PCI Consulting Australia

PCI DSS version 4.0 Update

PCI Consulting Australia

May 2022

Contents

Introduction

On 31 March 2022, PCI DSS version 4.0 was officially released. This is the next evolution of a mature standard in line with industry developments. Whilst the PCI Security Standards Council (PCI SSC) has released and will continue to release a number of guidance documents in conjunction with the new standard, we as a Qualified Security Assessor (QSA) firm wish to provide our own analysis.

About Us

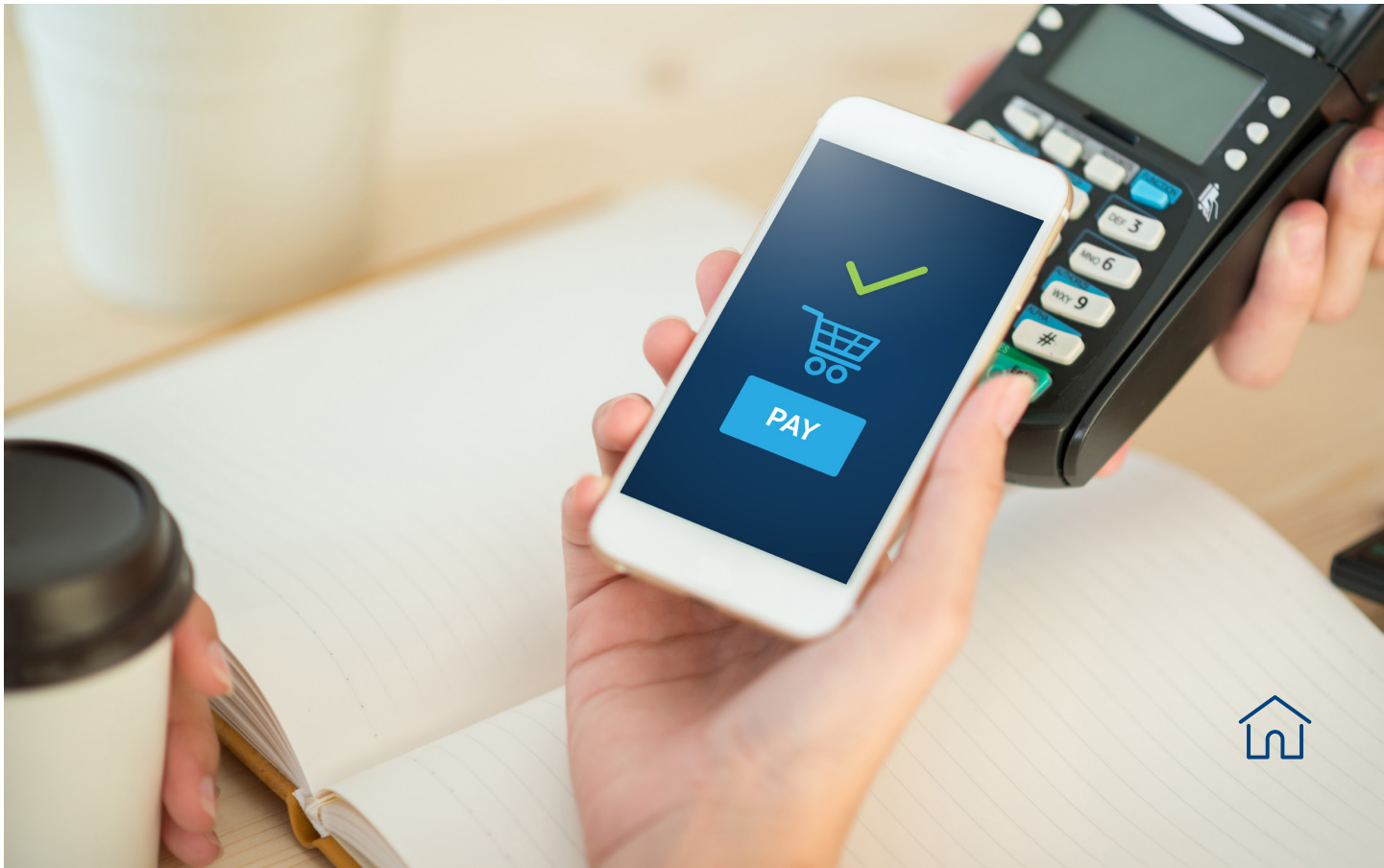
PCI Consulting Australia is a QSA firm operating since 2014, covering the Asia-Pacific region at the time of this document.

