PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING

2025
EUROPE
COMMUNITY
MEETING

From Stress to Success:

How Continuous Compliance Simplifies PCI DSS

PCI Security Standards Council

Peter O’Sullivan

QSA and 3DS-QSA

Principal Security Consultant

Blackfoot Cybersecurity

blackfoot cybersecurity

PCI Security Standards Council

Have you Been Here? Or Have you Seen This?

PCI Security Standards Council

Have you Been Here? Or Have you Seen This?

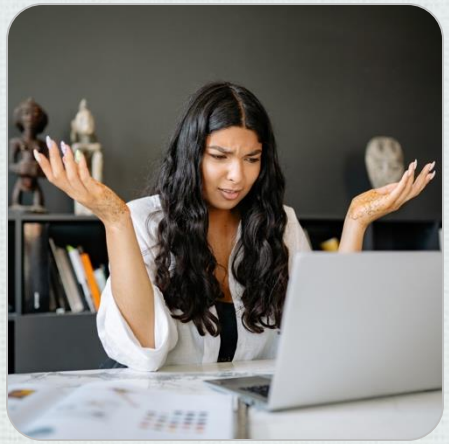
PCI Security Standards Council

1 Month Before Annual Assessment

The great documentation hunt

The missed vulnerability scan

Whose job was that?



The uneducated masses

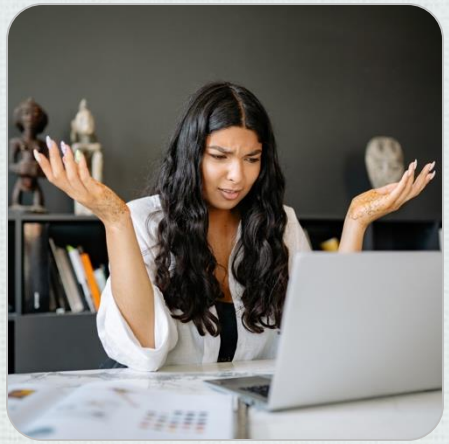
PCI Security Standards Council

1 Month Before Annual Assessment

The great documentation hunt

The missed vulnerability scan

Whose job was that?

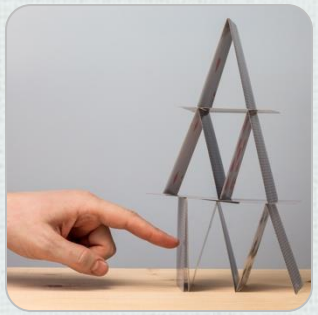


The uneducated masses

PCI Security Standards Council

When Business-as-Usual Compliance Fails

Fixable... Maybe?



- Missed training
- Documentation
- Service providers AOCs

Papering over the cracks. Painful and costly. Your QSA will probably notice.

Unfixable issues

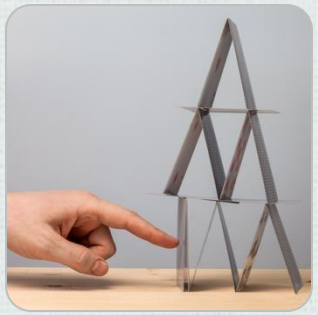
- Missed scans
- Incomplete reviews
- Missed code reviews or change control

Some issues can’t be papered over.

PCI Security Standards Council

When Business-as-Usual Compliance Fails

Fixable... Maybe?



- Missed training
- Documentation
- Service providers AOCs

Papering over the cracks. Painful and costly. Your QSA will probably notice.

Unfixable issues

- Missed scans
- Incomplete reviews
- Missed code reviews or change control

Some issues can’t be papered over.

