ANZ WORLDLINE
Payment Solutions

PCI DSS Compliance

2022 Information Pack for Merchants

Contents

Section I
Introduction to PCI DSS

PCI DSS COMPLIANCE IS ABOUT PROTECTING PAYMENT CARD DATA

PCI DSS stands for **Payment Card Industry Data Security Standard.**

The PCI DSS requirements are set by the PCI Security Standards Council (PCI SSC) whose founding members are the international card schemes shown below. They share equally in governance and execution of the Council's work.

PCI DSS specifies how Merchants and their service providers are expected to protect ***Payment Card Data***.

In order to accept payments via cards issued by the Card schemes it is important to understand and comply with these standards. They also form part of the ANZ Worldline Payment Solutions Merchant Agreement.

PCI DSS applies to all merchants that store, process and/or transmit Payment Card Data, regardless of their size or transaction volume. When compared with larger merchants, small merchants often have simpler environments, with limited amounts of cardholder data and fewer systems that need protecting, which can help reduce their PCI DSS compliance effort.

The effort required to comply relies on the business transaction volumes, payment channels and usage of PCI DSS compliant service providers.

PCI DSS PROTECTS DATA THROUGH DATA SECURITY CONTROLS

PCI DSS consists of 6 core principles which are accompanied by 12 requirements.

Becoming PCI DSS compliant requires that you can show that you have addressed all of the requirements that apply to you.

How your business handles Payment Card Data will govern how many of these principles will need to be complied with.

How you demonstrate compliance depends on your Merchant level and/or the type and number of payment channels.

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program Maximum borrowing (80% - $500,000)	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement String Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to systems components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

PCI DSS REGULATES THE STORING OF PAYMENT CARD DATA

PCI DSS requires strong encryption if storing the PAN, this requires information technology security expertise.

PCI DSS prohibits the storage of sensitive card data which includes the PIN, chip, magstripe and security code data.

Outsourcing the capture of card data to a PCI DSS compliant service provider and using compliant devices mitigates the risk of data compromises in the business.

What is Payment Card Data?

What Payment Card Data can be stored?

		Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[2]	Full Track Data[3]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID[4]	No	Cannot store per Requirement 3.2
		PIN/PIN Block[5]	No	Cannot store per Requirement 3.2

2 Sensitive authentication data must not be stored after authorization (even if encrypted).
3 Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere
4 The three- or four-digit value printed on the front or back of a payment card
5 Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message

Reference: PCI SSC PCI DSS Quick Reference Guide

OVERVIEW OF PCI DSS ROLES AND RESPONSIBILITIES

Each of the following stakeholders play an important role in ensuring PCI DSS compliance for all organisations that store, process or transmit payment card information. PCI DSS is an industry requirement for all acquiring banks and their merchants.

PCI Security Standards Council (PCI SSC)

The PCI Security Standards Council publishes and manages the standard.

Standards include:

- PCI DSS
- PCI PTS (Hardware)
- PA DSS (Software)

Maintain lists of Approved Vendors for:

- External network scanning
- QSA Organisations,
- Internal Security Assessors
- Payment Devices
- Payment Applications

Card Schemes

Ensure adherence to PCI standards by mandating timeframes for compliance, incentives, penalties and regular progress reporting.

Card Scheme Websites Provide:

- Merchant Level definitions
- Merchant Obligations
- Compliance Dates
- Education and training
- List of registered PCI DSS compliant Service Providers

Acquirer

Manage implementation of PCI Data Security Standards and the card schemes mandates with our merchants.

Report regularly to Visa and Mastercard on PCI DSS compliance progress of our merchants.

Provide education and support to ensure our merchants validate and maintain PCI DSS compliance.

Merchant

- Complete an annual Self-Assessment Questionnaire or Onsite Audit
- Manage non-compliance remediation activities using the 'Prioritised Approach' tool
- Submit a compliant network vulnerability scan each calendar quarter
- Report compliance status to ANZ Worldline Payment Solutions each quarter.
- Use of PCI-DSS compliant service providers
- Use of PA-DSS certified best practice applications.

Note: For details of American Express requirements, please speak to your American Express account manager.

PCI DSS GIVES MERCHANTS THE FRAMEWORK TO SECURE PAYMENT DATA IN THEIR PHYSICAL AND ONLINE STORES

Physical Store Security

Physical security is visible and well understood by merchants therefore increasing the difficulty of theft.

