HALOCK®

A Deep Dive into the New 4.0 DSS Requirements that are Applicable Immediately

Presented by:
Viviana Wesley, CISM, PCI QSA, ISO 27001 Auditor

About the Presenter

Viviana Wesley

- Principal Consultant with HALOCK Security Labs
- CISM, PCI QSA, ISO 27001 Auditor
- HALOCK's PCI DSS Subject Matter Expert and Solution Architect
- Serves as an expert witness for State Offices of Attorney General and Multidistrict litigation matters
- 23+ years of practical experience within Information Technology
- 13+ years specializing in Information Security
- University of Northern Iowa – Bachelor of Arts in Computer Science

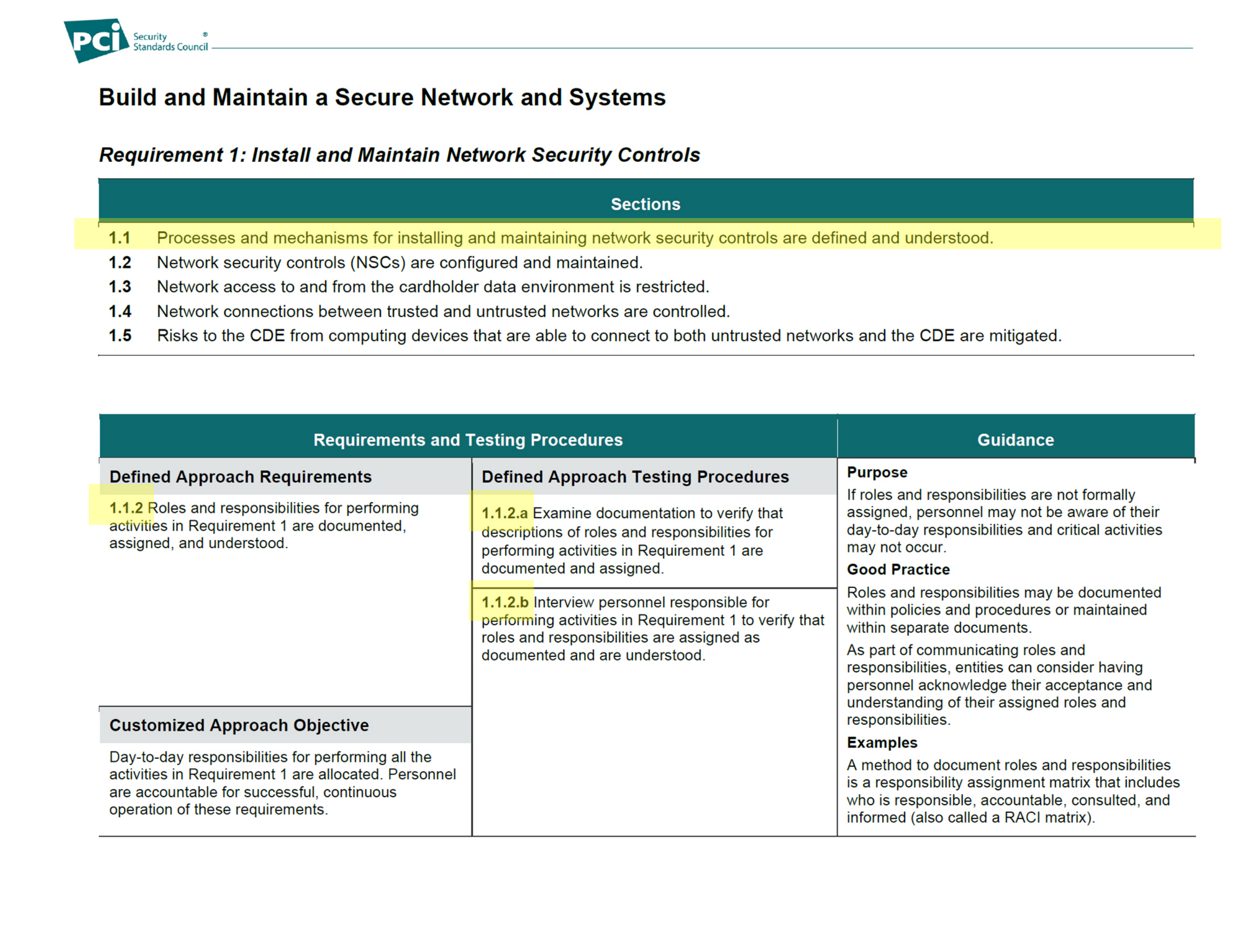
Agenda

- Introduction
- 14 Requirements with Immediate Applicability
- Review of Requirements: What, Purpose, Impact Process
- Why Now & Questions

14 New PCI DSS Requirements

Requirement #	PCI DSS v4.0 REQUIREMENT
1.1.2	Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.
2.1.2	Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.
3.1.2	Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.
4.1.2	Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.
5.1.2	Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.
6.1.2	Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.
7.1.2	Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.
8.1.2	Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.
9.1.2	Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.
10.1.2	Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.
11.1.2	Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.
12.3.2	A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach.
12.5.2	PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment.
12.9.2	Additional requirement for service providers only: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5.

Requirement 1.1.2



PCI Security Standards Council

Build and Maintain a Secure Network and Systems

Requirement 1: Install and Maintain Network Security Controls

Sections	
1.1	Processes and mechanisms for installing and maintaining network security controls are defined and understood.
1.2	Network security controls (NSCs) are configured and maintained.
1.3	Network access to and from the cardholder data environment is restricted.
1.4	Network connections between trusted and untrusted networks are controlled.
1.5	Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	**1.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 1 are documented and assigned. **1.1.2.b** Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 1 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

WHAT

Roles and Responsibilities for Network Security Controls (NSC) are documented, assigned, and maintained.

PURPOSE

If responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and processes may break down.

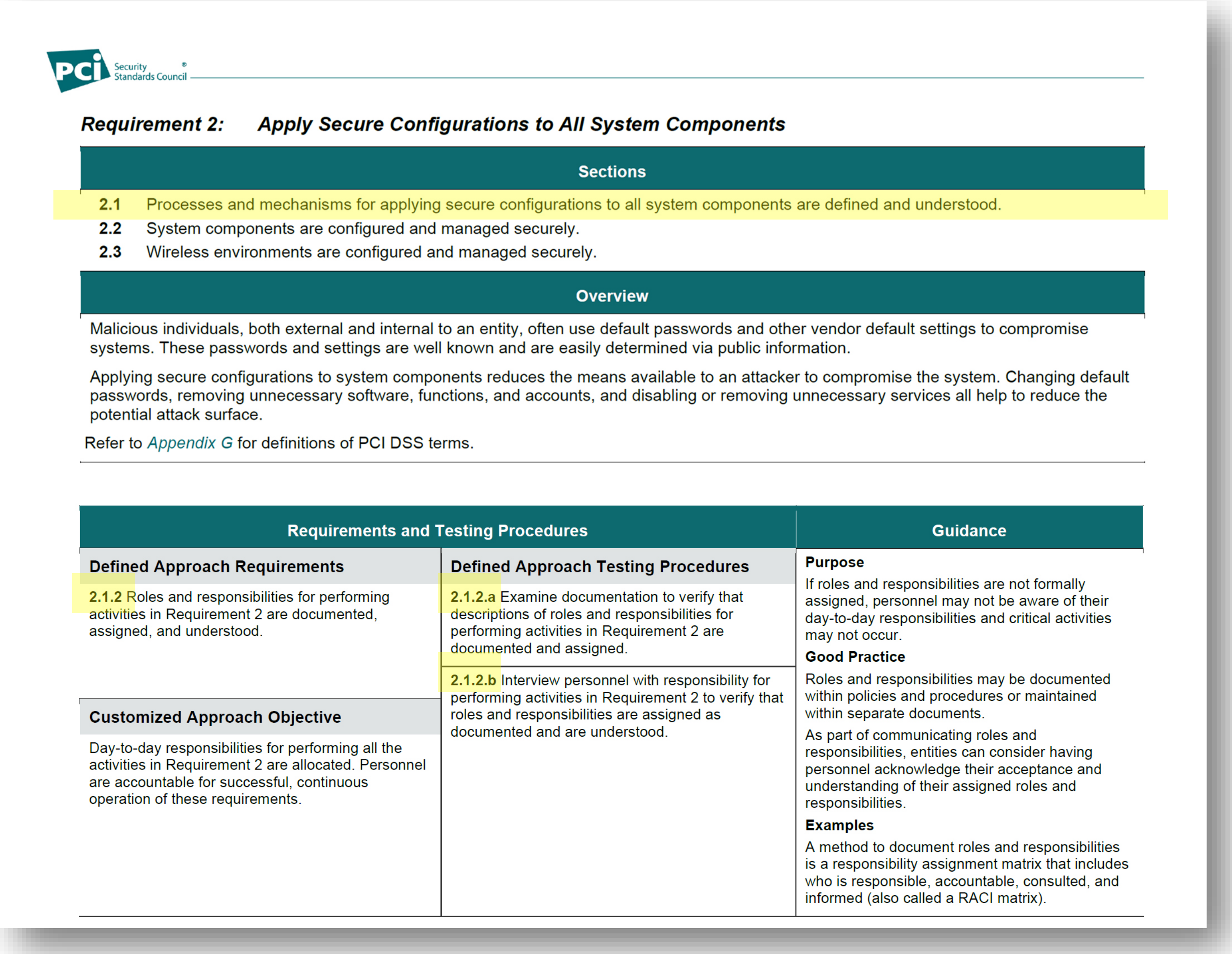
IMPACT

If this was not previously documented, it will need to be formally stated in a policy and/or procedure. RACI matrix can be used.

PROCESS

Organizations will need to ensure that these responsibilities are assigned and communicated to staff. Consider having employees acknowledge responsibilities.

Requirement 2.1.2



PCI Security Standards Council

Requirement 2: Apply Secure Configurations to All System Components

Sections	
2.1	Processes and mechanisms for applying secure configurations to all system components are defined and understood.
2.2	System components are configured and managed securely.
2.3	Wireless environments are configured and managed securely.

Overview

Malicious individuals, both external and internal to an entity, often use default passwords and other vendor default settings to compromise systems. These passwords and settings are well known and are easily determined via public information.

Applying secure configurations to system components reduces the means available to an attacker to compromise the system. Changing default passwords, removing unnecessary software, functions, and accounts, and disabling or removing unnecessary services all help to reduce the potential attack surface.

Refer to *Appendix G* for definitions of PCI DSS terms.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
2.1.2 Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.	2.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 2 are documented and assigned. 2.1.2.b Interview personnel with responsibility for performing activities in Requirement 2 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 2 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

WHAT

Roles and Responsibilities for applying secure configurations to all system components are documented, assigned, and maintained.

PURPOSE

If responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and processes may break down.