QSAs are the industry specialists who provide external validation of adherence to PCI DSS requirements for any business involved in storing, processing or transmitting card data.

Multiple assessors within our firm have been operating as QSAs well before PCI Consulting Australia was founded and we have positioned ourselves as a firm as pure PCI DSS experts. What we mean by that is we do not offer a broad range of services, instead primarily focusing on PCI DSS assessment and advisory services, and penetration testing. As such, we believe our team has a high working level of knowledge of PCI DSS requirements and have seen the standard evolve our many years. Therefore, we provide our analysis with confidence in our experience and approach.

Intention of this document

The PCI SSC has published a summary of changes document which lists every single change from version 3.2.1 to version 4.0. Therefore we do not intend to repeat the same analysis. Instead our intention is to highlight key changes so you can start planning for introduction of the new standard.



Glossary

PCI DSS	Payment Card Industry Data Security Standard
PCI SSC	PCI Security Standards Council
QSA	Qualified Security Assessor
ISA	Internal Security Assessor
CDE	Cardholder Data Environment
ROC	Report on Compliance
SAQ	Self-Assessment Questionnaire
AOC	Attestation of Compliance
MFA	Multi-factor Authentication
SAD	Sensitive Authentication Data
SSL	Secure Sockets Layer
TLS	Transport Layer Security

Key Observations

Those who are subscribed to our newsletter would have received the dot point information below already. For those who wish to subscribe or have further questions you can contact us at info@pciconsultingaustralia.com.au.

We will also be providing further analysis during 2022 as the PCI SSC releases further information such as Self-Assessment Questionnaires (SAQs).

- The new standard is an evolution of the existing standard. This is not a major overhaul of existing requirements.
- SAQ templates have only just been released. We will complete a separate analysis of the different SAQs.
- PCI DSS v4.0 is NOT mandatory until 31 March 2024.
- Any new v4.0 requirements (except a handful of documentation requirements) are NOT mandatory until 31 March 2025.
- Other official supporting documents will be released over the course of 2022.
- QSAs cannot undertake v4.0 assessments until they complete training, which is not available until at least June 2022.

Initial Observations

We believe the new standard is in line with industry movements and enhances existing controls in PCI DSS version 3.2.1. The PCI SSC introduced a level of collaboration not seen in other versions where multiple drafts were released to key stakeholders such as QSAs for feedback. As such, the release process was elongated but ultimately the right result was obtained, albeit with a couple of items we question. Except for all the changes in the requirement numbers, which us as QSAs have spent years memorising and now have to go back to the drawing board!

Giving entities 3 years to implement any new requirements means there are very few excuses for most businesses to not hit the deadline, with potentially the exception of incredibly complex environments. Some of the changes required may also end up being a process change rather than a technical change.

There are also 2 distinct approaches to an assessment: defined or customised approach. The defined approach is status quo as the standard is today with a listed requirement such as a password policy and key criteria to meet the requirement. The customised approach is new and to be utilised where an entity cannot strictly meet the defined requirement. This does not mean an entity can invent an answer to avoid an onerous requirement- in fact quite the opposite. A large amount of effort is required by the entity which includes significant documentation and rationale as to the effectiveness of their customised control. Similarly, the testing criteria and associated reporting for the QSA is elongated.

