards Council®

In Place With Remediation

Examples: In Place with Remediation

- Security patches not applied within 30 days
- A misconfigured network security control
- Users that missed security awareness training
- Accidental storage of unencrypted PAN
- A missing quarterly vulnerability scan

PCI Security Standards Council®

Difference Between Not Applicable And Not Tested

Not Applicable

Assessor documents testing performed to confirm the Not Applicable status

Example: No PAN exists in environment

Requirements specific to PAN are Not Applicable

Not Tested

Assessor does not perform any testing and does not know whether the requirement applies or is In Place

Example: Only requirements for Prioritized Approach Milestones 1-4 are included in the assessment

All other requirements are Not Tested

PCI Security Standards Council

Uses of Not Tested: the Good and the Bad…

Organization wants to include only certain requirements

Acquirer asks merchant to include only Prioritized Approach Milestones 1-4

An organization includes only requirements for a newly implemented technology

A service provider includes only requirements for a data center hosting service

Organization has requirements that are not in place

Organization wants “Not Tested” results while it implements corrective actions

NO!

PCI Security Standards Council

New Reporting Options

Full Assessment

Partial Assessment

PCI Security Standards Council

Compliant But With Legal Exception

There is a legal restriction that prevents an organization from meeting a PCI DSS requirement

- Meeting the requirement would violate a law or regulation

  Contractual obligations or legal advice are not legal restrictions

- Requirement is marked Not in Place

PCI Security Standards Council®

Enhanced Validation Methods and Procedures

PCI Security Standards Council®

Report on Compliance (ROC) Overview

The ROC is larger, but it should be easier to complete – really!

- **Align reporting and attestation documents for PCI DSS v4.0**
- **New reporting options and two new validation methods**
- **Less detailed reporting, more focus on evidence**

PCI Security Standards Council®

Report on Compliance (ROC) Overview

The ROC is larger, but it should be easier to complete – really!

- **Align reporting and attestation documents for PCI DSS v4.0**
- **New reporting options and two new validation methods**
- **Less detailed reporting, more focus on evidence**

PCI Security Standards Council®

Report on Compliance (ROC) Overview

The ROC is larger, but it should be easier to complete – really!

- **Align reporting and attestation documents for PCI DSS v4.0**
- **New reporting options and two new validation methods**
- **Less detailed reporting, more focus on evidence**

PCI Security Standards Council®

ROC Parts

The ROC is broken into three main parts:

- ROC Template Instructions
- Part I Assessment Overview
- Part II Findings and Observations

PCI Security Standards Council®

ROC Template Instructions

ROC Template Instructions

- **New** customizable title page
- Reflects PCI DSS changes and reporting changes
- Clarified confusing language
- ROC Template Instructions can now be deleted

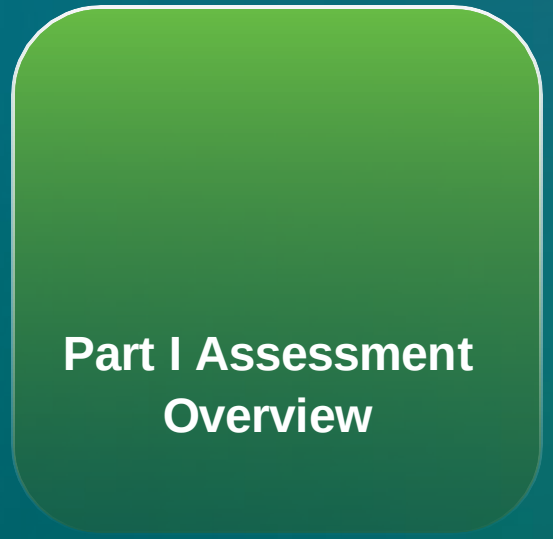
PCI Security Standards Council®

Part I Assessment Overview

Six sections with information about the entity and environment being assessed

New sections for:

- Remote Assessment Activities
- Use of Subcontractors
- Overall Assessment Result
- Attestation Signatures