IMPACT

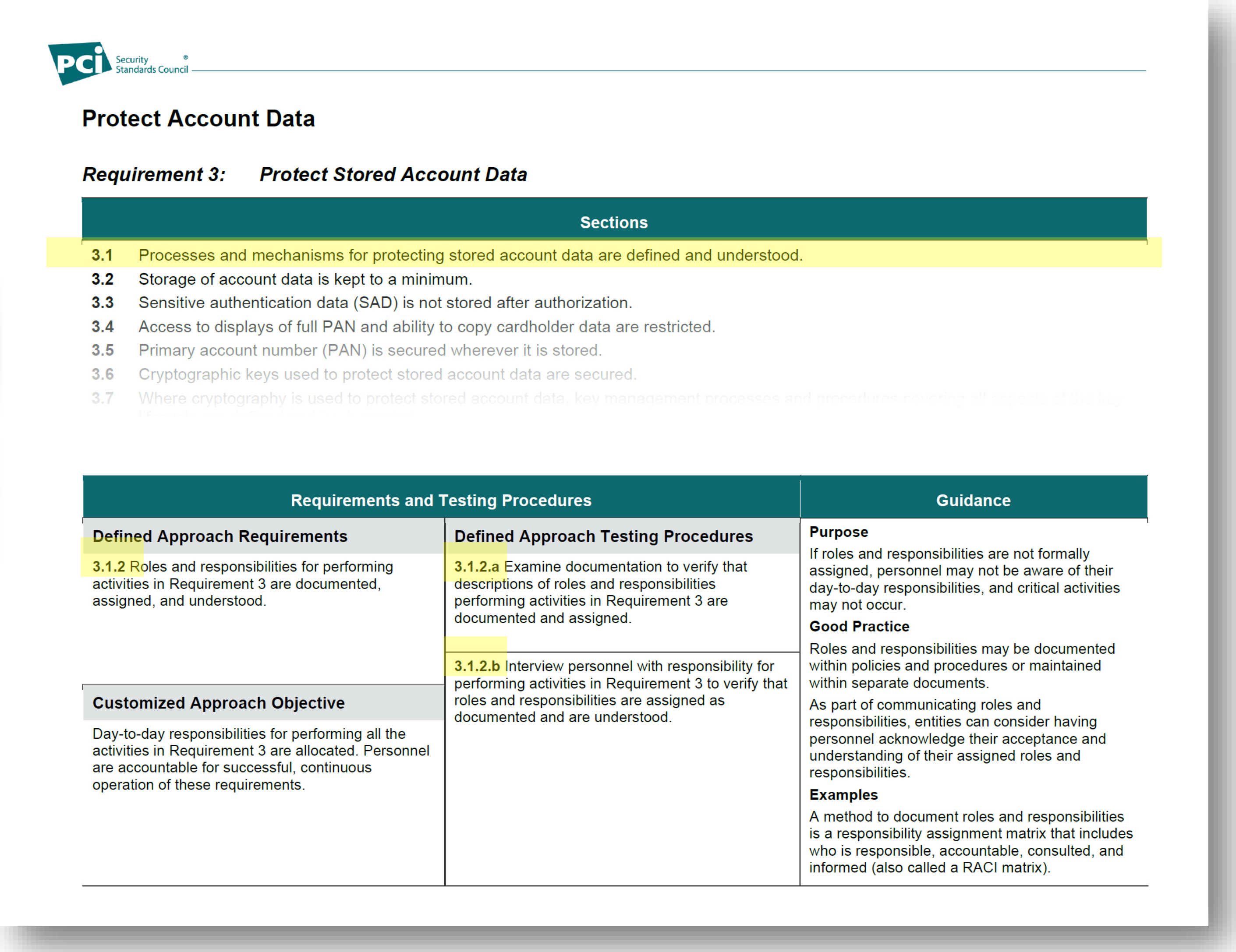
If this was not previously documented, it will need to be formally stated in a policy and/or procedure. RACI matrix can be used.

PROCESS

Organizations will need to ensure that these responsibilities are assigned and communicated to staff. Consider having employees acknowledge responsibilities.

HALOCK®

Requirement 3.1.2



PCI Security Standards Council

Protect Account Data

Requirement 3: Protect Stored Account Data

Sections	
3.1	Processes and mechanisms for protecting stored account data are defined and understood.
3.2	Storage of account data is kept to a minimum.
3.3	Sensitive authentication data (SAD) is not stored after authorization.
3.4	Access to displays of full PAN and ability to copy cardholder data are restricted.
3.5	Primary account number (PAN) is secured wherever it is stored.
3.6	Cryptographic keys used to protect stored account data are secured.
3.7	Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	**3.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities performing activities in Requirement 3 are documented and assigned. **3.1.2.b** Interview personnel with responsibility for performing activities in Requirement 3 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 3 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

WHAT

Roles and Responsibilities for protecting stored cardholder data are documented, assigned, and maintained.

PURPOSE

If responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and processes may break down.

IMPACT

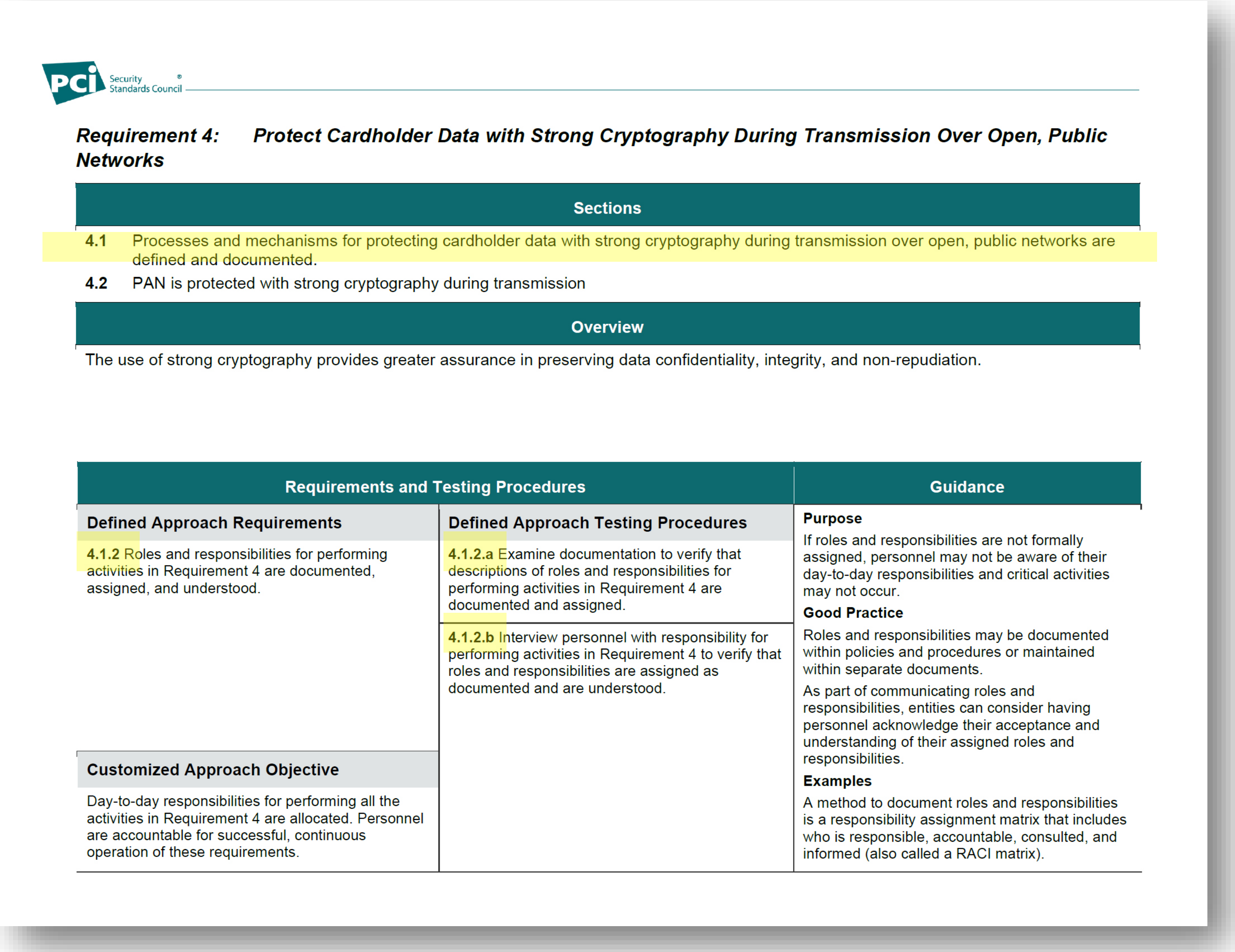
If this was not previously documented, it will need to be formally stated in a policy and/or procedure. RACI matrix can be used.

PROCESS

Organizations will need to ensure that these responsibilities are assigned and communicated to staff. Consider having employees acknowledge responsibilities.

HALOCK®

Requirement 4.1.2



PCI Security Standards Council

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Sections	
4.1	Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.
4.2	PAN is protected with strong cryptography during transmission

Overview

The use of strong cryptography provides greater assurance in preserving data confidentiality, integrity, and non-repudiation.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
4.1.2 Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.	**4.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 4 are documented and assigned. **4.1.2.b** Interview personnel with responsibility for performing activities in Requirement 4 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 4 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

WHAT

Roles and Responsibilities for protecting cardholder data during transmission over open public networks are documented, assigned, and maintained.

PURPOSE

If responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and processes may break down.

IMPACT

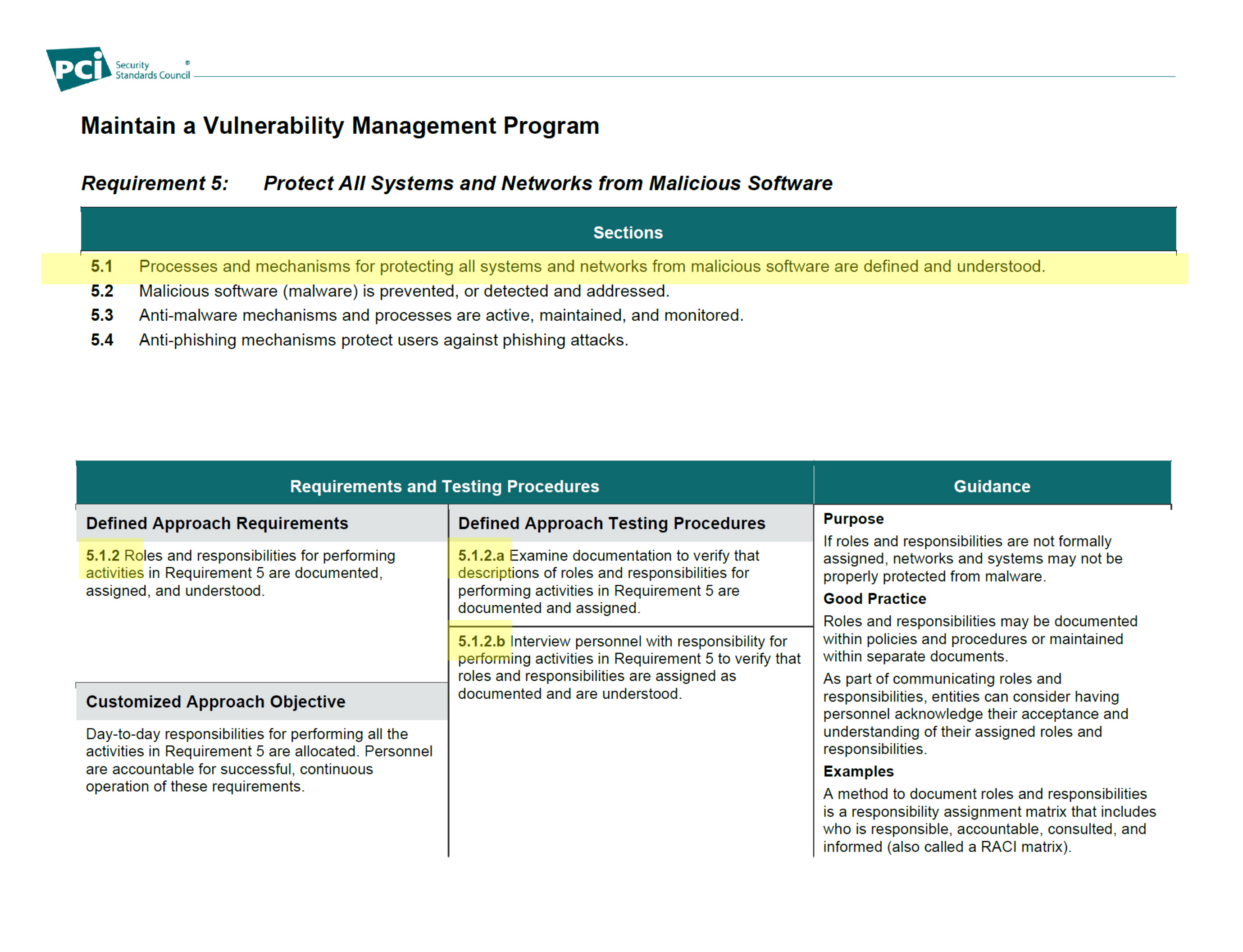
If this was not previously documented, it will need to be formally stated in a policy and/or procedure. RACI matrix can be used.