Merchants can install layers of security to ensure goods and sensitive data are not stolen.

Online Store Security

Online or internet access security is complex and not visible without testing which can result in unintentionally allowing entry to hackers.

Merchants usually don't have the expertise or knowledge to implement adequate layers of security in their online environment to protect their website and customer information.

Typical issues include:

- Selecting the lowest cost developer and service provider.
- No ongoing maintenance and security patch updates.
- No monitoring, alerts and no visibility.
- No security testing.
- Prone to Phishing
- Default passwords not removed and no complex passwords.
- Using non PCI compliant service providers or products.
- Unsecured storage of card data.

- Web developer not trained in information security.
- Online business exposed globally.

Bad customer experiences include:

- Stolen card details
- Reputational damage
- Large remediation costs.
- Shifts focus away from sales.

EXAMPLES OF HOW PCI DSS NON-COMPLIANCE CAN LEAD TO AN ACCOUNT DATA COMPROMISE

Extract from Forensic Investigation Report

The initial investigation has identified a number of non PCI DSS compliant practices within the merchant that could have contributed to unauthorised access to payment card data.

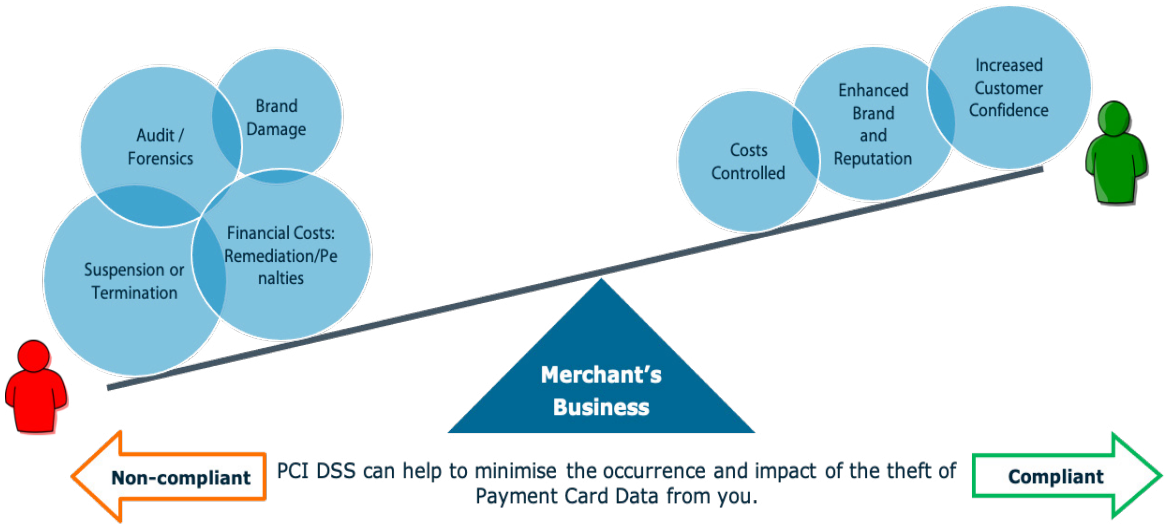
These include:

- Multiple website vulnerabilities identified by security testing using a PCI approved external vulnerability scan.
- Lack of updating new software releases and security patches.
- Stored email based orders that contain cardholder data.
- Recurring payments card data stored unencrypted.
- Use of non-compliant service providers such as a payment gateway, web host, shopping cart or POS application.
- Insecurely stored paper records used to take telephone orders.
- Default passwords were never changed and insufficient password complexity.
- Insecure software coding practices.

CONSEQUENCES OF AN ACCOUNT DATA COMPROMISE (ADC)

ADCs involve unauthorised access to cardholder data that is held within your business environment in either electronic or physical form. It is usually done by fraudsters who do not discriminate between small or large businesses.

- If payment card data is not protected and/or steps are not taken to ensure that service providers do the same, you could be subject to an ADC event.
- If you become the subject of an ADC event you risk financial penalties, suspension or termination of your merchant facility as well as remediation costs.
- You also risk damage to your brand and reputation. While many cardholder data compromises in Australia go unpublicised some have resulted in adverse publicity through national media outlets.