Whilst a more flexible approach being available is a positive, the reality is an entity is likely to use this approach for at most, a handful of requirements, if at all. It is also important to note that it is the responsibility of the assessed entity to devise the control. A QSA can be consulted but if the individual assessor assists in deriving the control, that individual cannot then assess it at a later date.

The customised approach is also only available for Report on Compliance (ROC) assessments. If you complete a Self-Assessment Questionnaire (SAQ), this will not be an option, unless absolutely essential and would require documentation into a ROC template. Also, it can only be assessed by a QSA or accredited Internal Security Assessor (ISA).

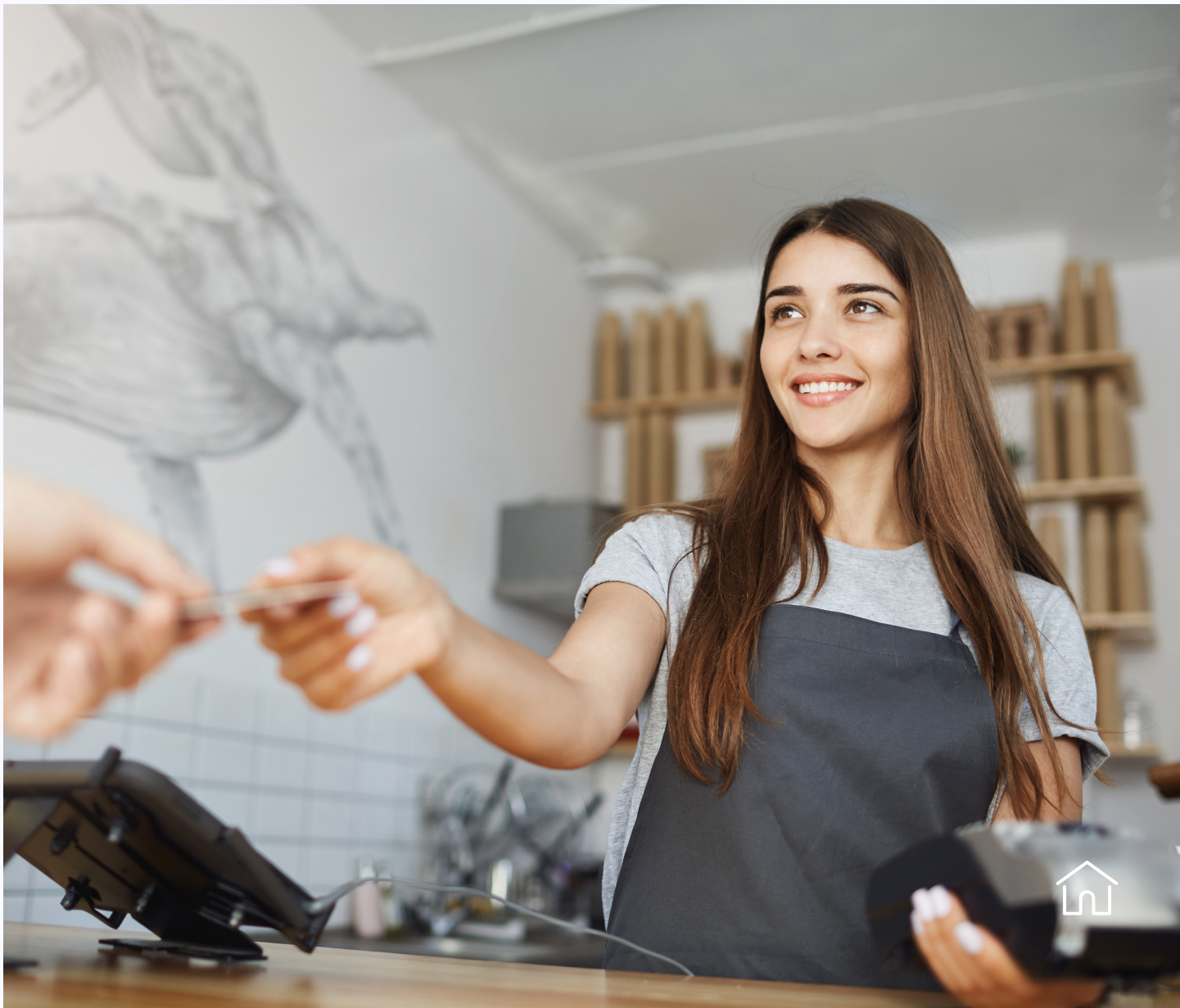
Report on Compliance (ROC) reporting has also changed for QSAs. There is now a fair greater emphasis on listing individual pieces of evidence as opposed to the QSA providing detailed answers. In the current standard, the assessor lists documents and interviewees in the initial ROC sections. For version 4.0, there are more detailed requirements including documentation, interview, observation, and system evidences. Rather than relying on a QSA explanation to answer an individual requirement, the onus is now on exact tabling and compilation of all evidence reported in the initial section of the ROC, and subsequent answer to individual requirements that reference these lists.