PROCESS

Organizations will need to ensure that these responsibilities are assigned and communicated to staff. Consider having employees acknowledge responsibilities.

HALOCK®

Requirement 5.1.2



PCI Security Standards Council

Maintain a Vulnerability Management Program

Requirement 5: ***Protect All Systems and Networks from Malicious Software***

Sections	
5.1	Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.
5.2	Malicious software (malware) is prevented, or detected and addressed.
5.3	Anti-malware mechanisms and processes are active, maintained, and monitored.
5.4	Anti-phishing mechanisms protect users against phishing attacks.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, networks and systems may not be properly protected from malware. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
5.1.2 Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.	**5.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 5 are documented and assigned.	
	5.1.2.b Interview personnel with responsibility for performing activities in Requirement 5 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 5 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

WHAT

Roles and Responsibilities for protecting components from malicious software are documented, assigned, and maintained.

PURPOSE

If responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and processes may break down.

IMPACT

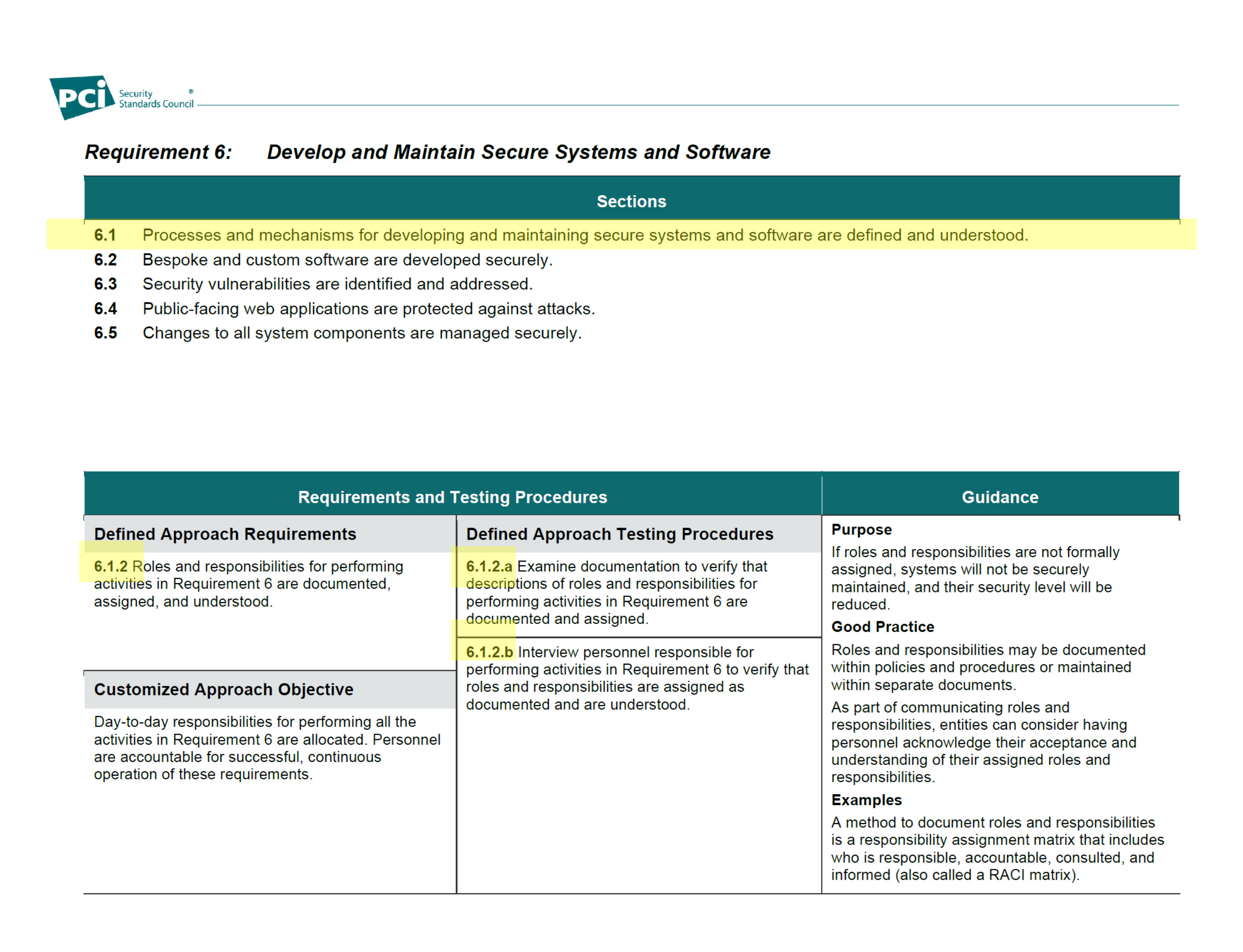
If this was not previously documented, it will need to be formally stated in a policy and/or procedure. RACI matrix can be used.

PROCESS

Organizations will need to ensure that these responsibilities are assigned and communicated to staff. Consider having employees acknowledge responsibilities.

HALOCK®

Requirement 6.1.2



PCI Security Standards Council

Requirement 6: Develop and Maintain Secure Systems and Software

Sections	
6.1	Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.
6.2	Bespoke and custom software are developed securely.
6.3	Security vulnerabilities are identified and addressed.
6.4	Public-facing web applications are protected against attacks.
6.5	Changes to all system components are managed securely.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, systems will not be securely maintained, and their security level will be reduced. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	**6.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 6 are documented and assigned. **6.1.2.b** Interview personnel responsible for performing activities in Requirement 6 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 6 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

WHAT

Roles and Responsibilities for developing and maintaining secure systems and software are documented, assigned, and maintained.

PURPOSE

If responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and processes may break down.

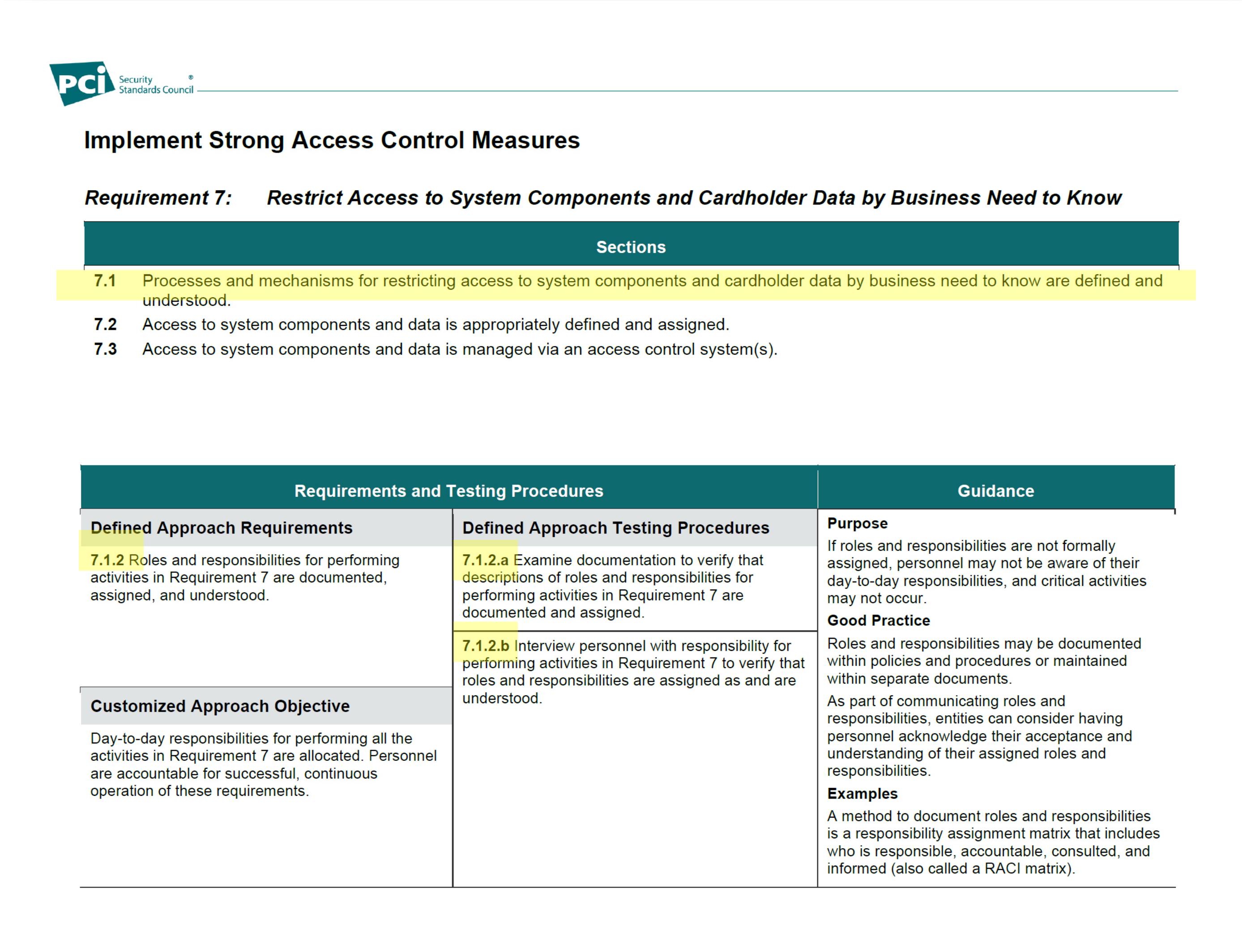
IMPACT

If this was not previously documented, it will need to be formally stated in a policy and/or procedure. RACI matrix can be used.

PROCESS

Organizations will need to ensure that these responsibilities are assigned and communicated to staff. Consider having employees acknowledge responsibilities.

Requirement 7.1.2



Security Standards Council

Implement Strong Access Control Measures

Requirement 7: ***Restrict Access to System Components and Cardholder Data by Business Need to Know***

Sections	
7.1	Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.
7.2	Access to system components and data is appropriately defined and assigned.
7.3	Access to system components and data is managed via an access control system(s).

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
7.1.2 Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.	7.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 7 are documented and assigned. 7.1.2.b Interview personnel with responsibility for performing activities in Requirement 7 to verify that roles and responsibilities are assigned as and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 7 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

WHAT

Roles and Responsibilities for strong access control mechanisms are documented, assigned, and maintained.