FINANCIAL CONSEQUENCES ASSOCIATED WITH PCI DSS NON-COMPLIANCE

The financial consequences of PCI DSS non-compliance include:

Fines for not validating compliance for Mastercard

Violations per calendar year	Mastercard (up to in US $) for L1 & L2 Merchants	Mastercard (up to in US$) for L3 Merchants
First violation	$25,000	$10,000
Second violation	$50,000	$20,000
Third violation	$100,000	$40,000
Fourth violation	$200,000	$80,000
Total of 4 violations per Merchant	**$375,000**	**$150,000**

Fines for not validating compliance for Visa

Revalidation Overdue With No Remediation Plan & Newly-Identified Merchants	Assessment	
	Level 1 (US$)	Level 2 (US$)
91 - 180 days after expiry of previous validation	$10,000 per month	$5,000 per month
181 - 270 days after expiry of previous validation	$25,000 per month	$10,000 per month
More than 270 days after expiry of previous validation	Risk reduction measures	

Please Note: In addition, ANZ Worldline Payment Solutions may have no choice but to terminate a merchant facility if PCI DSS compliance isn't achieved by any date communicated to a merchant. If the merchant facility is terminated, a record will be created with the card schemes, which could limit the ability to gain a merchant facility from another bank i.e. Trace List for Visa and MATCH List for Mastercard.

Account Data Compromises

If you suffer an ADC event, the financial consequences of a data compromise include:

Card Scheme Fines & Recovery Costs if you have an Account Data compromise

Reason	Visa assessments(up to in US$)	Mastercard assessments(up to in US$)
Account data compromise (ADC)	See Visa Fines Breakdown below	$5,000 to $500,000
Stolen card data Issuer reimbursement	$12.50 per card	$8.50 per card
PCI DSS non-compliant requirements	NA	$100,000 per non-compliant requirement (in addition to any assessments provided for elsewhere in the Standards)
Failure to report an ADC	NA	Up to US$25,000 per day of non-compliance
Remediation period and cost	Within 30 days / unplanned remediation cost is paid by the merchant	
Forensic Investigation	Scope dependant (require PCI approved forensic investigator) – Min. Cost $10,000	

Ongoing Fines if you have an Account Data compromise for Visa

Compromised Entity	Initial Non-compliance Assessment	Monthly PCI DSS Violation Assessment
L1 Merchants (>6M transactions p.a.)	$25,000	$25,000
L2 Merchants (1 – 6M transactions p.a.)	$10,000	$10,000
L3 Merchants (eCommerce only 20,000 – 999,999)	$5,000	$5,000
L4 Merchants	$5,000	$5,000

*Non-compliance assessments continue on a monthly basis until the merchant has submitted the appropriate PCI DSS validation documentation.

**Effective September 1, 2015, Visa may require breached entities, specifically Level 1 and Level 2 merchants, to comply with the PCI DSS Designated Entities Supplemental Validation (DESV) requirements as part of their post-breach PCI DSS assessment

Section 2
Being PCI DSS Compliant

YOUR LEVEL DETERMINES YOUR REPORTING OBLIGATIONS

Step 1: ANZ Worldline Payment Solutions determines your merchant level using the annual number of transactions processed

Merchant Level	Number of transactions per annum of either Visa or Mastercard transactions
Level 1	> 6m
Level 2	> 1m and <6m
Level 3	< 1m and >20,000 ecommerce
Level 4	<1m and <20,000 ecommerce

- Begin by identifying your merchant level, and keep track as your business grows.
- Your level is determined using the number of either Visa or Mastercard transactions per annum.
- Closed loop card schemes such as American Express will contact you separately.
- ANZ Worldline Payment Solutions is required to report this through to the card schemes.
- Your merchant level determines how you validate PCI compliance. Refer slide 15.
- The PCI DSS compliance requirements are the same for everyone, regardless of the transaction volumes.
- If suspected of a data compromise, merchants automatically become a level 1.

REPORTING YOUR COMPLIANCE STATUS IS MANDATORY

Step 2: Understand the reporting obligations to validate compliance

Merchant Level	Reports	Validation Method
Level 1	• Report of Compliance (ROC) • Attestation of Compliance • ASV scans	• Must use an external Qualified Security Assessor (QSA) or a PCI qualified Internal Security Assessor (ISA)
Level 2	• Self Assessment Questionnaire (SAQ) • Attestation of Compliance • ASV Scans	• Must use an external Qualified Security Assessor (QSA) or a PCI qualified Internal Security Assessor (ISA)
Level 3		• Self-Assessment
Level 4		• Self-Assessment

Reports to be provided to ANZ Worldline Payment Solutions include:

- Annual validation of compliance by either a Report of Compliance (ROC) or Self-Assessment Questionnaire (SAQ) to be provided each year on the anniversary date of the initial report.
- Quarterly external vulnerability scan results (also know as Approved Scanning Vendor - ASV scans).
- Where non-compliant, quarterly updates using the Prioritised Approach tool.
- Non-compliant merchants must report a target compliance date and a remediation plan.
- Merchant must report their compliance status to ANZ Worldline Payment Solutions each and every calendar quarter. Refer to reporting dates.