PCI Security Standards Council

Responding to the Imperfect

- The PCI DSS provides a mechanism, for use in exceptional circumstances
- Responding to the failure:
  - Investigate, fix, and document
  - Learn and improve
- Practice continuous compliance
  - Design the failure away
- Shift from sprint to stroll

Responding to the Imperfect

- The PCI DSS provides a mechanism, for use in exceptional circumstances
- Responding to the failure:
  - Investigate, fix, and document
  - Learn and improve
- Practice continuous compliance
  - Design the failure away
- Shift from sprint to stroll

Responding to the Imperfect

- The PCI DSS provides a mechanism, for use in exceptional circumstances
- Responding to the failure:
  - Investigate, fix, and document
  - Learn and improve
- Practice continuous compliance
  - Design the failure away
- Shift from sprint to stroll

Defining Continuous Compliance

A commitment to ensure your organisation always remains PCI DSS compliant

Provide oversight and monitoring to those who manage and operate requirements

Ensure focus and ongoing validation

PCI Security Standards Council

Defining Continuous Compliance

A commitment to ensure your organisation always remains PCI DSS compliant

Provide oversight and monitoring to those who manage and operate requirements

Ensure focus and ongoing validation

PCI Security Standards Council

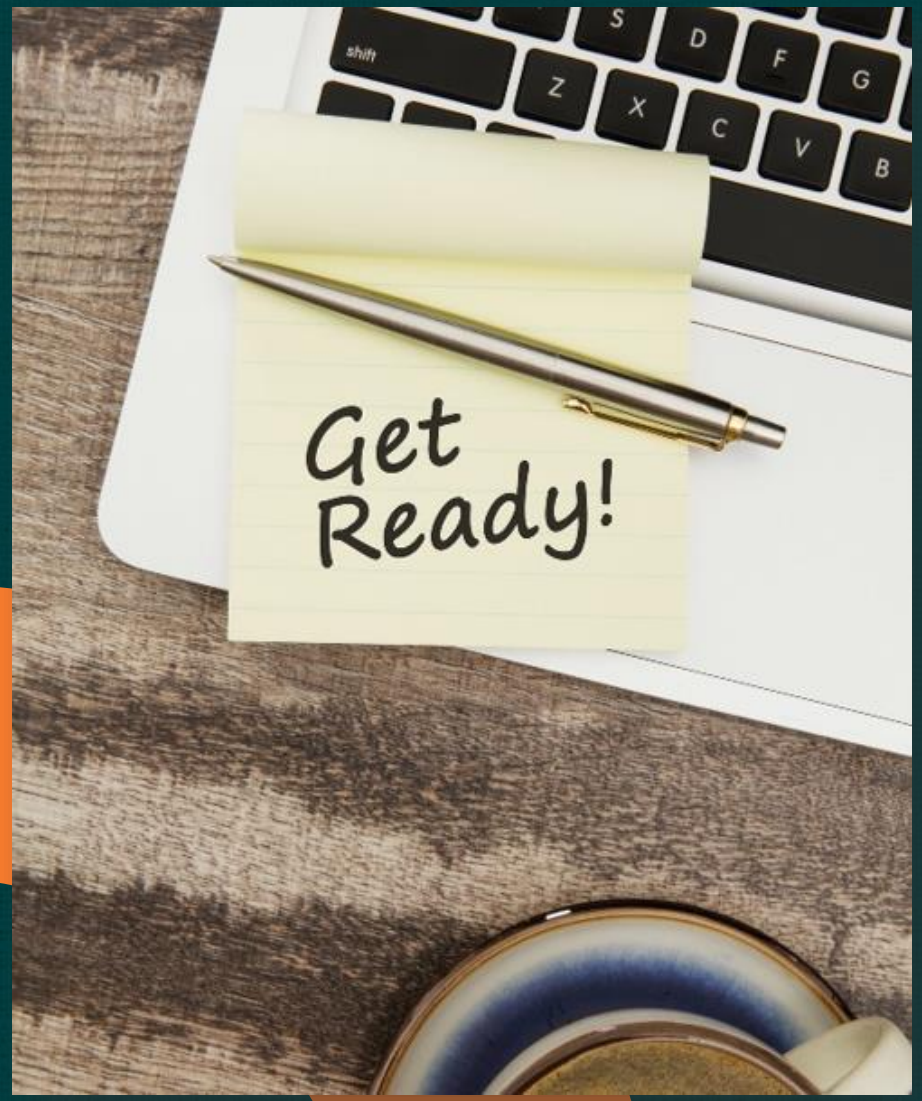
Defining Continuous Compliance

A commitment to ensure your organisation always remains PCI DSS compliant

Provide oversight and monitoring to those who manage and operate requirements

Ensure focus and ongoing validation

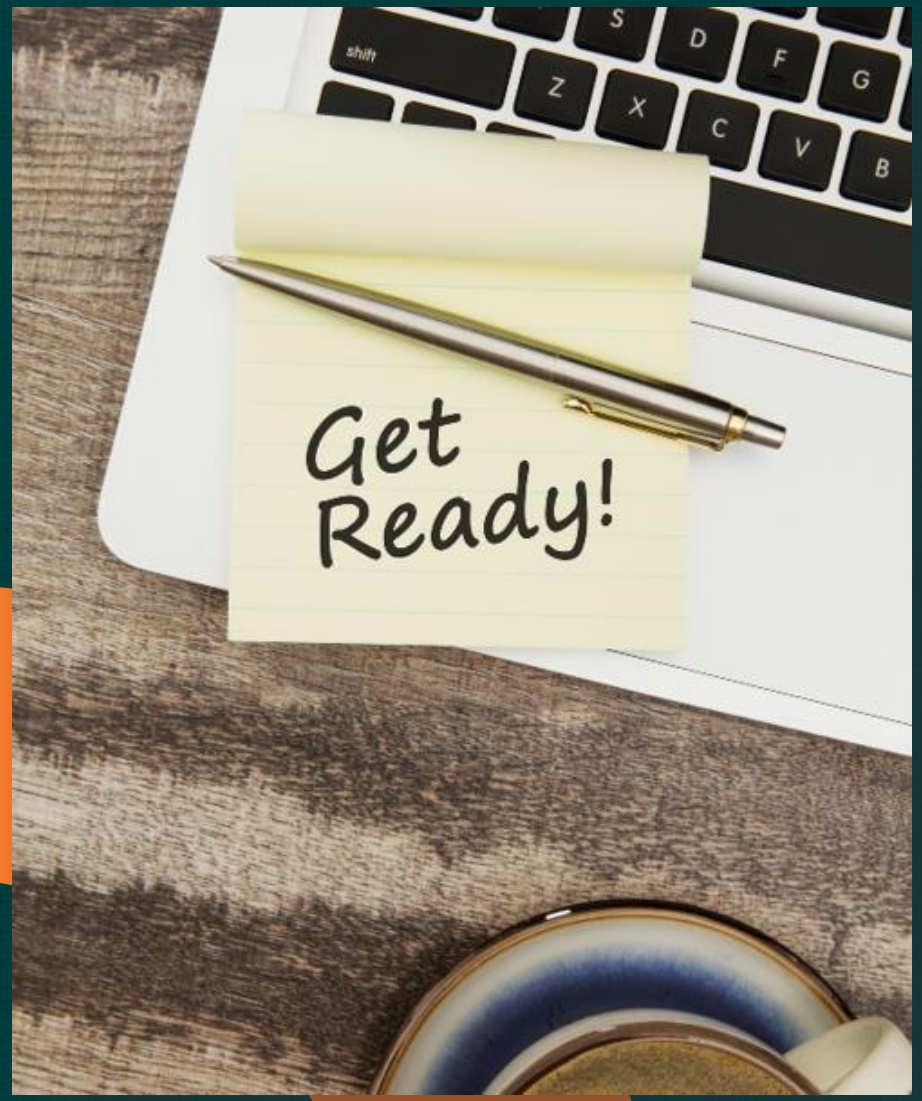
PCI Security Standards Council



What to do Before it Goes Wrong….