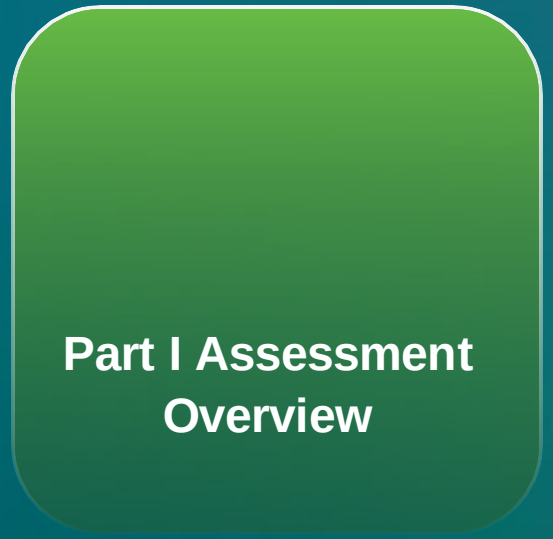
PCI Security Standards Council

Part I Assessment Overview

Six sections with information about the entity and environment being assessed

New sections for:

- Remote Assessment Activities
- Use of Subcontractors
- Overall Assessment Result
- Attestation Signatures



PCI Security Standards Council

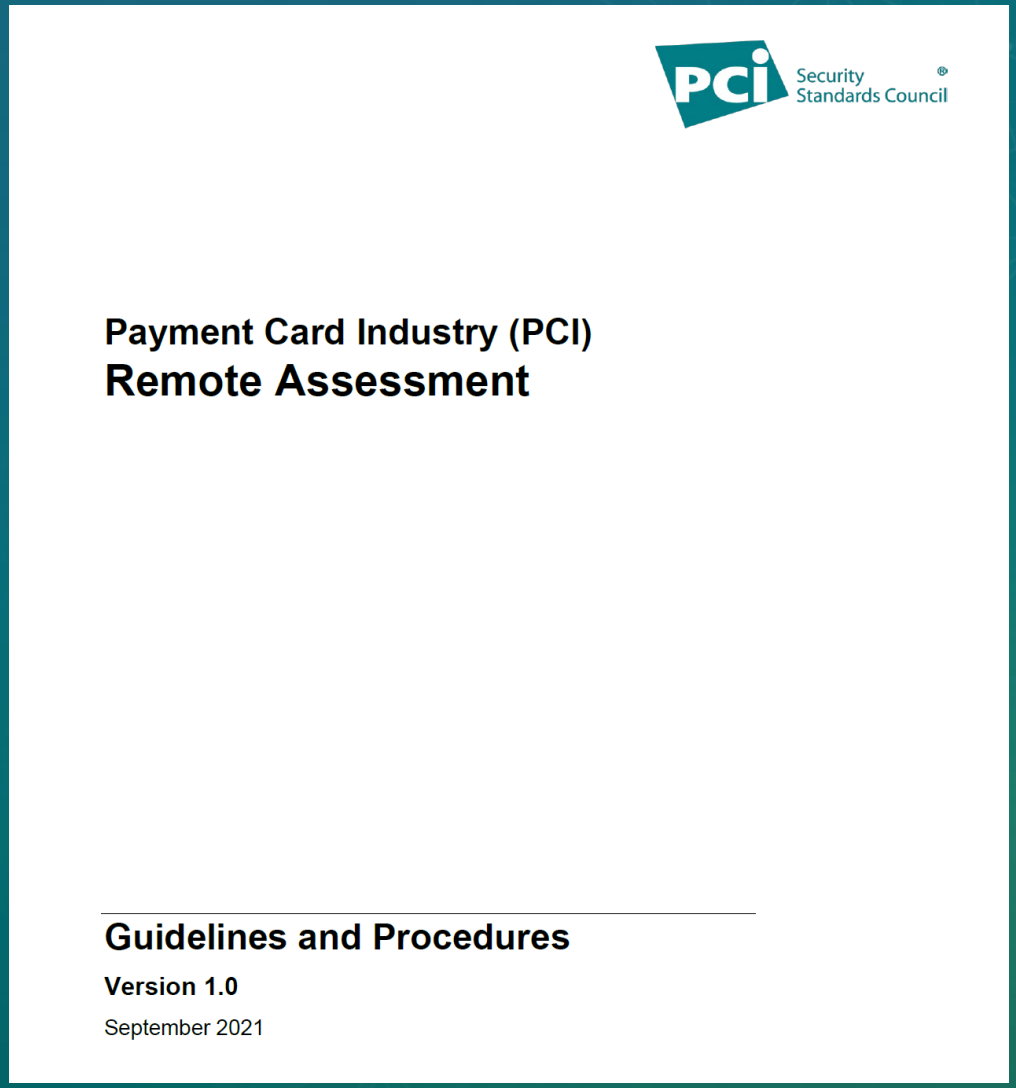
Part I Assessment Overview

Remote Assessment Activities

From the *PCI SSC Remote Assessment Guidelines*

Sections for Assessors To Describe:

- Overview of Remote Testing Activity
- Summary of Testing Performed Remotely
- Assessor Assurance in Assessment Result
- Requirements that Could Not be Fully Verified



PCI Security Standards Council

Part I Assessment Overview

Overall Assessment Result & Summary of Assessment

More transparency about assessment results

- Full or Partial Assessment
- Summary for each principal requirement:
  - Assessment findings
  - Indication if compensating controls or customized approach used

1.7 Overall Assessment Result

Indicate below whether a full or partial assessment was completed. Select only one.	
☐	**Full Assessment:** All requirements have been assessed and therefore no requirements were marked as Not Tested.
☐	**Partial Assessment:** One or more requirements have not been assessed and were therefore marked as Not Tested. Any requirement not assessed is noted as Not Tested in section 1.8.1 below.

Overall Assessment Result (Select only one)	
☐	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall COMPLIANT rating; thereby the assessed entity has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall NON-COMPLIANT rating; thereby the assessed entity has not demonstrated compliance with PCI DSS requirements.
