sysnet is now VikingCloud

VIKINGCLOUD™

EBOOK

PCI DSS Version 4.0

A review of what has been published and what has changed.

Prepared by: Natasja Bolton (PCI Qualified Security Assessor)
Client Engagement Manager, VikingCloud

Report issue date: April 29, 2022

Table of Contents

Introduction

Businesses have been assessing and validating compliance against the Payment Card Industry (PCI) Data Security Standard v3.2.1 since 1st January 2019. **On 31st March 2022, the PCI Security Standards Council (SSC) released the latest version of the PCI Data Security Standard: the PCI DSS v4.0,** along with the **Report on Compliance (ROC)** Template, the Attestation of Compliance (AOC) documents for **Merchants** and **Service Providers** to be used for on-site assessments. The PCI DSS v4.0 Self-Assessment Questionnaires (SAQs) and their associated Attestations of Compliance (AOC) **documents** were published later, on 29th April 2022.

In this article we examine the changes included in the final publication of the PCI DSS v4.0, and the Report on Compliance (ROC) Template and Attestations of Compliance (AOC) documents published at the same time, through a series of Questions to help to explain what these changes mean to you and your merchant customers.

The new standard is supported by a **PCI DSS v4.0 At-a-Glance** document. This provides an overview of the development of PCI DSS v4.0, implementation timelines and a high-level summary of the changes incorporated into version 4.0 that deliver the **goals** set out for this new version of the standard.
The PCI SSC's Resource Hub for PCI DSS v4.0 can be found **here.**

Our analysis of the v4.0 SAQs, exploring each SAQ type, their applicability and the new or amended PCI DSS Requirements included in each, is presented separately and can be found **here**.

What are the PCI SSC's aims in updating the PCI DSS?

Back in 2019, the PCI SSC set out their **goals** for PCI DSS v4.0:

- Ensure the standard continues to meet the security needs of the payments industry
- Add flexibility and support of additional methodologies to achieve security
- Promote security as a continuous process
- Enhance validation methods and procedures.

The PCI SSC recognized that the standard needed to change to better support businesses in their efforts to protect payment card data, to address changes in technology and in the threat landscape.

These goals have been carried through to and are reflected in the final publication. This new version of the DSS has been through multiple Request for Comments rounds, two on the Standard itself and one on the associated Validation Documents, providing the PCI SSC with over 6000 items of feedback to be considered during their review and update of the documentation.

What are the timelines for the new standard?

The PCI SSC has allowed a **two-year transition** period from publication of v4.0 to allow organizations to assess the changes in the PCI DSS, to identify implications for their compliance programs and to determine their own approach and timelines to migrate to PCI DSS v4.0 compliance.

PCI DSS v4.0	PCI DSS v3.2.1
Effective from:	Retired from:
Now	**March 31, 2024**

This extended transition period, one year longer than for the transition from v2. to v3.0, recognizes the significance of some of the changes included in v4.0. However, during the two-year transition period from 31st March 2022 to 31st March 2024, PCI DSS versions 3.2.1 and 4.0 are effective, and both can be used for assessments.

As was expected, given the PCI SSC's stated aims for version 4.0, the standard **introduces a number of new Requirements.**

Note: the two PCI DSS versions are not interchangeable, organizations must either assess their environments against all applicable Requirements in the PCI DSS v3.2.1 or PCI DSS v4.0. The customized validation approach – discussed **below** – cannot be utilized for a PCI DSS v3.2.1 assessment.

Although some of these new Requirements are effective immediately – i.e. there is no 'best practice' grace period – for the majority of the entirely new Requirements introduced with PCI DSS v4.0, organizations have a further 12 months to meet those Requirements; they remain **best practices until 31 March 2025**. These Requirements are identified in the PCI DSS with an applicability notes statement *'Best practices until 31 March 2025, after which these requirements will be required and must be fully considered during a PCI DSS assessment'*. This means that any assessments completed after the effective date must fully consider these new Requirements.

However, organizations need to recognize that the effective date statement for these new Requirements **does not mean that they can wait** until their next assessment date after 31st March 2025 to have them in place. To remain compliant, organizations must have implemented the new Requirements applicable them prior to the Requirements' effective date, even if the organization will not fully re-assess and validate their PCI DSS compliance again until many months after the effective date has passed.

When can organizations start assessing using PCI DSS version 4.0?

PCI DSS v4.0 is valid for assessments from the date of its publication and all key compliance documents to undertake v4.0 onsite assessments have been released; these include the **ROC Reporting Template** (the Report on Compliance template used for on-site assessments) and the Attestation of Compliance (AOC) documents for **Merchants** and **Service Providers**.

The Self-Assessment Questionnaires (SAQs) to be used by entities eligible to self-assess PCI DSS compliance to self-assess PCI DSS compliance against v4.0 are now available and are published **here**. Supporting documents for v4.0, including the SAQ Instructions and Guidelines and Prioritized Approach for v4.0, have yet to be published.

Only after version 3.2.1 is retired on 31st March 2024, will all compliance assessments need to be completed using the PCI DSS v4.0. This means that an organization could still choose to assess against v3.2.1 for their assessment due by 1st March 2024 and would not need to complete an assessment against PCI DSS v4.0 until their annual assessment in 2025 (unless their environment changes necessitating a re-scoping and re-assessment).

> Whether and when an organization can assess against PCI DSS v4.0 will depend on whether the entity is self-assessing or a QSA[1] or ISA[2] is completing the assessment and documenting a Report on Compliance.

[1] QSA: **PCI Qualified Security Assessor** [2] ISA: **PCI Internal Security Assessor**

Self-assessing organizations

Organizations eligible to self-assess may utilize the appropriate v4.0 SAQs to assess and validate their compliance. It is anticipated however, that with updates to the SAQ eligibility criteria, the additional guidance, clarification and consolidation of existing Requirements, and the inclusion of further Requirements in some SAQ types (Requirements that may be existing or be newly introduced with v4.0), most self-assessment eligible organizations will want to review the changes and their implications before taking the decision to migrate from v3.2.1 to v4.0.

Self-assessing merchants assessing and validating compliance via their acquirer's or merchant service provider's compliance management portal should also be made aware that the v4.0 SAQs will not be immediately available for use online. Each of the portal providers will need to time to transition their systems to the PCI DSS v4.0 and the new SAQs. Merchants will only be able to assess and validate against PCI DSS v4.0 once the compliance management portals have been upgraded to support v4.0.

