



## Payment Security & Compliance Conference



### **Self Assessment Questionnaires – Expected Testing and Evidence**

Chris Blackadder, Cyber Security Analyst, Queen's University Belfast

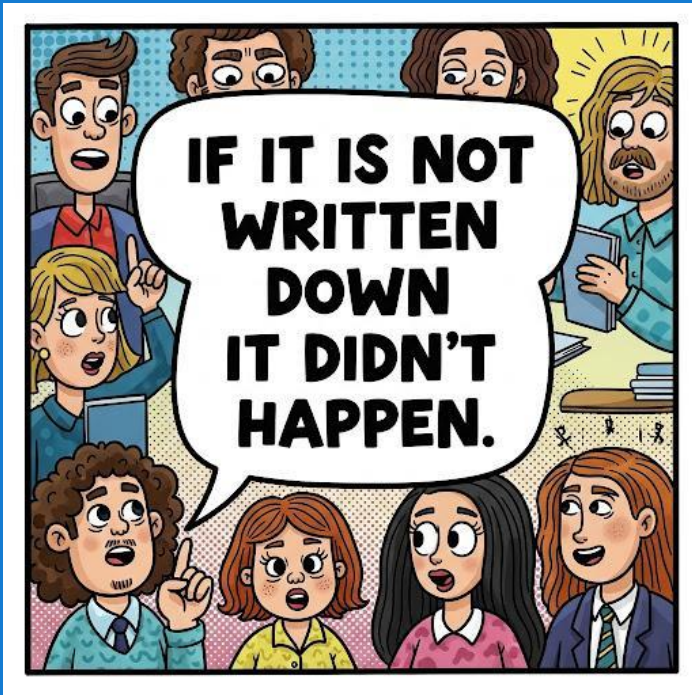
Dave Neild, Lead Security Consultant, Flywire

[slido.com #Flywire2025](https://slido.com/#Flywire2025)

# Self Assessment Questionnaires (SAQs)

SAQ	Summary	Requirements
<b>A</b>	Card-not-present Merchants, All Cardholder Data Functions Fully Outsourced. Typically applicable to e-commerce channels in HE sector.	29
<b>A-EP</b>	Partially Outsourced E-Commerce Merchants Using a Third-Party Website for Payment Processing.	139
<b>B</b>	Merchants with Only Imprint Machines or Only Standalone, Dial-Out Terminals.	27
<b>B-IP</b>	Merchants with Standalone, IP-Connected PTS Point-of-Interaction (POI) terminals.	48
<b>C-VT</b>	Merchants with Web-Based Virtual Terminals.	54
<b>C</b>	Merchants with Payment Application Systems Connected to the Internet.	121
<b>D</b>	SAQ D for Merchants. <b>(Full standard)</b>	235
<b>P2PE</b>	Merchants using Only Hardware Payment Terminals in a PCI SSC-listed P2PE Solution	21
<b>SPoC</b>	Merchants using a commercial off-the-shelf mobile device (for example, a phone or tablet) with a secure card reader included on PCI SSC's list of validated SPoC Solutions.	22

# Why expected testing and evidence?



## Expected testing

- Not a tick-box exercise
- To validate compliance
- Prescriptive
- Informs implementers

## Testing methods

- Examine
- Observe
- Interview

## Evidence

- Demonstrable compliance
- Can be audited
- Can be used in event of an incident

# Example

Requirements and Testing Procedures		Guidance
<b>12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.</b>		
<b>Defined Approach Requirements</b>	<b>Defined Approach Testing Procedures</b>	<b>Purpose</b>
<b>12.8.1</b> 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.	<b>12.8.1.a</b> 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.	Maintaining a list of all TPSPs identifies where potential risk extends outside the organization and defines the organization's extended attack surface.
	<b>12.8.1.b</b> Examine documentation to verify that a list of all TPSPs is maintained that includes a description of the services provided.	<b>Examples</b> Different types of TPSPs include those that:
<b>Customized Approach Objective</b>		<ul style="list-style-type: none"> <li>• Store, process, or transmit account data on the entity's behalf (such as payment gateways, payment processors, payment service providers (PSPs), and off-site storage providers).</li> <li>• Manage system components included in the entity's PCI DSS assessment (such as providers of network security control services, anti-malware services, and security incident and event management (SIEM); contact and call centers; web-hosting companies; and IaaS, PaaS, SaaS, and FaaS cloud providers).</li> <li>• Could impact the security of the entity's cardholder data and/or sensitive authentication data (such as vendors providing support via remote access, and bespoke software developers).</li> </ul>
<b>Records are maintained of TPSPs and the services provided.</b>		
<b>Applicability Notes</b>		
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.		





QUEEN'S  
UNIVERSITY  
BELFAST

SHAPING  
A BETTER  
WORLD  
SINCE 1845



[qub.ac.uk](http://qub.ac.uk)



# Self Assessment Questionnaires – Expected Testing and Evidence

**Chris Blackadder**

Cyber Security Analyst

# Queen's University Belfast

- Founded in 1845
- Became independent University in 1908
- One of 2 Universities in Northern Ireland
- 5,000 full time staff
- 26,000 students

# A bit about me

Chris Blackadder

- Founded in 1977 😊
- Started working at Queen's in February 2004
- Worked on the IT Service desk for 17 years
- Started as a Cyber Security Analyst 2022



# PCI DSS

- Cyber Security Manager retired in 2023



- To prepare for PCI DSS Ver 4.0
- Payment Security Foundation
- Payment Security Practitioner
- Payment Security Masterclass