☐	**Compliant but with Legal Exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall COMPLIANT BUT WITH LEGAL EXCEPTION rating, thereby the assessed entity has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.

1.8 Summary of Assessment

1.8.1 Summary of Assessment Findings and Methods

Indicate all the findings and assessment methods within each PCI DSS principal requirement. Select all that apply. For example, ***In Place*** and ***Not Applicable*** must both be selected for Requirement 1 if there is at least one sub-requirement marked ***In Place*** and one sub-requirement marked ***Not Applicable***. The columns for Compensating Controls and Customized Approach must be selected if there is at least one sub-requirement within the principal requirement that utilizes the respective method. For example, Compensating Control and Customized Approach must both be checked if at least one sub-requirement utilizes Compensating Controls and at least one sub requirement utilizes a Customized Approach. If neither Compensating Controls nor Customized Approach are used, then leave both blank.

PCI DSS Requirement	Assessment Finding Select all options that apply.					Select If Below Method(s) Was Used	
	In Place	In Place with Remediation	Not Applicable	Not Tested	Not in Place	Compensating Control	Customized Approach
Requirement 1:	☐	☐	☐	☐	☐	☐	☐
Requirement 2:	☐	☐	☐	☐	☐	☐	☐
Requirement 3:	☐	☐	☐	☐	☐	☐	☐
Requirement 4:	☐	☐	☐	☐	☐	☐	☐
Requirement 5:	☐	☐	☐	☐	☐	☐	☐
Requirement 6:	☐	☐	☐	☐	☐	☐	☐