In line with our approach to previous version changes, we will upgrade our entire solution to support PCI DSS v4.0 and its associated validation documentation during the transition period. We will not run v3.2.1 in parallel with v4.0. After the upgrade merchants will only be able to validate against PCI DSS v4.0. Continued provision for v3.2.1 will only be in place to support the record of existing attestations.

Assessments performed by a QSA or an ISA resulting in a documented Report on Compliance

Level 1 organizations will only be able to assess compliance against v4.0 **by engaging a QSA who has been qualified by the PCI SSC to assess PCI DSS v4.0.**

Note: The QSA annual re-qualification training as well as new QSA training will not transition to PCI DSS v4.0 until sometime in 2023. Therefore, even if the organization's QSA is due to undertake their 2022 PCI QSA re-qualification course and exam after the release of PCI DSS v4.0, their training will continue to be on PCI DSS v3.2.1 and the QSA will be unable to perform a version 4.0 onsite assessment for the organization until the transitional course and exam is completed.

The PCI SSC is developing a version 4.0 transitional training course for QSAs but this won't be available until June 2022. QSAs must have completed this CBT transitional training and passed the associated exam in order to be qualified to undertake a PCI DSS v4.0 assessment. Therefore, entities whose compliance assessments are due to take place prior to the availability of this training/exam will not be able to undertake a QSA-led PCI DSS v4.0 onsite assessment. The PCI SSC will be updating their **QSA listing** to enable organizations to identify those QSAs qualified to assess v4.0 and those only able to assess against v3.2.1.

It is anticipated that the payment brands' merchant compliance validation programs will restrict the use of the Customized Approach to Level 1 organizations engaging a QSA qualified for PCI DSS v4.0 to complete their Report on Compliance, even though many of the brands do currently permit Level 1 assessments and Reports on Compliance to be completed by an internal resource or ISA. This restriction is expected because, although the PCI SSC has stated that the PCI DSS v4.0 transitional training course and exam will also be available to ISAs, ISAs will only be encouraged but not required to undertake this course. In addition, the ISA qualification does not require the same verification of assessor skills, experience, or certifications as the QSA Program; therefore, ISAs may not have the necessary capability to fully understand the entity's customized implementation and derive appropriate testing procedures.

What are the implications for an entity's PCI DSS compliance if they use a service provider validated to v3.2.1, when the entity itself completes a v4.0 assessment?

The PCI SSC has addressed this question in **FAQ 1282**. Due to the lengthy transition period and the many additional new Requirements that apply only to service providers, it is likely that customer entities will want to validate compliance using v4.0 while their third-party service providers continue to assess using v3.2.1. The customer entity will still be considered compliant if the service provider they rely upon is completing their v3.2.1 PCI DSS compliance assessment prior to the 31st March 2024 retirement date.

Is the PCI DSS v4.0 a completely new Standard?

PCI DSS v4.0 is a new version of the standard not an iteration as was the case for the last three releases of the standard. Versions 3.1, 3.2 and 3.2.1 all built on version 3.0 (published in November 2013). Every aspect of the Data Security Standard and all of the associated documentation has been reviewed in detail over the three years of version 4.0's development.

Version 4.0 has been subject to multiple Requests for Comment and includes changes not just to the *'Detailed PCI DSS Requirements and Security Assessment Procedures'* (the Requirements) but also changes to the structure and format of the standard and to sections of the standard before and after the Requirements.

The PCI SSC has published a **Summary of Changes** document describing these. Three main types of change have been made:

- **Evolving requirement –** addition, modification or removal of requirements to address the changes in the threat landscape, in technologies, and in the payment industry
- **Clarification or guidance –** changes to wording, definitions, instructions, explanatory and/or guidance text to confirm or increase understanding or to provide further information
- **Structure or format –** re-organization of the Standard's content including moving, separating or combining Sections or Requirements

It is useful to reference the Summary of Changes document while reviewing the PCI DSS as it highlights the major areas of change in summary tables:

- **Changes to the PCI DSS Introductory Sections –** i.e. changes to the sections before the *'Detailed PCI DSS Requirements and Security Assessment Procedures'*
- **General Changes to PCI DSS Requirements –** summary of the changes made across all twelve Requirements such as reformatting, renumbering, rewording and reorganization of content

- **Changes per Requirement –** comparison table of v3.2.1 Requirements against new v4.0 Requirements with description and type of change. This table includes the Appendices and highlights all new Requirements
- **Summary of Requirements –** lists each new Requirement, identifying
  - The entities they are applicable to (all or service providers only)
  - The effective date of the new Requirement (immediately or future-dated)

Although many changes have been made, the underlying goals and principles of PCI DSS remain the same with Version 4. As can be seen in the table below, all but one of the 6 goals remain exactly the same (the only change clarifying that the goal applies to Account Data not just Cardholder Data). The 12 core Requirements have not fundamentally changed; however, updates have been made updated to better reflect the intent of and the changes made to the PCI DSS control requirements under each of them:

PCI DSS v4.0 Goals and core Requirements	Previous PCI DSS Goals and core Requirements
Build and Maintain a Secure Network and Systems	**Build and Maintain a Secure Network and Systems**
Requirement 1: Install and Maintain **Network Security Controls**	Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: **Apply Secure Configurations to All System Components**	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Protect *Account* Data	**Protect Cardholder Data**
Requirement 3: Protect stored **account** data	Requirement 3: Protect stored cardholder data
Requirement 4: **Protect Cardholder Data with Strong Cryptography** During Transmission Over Open, Public Networks	Requirement 4: Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**Maintain a Vulnerability Management Program**
Requirement 5: Protect All Systems **and Networks from Malicious Software**	Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
Requirement 6: Develop and Maintain Secure Systems and **Software**	Requirement 6: Develop and maintain secure systems and applications

PCI DSS v4.0 Goals and core Requirements	Previous PCI DSS Goals and core Requirements
Implement Strong Access Control Measures	**Implement Strong Access Control Measures**
Requirement 7: Restrict Access to **System Components and** Cardholder Data by Business Need to Know	Requirement 7: Restrict access to cardholder data by business need to know
Requirement 8: Identify **Users** and Authenticate Access to System Components	Requirement 8: Identify and authenticate access to system components
Requirement 9: Restrict Physical Access to Cardholder Data	Requirement 9: Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**Regularly Monitor and Test Networks**
Requirement 10: **Log** and Monitor All Access to **System Components** and Cardholder Data	Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: **Test Security of Systems and Networks Regularly**	Requirement 11: Regularly test security systems and processes
Maintain an Information Security Policy	**Maintain an Information Security Policy**
Requirement 12: **Support Information Security with Organizational Policies and Programs**	Requirement 12: Maintain a policy that addresses information security for all personnel

How have the Requirements changed?