PURPOSE

If responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and processes may break down.

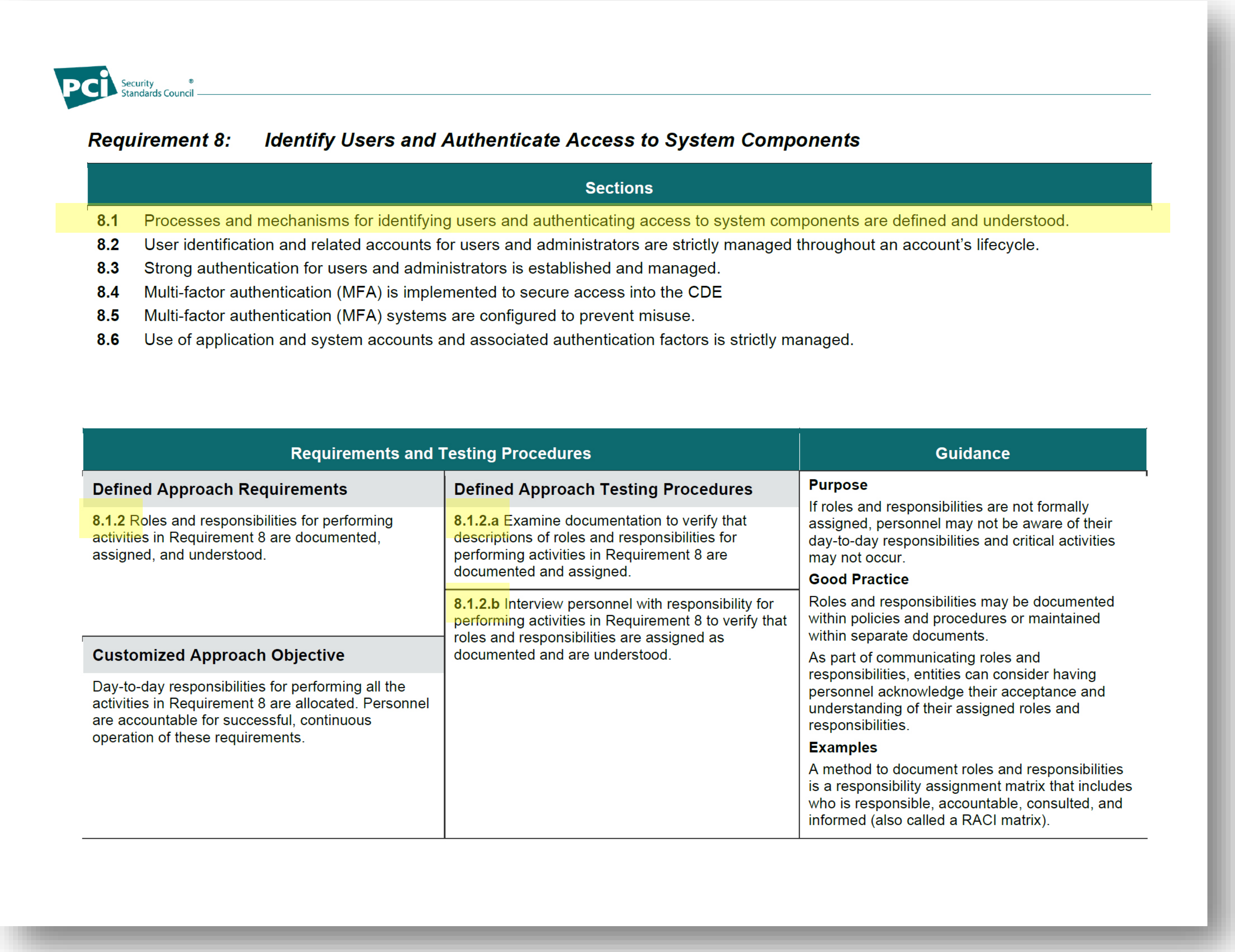
IMPACT

If this was not previously documented, it will need to be formally stated in a policy and/or procedure. RACI matrix can be used.

PROCESS

Organizations will need to ensure that these responsibilities are assigned and communicated to staff. Consider having employees acknowledge responsibilities.

Requirement 8.1.2



PCI Security Standards Council

Requirement 8: Identify Users and Authenticate Access to System Components

Sections	
8.1	Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.
8.2	User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.
8.3	Strong authentication for users and administrators is established and managed.
8.4	Multi-factor authentication (MFA) is implemented to secure access into the CDE
8.5	Multi-factor authentication (MFA) systems are configured to prevent misuse.
8.6	Use of application and system accounts and associated authentication factors is strictly managed.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
8.1.2 Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.	8.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 8 are documented and assigned. 8.1.2.b Interview personnel with responsibility for performing activities in Requirement 8 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 8 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

WHAT

Roles and Responsibilities for strong authentication mechanisms are documented, assigned, and maintained.

PURPOSE

If responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and processes may break down.

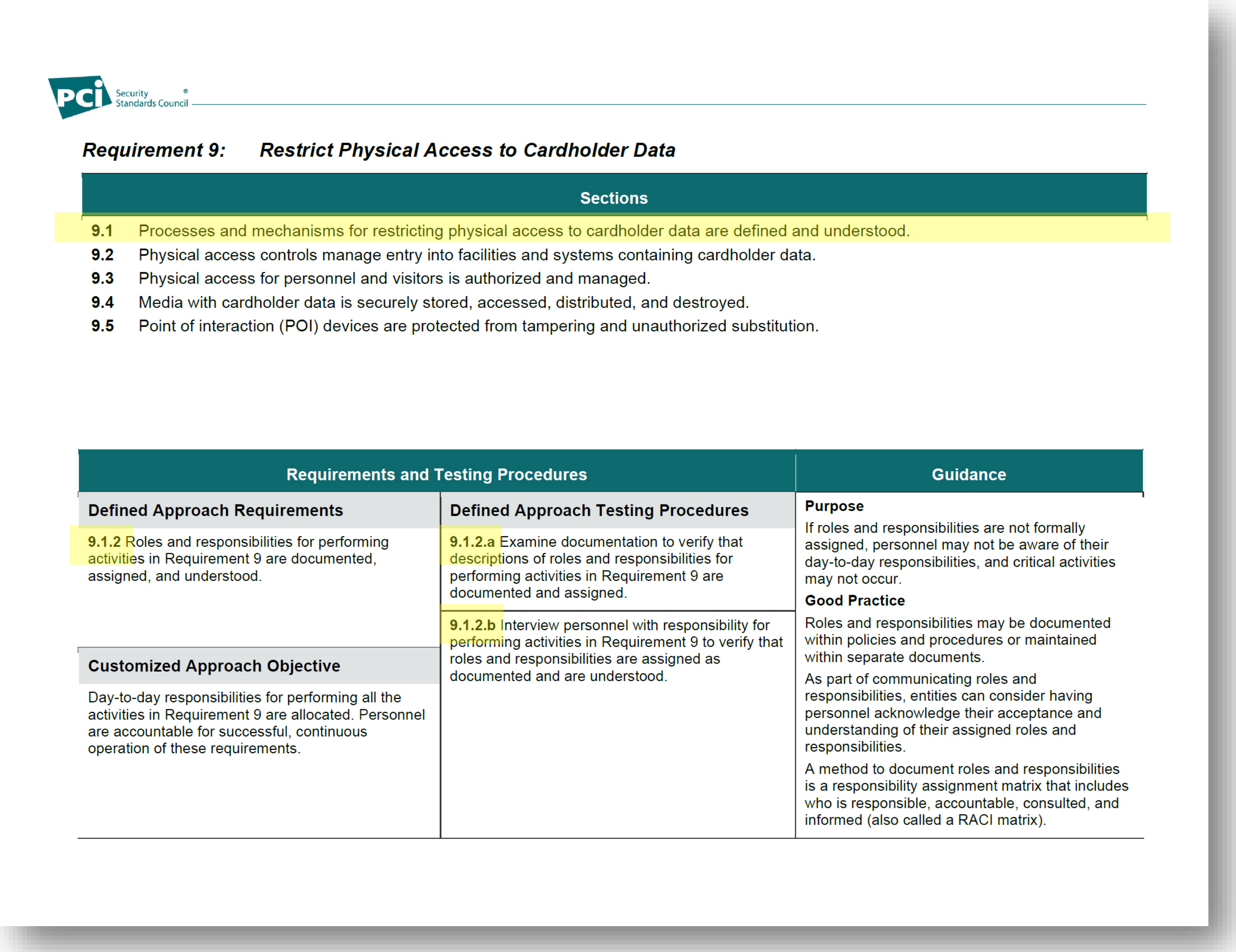
IMPACT

If this was not previously documented, it will need to be formally stated in a policy and/or procedure. RACI matrix can be used.

PROCESS

Organizations will need to ensure that these responsibilities are assigned and communicated to staff. Consider having employees acknowledge responsibilities.

Requirement 9.1.2



PCI Security Standards Council

Requirement 9: ***Restrict Physical Access to Cardholder Data***

Sections

9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

9.2 Physical access controls manage entry into facilities and systems containing cardholder data.

9.3 Physical access for personnel and visitors is authorized and managed.

9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.

9.5 Point of interaction (POI) devices are protected from tampering and unauthorized substitution.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities, and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
9.1.2 Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	**9.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 9 are documented and assigned. **9.1.2.b** Interview personnel with responsibility for performing activities in Requirement 9 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 9 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

WHAT

Roles and Responsibilities for physical access controls are documented, assigned, and maintained.

PURPOSE

If responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and processes may break down.