PCI Security Standards Council®

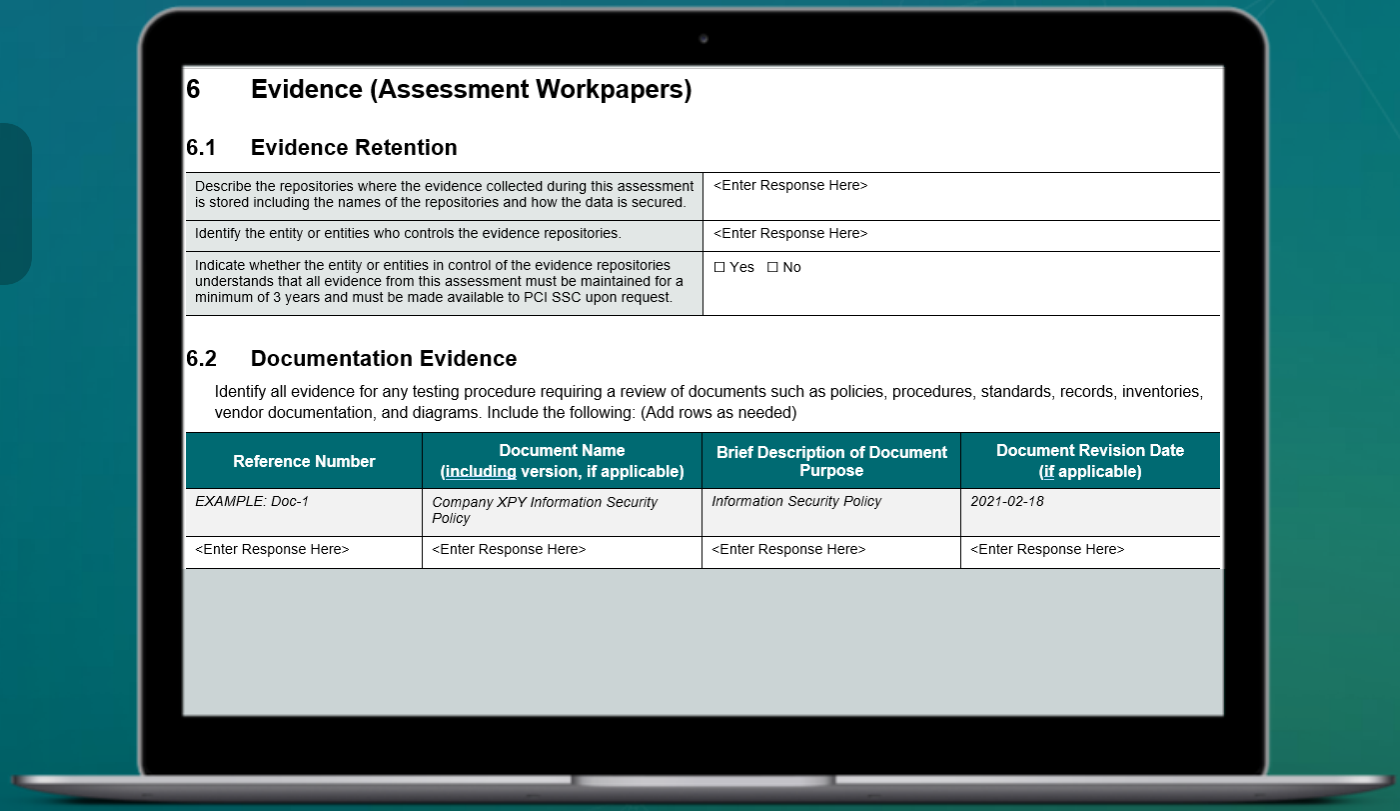
Part I Assessment Overview

Evidence (Assessment Workpapers)

Records the evidence the assessor reviewed that supports their conclusions for each requirement.

Four evidence categories:

- Documentation Evidence
- Interview Evidence
- Observation Evidence
- System Evidence



6 Evidence (Assessment Workpapers)

6.1 Evidence Retention

Describe the repositories where the evidence collected during this assessment is stored including the names of the repositories and how the data is secured.	<Enter Response Here>
Identify the entity or entities who controls the evidence repositories.	<Enter Response Here>
Indicate whether the entity or entities in control of the evidence repositories understands that all evidence from this assessment must be maintained for a minimum of 3 years and must be made available to PCI SSC upon request.	☐ Yes ☐ No

6.2 Documentation Evidence

Identify all evidence for any testing procedure requiring a review of documents such as policies, procedures, standards, records, inventories, vendor documentation, and diagrams. Include the following: (Add rows as needed)

Reference Number	Document Name (including version, if applicable)	Brief Description of Document Purpose	Document Revision Date (if applicable)
EXAMPLE: Doc-1	*Company XPY Information Security Policy*	*Information Security Policy*	*2021-02-18*
<Enter Response Here>	<Enter Response Here>	<Enter Response Here>	<Enter Response Here>