At first glance, the PCI DSS version 4.0 looks considerably larger than v3.2.1, over 60 more Requirements!

However, the PCI SSC has gone to great lengths to ensure the new standard is consistent in its structure and numbering. Where, under v3.2.1 Requirements might be assessed at the X.X level and/or at the X.X.X, or lower, level; with version 4.0 Requirements are always assessed at the X.X.X level or lower, following this structure:

- X Principal Requirement
- X.X Requirement Sections
- X.X.X Assessed Requirements (may expand to lower levels: X.X.X.X and X.X.X.X.X)

Comparing the number of assessable Requirements shows a much smaller difference between v3.2.1 and v4.0. In fact, there are only 7 additional assessable Requirements under the twelve Principal Requirements:

	PCI DSS V3.2.1	**PCI DSS V4.0**
Under the twelve Principal Requirements		
Total no. of X.X and sub-requirements	252	**313**
Total no. of assessable[1] requirements	243	**250**
Total no. of assessable requirements applicable to all entities (excl. service provider / Issuer only)	235	**233**
Total no. of assessable requirements applicable only to service providers (1 requirement is specific to Issuers only)	8	**17**
In the Appendices		
No. of requirements in Appendix A1 (Multi-Tenant Service Providers)	4	**7**
No. of requirements in Appendix A2 (Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections)	3	**3**
No. of requirements in Appendix A3 (Designated Entities Supplemental Validation)	20	**20**

What are the new Requirements?

Version 4.0 introduces 49 entirely new Requirements to address the evolving risks associated with the changes in payment methods and solutions, changes in IT and security technology, and in the threat landscape.

Changes have been made within a number of existing Requirements, shown in the table below as 'partial new' Requirements. For example, the existing Requirement for monitoring and responding to alerts from security monitoring systems (12.10.5 in both v3.2.1 and v4.0) now includes one additional system: the change-and tamper-detection mechanism for payment pages.

[1] Unlike v3.2.1, PCI DSS v4.0 is consistent in structure, it is only the Requirements below the X.X level that are assessable (e.g. compliance with Requirement 4.1 is confirmed through assessment of 4.1.1 and 4.1.2).

As is detailed below, the majority of the new Requirements apply to all assessing organizations (when applicable to their environment); however, a number Requirements are identified as being applicable only to third-party service providers.

			Entirely New:		Partial New[2]:		
V4.0 Reqt#	Effective Immediately	Future-dated	Applicable to All Entities	Applicable to Service Providers only	Applicable to All Entities	Applicable to Service Providers only	Applicable to Issuers only
Requirement 2: Apply Secure Configurations to All System Components							
2.1.2	x		x				
Requirement 3: Protect Stored Account Data							
3.1.2	x		x				
3.2.1		x			x		
3.3.2		x	x				
3.3.3		x					x
3.4.2		x	x				
3.5.1.1		x	x				
3.5.1.2		x	x				
3.6.1.1		x				x	
Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks							
4.1.2	x		x				
4.2.1		x			x		
4.2.1.1		x	x				
Requirement 5: Protect All Systems and Networks from Malicious Software							
5.1.2	x		x				
5.2.3.1		x	x				
5.3.2.1		x	x				
5.3.3		x	x				
5.4.1		x	x				
Requirement 6: Develop and Maintain Secure Systems and Software							
6.1.2	x		x				
6.3.2		x	x				
6.4.2		x	x				
6.4.3		x	x				

[2] Partial New: The Requirement and its Purpose are not entirely new but one or more new element is now required

			Entirely New:		Partial New[2]:		
V4.0 Reqt#	Effective Immediately	Future-dated	Applicable to All Entities	Applicable to Service Providers only	Applicable to All Entities	Applicable to Service Providers only	Applicable to Issuers only
Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know							
7.1.2	x		x				
7.2.4		x	x				
7.2.5		x	x				
7.2.5.1		x	x				
Requirement 8: Identify Users and Authenticate Access to System Components							
8.1.2	x		x				
8.3.6		x	x				
8.3.10.1		x	x				
8.4.2		x	x				
8.5.1		x	x				
8.6.1		x	x				
8.6.2		x	x				
8.6.3		x	x				
Requirement 9: Restrict Physical Access to Cardholder Data							
9.1.2	x		x				
9.5.1.2.1		x	x				
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data							
10.1.2	x		x				
10.4.1.1		x	x				
10.4.2.1		x	x				
10.7.2		x	x			x (supersedes 10.7.1)	
10.7.3		x	x (already applies to service providers)				
Requirement 11: Test Security of Systems and Networks Regularly							
11.1.2	x		x				
11.3.1.1		x	x				
11.3.1.2		x	x				
11.4.7		x		x			

			Entirely New:		Partial New[2]:		
V4.0 Reqt#	Effective Immediately	Future-dated	Applicable to All Entities	Applicable to Service Providers only	Applicable to All Entities	Applicable to Service Providers only	Applicable to Issuers only
11.5.1.1		x		x			
11.6.1		x	x				
Requirement 12: Support Information Security with Organizational Policies and Programs							
12.3.1		x	x				
12.3.2	x		x				
12.3.3		x	x				
12.3.4		x	x				
12.5.2	x		x				
12.5.2.1		x		x			
12.5.3		x		x			
12.6.2		x	x				
12.6.3.1		x	x				
12.6.3.2		x	x				
12.9.2	x			x			
12.10.4.1		x	x				
12.10.5		x			x		
12.10.7		x	x				
Requirements 1-12 Totals	**13**	**47**	**41**	**5**	**6**	**1**	**1**
Appendix A1 Additional PCI DSS Requirements for Multi-Tenant Service Providers							
A1.1.1		x		x			
A1.1.4		x		x			
A1.2.3		x		x			
Appendix A3 Designated Entities Supplemental Validation (DESV)							
A3.3.1		x			x		
Totals	**13**	**51**	**41**	**8**	**7**	**1**	**1**

Changes in the Appendices

In addition to the PCI DSS Requirements included under each of the twelve principal Requirements above, there are additional Requirements applicable to different types of entities in the three appendices under Appendix A.