- Document a continuous compliance process
- Somebody needs to own it
- Collect and review evidence regularly
- Stay independent

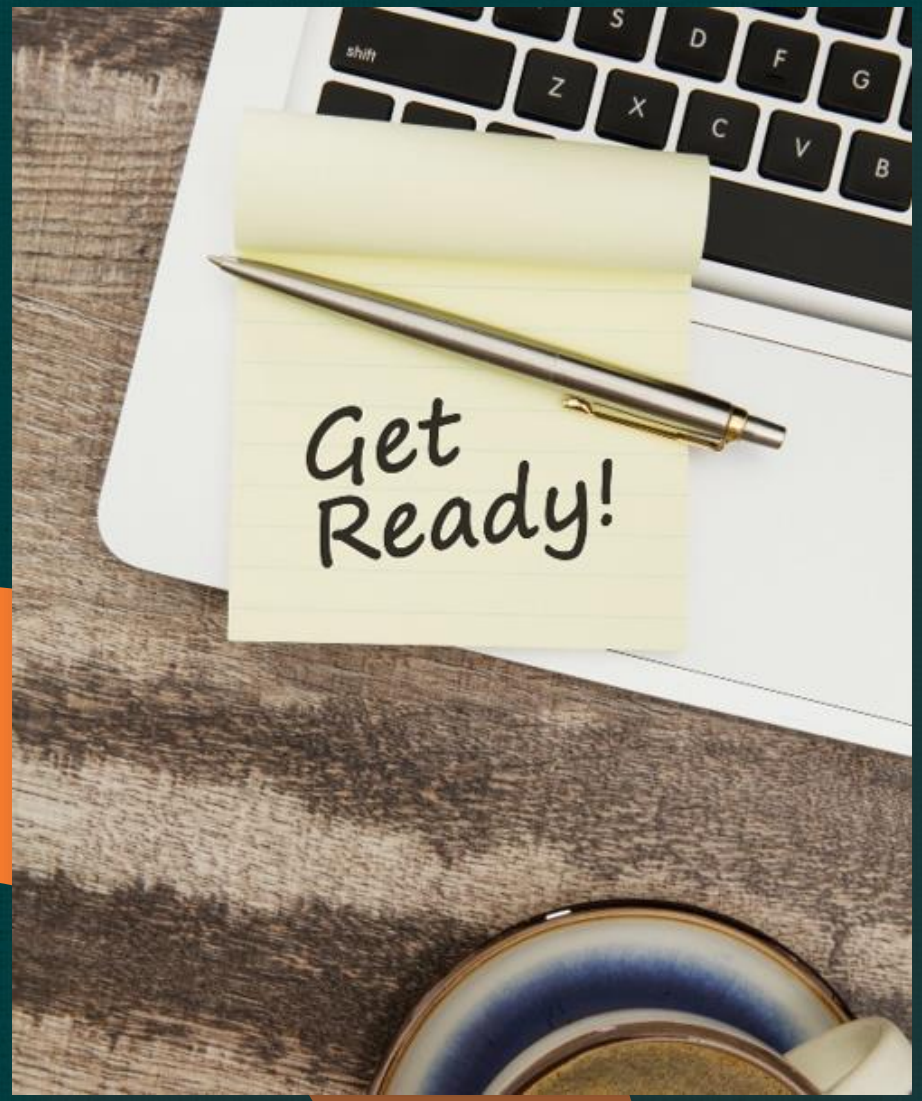
PCI Security Standards Council



What to do Before it Goes Wrong….

- Document a continuous compliance process
- Somebody needs to own it
- Collect and review evidence regularly
- Stay independent