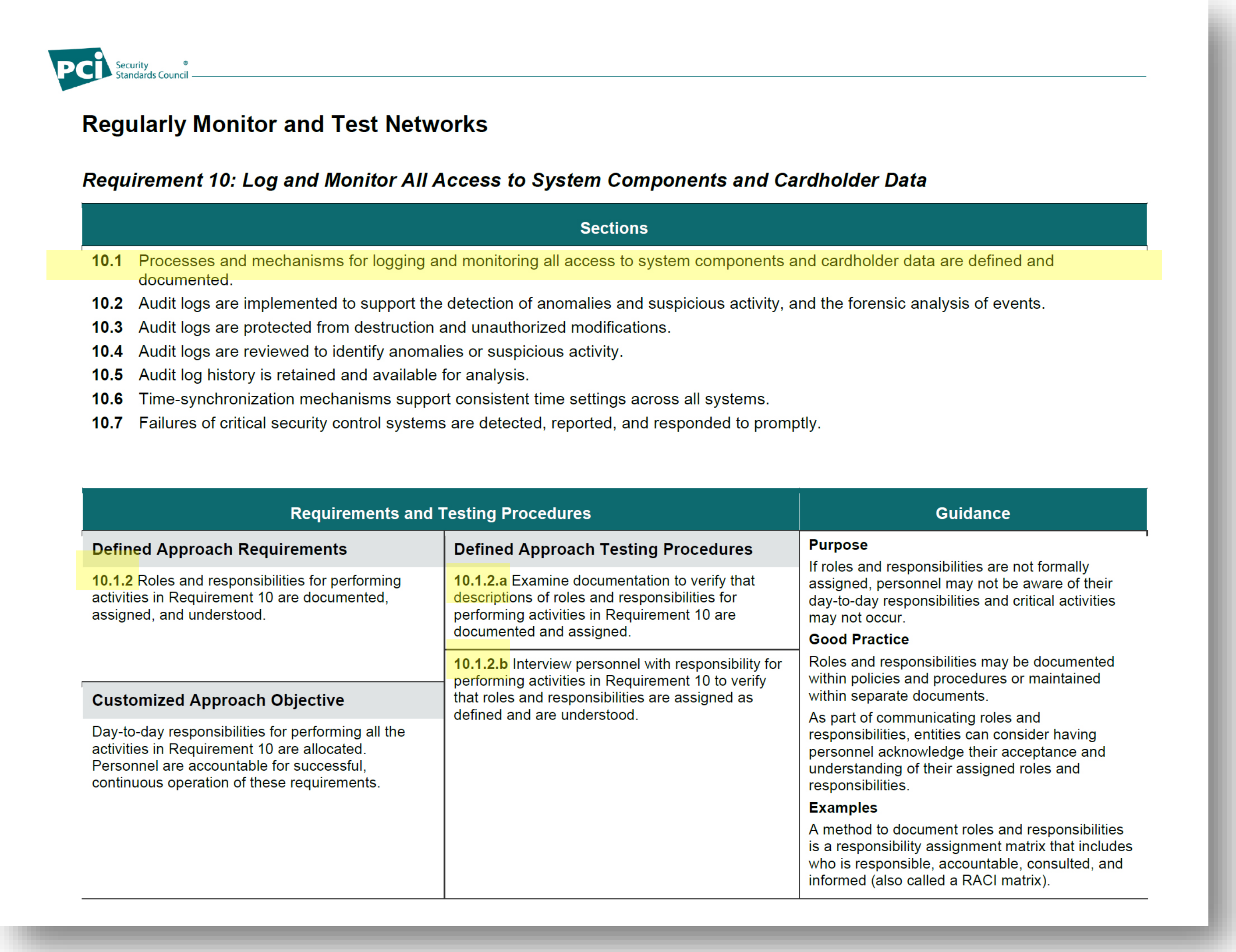
IMPACT

If this was not previously documented, it will need to be formally stated in a policy and/or procedure. RACI matrix can be used.

PROCESS

Organizations will need to ensure that these responsibilities are assigned and communicated to staff. Consider having employees acknowledge responsibilities.

Requirement 10.1.2



Security Standards Council

Regularly Monitor and Test Networks

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

Sections

10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.

10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.

10.3 Audit logs are protected from destruction and unauthorized modifications.

10.4 Audit logs are reviewed to identify anomalies or suspicious activity.

10.5 Audit log history is retained and available for analysis.

10.6 Time-synchronization mechanisms support consistent time settings across all systems.

10.7 Failures of critical security control systems are detected, reported, and responded to promptly.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	**10.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 10 are documented and assigned. **10.1.2.b** Interview personnel with responsibility for performing activities in Requirement 10 to verify that roles and responsibilities are assigned as defined and are understood.	
Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 10 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

WHAT

Roles and Responsibilities for logging and monitoring are documented, assigned, and maintained.

PURPOSE

If responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and processes may break down.

IMPACT

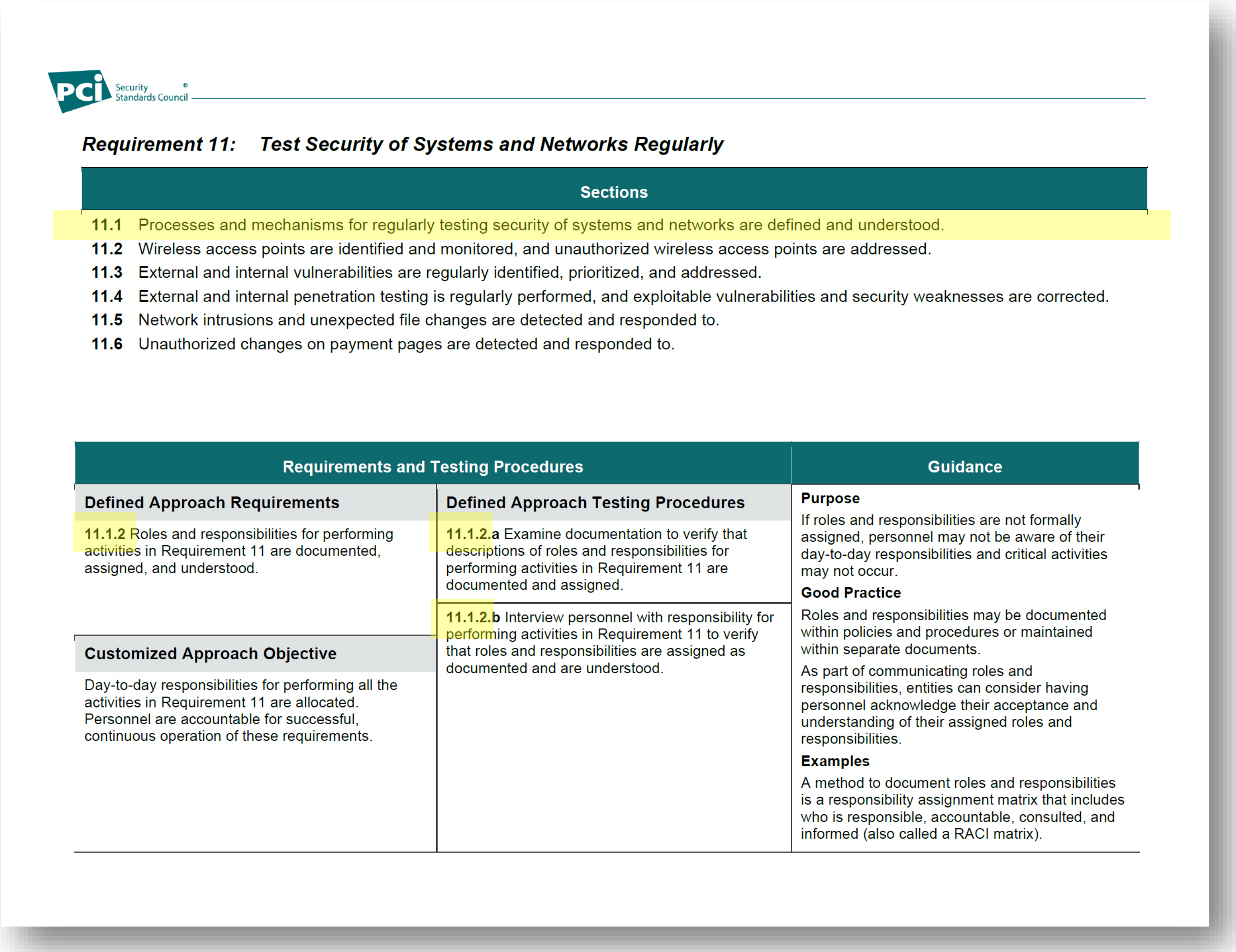
If this was not previously documented, it will need to be formally stated in a policy and/or procedure. RACI matrix can be used.

PROCESS

Organizations will need to ensure that these responsibilities are assigned and communicated to staff. Consider having employees acknowledge responsibilities.

HALOCK®

Requirement 11.1.2



PCI Security Standards Council

Requirement 11:* *Test Security of Systems and Networks Regularly

Sections	
11.1	Processes and mechanisms for regularly testing security of systems and networks are defined and understood.
11.2	Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.
11.3	External and internal vulnerabilities are regularly identified, prioritized, and addressed.
11.4	External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.
11.5	Network intrusions and unexpected file changes are detected and responded to.
11.6	Unauthorized changes on payment pages are detected and responded to.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. **Good Practice** Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. **Examples** A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
11.1.2 Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	**11.1.2.a** Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 11 are documented and assigned.	
	11.1.2.b Interview personnel with responsibility for performing activities in Requirement 11 to verify that roles and responsibilities are assigned as documented and are understood.	
Customized Approach Objective		
Day-to-day responsibilities for performing all the activities in Requirement 11 are allocated. Personnel are accountable for successful, continuous operation of these requirements.		

WHAT

Roles and Responsibilities for testing security of systems and networks are documented, assigned, and maintained.

PURPOSE

If responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and processes may break down.

IMPACT

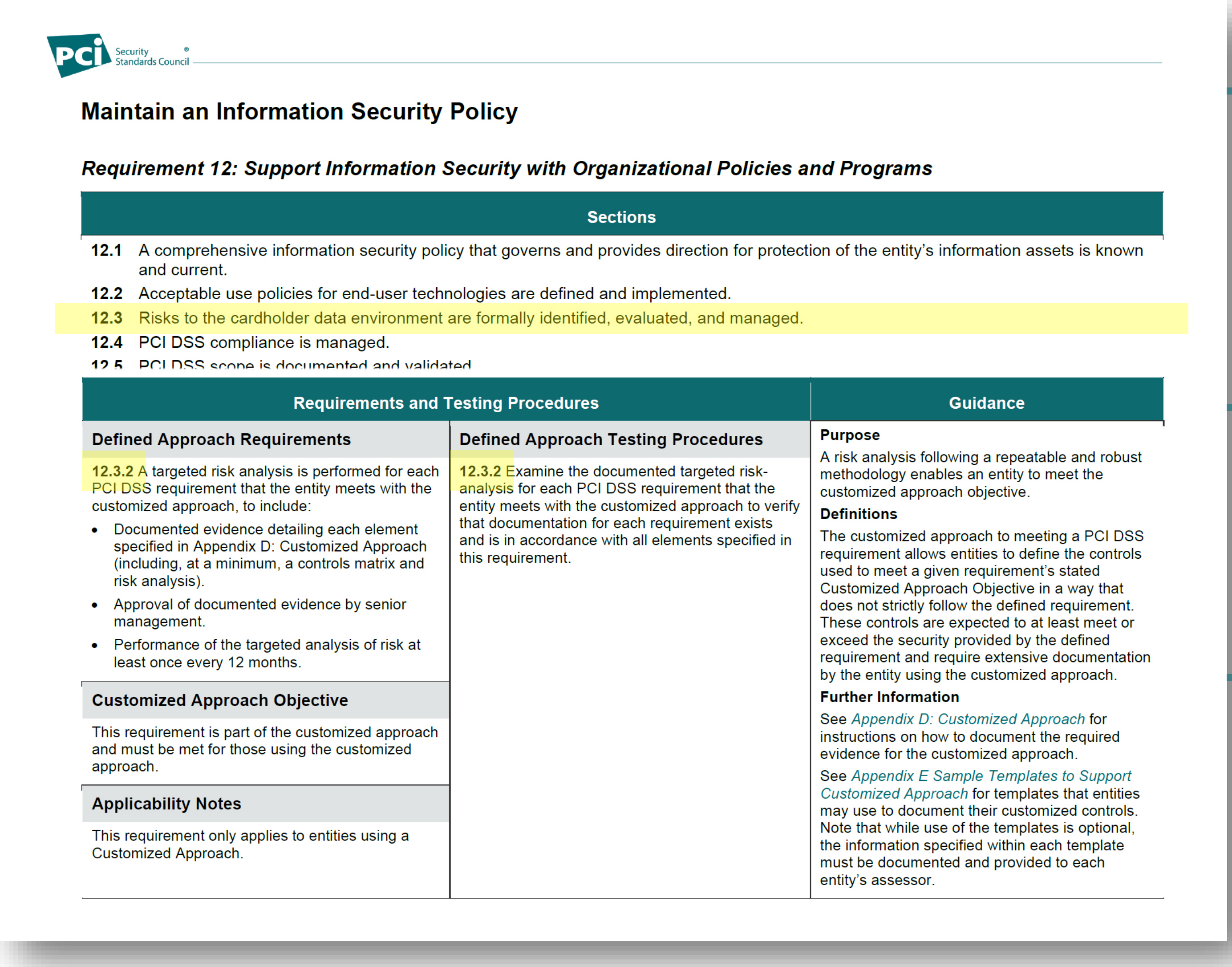
If this was not previously documented, it will need to be formally stated in a policy and/or procedure. RACI matrix can be used.