While there are no major changes to these three Appendices, **Appendix A1 has been expanded in its applicability.** Under PCI DSS v3.2.1, Appendix A1 applied to Shared Hosting Providers; in version 4.0 the appendix applies to Multi-Tenant Service Providers. This change is a reflection of expansion in the range and scope of third-party hosted or cloud-based services that can be offered to merchants and other service providers.

Appendix A1 includes **3 new future-dated Requirements** intended to:

- Ensure logical separation between the provider's environment and the customer's environment
- Test the effectiveness of separation controls between customers in a multi-tenant service provider environment
- Ensure suspected or confirmed security incidents and vulnerabilities are reported and addressed by the provider

Appendix A2 (Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections) remains the same in its applicability as under v3.2.1. Only minor clarification changes have been made to Appendix A2.

'Multi-tenant service provider' is one of a full range of a terms, abbreviations and acronyms, referenced within the Standard, that are explained in the glossary that is now included within the PCI DSS in Appendix G.

Appendix A3 (Designated Entities Supplemental Validation) also remains the same in its applicability and need only be assessed if the entity is instructed to by an acquirer or a payment brand. This appendix duplicates some Requirements from the main body of the PCI DSS (as not all PCI DSS Requirements apply to all entities that may undergo a PCI DSS assessment). It also includes future-dated Requirements (expanding the scope of an existing Requirement) related to failure of automated audit log review mechanisms and automated code review tools, as well as an update to / alignment of its Requirement relating to PCI DSS scope.

Which new Requirements are effective immediately?

While most of the new Requirements are future-dated, **13 are effective immediately.** These Requirements must be met in all PCI DSS v4.0 compliance assessments, if they are applicable to the entity:

		Applicable to	
V4.0 Reqt# Effective Immediately	Explanation	All Entities	Service Providers only
All Requirements			
x.1.2	New for Requirements 2 to 11 Personnel need to be aware of their assigned role and responsibilities to make sure each Requirement is operated / performed	x	
Requirement 12: Support Information Security with Organizational Policies and Programs			
12.3.2	Applicable only for entities using the customized approach. Replaces the organization-wide 12.2 'Implement a risk-assessment process'. Assessed entity must provide a detailed targeted risk analysis for each requirement met using the customized approach. Risk assessment must be performed at least once every 12 months	x	
12.5.2	The assessed entity must document and confirm their PCI DSS scope at least once every 12 months. The entity needs to identify all locations and flows of account data and all systems that are connected to or, if compromised, could impact their CDE to ensure they are included in their PCI DSS scope. This Requirement and the guidance on 'Annual PCI DSS Scope Confirmation' (page 17) emphasizes that it is the assessing entity that is responsible for defining and documenting their assessment scope. It is not the same exercise as scope confirmation that is the assessor's responsibility and is performed during the annual assessment	x	
12.9.2	This Requirement and the guidance in 'Importance of Understanding Responsibilities Between TPSP Customers and TPSPs' (page 22), requires Third Party Service Providers (TPSPs) to support their customers' requests for information on their compliance status and the requirements the TPSP is responsible for or that are shared, such that their customers can meet Requirements 12.8.4 and 12.8.5		x
	Total	**12**	**1**

What are the new future-dated Requirements?

Broadly the new future-dated Requirements can be divided into two categories:

- Requirements that are primarily people and process changes
- Requirements that are technology changes or need new technologies

Requirements that are primarily people and process changes

Many of these new Requirements expect the assessed entity to have a more detailed record of and greater understanding of the status of their environment. The standard asks for additional record and inventory requirements, or additional management and review requirements; some of these are highlighted below. In many cases, the assessed entity will already have the mechanisms, controls or technologies in place relevant to the PCI DSS Requirement.

Risk analysis must be used to support the nine Requirements (identified below) that provide flexibility for how frequently they are performed, to ensure that the frequency is appropriate given the likelihood of the threat the control is designed to address.

V4.0 Reqt# Effective Immediately	Explanation
Requirement 3: Protect Stored Account Data	
3.2.1	Expanded scope of account data retention and disposal policies, procedures, and processes requirements **to include any stored pre-authorisation sensitive authentication data (SAD)**
Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	
4.2.1.1	An **inventory of the entity's trusted keys and certificates** used to protect PAN during transmission is maintained (as per Requirement 4.2.1)
Requirement 5: Protect All Systems and Networks from Malicious Software	
5.2.3.1	Entity must **use targeted risk analysis** to determine frequency of periodic evaluations of system components identified as not at risk for malware
5.3.2.1	Entity must **use targeted risk analysis** to determine frequency of periodic malware scans performed to meet Requirement 5.3.2
Requirement 6: Develop and Maintain Secure Systems and Software.	
6.3.2	Requires **an inventory of all bespoke and custom software**, including any third-party software components incorporated into that software. Applies to all bespoke and custom software that stores, processes, or transmits account data, or that could impact the security of account data or a CDE