What this really means is for every PCI requirement that requires a settings review, the assessor is going to have to have formal evidence such as screenshots saved and documented. This will certainly add time to both assessments and quality review. We as assessors need to adapt to this so PCI Consulting Australia will be releasing an online portal later in 2022 for entities to upload evidence during the assessment so that no requirements are missed. This portal is likely to be specific to v4.0.

It certainly means that dotting the I's and crossing the T's is more precise and important than ever.

The concept of scoping and planning an assessment is similar, although scoping requirements have now been enhanced. It is now a specific PCI requirement for the assessed entity to provide formal evidence of scoping as part of the annual assessment and will be requested by QSAs as a starting point for any assessment. For service providers, this is a 6 monthly requirement.

Whilst we discuss the new requirements below, remember some or many of these may not be relevant to your environment. We recommend consultation with your QSA to assist in confirming your scope under the new standard at the appropriate time, which is likely to be after QSAs have completed formal PCI DSS version 4.0 training.



New Requirements Review

Below is a high-level review of key new requirements as a summary. A more detailed analysis of all 12 requirements will be provided in the next section.

Risk assessments

The current standard is fairly loose on what constitutes a risk assessment. This is tightened up considerably in version 4.0. It is now a 'targeted risk analysis' as opposed to an enterprise-wide risk assessment and focuses on items that are 'periodic' as opposed to defined as weekly or monthly. Any customised approach used must also have a targeted risk analysis specific to that requirement.

Accountability

At the start of each PCI requirement, roles and responsibilities for performing activities under that requirement must be documented, assigned and understood. This is more specific than the current standard which focuses only on policies and procedures. This will also help assessors understand who they need to engage with to address each PCI requirement.

Web Application Protection

A web application firewall will become mandatory so web application scanning only will not meet requirements. Entities will also have to implement script and header monitoring on payment pages so malicious actors cannot introduce new scripts or change existing ones to introduce malware. There are also formal processes required to monitor and respond to any unauthorised changes on payment pages.

Authentication

Multi-factor authentication (MFA) is required for ALL access into the Cardholder Data Environment (CDE). This changes from the present standard which prescribes all remote access, or all non-console admin access only to utilise MFA. This still does not apply in a retail POS environment. Enhanced password requirements now require a minimum 12-character password, up from 7.

Testing

Internal vulnerability assessments must be authenticated. This does not apply for systems that do not accept credentials such as containers.

Training

Employee training must now include awareness of phishing and social engineering attacks.

Service Provider Management

Clarification on Requirement 12.8.2 as to what constitutes written acknowledgement for responsibility for card data protection.

Detailed Review

We will now provide a summary of key changes per each of the 12 PCI requirements and add our commentary accordingly where appropriate. The PCI SSC has released a summary of changes document that describes every single change in the standard.