PROCESS

Organizations will need to ensure that these responsibilities are assigned and communicated to staff. Consider having employees acknowledge responsibilities.

HALOCK®

Requirement 12.3.2



Maintain an Information Security Policy

Requirement 12: Support Information Security with Organizational Policies and Programs

Sections	
12.1	A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.
12.2	Acceptable use policies for end-user technologies are defined and implemented.
12.3	Risks to the cardholder data environment are formally identified, evaluated, and managed.
12.4	PCI DSS compliance is managed.
12.5	PCI DSS scope is documented and validated

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** A risk analysis following a repeatable and robust methodology enables an entity to meet the customized approach objective. **Definitions** The customized approach to meeting a PCI DSS requirement allows entities to define the controls used to meet a given requirement's stated Customized Approach Objective in a way that does not strictly follow the defined requirement. These controls are expected to at least meet or exceed the security provided by the defined requirement and require extensive documentation by the entity using the customized approach. **Further Information** See *Appendix D: Customized Approach* for instructions on how to document the required evidence for the customized approach. See *Appendix E Sample Templates to Support Customized Approach* for templates that entities may use to document their customized controls. Note that while use of the templates is optional, the information specified within each template must be documented and provided to each entity's assessor.
12.3.2 A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: • Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). • Approval of documented evidence by senior management. • Performance of the targeted analysis of risk at least once every 12 months.	**12.3.2** Examine the documented targeted risk-analysis for each PCI DSS requirement that the entity meets with the customized approach to verify that documentation for each requirement exists and is in accordance with all elements specified in this requirement.	
Customized Approach Objective		
This requirement is part of the customized approach and must be met for those using the customized approach.		
Applicability Notes		
This requirement only applies to entities using a Customized Approach.		

WHAT

If using the Customized Approach to validate a PCI DSS requirement, a Controls Matrix and Targeted Risk Analysis needs to be completed.

PURPOSE

To add flexibility for risk mature organizations validating PCI DSS compliance. Explain what is implemented, how control(s) meet objectives, how control(s) provide at least an equivalent level of protection, and assurance of control effectiveness.

Only for Onsite Assessment Validations.

IMPACT

The flexibility that comes with using the Customized Approach also requires an additional documented process from the assessed entity.

PROCESS

The assessed entity completes a Controls Matrix and Targeted Risk Analysis, at least annually that is approved by management and provide to QSA. QSA then creates custom testing procedures to validate controls.

Requirement 12.3.2 Details

Appendix D in PCI DSS v4.0 contains additional information and guidance on using the Customized Approach for validating compliance.

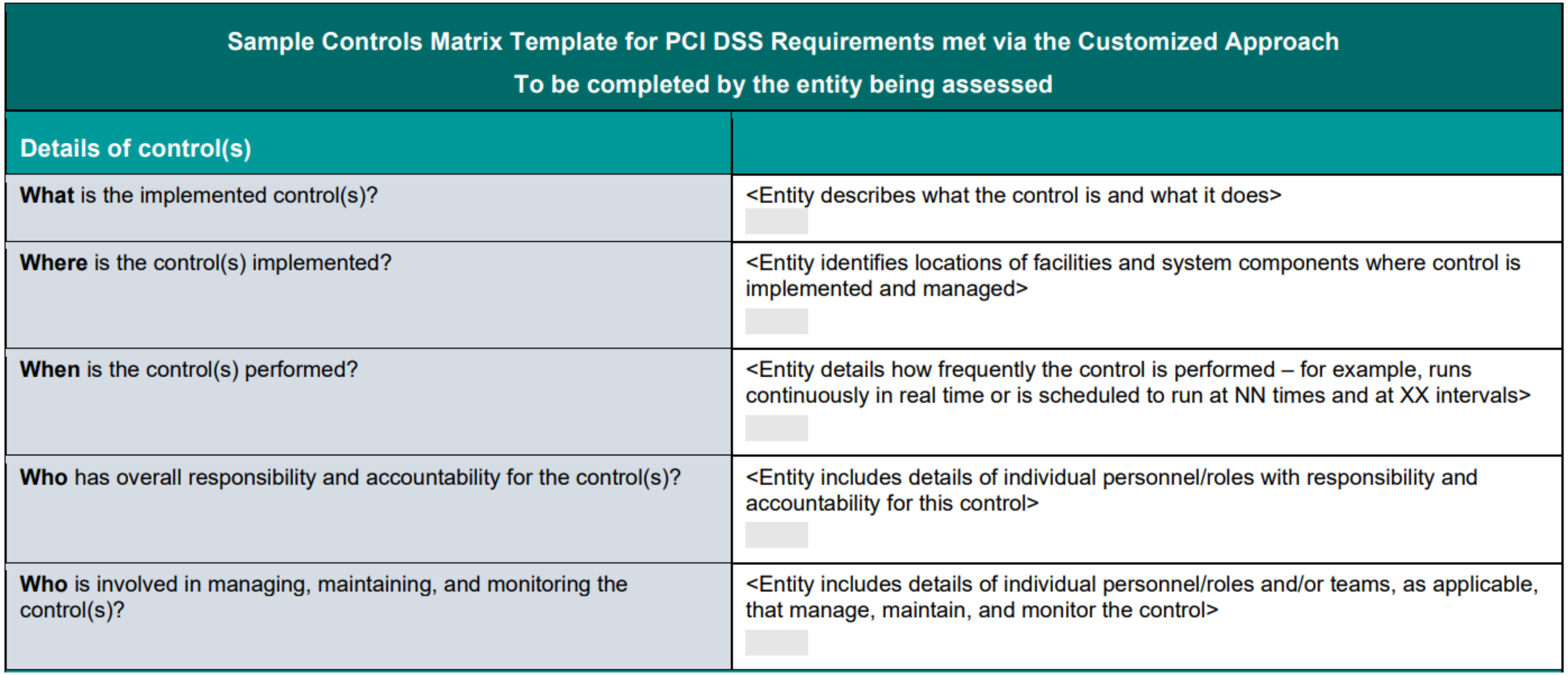
Appendix E in PCI DSS v4.0 provides a Sample Controls Matrix template and a Sample Targeted Risk Analysis template.

One for each requirement that is validated with the Customized Approach.

1) Identify PCI DSS requirement and control objective (both within the PCI DSS) as seen below.

Requirement 12.3.2 Details Continued

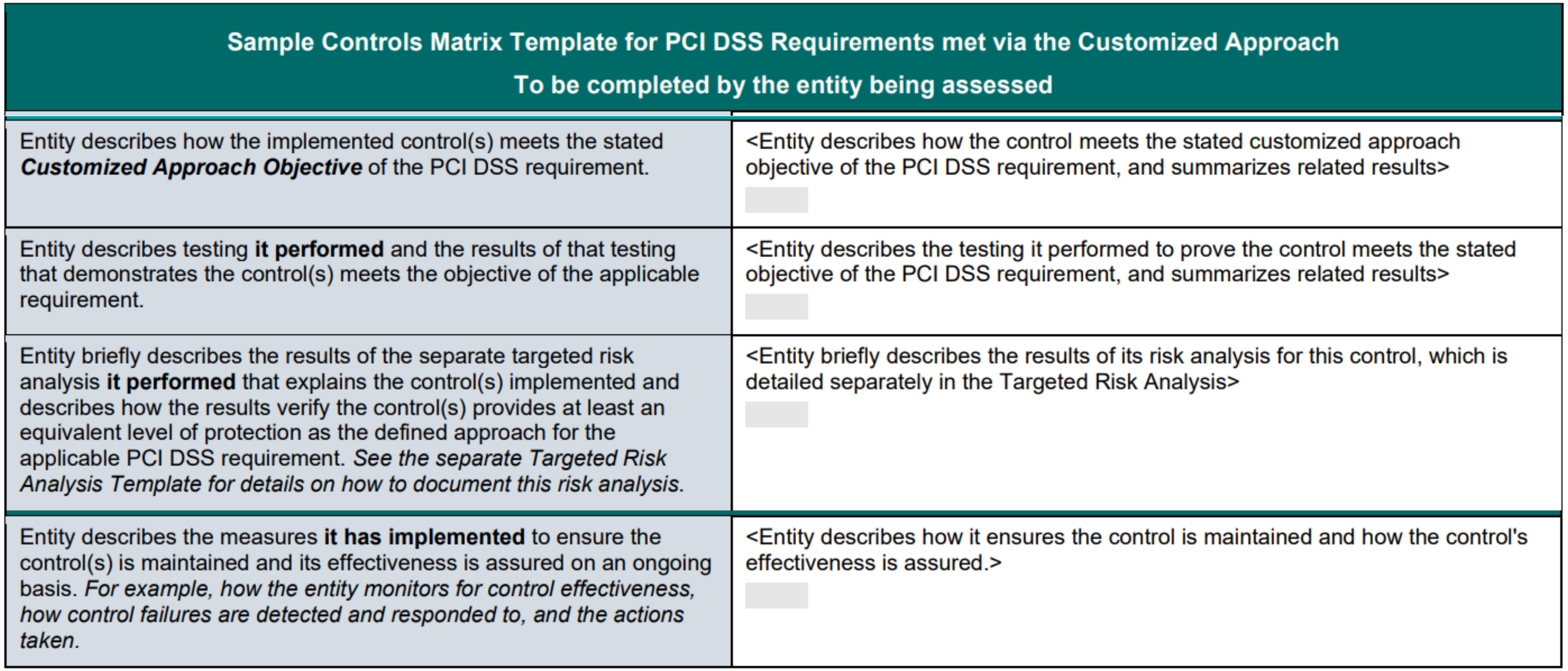
2) Provide details of control(s) – the What, Where, When and Who.