V4.0 Reqt# Effective Immediately	Explanation
6.4.3	Requires **inventory of payment page scripts** (loaded and executed in the consumer's browser) and controls to authorise and assure the integrity of those scripts
Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know.	
7.2.4	**Six monthly review** of user accounts and related access privileges, including third-party/vendor accounts
7.2.5	**Management of all application and system accounts and related access privileges** in line with need to know and least privilege principles
7.2.5.1	**Review of application and system accounts access and related access privileges** including management acknowledgement
Requirement 8: Identify Users and Authenticate Access to System Components	
8.6.1	**Management of systems or application accounts** that can be used for interactive login requiring business justification and management approval
8.6.3	**Protect passwords/passphrases for application and system accounts** against misuse through periodic change and construction with sufficient complexity
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data	
10.7.3	**Failures of any critical security controls systems** are responded to promptly
Requirement 11: Test Security of Systems and Networks Regularly	
11.3.1.1	Applicable vulnerabilities identified by internal vulnerability scan (those not ranked as high-risk or critical) are addressed **based on the risk defined in the entity's targeted risk analysis**
Requirement 12: Support Information Security with Organizational Policies and Programs	
12.3.1	Each PCI DSS requirement that provides flexibility for how frequently it is performed is **supported by a targeted risk analysis.** This risk analysis applies to 9 new Requirements: 5.2.3.1, 5.3.2.1, 7.2.5.1, 8.6.3, 9.5.1.2.1, 10.4.2.1, 11.3.1.1, 11.6.1, 12.10.4.1
12.3.3	**Document and review cryptographic cipher suites and protocols in use** at least once every 12 months
12.3.4	**Review hardware and software technologies in use** at least once every 12 months
12.6.2	**Review and update (as needed) the security awareness program** at least once every 12 months
12.6.3.1	Security awareness training shall include **awareness of threats and vulnerabilities** that could impact the security of the CDE, including but not limited to: **Phishing and related attacks; Social engineering**
12.6.3.2	Security awareness training shall include **awareness about the acceptable use of end-user technologies**

V4.0 Reqt# Effective Immediately	Explanation
12.10.5	Security incident response plan shall include monitoring and responding to alerts from security monitoring systems, including but not limited to: [new] **The change-and tamper-detection mechanism for payment pages**
12.10.7	Security incident response procedures to be in place and initiated **upon detection of stored PAN anywhere it is not expected**

Requirements that are technology changes or need new technologies

Many of the new future-dated Requirements will also require changes to existing technologies or new investment in technologies, some of these are highlighted below:

V4.0 Reqt# Effective Immediately	Explanation
Requirement 3: Protect Stored Account Data	
3.3.2	SAD stored electronically prior to completion of authorization is **encrypted using strong cryptography**
3.4.2	When using remote-access technologies, **technical controls prevent copy and/or relocation of PAN** for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need
3.5.1.1	Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are **keyed cryptographic hashes of the entire PAN**
3.5.1.2	If **disk-level or partition-level encryption** (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only on **removable electronic media** Or if used for non-removable electronic media, PAN is **also rendered unreadable via another mechanism** that meets Requirement 3.5.1
Requirement 5: Protect All Systems and Networks from Malicious Software	
5.3.3	**Anti-malware solution(s) for removable electronic media** must either perform automatic scans, or perform continuous behavioral analysis of systems or processes, when the media is inserted, connected, or logically mounted
5.4.1	Processes and automated mechanisms shall be in place to **detect and protect personnel against phishing attacks**
Requirement 6: Develop and Maintain Secure Systems and Software.	
6.4.2	An **automated technical solution must be deployed for public-facing web applications** to continually detect and prevent web-based attacks. The option to address new threats and vulnerabilities for public-facing web applications through review via manual or automated application vulnerability security assessment tools or methods will no longer be available
6.4.3	**Manage all payment page scripts** loaded and executed in the consumer's browser are managed using methods that confirm both the **authorization and integrity** of each script

V4.0 Reqt# Effective Immediately	Explanation
Requirement 8: Identify Users and Authenticate Access to System Components	
8.3.6	If password/passphrases are used, **password length shall be a minimum length of 12 characters** (or if the system does not support 12 characters, a minimum length of eight characters)
8.4.2	**Multi-factor authentication (MFA) is required for all access** into the CDE
8.5.1	Extension of the PCI DSS MFA system requirements in line with the PCI SSC Multi-factor Authentication guidance. New requirements are to ensure: the MFA system is **not susceptible to replay attacks, cannot be bypassed by any users** (with any requests managed on an exception basis), **access is granted only after all authentication factors are successful**
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data	
10.4.1.1	Requires the use of **automated mechanisms to perform audit log reviews**
10.7.2	**Failures of critical security control systems are detected,** alerted, and addressed promptly. Now including **two additional critical control systems**: audit log review mechanisms and automated security testing tools (if used)
Requirement 11: Test Security of Systems and Networks Regularly	
11.3.1.2	Internal vulnerability scans must be performed via **authenticated scanning**
11.6.1	**A change- and tamper-detection mechanism** must be deployed to alert personnel to unauthorized modification to the **HTTP headers and the contents of payment pages**

How have the Reporting and Validation Documents changed?

Report on Compliance template

The PCI DSS v4.0 **Report on Compliance Template** (ROC template) is published in PDF in the Document Library on the PCI SSC website; the Word version to be used by Assessors to record all v4.0 PCI DSS assessments is only available to download from **https://www.programs.pcissc.org**.

As with previous ROC templates, it is the **mandatory reporting document for assessor-led PCI DSS assessments** with only very limited changes permitted (such as addition of company logos, changes to title pages or page headers and removal of ROC template instructions).

Any ROC containing prohibited changes, such as changes to the format, order of sections or requirements, or removal of any part of the Assessment Overview or Findings and Observations, should not be considered valid and may not be accepted for compliance validation by the payment brands or acquirers.

The ROC template is supported by **Frequently Asked Questions.**
The FAQs provide:

- A **detailed breakdown of the changes** in the v4.0 ROC Template
- Discussion of the New ROC Reporting Features including:
  - **New Section 1.7 'Overall Assessment Result'** which allows for reporting of an overall 'full' or 'partial' assessment as Compliant, Compliance with Legal Exception or Non-Compliant. A partial assessment is one in which only a subset of Requirements has been assessed, one or more Requirements are marked as Not Tested.
  - **New 'In Place with Remediation' assessment finding** for use in Part II 'Findings and Observations'. This finding allows the assessor to note that a Requirement was not in place at some point during the assessment period, such as a missed quarterly ASV external vulnerability scan. The assessor can mark a Requirement as 'In Place with Remediation' if the assessed entity can demonstrate that the reason for control failure has been addressed, the control is now implemented, and mechanisms are in place to prevent a future control failure.
  - **New section 1.9 'Attestation Signatures'** requiring the Lead Assessor to confirm and attest to the independence of the assessment and to the accuracy of scoping.
- **Detailed explanation of each available assessment finding** and each of the responses that should be used (i.e. In Place, In Place with Remediation, Not Tested, Not in Place), in particular different scenarios for use of Not Applicable vs. Not Tested.
- **Answers to general questions** such as confirming that:
  - Requirements noted as best practice until 31 March 2025 are not required to be tested and as such can be marked as 'Not Applicable' in the ROC.
  - If the assessed entity is concerned about the inclusion of the account data storage table (ROC section 4.3), this can be excluded from the ROC as long as the assessor records and attests in the ROC that stored account data is documented as required by 4.3 and is retained in the assessor's work papers.