This is more a practical guide to changes rather than at the level of detail provided by the PCI SSC.

Requirement 1

The good news is, there is not much to see here. Other than the accountability requirement- which applies to all requirements- any changes are clarifications or guidance updates. The general principle of limiting inbound and outbound access to the CDE to a legitimate business need remains.

Requirement 2

Very similar to Requirement 1 in no major changes to discuss.

Requirement 3

If you do NOT store card data electronically: Then there are no material changes relevant.

If you DO store card data electronically: There are a number of changes to consider.

1. The PCI DSS has always addressed storage of card data post payment authorisation. Now, in the rare event you need to store sensitive authentication data (SAD) pre-authorisation then it must be encrypted. Any SAD storage must always be fully justified as business critical.
2. If full card data can be accessed remotely, a technical solution must exist to ensure an individual cannot copy card data out of the environment. The first question you would need to address is whether a business need exists to view full card data remotely or not. Eliminating the ability to do so removes the requirement from scope. Otherwise consultation with your vendor to discuss technical solutions is required.
3. Disk-level encryption can only be used as an effective control on removable media. We are happy that the final version does not enforce automated scans for card data and manual scans can be performed. Of course automated scans are preferred, particularly for enterprise sized entities, but we were concerned the cost of automated solutions would be onerous for small entities with very small, simple CDEs.

Requirement 4

A couple of changes in process and documentation. A formal process to confirm certificates are in use to protect card data in transmission are valid and not expired is required. A documented inventory of trusted keys and certificates in use is required to be maintained.

The requirement to protect card data in transmission remains in scope for 'open, public networks' only, and not within the CDE.

Requirement 5

The primary change here is ensuring anti-malware software has mechanisms to detect and protect against phishing attacks. This is a technical control to supplement employee training- both are required for a compliant environment. The software should also be able to detect and scan when removable media is used.

Entities will be reliant on vendors to meet these requirements so ensure you're asking the right questions before selecting a solution that fits your needs. Spam filters of course are becoming more sophisticated to assist in meeting phishing or social engineering challenges.

The frequency of both scans and evaluations of systems not at risk for malware can now be determined by the entity as part of their targeted risk analysis.

Requirement 6

The primary changes here we mentioned under 'web application protection'. Implementation of a web application firewall that provides real-time protection rather than a periodic scanning option makes logical sense. If introducing this causes fundamental performance issues then compensating controls are still available. Adding formal requirements to protect against malicious code on payment pages was inevitable, with the vast majority of card data breaches originating from web-based environments. The assessed entity will have to submit an inventory of all necessary scripts with their justification as part of the assessment.

There is now a requirement for an inventory of critical software. In Level 1 assessments we as assessors have always asked for this anyway as it is part of our reporting requirements. This now extends to SAQ assessments as a compulsory item.

Significant changes should also be documented under annual scoping efforts.

Requirement 7

Whilst there are 3 'new' requirements, these do not have a major impact for an organisation with good access controls. They are still based on the same existing principles of least privilege. One of the new requirements allows flexibility on review of application and system accounts depending on the results of the targeted risk analysis.

Requirement 8

There are a number of changes to discuss here.

As we flagged earlier, implementation of MFA for **all** CDE access is the primary change. This is not surprising considering the move to cloud computing where MFA is already actively encouraged in almost every circumstance as an industry standard. There is also a new requirement to review and ensure the integrity of the MFA implemented so that it cannot be bypassed in any way.

Note- if you are accessing the CDE from within your corporate network then MFA is required, even if you used MFA originally to access the corporate environment. The premise is wherever you connect from, MFA is mandatory. This is likely a requirement to discuss with your QSA to determine which systems are deemed in scope as version 4.0 gives many examples such as cloud systems, on-premise, workstations, servers, and endpoints.

Interestingly the invalid authentication attempts lockout requirement has been relaxed from 6 attempts in version 3.2.1 to 10 attempts in version 4.0. Unless 6 attempts is causing significant issues for you, we recommend retaining current policies.