Sample Controls Matrix Template for PCI DSS Requirements met via the Customized Approach To be completed by the entity being assessed	
Details of control(s)	
What is the implemented control(s)?	<Entity describes what the control is and what it does>
Where is the control(s) implemented?	<Entity identifies locations of facilities and system components where control is implemented and managed>
When is the control(s) performed?	<Entity details how frequently the control is performed – for example, runs continuously in real time or is scheduled to run at NN times and at XX intervals>
Who has overall responsibility and accountability for the control(s)?	<Entity includes details of individual personnel/roles with responsibility and accountability for this control>
Who is involved in managing, maintaining, and monitoring the control(s)?	<Entity includes details of individual personnel/roles and/or teams, as applicable, that manage, maintain, and monitor the control>

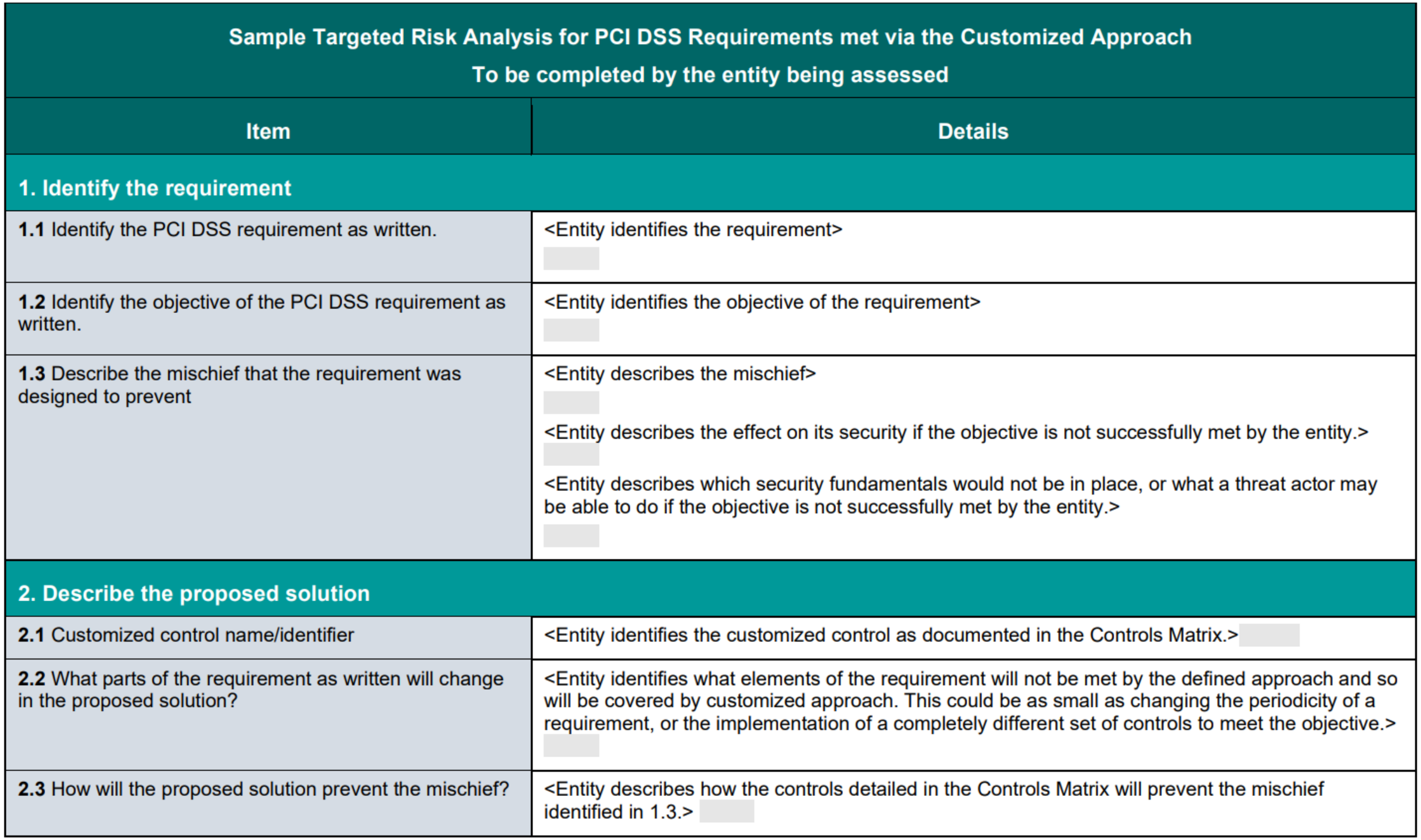
Requirement 12.3.2 Details Continued

3) Explain how control objective is being met.
4) Explain how assessed entity tested control to ensure control objectives are met.
5) Describe the results of the risk analysis of the control.
6) Describe how the control is maintained and the control's effectiveness is assured.



Sample Controls Matrix Template for PCI DSS Requirements met via the Customized Approach **To be completed by the entity being assessed**	
Entity describes how the implemented control(s) meets the stated ***Customized Approach Objective*** of the PCI DSS requirement.	<Entity describes how the control meets the stated customized approach objective of the PCI DSS requirement, and summarizes related results>
Entity describes testing **it performed** and the results of that testing that demonstrates the control(s) meets the objective of the applicable requirement.	<Entity describes the testing it performed to prove the control meets the stated objective of the PCI DSS requirement, and summarizes related results>
Entity briefly describes the results of the separate targeted risk analysis **it performed** that explains the control(s) implemented and describes how the results verify the control(s) provides at least an equivalent level of protection as the defined approach for the applicable PCI DSS requirement. *See the separate Targeted Risk Analysis Template for details on how to document this risk analysis.*	<Entity briefly describes the results of its risk analysis for this control, which is detailed separately in the Targeted Risk Analysis>
Entity describes the measures **it has implemented** to ensure the control(s) is maintained and its effectiveness is assured on an ongoing basis. *For example, how the entity monitors for control effectiveness, how control failures are detected and responded to, and the actions taken.*	<Entity describes how it ensures the control is maintained and how the control's effectiveness is assured.>

Requirement 12.3.2 Details Continued



Sample Targeted Risk Analysis for PCI DSS Requirements met via the Customized Approach
To be completed by the entity being assessed

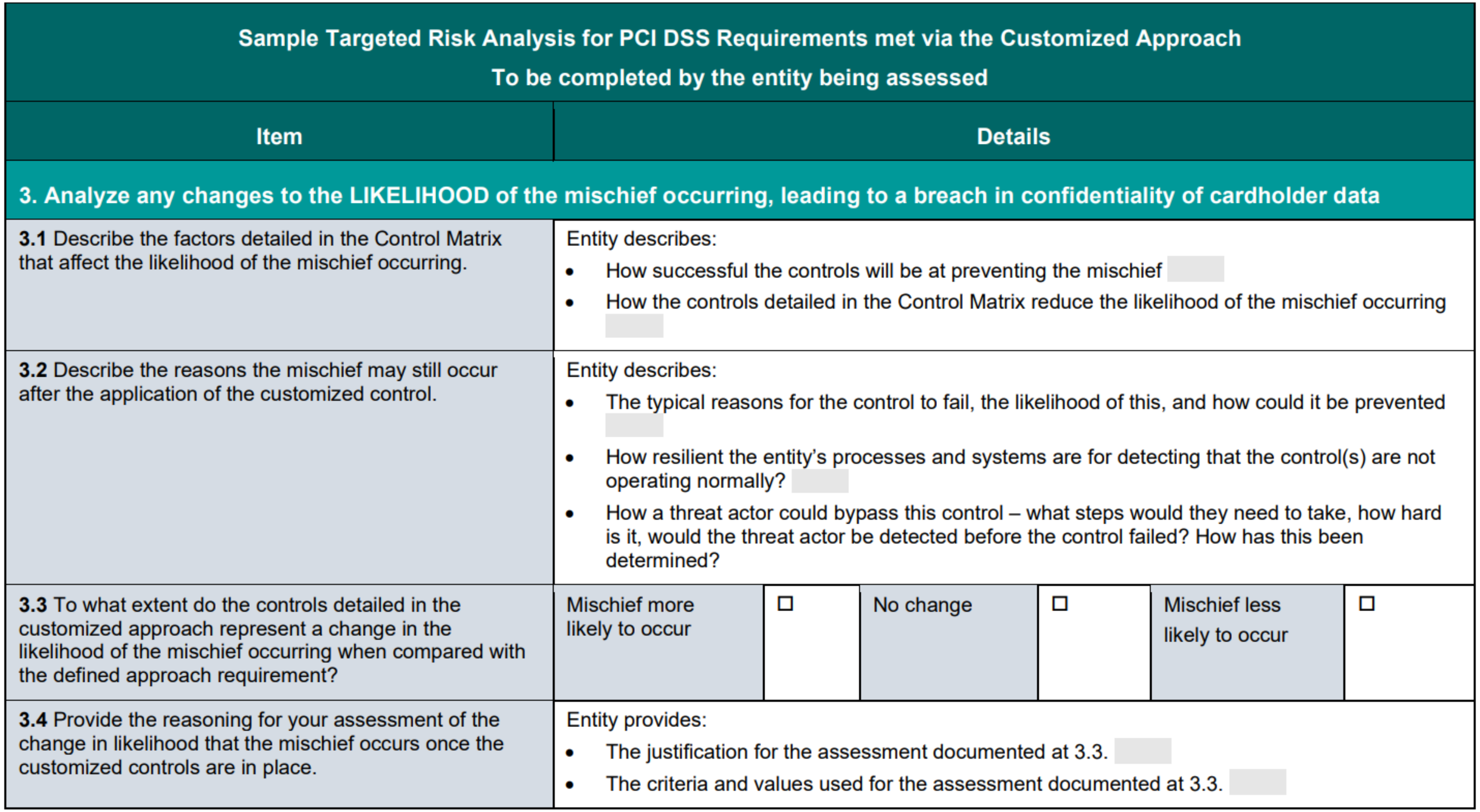
Item	Details
1. Identify the requirement	
1.1 Identify the PCI DSS requirement as written.	<Entity identifies the requirement>
1.2 Identify the objective of the PCI DSS requirement as written.	<Entity identifies the objective of the requirement>
1.3 Describe the mischief that the requirement was designed 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.>

This template is only for the Customized Approach Targeted Risk Analysis.

You do not have to use the PCI SSC's template, but all items in their template must be included.

Mischief managed.

Requirement 12.3.2 Details Continued



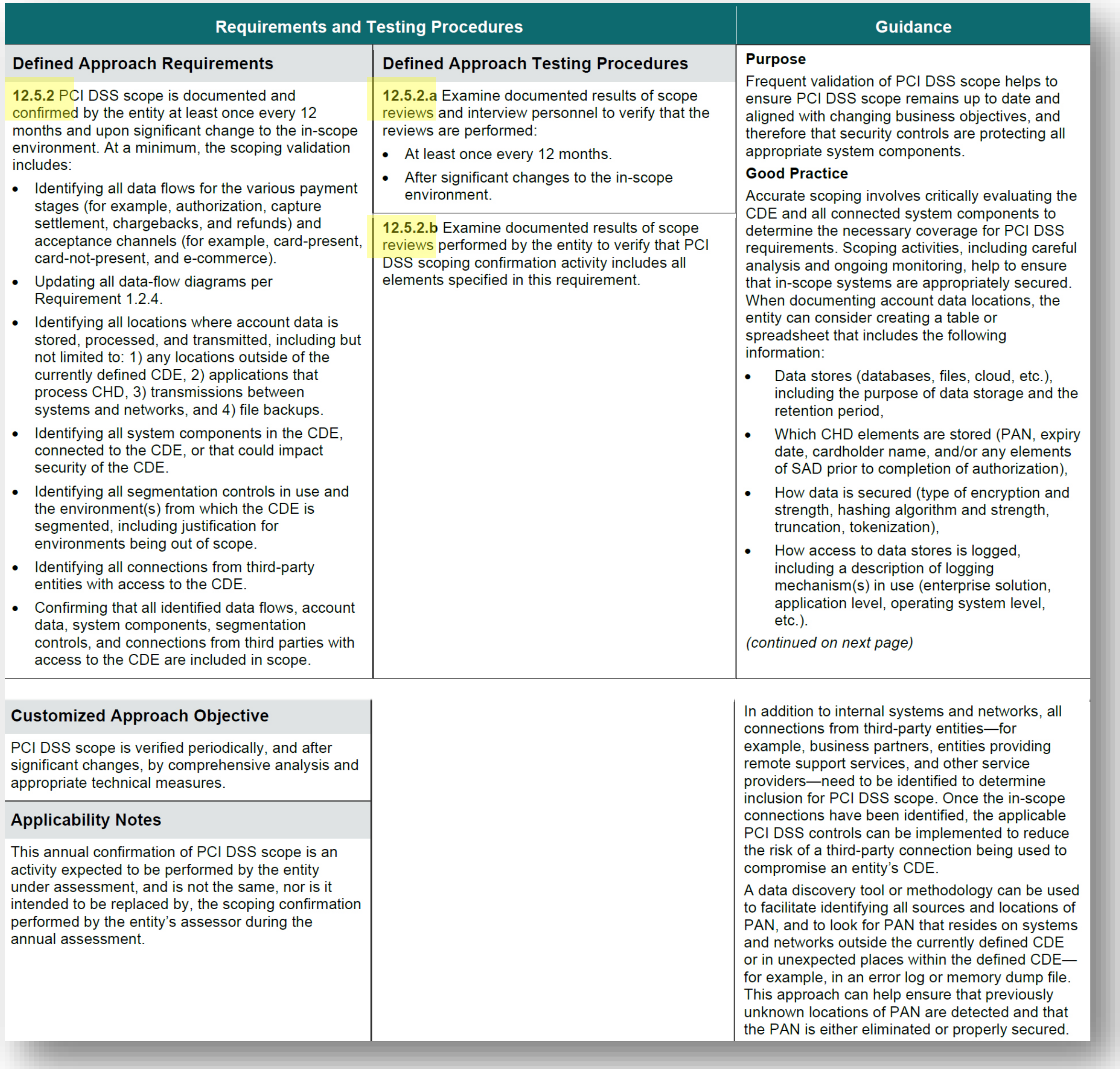
Sample Targeted Risk Analysis for PCI DSS Requirements met via the Customized Approach