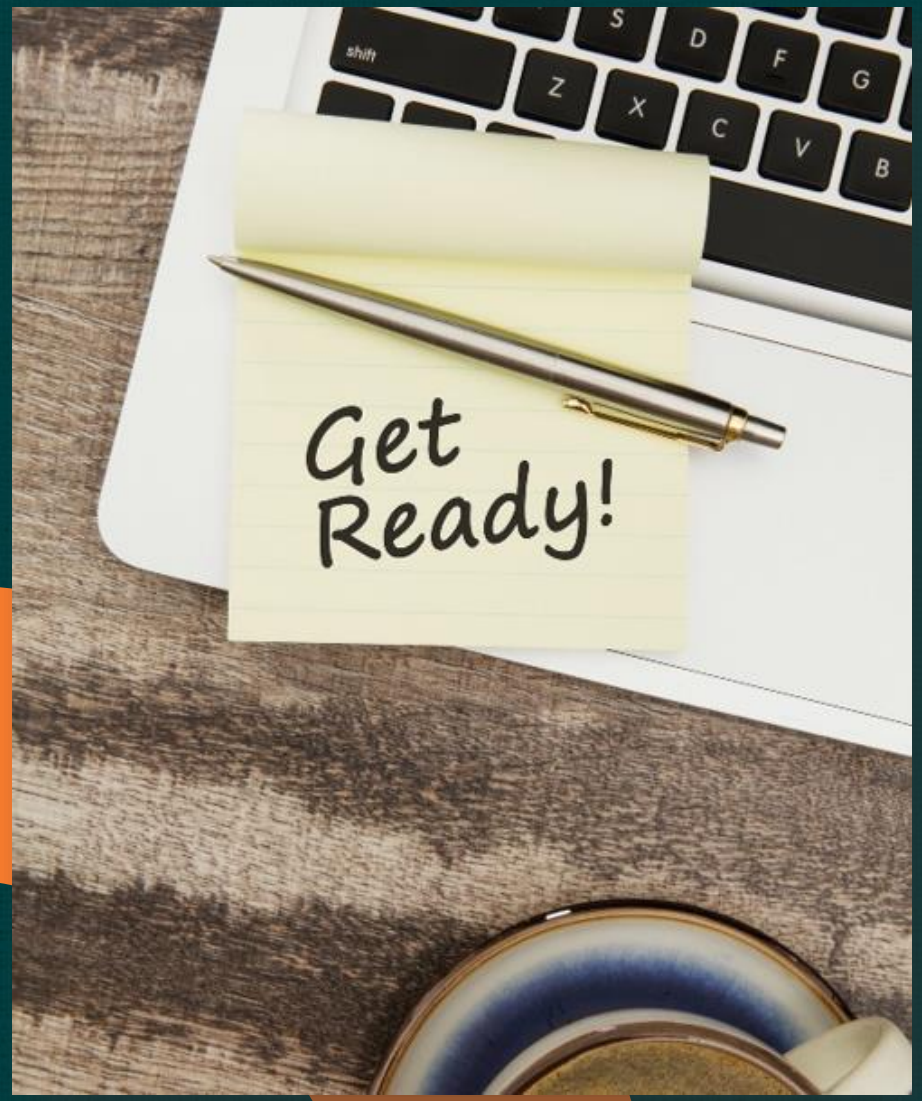
PCI Security Standards Council



What to do Before it Goes Wrong….

- Document a continuous compliance process
- Somebody needs to own it
- Collect and review evidence regularly
- Stay independent

PCI Security Standards Council



What to do Before it Goes Wrong….

- Document a continuous compliance process
- Somebody needs to own it
- Collect and review evidence regularly
- Stay independent

PCI Security Standards Council

What to do if it does go wrong…

- Acknowledge, communicate, notify
- Follow process
- Investigate
- Get back on track
- Document
- Learn, improve

PCI Security Standards Council

What to do if it does go wrong…

- Acknowledge, communicate, notify
- Follow process
- Investigate
- Get back on track
- Document
- Learn, improve

PCI Security Standards Council

6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Patches/updates for critical vulnerabilities (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.

12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.

Examples:
- A Frequency requirement
- An On-Demand requirement

- Control Owner considerations
- When?
- Verify vs Validate
- Collecting and storing evidence
- Leaning on other requirements

PCI Security Standards Council

6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Patches/updates for critical vulnerabilities (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.

12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.

Examples:
- A Frequency requirement
- An On-Demand requirement

- Control Owner considerations
- When?
- Verify vs Validate
- Collecting and storing evidence
- Leaning on other requirements

PCI Security Standards Council

6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Patches/updates for critical vulnerabilities (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.

12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.

Examples:
- A Frequency requirement
- An On-Demand requirement

- Control Owner considerations
- When?
- Verify vs Validate
- Collecting and storing evidence
- Leaning on other requirements

PCI Security Standards Council

6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Patches/updates for critical vulnerabilities (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.

12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.