HOW TO GET STARTED WITH PCI DSS

Step 3: Start assessing your business to determine the scope

	Recommended Actions
1	**Organisational engagement:** You will require good governance with senior management support. Determine who in your business must be involved such as technology, operations, project management, audit and payment process knowledge.
2	**Investigate how payments are processed today:** Document your current transaction flows and understand your assessment scope. This should include cardholder data flows, processes, people and systems. Consider all payment channels including in-store, online, over the phone, email, mail and forms.
3	**Define the future state:** Consider how you may reduce the scope, risk and effort by changing processes, removing card data or investing in new technology. Leverage the experience of PCI DSS experts to help you at this stage.
4	**Benefit from service providers compliance and security investment:** Leverage PCI DSS compliant service providers, for websites consider using an iFrame or Hosted Payment page which outsources the capture of card data.
5	**Validate by running scans:** Run the external vulnerability scan for your website using the ANZ Worldline Payment Solutions PCI portal.
6	**No sensitive data:** Remove all sensitive data and delete any stored PANs immediately to eliminate risk. Use payment gateway tokens instead.

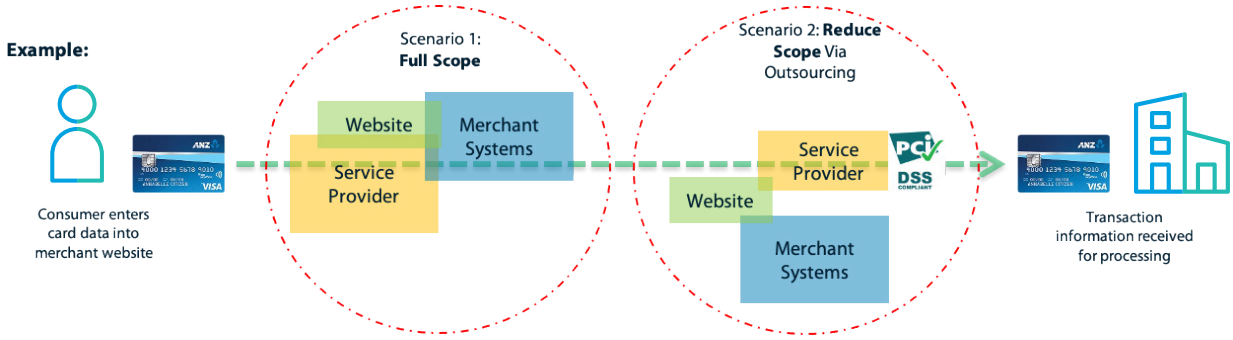
7	**Understand the PCI DSS requirements:** Use the ANZ Worldline Payment Solutions PCI Portal Wizard to determine your requirements. Complete all the questions you can and get support as needed.
8	**Develop a remediation plan:** Develop a project plan for remediation activities, along with a target compliance date. Include this in your reporting to ANZ Worldline Payment Solutions. Where not compliant, complete the SAQ and Prioritised Approach tool.
9	**Report to ANZ Worldline Payment Solutions:** Submit your reports to ANZ Worldline Payment Solutions on the due dates. Refer to page 16.

DETERMINE THE SCOPE OF YOUR PAYMENT CARD DATA ENVIRONMENT

Scope of PCI DSS Requirements

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment.

- The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data.
- Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement. However, it is strongly recommended as a method that may reduce scope and cost.
- Merchants may use a third-party service provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment and should be included as part of the review. Discuss with your service provider who is responsible for which PCI requirements.
- Outsourcing the capture, processing and storing of card data to a PCI DSS compliant service provider such as a payment gateway may also reduce your CDE and therefore your scope and costs.