# PCI DSS 4.0 the work begins

## Descoping exercise June 2024

- Dave Neild came over to Belfast in June for descoping talk with all PCI DSS Stakeholders
- Discuss SAQs that will need completed
- Advice and guidance around Version 4 compliance
- Discussion around resources

## Takeaways were

- Try to get as much on prem E-commerce applications and servers off to either
  - Payment as a service
  - Software as a service
- Segmentation
- Ensure all physical devices are P2PE
- Ensure we are only going to complete SAQs
- Fieldwork

# PCI DSS 4.0 the work begins

## What we did

- We joined the PSMS programme June 2024 (Payment Security Management System)
  - Had biweekly catch-up calls with Phil, Dave and Mike
- Fieldwork started
  - We identified the scope of the work
  - Network team created a network diagram
  - IT identified systems and services and owners
  - Finance identified areas with compliant and non-compliant handsets
- Spoke to server owners and on premises E-commerce owners
- PSMS Calls to identify all relevant requirements for the relevant SAQs
  - SAQ A
  - SAQ P2PE





## Activity

→ 5 minutes

**How do you perform expected testing?**

- A. None / tick box exercise**
- B. Best endeavors**
- C. Follow SAQ testing procedures**
- D. Other**

**How do you collate evidence?**

- A. None**
- B. Multiple locations**
- C. Central repository**
- D. Other**



## Activity

→ Feedback

### How do you perform expected testing?

- A.** None / tick box exercise
- B.** Best endeavors
- C.** Follow SAQ testing procedures
- D.** Other

### How do you collate evidence?

- A.** None
- B.** Multiple locations
- C.** Central repository
- D.** Other

# Testing and Evidence

## What we did

- Started talking to colleagues who play a part in managing the servers and systems  
Showing us what processes they go through to prove PCI compliance is in place and working
- Gathering screenshots of Group Policies to show security settings are in place e.g. Password length and complexity, giving information for context around our PAM system
- Gathering all our policies and procedures into one place for evidence













# Testing and Evidence

## What we did

- Teams Site Created
  - For messaging and evidence
  - Phil populated the site with required documents
  - Single point of contact (keep everything in one place)
  - Evidence was all based on our SAQs testing criteria
  - Supporting Evidence Folder
    - 2 folders 1 for SAQA and 1 for SAQ P2PE
    - Broken down into sections 1-12
    - Each section contained a word document with the relevant requirements needed to pass our compliance.



Microsoft Teams

	Name ▾
	00 - PSMS Document Management
	01 - PSE Management
	02 - Programme Management
	03 - Policies and Procedures
	04 - Incident Response
	05 - Risk Management
	06 - Supporting Evidence
	07 - Audit
	08 - Support



QUEEN'S  
UNIVERSITY  
BELFAST

Policies referred to in the PCI DSS guidance					
Policy	PSMS Requi	Responsible	Accountable	Consulted	Informed
Management of Credit and Debit Card Data Policy	Mandatory	D&IS / Finance	Directors of D&IS / Finance	PCI Compliance Group	All Employees
Data Retention and Disposal Policy	Mandatory	see PCI DSS Policy			
Media Protection and Management Policy	Mandatory	see PCI DSS Policy section 7			
Third Parties Management Policy	Mandatory	Cyber Security / Finance	Cyber Security / Finance	D&IS, Procurement, Legal	All Departments
Information Security Policy	Mandatory	Cyber Security	Cyber Security Manager	D&IS	All Employees
	Must	Cyber Security	Cyber Security Manager	D&IS	All Employees
Anti-Malware and Anti-Virus Policy					
Cardholder Data Protection Policy	Must	Finance	Finance Head	PCI Compliance Group	Finance and IT Teams
Data Access Control Policy	Must	Cyber Security / Finance	Cyber Security / Finance	PCI Compliance Group	All Employees
Employee Background Checks Policy	Must	see PCI DSS Policy section 8.5			
<a href="#">File Integrity Monitoring Policy</a>	Must				
<a href="#">Firewall and Router Policy</a>	Must	Network Team	Head of Networks	Cyber Security	Network Team
<a href="#">Information Security Management System Policy</a>	Must	Cyber Security	Cyber Security Manager	PCI Compliance Group	All Departments
<a href="#">Initial Configuration Policy</a>	Must				
<a href="#">Patching Policy</a>	Must				
<a href="#">Physical Access Policy</a>	Must	Cyber Security	Cyber Security Manager	DIS	Relevant Departments
<a href="#">Risk Assessment Policy</a>	Must	Cyber Security	Cyber Security Manager	Cyber Security	Relevant Teams
<a href="#">Roles and Responsibilities Policy</a>	Must	Finance / Cyber Sec			
<a href="#">Security Awareness Policy</a>	Must	Cyber Security	Cyber Security Manager	Cyber Security	Relevant Teams
<a href="#">Security Testing Policy</a>	Must	Cyber Security			
<a href="#">Time Management Policy</a>	Must	Time Management Policy.docx			
Software Development Life Cycle (no template for this)	Must				
Data Classification Procedure (no template for this)	Must	Compliance	Head of Compliance	Cyber Security	All Employees

# PCI DSS Maturity

## Next Steps

- Just because compliance is completed, it's NOT over!
- Get meetings booked in the calendar
- We are now looking at our new starting point
  - Continue with the normal day to day PCI DSS
  - What can we do to move forward with our Maturity
  - Ensure any new payment channels are appropriately assessed for impact and scope
  - Ensure any new payment channel is Saas
  - We have a new Security Awareness platform which also has PCI DSS Training options
    - It's more automated
    - It also means we can do targeted training for different staff
  - I have said that I will do ISA training and hopefully complete the exams.





QUEEN'S  
UNIVERSITY  
BELFAST