Password length increases to a minimum 12 characters. There is an existing FAQ 1467 on the PCI SSC's website which allows for removal of password rotation should extra controls be implemented. We as assessors are happy to consider scenarios to remove password rotation where complex passphrases and MFA are utilised as examples. The new standard also allows for this where dynamic analysis is utilised such as rapid detection of compromised credentials or device location tracking, with the ability to immediately disable the account if any compromise is suspected.

If service providers offer a platform for their customers to view full card data they are then required to implement PCI compliant password policies onto their customers as opposed to simply recommending the customers implement compliant policies. It would be worth reviewing the process of allowing customers access to full card data as a necessary business function before implementing technical controls. We assess multiple payments' providers and cannot think of too many examples where they allow customers access to full card data.

Lastly, there are now newly defined requirements for system or application accounts. This involves preventing interactive use of these accounts; not hard coding passwords into scripts or source code; and changing passwords periodically based on a targeted risk analysis.

Requirement 9

There is a large number of requirements renumbering and consolidation but no material changes. The frequency of payment terminal inspections commonly performed in a retail environment must be supported by a targeted risk analysis.

Requirement 10

Once again, the 'periodic' review of logs for non-critical system components will need to be defined in the targeted risk analysis.

A primary change is enforcement of automated mechanisms to perform log reviews. This really has been implied for some time but now strictly enforced. Manual log reviews are unlikely to be effective or comprehensive without some sort of system alerting important events to key personnel.

PCI DSS version 3.2.1 has Requirement 10.8 in scope for service providers only. This now extends to merchants in version 4.0, which involves timely detection of failures of key systems such as firewalls, IDS/IPS or anti-virus. Note we have experienced customer confusion in this requirement previously with security incidents, which is addressed under incident response requirements. This requirement is specific to a failure of the firewall doing its job as an example, as opposed to detection and alerting of suspected attacks which is part of your incident response process.

Requirement 11

Introduction of authenticated internal scanning will require changes for many entities. The theory being that authenticated scans are more comprehensive and can detect vulnerabilities unauthenticated scans cannot. Protecting issued credentials should also be in line with PCI requirements 7 and 8.

A targeted risk analysis is also required to address vulnerabilities at a lower level that do not affect PCI compliance. This also requires planning as only addressing those vulnerabilities required for compliance is now obsolete, unless your risk analysis can justify allowing a low-level vulnerability to remain.

There are no major changes to penetration testing procedures, which brought a sigh of relief to our testing team! Only one new requirement for multi-tenant service providers to allow their customers to complete external penetration testing of their systems. But they really should be allowing that today anyway.

Service providers are subject to tighter IDS/IPS provisions, with a new requirement to detect, alert or prevent, and address covert malware communication attempts such as DNS tunnelling. Engagement with vendor(s) will be required nice and early to ensure they can accommodate. Solutions may be able to identify suspicious domains and IP addresses via threat intelligence matches.

And considering the high percentage of web-based breaches in overall numbers, a predictable change is introduction of monitoring for unauthorised changes on payment pages. Software detecting header or script changes requires implementation. The new standard lists some good examples in guidance notes here- Requirement 11.6.1. Embedding tamper-resistant script to block malicious activity is one example.

Requirement 12

There are a number of changes in documentation so we'll summarise here and label, then discuss.

- 12.3.1- Enhanced risk analysis requirements as we have mentioned.
- 12.3.2- Requirement to use a targeted risk analysis where a customised approach is used.
- 12.3.3- Requirement to document cryptographic cipher suites and protocols and review at least annually.
- 12.3.4- Requirement to document and review hardware and software in use at least annually.
- 12.5.2, 12.5.2.1, 12.5.3- Requirement to document PCI DSS scope at least annually or after significant change for merchants. This is required every 6 months for service providers.
- 12.6.2, 12.6.3, 12.6.3.2- Requirement to review and update (if required) security awareness training material at least annually. Training material is required to include provisions on phishing or social engineering attacks, and knowledge of end-user technologies in use.
- 12.8.2- Clarification of required evidence for a service provider to acknowledge responsibility for security of card data.