Examples:
- A Frequency requirement
- An On-Demand requirement

- Control Owner considerations
- When?
- Verify vs Validate
- Collecting and storing evidence
- Leaning on other requirements

PCI Security Standards Council

Tips and Ideas

Automate

Track

Documented Processes

Evidence

PCI Security Standards Council

Tips and Ideas

Automate

Track

Documented Processes

Evidence

PCI Security Standards Council

Efficiency Gains for the Assessment

- QSA has a job to do, but…
- Easier evidence collection
- No audit nerves
- Fewer delays
- Lower risk of non-compliance
- Happy QSA ☺

PCI Security Standards Council

Efficiency Gains for the Assessment

- QSA has a job to do, but…
- Easier evidence collection
- No audit nerves
- Fewer delays
- Lower risk of non-compliance
- Happy QSA ☺

PCI Security Standards Council

ROCs Based on SAQs and Hidden Details

FAQ 1331 was updated in May 2025, and highlights something that has always been there

Any merchant who is using eligibility requirements to use an SAQ as the basis of a ROC, must also complete requirement 12.5.2 – Documenting Scope and……

Use the ROC Reporting Template from the Document Library to identify the documented policies and procedures, and likely evidence too

PCI Security Standards Council

ROCs Based on SAQs and Hidden Details

FAQ 1331 was updated in May 2025, and highlights something that has always been there

Any merchant who is using eligibility requirements to use an SAQ as the basis of a ROC, must also complete requirement 12.5.2 – Documenting Scope and……

Use the ROC Reporting Template from the Document Library to identify the documented policies and procedures, and likely evidence too

PCI Security Standards Council

ROCs Based on SAQs and Hidden Details

FAQ 1331 was updated in May 2025, and highlights something that has always been there

Any merchant who is using eligibility requirements to use an SAQ as the basis of a ROC, must also complete requirement 12.5.2 – Documenting Scope and……

Use the ROC Reporting Template from the Document Library to identify the documented policies and procedures, and likely evidence too

PCI Security Standards Council

Where we Find the Truth

ROCs Based on SAQs and Hidden Details

PCI DSS Requirement		Expected Testing	Response* (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.						
12.8.1	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	• Examine policies and procedures. • Examine list of TPSPs.	☐	☐	☐	☐
	Applicability Notes					
	The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.					

Where we Find the Truth

ROCs Based on SAQs and Hidden Details

PCI DSS Requirement					
12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	Not Applicable	Not Tested	Not in Place	Compensating Control*	Customized Approach*
☐	☐	☐	☐	☐	☐
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.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**	**Reporting Details: Assessor's Response**			
12.8.1.a Examine policies and procedures to verify that processes are defined to maintain a list of TPSPs, including a description for each of the services provided, for all TPSPs with whom account data is shared or that could affect the security of account data.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.				
12.8.1.b Examine documentation to verify that a list of all TPSPs is maintained that includes a description of the services provided.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				

PCI Security Standards Council

Where we Find the Truth

ROCs Based on SAQs and Hidden Details

PCI DSS Requirement					
12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.					
Assessment Findings (select one)				**Select If Below Method(s) Was Used**	
In Place	Not Applicable	Not Tested	Not in Place	Compensating Control*	Customized Approach*
☐	☐	☐	☐	☐	☐
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.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**	**Reporting Details: Assessor's Response**			
12.8.1.a Examine policies and procedures to verify that processes are defined to maintain a list of TPSPs, including a description for each of the services provided, for all TPSPs with whom account data is shared or that could affect the security of account data.	**Identify** the evidence reference number(s) from Section 6 for all **policies and procedures** examined for this testing procedure.				
12.8.1.b Examine documentation to verify that a list of all TPSPs is maintained that includes a description of the services provided.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.				

PCI Security Standards Council

The Benefits

A shift in mindset to think continuously, not annually, and minimises risks to cardholder data

Reduces stress and spikes in workload, ensuring your teams are match fit for assessments

Saves time by being assessment-ready and avoiding delays and quick-fix remediation

PCI Security Standards Council

Thanks for listening

Peter O’Sullivan | QSA and 3DS-QSA
Principal Security Consultant
Blackfoot Cybersecurity

blackfoot cybersecurity

PCI Security Standards Council