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.

Likelihood of mischief occurring and how your customized control(s) impact that likelihood.

Requirement 12.5.2



Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Frequent validation of PCI DSS scope helps to ensure PCI DSS scope remains up to date and aligned with changing business objectives, and therefore that security controls are protecting all appropriate system components. **Good Practice** Accurate scoping involves critically evaluating the CDE and all connected system components to determine the necessary coverage for PCI DSS requirements. Scoping activities, including careful analysis and ongoing monitoring, help to ensure that in-scope systems are appropriately secured. When documenting account data locations, the entity can consider creating a table or spreadsheet that includes the following information: • Data stores (databases, files, cloud, etc.), including the purpose of data storage and the retention period, • Which CHD elements are stored (PAN, expiry date, cardholder name, and/or any elements of SAD prior to completion of authorization), • How data is secured (type of encryption and strength, hashing algorithm and strength, truncation, tokenization), • How access to data stores is logged, including a description of logging mechanism(s) in use (enterprise solution, application level, operating system level, etc.). *(continued on next page)*
12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). • Updating all data-flow diagrams per Requirement 1.2.4. • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. • Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. • Identifying all connections from third-party entities with access to the CDE. • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.	**12.5.2.a** Examine documented results of scope reviews and interview personnel to verify that the reviews are performed: • At least once every 12 months. • After significant changes to the in-scope environment. **12.5.2.b** Examine documented results of scope reviews performed by the entity to verify that PCI DSS scoping confirmation activity includes all elements specified in this requirement.	
Customized Approach Objective PCI DSS scope is verified periodically, and after significant changes, by comprehensive analysis and appropriate technical measures. **Applicability Notes** This annual confirmation of PCI DSS scope is an activity expected to be performed by the entity under assessment, and is not the same, nor is it intended to be replaced by, the scoping confirmation performed by the entity's assessor during the annual assessment.		In addition to internal systems and networks, all connections from third-party entities—for example, business partners, entities providing remote support services, and other service providers—need to be identified to determine inclusion for PCI DSS scope. Once the in-scope connections have been identified, the applicable PCI DSS controls can be implemented to reduce the risk of a third-party connection being used to compromise an entity's CDE. A data discovery tool or methodology can be used to facilitate identifying all sources and locations of PAN, and to look for PAN that resides on systems and networks outside the currently defined CDE or in unexpected places within the defined CDE—for example, in an error log or memory dump file. This approach can help ensure that previously unknown locations of PAN are detected and that the PAN is either eliminated or properly secured.

WHAT

PCI DSS Scope is defined and confirmed by the assessed entity, at least annually. Independent of the QSA's scope validation efforts.

PURPOSE

PCI DSS scoping can be the most difficult to understand, therefore extremely important to understand and manage, before a QSA starts their validation.

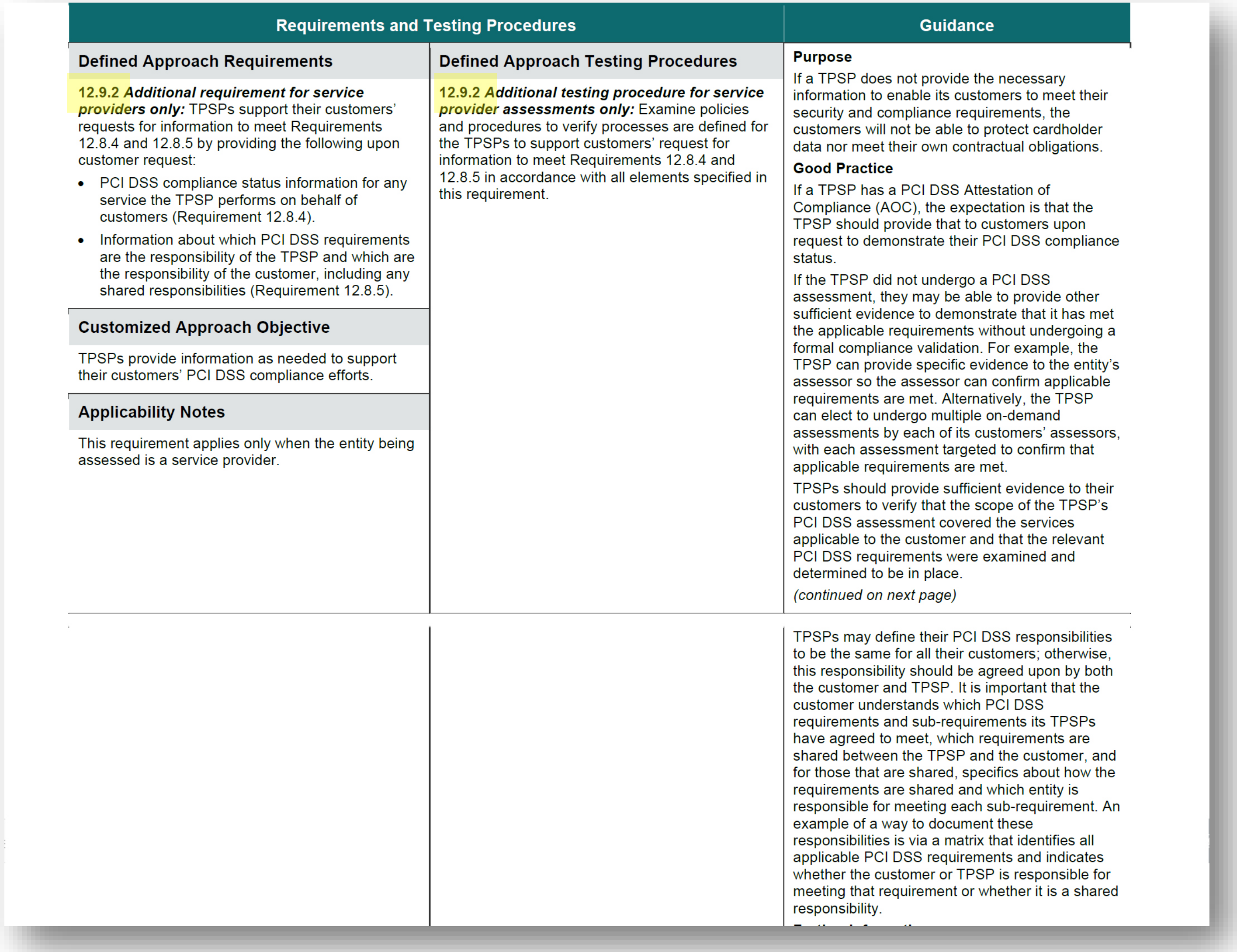
IMPACT

Assessed entities will need to develop a process to define and confirm scope, at least annually.
Note: Service Providers will be required to do this bi-annually in March of 2025.

PROCESS

Organizations will need to ensure a process exists to validate PCI DSS scope annually. The Defined Approach Details explains what needs to be included. This requirement Good Practice guidance is very helpful.

Requirement 12.9.2



Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** If a TPSP does not provide the necessary information to enable its customers to meet their security and compliance requirements, the customers will not be able to protect cardholder data nor meet their own contractual obligations. **Good Practice** If a TPSP has a PCI DSS Attestation of Compliance (AOC), the expectation is that the TPSP should provide that to customers upon request to demonstrate their PCI DSS compliance status. If the TPSP did not undergo a PCI DSS assessment, they may be able to provide other sufficient evidence to demonstrate that it has met the applicable requirements without undergoing a formal compliance validation. For example, the TPSP can provide specific evidence to the entity's assessor so the assessor can confirm applicable requirements are met. Alternatively, the TPSP can elect to undergo multiple on-demand assessments by each of its customers' assessors, with each assessment targeted to confirm that applicable requirements are met. TPSPs should provide sufficient evidence to their customers to verify that the scope of the TPSP's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place. *(continued on next page)* TPSPs may define their PCI DSS responsibilities to be the same for all their customers; otherwise, this responsibility should be agreed upon by both the customer and TPSP. It is important that the customer understands which PCI DSS requirements and sub-requirements its TPSPs have agreed to meet, which requirements are shared between the TPSP and the customer, and for those that are shared, specifics about how the requirements are shared and which entity is responsible for meeting each sub-requirement. An example of a way to document these responsibilities is via a matrix that identifies all applicable PCI DSS requirements and indicates whether the customer or TPSP is responsible for meeting that requirement or whether it is a shared responsibility.
12.9.2 ***Additional requirement for service providers only:*** 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).	12.9.2 ***Additional testing procedure for service provider assessments only:*** Examine policies and procedures to verify processes are defined for the TPSPs to support customers' request for information to meet Requirements 12.8.4 and 12.8.5 in accordance with all elements specified in this requirement.	
Customized Approach Objective		
TPSPs provide information as needed to support their customers' PCI DSS compliance efforts.		
Applicability Notes		
This requirement applies only when the entity being assessed is a service provider.		

WHAT

PCI DSS Service Providers will need to support their customers' requests for information regarding PCI DSS compliance and responsibilities.

PURPOSE

Third Party Service Providers are expected to already be doing this. However, this is still an issue in the payment community.

IMPACT

This requirement should help support merchant needs to receive this cooperation from third party service providers.

PROCESS

Third Party Service Provider will need to have documented policies and procedures to support customer's requests for PCI compliance information.

Why are these applicable immediately?

These requirements are applicable immediately because organizations are expected to already have these controls in place.

These requirements are not asking for new technologies, they are all related to new documentation and processes to support existing PCI DSS requirements.

Implementing these changes should not be time or resource intensive.

Questions?

HALOCK®

Viviana Wesley, CISM, PCI QSA, ISO 27001 Auditor vwesley@halock.com

https://www.halock.com

PCI Compliance articles