QUARTERLY TASK – PERFORM AN EXTERNAL VULNERABILITY SCAN

There are ***ongoing quarterly*** obligations associated with demonstrating (proving) your level of PCI compliance:

Quarterly Network Vulnerability Scan	**PCI External Vulnerability Security Scans** are scans conducted over the Internet by an Approved Scanning Vendor (ASV), this is available via the ANZ Worldline Payment Solutions PCI Portal.
PCI DSS Requirement 11.2	**Why Scan?** Scans help identify vulnerabilities and misconfigurations of web sites, applications, and your IT infrastructure with Internet-facing IP addresses. Scan results provide valuable information that support efficient patch management and other security measures that improve protection against Internet attacks. A full technical description of the scan scope can be found on pages 15-20 of the ASV Approved Scanning Vendors Program Guide. **Where do they apply?** PCI Security Scans may apply to all merchants and service providers with Internet-facing IP addresses. Even if an entity does not offer Internet-based transactions, other services may make systems Internet accessible. Basic functions such as e-mail and employee internet access will result in the company's network being accessible via the internet. Such seemingly insignificant paths to and from the Internet can provide unprotected pathways into merchant and service provider systems and potentially expose cardholder data if not properly controlled. Quarterly Scans are compulsory if you qualify for either the SAQ A-EP, SAQ B-IP, SAQ C or SAQ D versions.

SELF ASSESSMENT QUESTIONNAIRES

The Self Assessment Questionnaire is determined by your payment channels and handling of card data. Outsourcing payment channels to PCI DSS compliant Service Providers can help reduce the number of requirements.

SAQ	Description	Requirements	Product Types
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Not applicable to face-to-face channels.	22	Payment Gateway Hosted Payment Page and iFrame OR Hosted shopping cart PCI Complaint Software As a Service (SAS)
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website/s that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Applicable only to e-commerce channels.	194	Direct post from the client side directly to the payment gateway, bypassing the merchant's web server.
B	Merchants using only: • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. Not applicable to e-commerce channels.	41	Standalone terminal
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. Not applicable to e-commerce channels.	80	Standalone terminal with an IP connection
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. Not applicable to e-commerce channels.	81	Virtual terminal using a payment gateway
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. Not applicable to e-commerce channels.	164	Integrated terminal
D	SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types. Including: Merchant hosted ecommerce and cardholder data storage.	366	All other products, integration methods and combination of products.

PAYMENT SERVICE PROVIDERS

Utilising PCI Compliant Service Providers is an integral part of your own PCI DSS Compliance.

The PCI SSC defines a Service Provider this way:

Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS (Intrusion Detection System) and other services as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).

For further information and more definitions visit: https://www.pcisecuritystandards.org/pci_security/glossary

- ☐ You should only use PCI DSS 'compliant' Level 1 certified Payment Service Providers to protect your customer's cardholder data.
- ☐ If your Service Provider isn't PCI compliant, your customer's card data is at risk of being breached/stolen.
- ☐ Level 1 certified Service Providers have their PCI Compliance revalidated by a QSA every 12 months.
- ☐ A list of Level 1 certified Service Providers can be found on the Visa Website: https://www.visa.com/splisting/ - we recommend that you should only use Service Providers on this list. However, if your Service Provider is not on this list, and they provide you with a PCI AoC, signed by a QSA – then that is equally acceptable.
- ☐ Ensure that your Service Provider recertifies their PCI DSS Compliance annually.

Note

Using a compliant Service Provider doesn't mean that you, the Merchant, are now automatically PCI DSS Compliant. You still need to validate your own businesses PCI DSS Compliance separately. However, due diligence in selecting a service saves you from running into problems later and it reduces the cost and effort required to achieve your PCI DSS Compliance.

MANDATORY PCI DSS REPORTING DUE DATES FOR 2022

The 2022 reporting dates are set out below:

	Q1	Q2	Q3	Q4
Scheme reporting				
Merchant due dates:				
Must submit quarterly PCI DSS reports to ANZ Worldline Payment Solutions	11 March 2022	10 June 2022	9 September 2022	2 December 2022
Reports to be submitted:				
External Vulnerability Scan with "PASS" Results	✓	✓	✓	✓
Signed SAQ or AOC		Must be provided on your anniversary date (every 12 months)		
Prioritised Approach report when not PCI compliant	✓	✓	✓	✓

Merchants who do not submit their reports by the merchant due dates may be subject to fines issued by the Card Schemes (Visa and Mastercard).