PCI Security Standards Council®

Part II Findings and Observations

Requirements and Testing Results

- Requirements updated to **PCI DSS v4.0**
- New Finding Option: **“In Place with Remediation”**
- New Approach: **“Describe why the assessment finding was selected”**

Part II Findings and Observations

PCI Security Standards Council®

Part II Findings and Observations

Reporting Results for each PCI DSS Requirement

- Assessment Findings - five options
- Single narrative response for each requirement
  - For each test: Identify evidence rather than detailed report results
- Reporting for Customized Approach and Compensating Controls

PCI DSS Requirement				
3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.				
Assessment Findings (select one)				
In Place	**In Place with Remediation**	**Not Applicable**	**Not Tested**	**Not in Place**
☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.*			<Enter Response Here>	
Validation Method – Customized Approach				
Indicate whether a Customized Approach was used:			☐ Yes ☐ No	
If "Yes", Identify the aspect(s) of the requirement where the Customized Approach was used. ***Note:** The use of Customized Approach must also be documented in Appendix E.*			<Enter Response Here>	
Validation Method – Defined Approach				
Indicate whether a Compensating Control was used:			☐ Yes ☐ No	
If "Yes", Identify the aspect(s) of the requirement where the Compensating Control(s) was used. ***Note:** The use of Compensating Controls must also be documented in Appendix C.*			<Enter Response Here>	
Testing Procedures	**Reporting Instructions**		**Reporting Details: Assessor's Response**	
3.6.1.3 Examine user access lists to verify that access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	**Identify** the evidence reference number(s) from Section 6 for all **user access lists** examined for this testing procedure.		<Enter Response Here>	

PCI Security Standards Council

Part II Findings and Observations

Reporting Results for each PCI DSS Requirement

PCI DSS Requirement				
3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.				
Assessment Findings (select one)				
In Place	**In Place with Remediation**	**Not Applicable**	**Not Tested**	**Not in Place**
☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.*	<Enter Response Here>

PCI Security Standards Council

Part II Findings and Observations

Reporting Results for each PCI DSS Requirement

PCI DSS Requirement				
3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.				
Assessment Findings (select one)				
In Place	**In Place with Remediation**	**Not Applicable**	**Not Tested**	**Not in Place**
☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.*	<Enter Response Here>

PCI Security Standards Council

Part II Findings and Observations

Reporting Results for each PCI DSS Requirement

PCI DSS Requirement				
3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.				
Assessment Findings (select one)				
In Place	**In Place with Remediation**	**Not Applicable**	**Not Tested**	**Not in Place**
☐	☐	☐	☐	☐

Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.*	<Enter Response Here>

PCI Security Standards Council

Part II Findings and Observations

Reporting Results for each PCI DSS Requirement

Validation Method – Customized Approach	
Indicate whether a Customized Approach was used:	☐ Yes ☐ No
If "Yes", Identify the aspect(s) of the requirement where the Customized Approach was used. ***Note:*** *The use of Customized Approach must also be documented in Appendix E.*	<Enter Response Here>

Validation Method – Defined Approach	
Indicate whether a Compensating Control was used:	☐ Yes ☐ No
If "Yes", Identify the aspect(s) of the requirement where the Compensating Control(s) was used. ***Note:*** *The use of Compensating Controls must also be documented in Appendix C.*	<Enter Response Here>

PCI Security Standards Council ®

Part II Findings and Observations

Reporting Results for each PCI DSS Requirement

Validation Method – Customized Approach	
Indicate whether a Customized Approach was used:	☐ Yes ☐ No
If "Yes", Identify the aspect(s) of the requirement where the Customized Approach was used. ***Note:*** *The use of Customized Approach must also be documented in Appendix E.*	<Enter Response Here>

Validation Method – Defined Approach	
Indicate whether a Compensating Control was used:	☐ Yes ☐ No
If "Yes", Identify the aspect(s) of the requirement where the Compensating Control(s) was used. ***Note:*** *The use of Compensating Controls must also be documented in Appendix C.*	<Enter Response Here>

Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
3.6.1.3 Examine user access lists to verify that access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	**Identify** the evidence reference number(s) from Section 6 for all **user access lists** examined for this testing procedure.	<Enter Response Here>

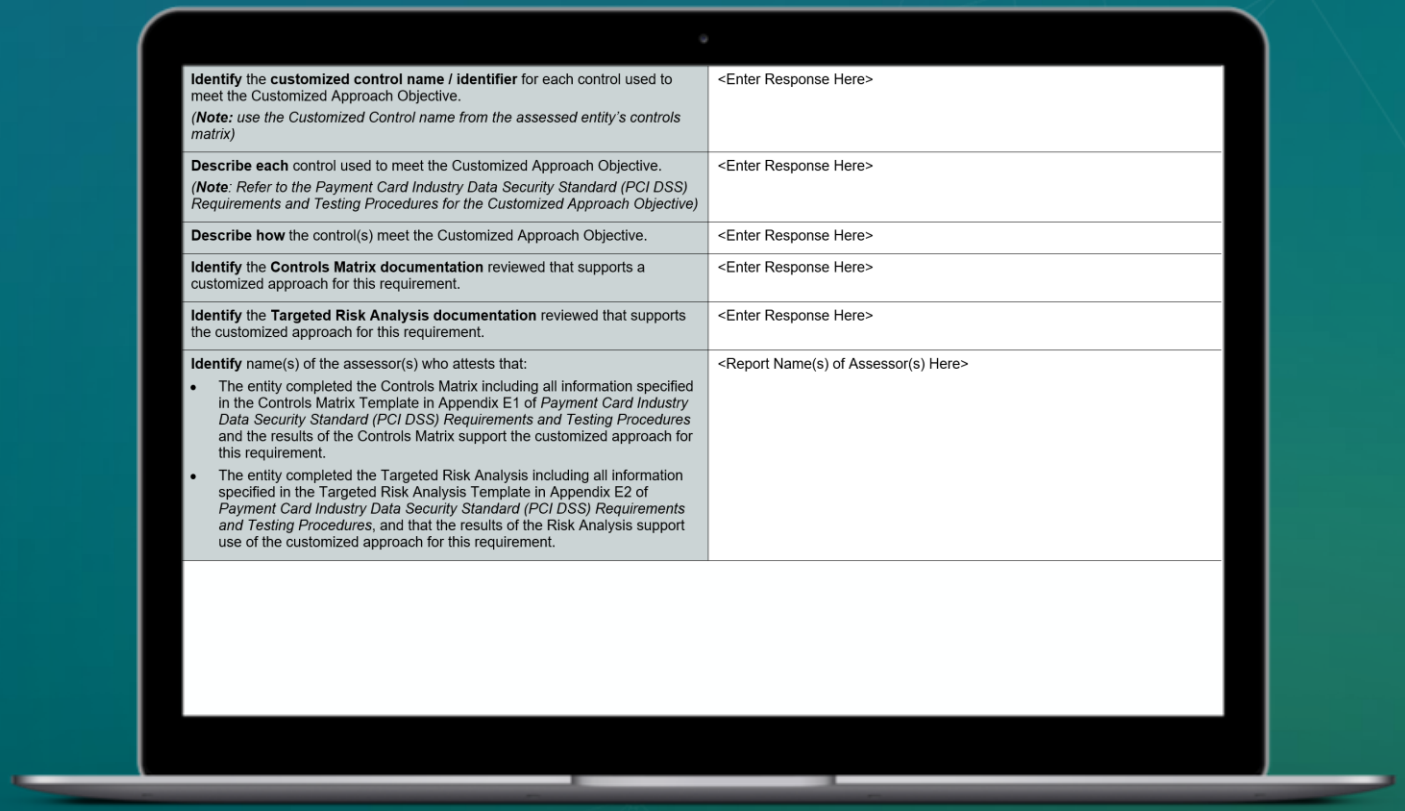
PCI Security Standards Council ®

Part II Findings and Observations

Appendix E Customized Approach Template

The Assessor must identify and describe each customized control used.

Controls Matrix and Targeted Risk Analysis documentation must be identified and confirmed to support the use of the Customized Approach.