- 12.9.2- Requirement for service providers to satisfy customer requests for key PCI DSS information including which PCI DSS requirements are the responsibility of the service provider, the customer, or shared.
- 12.10.4.1- Requirement for a targeted risk analysis for frequency of incident response training.
- 12.10.7- Requirement for incident response procedures to be in place should card data be discovered anywhere it is not expected.

We've already discussed a number of these such as risk analysis, scoping and training. Requirement 12.9.2 basically enforces service providers now to have a roles and responsibilities matrix. If there was any existing ambiguity that is now clarified.

For 12.10.7, we already work with many of our customers in completing quarterly reviews to ensure card data checks are performed with the appropriate remediation performed. Often the source of unexpected card data is via a service provider platform where a customer enters data into the wrong fields. Whilst we've already observed sound processes, greater documentation of the process is clearly required.

12.8.2 is one where business practicality needs to be applied and it seems the PCI SSC has taken a black and white approach. The new guidance states: *Evidence that a TPSP is meeting PCI DSS requirements (for example, a PCI DSS Attestation of Compliance (AOC) or a declaration on a company's website) is not the same as a written agreement specified in this requirement.*

Getting an AOC from service providers for many merchants is often problematic- getting a written formal acknowledgement for security of card data even more difficult. How do you enforce a local level 3 or 4 merchant to get such a formal statement from a global payments provider with millions of customers?

Hopefully introduction of Requirement 12.9.2 assists in this venture as it's a very common story we hear from customers today- the entity has tried and tried but received nothing out of the service provider. If we take a black and white approach, that entity could be non-compliant for many years or be forced to change to a provider potentially cost prohibitive. It's a lose-lose scenario and surely not the intent of the PCI DSS.

As for the company website declaration, we agree that an entity simply stating 'we are PCI compliant' does not suffice. However, formal terms and conditions publicly available meets requirements in our opinion and we have always suggested this to our service provider customers. We hope that is the path most service providers choose and suggest to customers that is the best place to begin discovery should you be unsure what the clauses lie. If it's not there today, we would suggest early collaboration with your service provider and ask how they intend to meet this clarification in requirement. If you're not getting enough collaboration, engage with your QSA before your assessment. They may know where the appropriate clauses lie from other completed assessments or they may have industry contacts who can assist.