Reports can be submitted via the ANZ Worldline Payment Solutions provisioned SecureTrust PCI portal or emailed to pcicompliance@anz.com.

SUMMARY – PCI DSS COMPLIANCE REQUIRES GOOD GOVERNANCE

In order to meet the various PCI DSS validation requirements, most Merchants will need to do the following types of things:

- ☑ Understand your Merchant Level
- ☑ Determine the scope of your Card Data Environment – that is, understand where and how Payment Card Data forms part of your payment processing activities
- ☑ Complete a compliant Network Vulnerability Scan (every 3 months (ongoing)) for externally facing IP addresses if they form part of your Card Data Environment
- ☑ Complete an annual PCI DSS Assessment of your Card Data Environment – onsite or SAQ as required – determine what SAQ applies to you
- ☑ If you are a Level 1 or Level 2 Merchant, you will need to decide whether you will engage a QSA or go down the ISA path
- ☑ Develop a plan to fix (remediate) any areas of non-compliance – use the 'Prioritised Approach' tool
- ☑ Only use PCI DSS 'compliant' Level 1 certified Payment Service Providers
- ✉ Quarterly submit your compliant Scan and PCI DSS update to ANZ Worldline Payment Solutions by the report due date

Hint

Keeping good records and an audit trail will help you stay on top of your PCI DSS requirements

Section 3
How can ANZ Worldline Payment Solutions assist?

ANZ WORLDLINE PAYMENT SOLUTIONS IS COMMITTED TO ASSIST MERCHANTS WITH PCI DSS COMPLIANCE

ANZ Worldline Payment Solutions is proud of its achievements to date in helping its merchants address their PCI DSS compliance obligations and can provide the following support services to assist attaining and maintaining PCI DSS compliance.

- ☐ Dedicated ANZ Worldline Payment Solutions PCI Compliance Manager to assist your business in reaching compliance with PCI DSS. The PCI Compliance Manager provides education, support, management and reporting frameworks and engagement with expert information security resources to assist your business with your PCI compliance journey.
- ☐ ANZ Worldline Payment Solutions offers customers regular planning session for PCI DSS, to identify activities, support requirements and reporting timeframes for the coming year.
- ☐ Progress meetings as required to support your PCI program.
- ☐ Access to industry benchmarks and best practice for PCI program management.
- ☐ Participate in ANZ Worldline Payment Solutions PCI DSS Merchant Forums - network, learn and share experience with other merchants.

INTRODUCING THE ANZ WORLDLINE PAYMENT SOLUTIONS PCI PORTAL

ANZ Worldline Payment Solutions can provide complimentary access for selected merchants to its ANZ Worldline Payment Solutions PCI Portal: https://portal.securetrust.com/

PCI Compliance Validation Task	How the ANZ Worldline Payment Solutions PCI Portal can help you
PCI Self Assessment	Use the wizard to determine your questionnaire and complete the mandatory reporting online. Once completed then remediate the non-compliant requirements. **Save time!**
Vulnerability Scans	Scans on your website run monthly and the result outcome is emailed so you know when you need to remediate. **Save money!**
Fully supported by a Help Desk	24×7 Phone and email support provided: Phone 1800 363 1621 or email support@trustwave.com **Expert support!**
Additional Services	• Card data discovery • QSA ad-hoc support • Export reports • Security templates