The ROC template is **provided only in English**; therefore, QSA translated versions are permitted as long as the PCI SSC's conditions are met, including that both the official PCI SSC English version and the QSA's translated version of the ROC must be provided to the assessed entity.

- The PCI SSC will not be providing definitions for the services listed in Part 2a of the Service Providers' PCI DSS v4.0 Attestation of Compliance (AOC) for Report on Compliance.

PCI DSS v4.0 Attestation of Compliance for Report on Compliance

The table below summarises the changes made to each of the Merchant and Service Provider versions of the PCI DSS v4.0 Attestation of Compliance (AOC) for Report on Compliance. The **majority of these changes have been made for clarity**, addressing those parts of the v3.2.1 AOC that were often misunderstood or incorrectly completed, and **to ensure consistency** with the PCI DSS v4.0.

One significant change in the AOCs is that **an entity that has undergone a 'partial' assessment can now be found Compliant.** Under v3.2.1 a Compliant 'partial' assessment was not possible as a 'Not Tested' result was not considered an affirmative assessment answer for a Requirement. Now, under v4.0 as long as the entity subject to the 'partial' assessment has demonstrated compliance with all other Requirements, the entity can be confirmed as Compliant.

Note: A **'partial' assessment** is one in which one or more Requirements have not been assessed and are marked in the ROC as 'Not Tested'.

		PCI DSS v4.0 Attestation of Compliance for Report on Compliance	
Section	Change	Merchant AOC Change	Service Provider AOC Change
New cover page	Requests entity name, assessment end date (from ROC) and date of report as noted in the ROC	X	X
All	Each Section or Part of the AOC references the associated ROC section	X	X
Section 1			
Part 1b	References the Assessed Entity (i.e. the Merchant or service Provider) and the Assessor. Now includes space for a named PCI SSC ISA as the Assessor. The Leader Assessor must also now provide their certificate number	X	X
Part 2a	‘Type of Merchant Business’ is now ‘Merchant Business Payment Channels’ The layout and language of Part 2a simplifies identification of merchant payment channels and those excluded in the assessment. An explanation of exclusion is now also required	X	
	‘Type of service(s) assessed’ has replaced Shared Hosting Provider’ with Multi-Tenant Service Provider’ to reflect the same change in the PCI DSS v4.0. ‘POS / card present’ is now ‘POI / card present’		X
Part 2b	Is now ‘Description of Role with Payment Cards’	X	
	‘Description of Role with Payment Cards’ references the merchant business payment channels indicated under Part 2a which should ensure a more accurate description of the merchant’s role	X	
	‘Description of Role with Payment Cards’ requires the Service Provider to also describe the ‘system components that could impact the security of account data’.		X
Part 2c	Is now ‘Description of Payment Card Environment’, what was Part 2e. Re-worded the network segmentation question to be specific to segmentation for assessment scope reduction	X	X
Part 2d	Is now’ In-scope Locations/Facilities, what was Part 2c. Re-worded to request listing of all physical locations/facilities in-scope for the Assessment	X	X
Part 2e	Is now 'PCI SSC Validated Products and Solutions', what was Part 2d. Asks entity to identify and list any PCI SSC Validated Products or Solutions in use, not just Payment Applications but also: 3DS SDKs, Approved PTS Devices, Validated Payment Software, PA-DSS Payment Applications, P2PE, SPoC and CPoC Solutions	X	X
Part 2f	Third-Party Service Providers part no longer asks about relationship with Qualified Integrators & Resellers (QIR). Asks three separate questions to identify the entity’s relationships with third party service providers: those that store, process or transmit account data on the entity’s behalf; those that manage in-scope system components; those that could impact the security of the entity’s CDE.	X	X

		PCI DSS v4.0 Attestation of Compliance for Report on Compliance	
Section	Change	Merchant AOC Change	Service Provider AOC Change
Part 2g	New part providing 'Summary of Assessment' provides a more detailed summary than what was included in the v3.2.1 Merchant AOC Section 2.	X	
	For each of the 12 principal Requirements, indicate the Requirement Findings (e.g. In Place) and if Customized Approach of Compensating Controls were used		
	The summary of 'Full' and 'Partial' testing of Requirements in v3.2.1 Service Provider AOC Part 2g, is now covered under Section 3 Part3. No justification for approach is required and the information does not need to be provided for each service covered by the AOC. Part 2g. requires, for each of the 12 principal Requirements, indication of the Requirement Findings (e.g. In Place) and if Customized Approach of Compensating Controls were used		X
Section 2			
Report on Compliance	Now provides detail on the Assessment and ROC, including start and end dates of the Assessment, whether any Requirements could not be met due to legal constraint and on any testing activities that were performed remotely	X	X
Section 3			
Part 3	Clarifies that the required ROC Date is the 'Date of Report'. Requires indication whether a Full or Partial (i.e. one or more Requirements are marked as Not Tested) Assessment was completed. A Partial Assessment can now be asserted as 'Compliant' as the entity has 'demonstrated compliance with all PCI DSS Requirements except those noted as Not Tested above'. An assessment can be asserted as Complaint when assessment requirements are marked as 'In Place with Remediation', as well as 'In Place' or 'Not Applicable'. Extra detail has been added to the 'Compliant with Legal exception' result	X	X
Part 3a	Acknowledgement of Status is now specified as 'Merchant Acknowledgment' or 'Service Provider Acknowledgment'. Now includes only three statements: consolidating two statements into one on maintaining PCI DSS controls and removing the two statements re sensitive authentication data and the statement on ASV scans.	X	X
Part 3c	Now requires 'Signature of Lead QSA' as well as 'Signature of Duly Authorized Officer of QSA Company'	X	X
Part 3d	ISA (if involved or assisted) is now named in Section 1 Part 1b. Requires indication of the role performed by the ISA	X	X
Part 4	Added clarification that 'Action Plan for Non-Compliant Requirements' need only be completed upon request of the entity to which the AOC is submitted and only if the Assessment has Non-Compliant results noted in Section 3	X	X

> For an understanding of the changes introduced with the v4.0 SAQs, please see our separate **eBook** which explores each of the SAQs, their applicability and the new or amended PCI DSS Requirements they include.