Identify the **customized control name / identifier** for each control used to meet the Customized Approach Objective. *(**Note:** use the Customized Control name from the assessed entity's controls matrix)*	<Enter Response Here>
Describe each control used to meet the Customized Approach Objective. *(**Note**: Refer to the Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures for the Customized Approach Objective)*	<Enter Response Here>
Describe how the control(s) meet the Customized Approach Objective.	<Enter Response Here>
Identify the **Controls Matrix documentation** reviewed that supports a customized approach for this requirement.	<Enter Response Here>
Identify the **Targeted Risk Analysis documentation** reviewed that supports the customized approach for this requirement.	<Enter Response Here>
Identify name(s) of the assessor(s) who attests that: • The entity completed the Controls Matrix including all information specified in the Controls Matrix Template in Appendix E1 of *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures* and the results of the Controls Matrix support the customized approach for this requirement. • The entity completed the Targeted Risk Analysis including all information specified in the Targeted Risk Analysis Template in Appendix E2 of *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures*, and that the results of the Risk Analysis support use of the customized approach for this requirement.	<Report Name(s) of Assessor(s) Here>

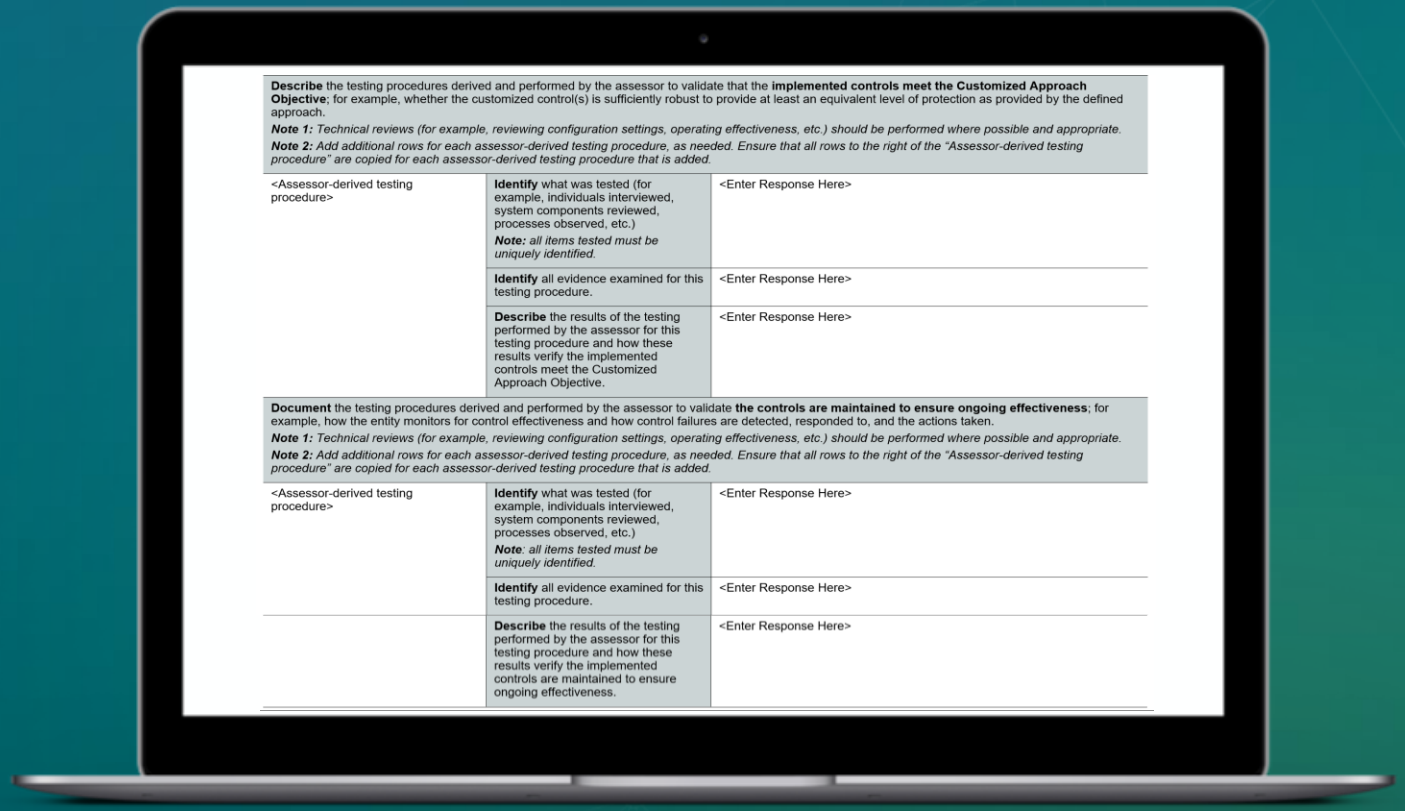
PCI Security Standards Council®

Part II Findings and Observations

Appendix E Customized Approach Template

The Assessor must develop and document testing procedures, perform the testing, document the results.

Testing procedures must validate that implemented controls meet the Customized Approach Objective and the controls are maintained to ensure ongoing effectiveness.



Describe the testing procedures derived and performed by the assessor to validate that the **implemented controls meet the Customized Approach Objective**; for example, whether the customized control(s) is sufficiently robust to provide at least an equivalent level of protection as provided by the defined approach. ***Note 1:*** *Technical reviews (for example, reviewing configuration settings, operating effectiveness, etc.) should be performed where possible and appropriate.* ***Note 2:*** *Add additional rows for each assessor-derived testing procedure, as needed. Ensure that all rows to the right of the "Assessor-derived testing procedure" are copied for each assessor-derived testing procedure that is added.*		