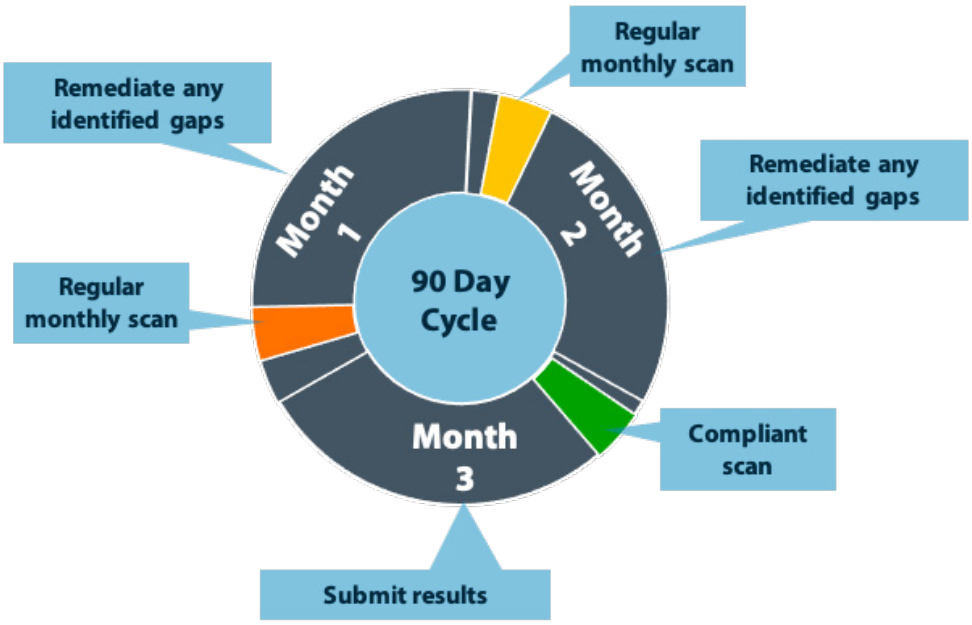
Section 4
Education Tools & References

EDUCATION TOOLS & REFERENCES

Monthly activity required to achieve a PASS scan result by the reporting due dates.

- You must have a compliant scan to be PCI compliant for the first time.
- To stay PCI compliant you need to demonstrate a compliant scan every 90 days.
- Scans are updated to identify any new vulnerabilities, so perform your scan monthly to allow for any unexpected remediation.

Scans within the ANZ Worldline Payment Solutions Portal run monthly and are automatically reported to ANZ Worldline Payment Solutions.



Definitions

'ASV' means PCI Council 'Approved Scanning Vendor'

COMPLETING A SELF-ASSESSMENT QUESTIONNAIRE

The PCI Council has combined the 2 reference documents which includes **test procedures** and the **guidance** into the single document to help your business complete the Self-Assessment Questionnaire.

Extract from PCI DSS Version 3.2.1 with the extended guidance below:

PCI DSS Requirements	Testing Procedures	Guidance
	3.1.c For a sample of system components that store cardholder data: • Examine files and system records to verify that the data stored does not exceed the requirements defined in the data retention policy • Observe the deletion mechanism to verify data is deleted securely.	Identifying and deleting stored data that has exceeded its specified retention period prevents unnecessary retention of data that is no longer needed. This process may be automated or manual or a combination of both. For example, a programmatic procedure (automatic or manual) to locate and remove data and/or a manual review of data storage areas could be performed. Implementing secure deletion methods ensure that the data cannot be retrieved when it is no longer needed. ***Remember, if you don't need it, don't store it!***
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:* • *There is a business justification and* • *The data is stored securely.* Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	**3.2.a** For issuers and/or companies that support issuing services and store sensitive authentication data, review policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data. **3.2.b** For issuers and/or companies that support issuing services and store sensitive authentication data, examine data stores and system configurations to verify that the sensitive authentication data is secured. **3.2.c** For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization.	Sensitive authentication data consists of full track data, card validation code or value, and PIN data. Storage of sensitive authentication data after authorization is prohibited! This data is very valuable to malicious individuals as it allows them to generate counterfeit payment cards and create fraudulent transactions. Entities that issue payment cards or that perform or support issuing services will often create and control sensitive authentication data as part of the issuing function. It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data ONLY IF they have a legitimate business need to store such data. It should be noted that all PCI DSS requirements apply to issuers, and the only exception for issuers and issuer processors is that sensitive authentication data may be retained if there is a legitimate reason to do so. A legitimate reason is one that is necessary for the performance of the function being provided for the issuer and not one of convenience. Any such data must be stored securely and in accordance with all PCI DSS and specific payment brand requirements. *(Continued on next page)*

Payment Card Industry (PCI) Data Security Standard, v3.2.1 *Page 37*

ANNUAL ASSESSMENT REQUIREMENTS FOR LEVEL 1 & 2 MERCHANTS

- If you are a Level 1 or Level 2 Merchant, your PCI DSS Assessments must be conducted under the supervision of a Qualified Security Assessor (QSA) or one of your own staff members certified as Internal Security Assessor (ISA).
- Qualified Security Assessor (QSA) companies are organisations that have been qualified by the PCI Security Council to have their employees assess compliance to the PCI DSS standard – details of QSA's located in Australia can be found at: QSA Organisations.
- Internal Security Assessors are Merchant's staff that have become qualified by the PCI Council. The Internal Security Assessor (ISA) Program consists of training from the Council to audit or simply improve the organisation's understanding of PCI DSS.
- There are a number of requirements around ISA certification at this link ISA Training Information - including pre-registration of your organisation with the PCI Security Standards Council, expertise requirements for the staff participants, online training and assessment prior to attending the training.
- Penalties from the schemes apply where level 1 or 2 merchants do not report their compliance status.