How has PCI DSS v4.0 changed how entities might approach implementing and validating compliance?

Version 4.0 adds flexibility for implementation and validation of the PCI DSS. **The PCI SSC recognized** early on in the development of the new version that organizations manage, monitor and secure their environments using a vast range of methods and technologies, not all of which are suited to the fulfilment of PCI DSS Requirements exactly as they are defined. To address this PCI DSS version 4.0 offers two approaches for implementing and validating PCI DSS

- **Defined Approach** – the existing method
  - The assessed entity implements controls that meet each PCI DSS Requirement as it is stated
  - The assessor follows the defined PCI DSS Testing Procedures to verify each Requirement is met as stated
  - The assessed entity may implement Compensating Controls if a PCI DSS Requirement cannot be met as stated due a legitimate and documented technical or business constraint
- **Customized Approach** – a new method
  - The assessed entity defines and implements controls to meet the stated Objective of each PCI DSS Requirement
  - The assessor derives testing procedures for each Requirement appropriate to the entity's specific implementation to verify that the implemented controls meet the stated Objective

Compensating controls are not an option with the Customized Approach nor is there any expectation or requirement for there to be a technical or business constraint to justify use of the Customized Approach. The assessed entity simply defines and implements the controls needed to meet the Objective of a PCI DSS Requirement.

Not only can entities choose the implementation and validation approach that best suits their security technologies and methodologies they can also select their approach on a **'mix and match'** basis.

The entity **does not need to follow one approach or the other for their entire assessment,** they can use the Customized Approach only for selected Requirements and continue to follow the Defined Approach for the majority of their assessment or vice versa. Entities may also use both approaches to address different implementations of the same Requirement – for example implement and validate the Requirement using the Defined Approach for one type of system component, and for another use the Customized Approach.

Can all PCI DSS Requirements be met using the Customized Approach?

The majority of PCI DSS Requirements may be met using either approach: Customized Approach or Defined Approach. However, Requirements relating to Sensitive Authentication Data Requirement 3.3.x, to disk-level or partial-level encryption and ASV external vulnerability scans **must** be met through the Defined Approach. These are:

Requirements where implementation and validation through the Customized Approach is prohibited	
3.3.1	SAD is not retained after authorization, even if encrypted.All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.
3.3.1.1	The full contents of any track are not retained upon completion of the authorization process.
3.3.1.2	The card verification code is not retained upon completion of the authorization process
3.3.1.3	The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process
3.3.2	SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.
3.5.1.2	If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media or • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.
11.3.2	External vulnerability scans are performed as follows: • At least once every three months. • By PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.

In addition, Requirements in **Appendix A2:** Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections and **Appendix A3:** Designated Entities Supplemental Validation (DESV) are **not eligible for the Customized Approach.**

Are all organizations eligible to use the Customized Approach for implementing and validating PCI DSS?

The PCI DSS v4.0 explains that the Customized Approach may be utilized by organizations whose assessments are performed by a QSA or an ISA when following the *'PCI DSS Requirements and Security Assessment Procedures'* and resulting in a documented ROC.

It is not yet clear how the payment brands' compliance programs (or acquirers in enforcing their compliance management obligations on their merchants) will support the Customized Approach. Self-assessing entities wishing to make use of customized validation may be required to engage a QSA to complete and document their self-assessment in a ROC.

It is anticipated that the payment brands' compliance programs may not permit ISAs to perform customized validations for their Level 1 organization. This is because pre-requisite PCI ISA skills, experience and industry certifications are not the same as for the QSA qualification. ISA qualification therefore does not ensure (and is not intended to ensure) that an individual ISA has the necessary qualifications and skills to perform a customized validation.

ISAs are able to help their organization's implementation of the customized approach for a PCI DSS Requirement. That can include supporting the definition of the customized controls, performing the required risk analysis to ensure the customized control provides at least the equivalent level of protection as the defined control, testing and monitoring the effectiveness of the customized control implementation, and ensuring the required documentation and evidence is provided to the assessing QSA.

Organizations that self-assess their compliance and complete an SAQ are **not eligible** to use the Customized Approach, even if that self-assessment is performed by a QSA or ISA. However, it is noted in the SAQs that *'entities wishing to validate using the Customized Approach may be able to use the PCI DSS Report on Compliance (ROC) Template to document the results of their assessment'*.

The assessing QSA will review the controls matrix, risk analysis, and evidence of control effectiveness provided by the organization and/or their ISA in order to define testing procedures for each customized control.

The assessing QSA will perform the testing procedures and determine whether they find each control ‘in place’; an ISA may facilitate and support the QSA’s testing activities.

What are the responsibilities of the assessed entity and their assessor when using the Customized Approach?

It is the assessed entity that determines when the Customized Approach is to be used in their assessment. The assessed entity is responsible for completing the required documentation for each customized control and providing it to the assessor completing the assessment. The assessor uses the provided information to plan the customized validation. The Customized Approach responsibilities and steps for each entity are set out in both the PCI DSS and ROC Template’s Appendix D.

The assessed entity

Designs, implements and tests the effectiveness of the customized controls - generating evidence to be shared with their assessor to proves the controls are effective and meet the stated objective for each Requirement. This testing, performed by the assessed entity, needs to be completed prior to the start of the entity’s assessment. The entity’s own testing is not a replacement for or alternative to the assessor’s derived testing of each customized control.

The entity must provide details to their assessor for each customized control including what has been implemented, how the control provides protection that is at least equivalent to that of the defined Requirement, and the results of testing that provides assurance of the effectiveness of the control. The entity must include all information specified in the Controls Matrix provided in the **PCI DSS** Appendix E1 and in the Targeted Risk Analysis from the **PCI DSS** Appendix E2.

The assessing QSA

Will review the entity’s documentation and testing evidence for each customized control as well as perform their own derived testing to validate that a customized implementation is ‘In Place’. The assessed entity’s documentation must evidence that the controls meet the stated objective for the applicable Requirement, their risk analysis must show that the customized controls are robust and provide an equivalent level of protection, and evidence that controls are effective and maintained on an ongoing basis.