<Assessor-derived testing procedure>	**Identify** what was tested (for example, individuals interviewed, system components reviewed, processes observed, etc.) ***Note:*** *all items tested must be uniquely identified.*	<Enter Response Here>
	Identify all evidence examined for this testing procedure.	<Enter Response Here>
	Describe the results of the testing performed by the assessor for this testing procedure and how these results verify the implemented controls meet the Customized Approach Objective.	<Enter Response Here>
Document the testing procedures derived and performed by the assessor to validate **the controls are maintained to ensure ongoing effectiveness**; for example, how the entity monitors for control effectiveness and how control failures are detected, responded to, and the actions taken. ***Note 1:*** *Technical reviews (for example, reviewing configuration settings, operating effectiveness, etc.) should be performed where possible and appropriate.* ***Note 2:*** *Add additional rows for each assessor-derived testing procedure, as needed. Ensure that all rows to the right of the "Assessor-derived testing procedure" are copied for each assessor-derived testing procedure that is added.*		
<Assessor-derived testing procedure>	**Identify** what was tested (for example, individuals interviewed, system components reviewed, processes observed, etc.) ***Note:*** *all items tested must be uniquely identified.*	<Enter Response Here>
	Identify all evidence examined for this testing procedure.	<Enter Response Here>
	Describe the results of the testing performed by the assessor for this testing procedure and how these results verify the implemented controls are maintained to ensure ongoing effectiveness.	<Enter Response Here>

PCI Security Standards Council®

Updates to Attestations of Compliance

- Align content with ROC
- More transparency for AOC reviewers
- Address general stakeholder feedback
- Promote security as a continuous process
- Enhance validation methods and procedures

AOC Summary of Assessment

Part 2g. Summary of Assessment
(ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.					Select If Below Method(s) Was Used	
	In Place	In Place with Remediation	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
Requirement 1:	☐	☐	☐	☐	☐	☐	☐
Requirement 2:	☐	☐	☐	☐	☐	☐	☐
Requirement 3:	☐	☐	☐	☐	☐	☐	☐
Requirement 4:	☐	☐	☐	☐	☐	☐	☐
Requirement 5:	☐	☐	☐	☐	☐	☐	☐

Conclusion

- Formatting of ROC changed – intent is to simplify and support v4.0 features
- AOC updates align with ROC content and provide transparency
- Not possible without the feedback received from the industry

PCI Security Standards Council®

A Look Into Self Assessments

John Bloomfield, Standards Development Manager

PCI Security Standards Council

PCI Security Standards Council®