Note

For Level 1 and 2 Merchants, choosing whether you will appoint a QSA or train your own staff through the ISA program is an important decision and will require time and resources. We recommend that you address these questions early so that you can comply with your annual assessment requirements.

Starting with QSA guidance is recommended.

WHAT IF YOU ARE PCI DSS NON-COMPLIANT?

- Merchants often find that they are non-compliant with PCI DSS after they have completed their annual assessment.
- In addition, a merchant's payment environment can change and just because PCI DSS compliance has been achieved at one point in time, does not mean that the Merchant will always be compliant.
- PCI DSS recognises that Merchants may not be compliant and requires that the merchant develop a remediation plan to fix any areas of non-compliance – your remediation plan should list and prioritise any remediation activities required for PCI validation. This ensures that you are remediating with a risk based approach, dealing with the risks with the greatest impact to your business and customers first.
- The PCI Council has developed the PCI DSS Prioritised Approach and the PCI DSS Prioritised Tool and Instructions
- Input audit results from your completed Self Assessment Questionnaire into the Prioritised Approach Tool to provide an assessment of priority to remediate non-compliant requirements, based on risk and impact. The Prioritised Approach Tool groups the PCI DSS requirements into risk-based 'Milestones'.

Tip

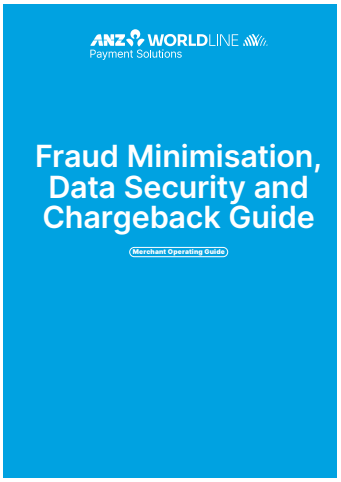
It is important that you are able to demonstrate your commitment to rectify any areas of PCI DSS non-compliance by developing and implementing a remediation plan that is acceptable to ANZ Worldline Payment Solutions. This can assist in minimising any card scheme fines due to non-compliance.

Target compliance dates must be included.

PCI DSS EDUCATION AND REFERENCES

The following information may be helpful in further understanding your PCI DSS obligations:

PCI SECURITY STANDARDS COUNCIL	• PCI Council Website • PCI DSS (Full Requirements) v3.2.1 • PCI DSS Quick Reference Guide • PCI DSS Prioritised Approach
PCI TRAINING	• PCI DSS Awareness Training Online • Internal Security Assessor (ISA) Training and Certification • Guidelines for Securing Cardholder Data for your Website
FRAUD MINIMISATION	• Fraud Minimisation, Data Security and Chargeback Guide



ANZ WORLDLINE
Payment Solutions

On 15 December 2020 Australia and New Zealand Banking Group Limited announced that it was setting up a partnership with Worldline SA to provide leading payments technology and merchant services in Australia.

The joint venture formed by ANZ and Worldline SA is known as ANZ Worldline Payment Solutions and aims to give merchant customers in Australia access to Worldline SA's market-leading payments technology and future innovations. ANZ Worldline Payment Solutions commenced operations on the 1st April, 2022.

Pairing Worldline SA's global leadership with ANZ's local expertise and existing relationships, ANZ Worldline Payment Solutions aims to offer fast, reliable and secure point-of-sale and online payment acceptance for merchants and their customers in Australia, and strives to deliver a suite of competitive products and an innovative roadmap to help your business grow.

ANZ Worldline Payment Solutions means Worldline Australia Pty Ltd ACN 645 073 034 ("Worldline"), a provider of merchant solutions. Worldline is not an authorised deposit taking institution (ADI) and entry into any agreement with Worldline is neither a deposit nor liability of Australia and New Zealand Banking Group Limited ACN 005 357 522 ("ANZ") or any of its related bodies corporate (together "ANZ Group"). Neither ANZ nor any other member of the ANZ Group stands behind or guarantees Worldline.

anzworldline.com.au

Item No. AW2040 09.2022 WZ123220 200.0138.02_AUS_EN/09.2022