From this documentation, the QSA derives testing procedures that will validate each control implementation, confirming the customized control is place and meeting the objective for the Requirement.

In the entity's ROC, use of the customized approach is indicated in Part II Findings and Observations in each applicable PCI DSS Requirement section and the detail recorded in a completed Customized Approach Template (Appendix E ROC Template) for each Requirement where the customized approach is used.

The Customized Approach Template includes the assessor's attestation that the entity completed all the information specified in PCI DSS Appendices E1 and E2 and documents the testing procedures derived and performed by the assessor to validate that:

- The implemented controls meet the Customized Approach Objective
- The controls are maintained to ensure ongoing effectiveness

Can an organization work with their QSA to design and test their security controls to meet a PCI DSS requirement using the Customized Approach?

The assessed entity may use the services of a QSA to help them design, implement and test the effectiveness of their customized controls.

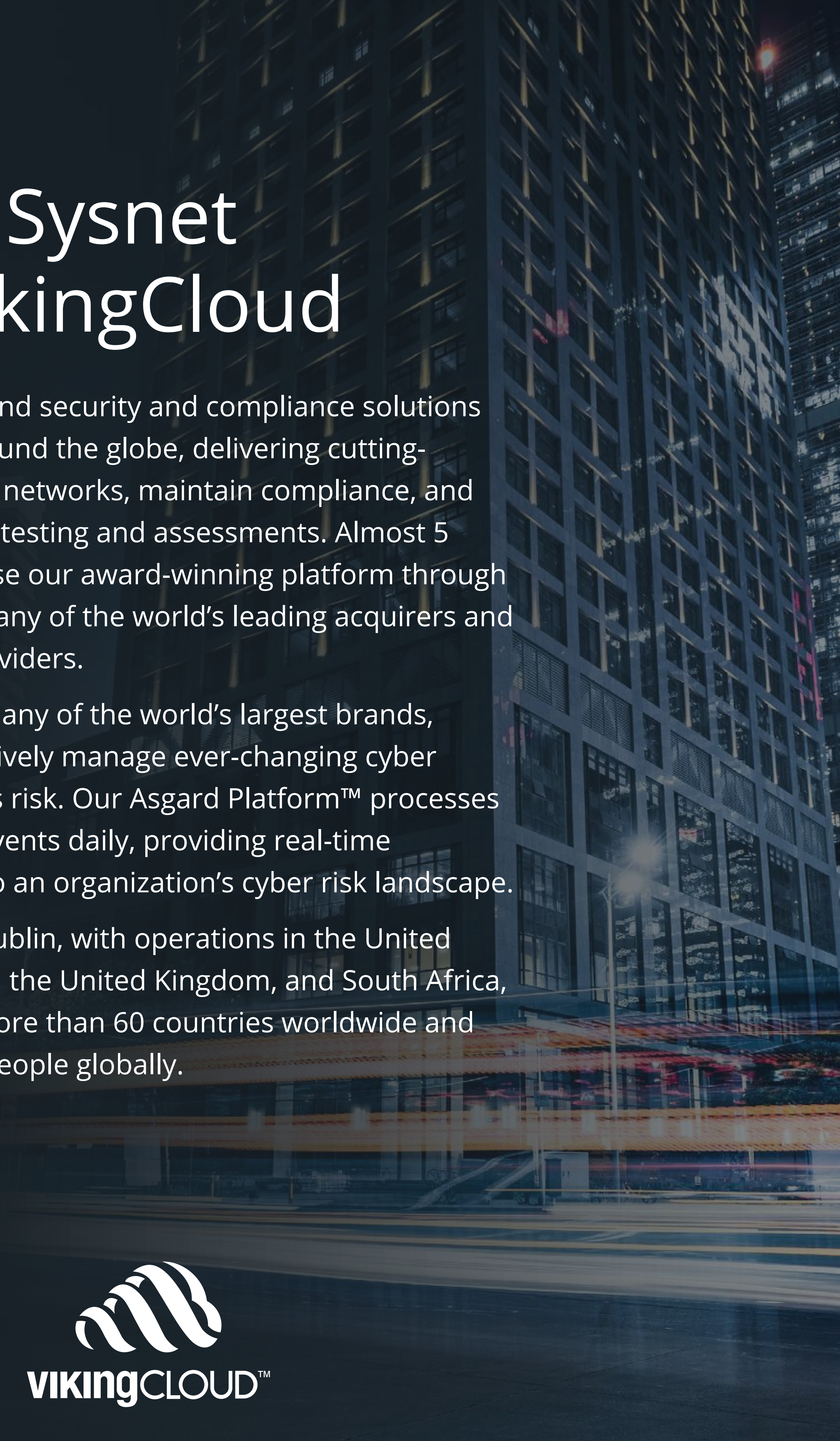
However, if they do then **that same QSA cannot perform the assessment of that PCI DSS requirement/control;** a QSA cannot assess their own work. This is in line with the independence requirements specified in QSA Qualification Requirements and Program Guide which require QSA Companies to have separation of duties controls in place to ensure that QSA Employees conducting or assisting with a PCI DSS assessment are independent and not subject to any conflict of interest.

Next Steps: For an understanding of the changes introduced with the v4.0 SAQs, please see our separate **eBook** or for support on your transition to PCI DSS v4.0, then why not reach out to **Sysnet | VikingCloud** today by filling out our Request a Call Back Form, sending an email to:

marketing@vikingcloud.com

or visiting our 'contact us' page to view a list of our global office phone numbers:

Click here to visit our page.



About Sysnet and VikingCloud

We provide end-to-end security and compliance solutions to businesses all around the globe, delivering cutting-edge ways to secure networks, maintain compliance, and complete assurance testing and assessments. Almost 5 million merchants use our award-winning platform through partnerships with many of the world's leading acquirers and payment service providers.

We also work with many of the world's largest brands, helping them proactively manage ever-changing cyber threats and business risk. Our Asgard Platform™ processes billions of security events daily, providing real-time intelligence access to an organization's cyber risk landscape.

Headquartered in Dublin, with operations in the United States, India, Poland, the United Kingdom, and South Africa, we have clients in more than 60 countries worldwide and employ over 1,000 people globally.

sysnet®
is now VikingCloud

VIKINGCLOUD™

For more information, visit:
www.sysnetgs.com or **www.vikingcloud.com**