Appendices

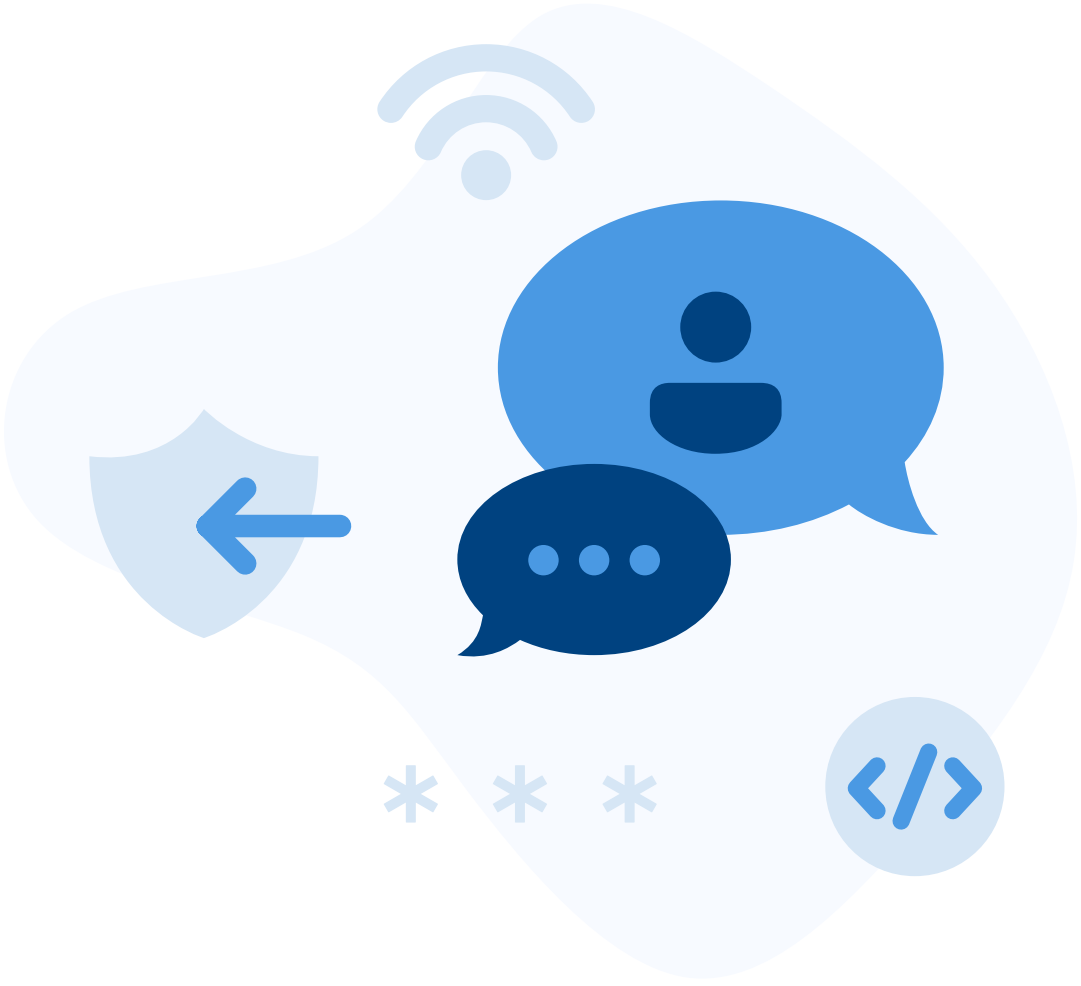
These are only used infrequently but here is a brief summary.

A1: Only used for service providers who offer shared services such as hosting multiple entities on a shared server. This is not in scope for a co-location data centre for physical equipment. New requirements include:

- The provider must also separate its own environment from customers, not just separation between all customers
- 6-monthly penetration testing required to confirm effective segmentation
- Enhanced customer incident notification processes to ensure timely and effective responses from the provider

A2: Only if SSL/Early TLS is used. Negligible change. We hope this is a non-issue and no customers use these obsolete technologies.

A3: Only used if instructed by your bank or the payment brands. Typically if an entity is subject to a major security incident. The only new requirement is to detect, alert and report failures in automated log reviews.



Next Steps

Whilst the new standard is a while away, it will arrive surprisingly quickly for those unprepared. Here are some suggested next steps:

1. Clarify your scope.

This will need to consider existing but also future states when the new standard is mandatory. Work with your QSA to understand which requirements are relevant to your CDE.

2. Develop a plan.

This may be proceeded by a gap assessment depending on the environment and/or number of changes required. A documented understanding of necessary action required to meet the new standard should be implemented.

3. Validate controls.

Don't wait for your first version 4.0 audit to test the validity of implemented controls. Ensure expert validation of controls is performed well in advance.

Need Help?

PCI Consulting Australia is available to assist your program.

Reach out at **info@pciconsultingaustralia.com.au** to obtain a quote for expert guidance from resources dedicated to PCI DSS assessment and advisory services.

Get your personalised quote

PCI Consulting Australia

1300 997 290

info@pciconsultingaustralia.com.au

LinkedIn