ITSMA AY 2020/2021 OCT SEMESTER GROUP RESEARCH REPORT

Written and Collated By:

Siti Aisyah | 1902609E
Izzah Nia Sara | 1900643F
Tan Yi Ching | 1902249J
Ye TingKai | 1901102B
Zachary Phoon Jun Ze | 1900353B

Diploma & Class:

Diploma in Cybersecurity and Digital Forensics
P02

Declaration of Plagiarism:

We understand that plagiarism is the blatant copying of information, codes or any other material (including ideas, music, pictures etc) and passing it off as our own original work. We undertake to ensure that all information in all the assessments and assignments that we undertake will be original.

We shall not include information without giving proper citations and reference lists. All pictures (if any) will be either original or from a free source.

We realise the serious nature of plagiarism and know that we will fail a subject, and possibly all subjects this semester if we plagiarise.

Signatures:

Siti Aisyah | 1902609E	
Izzah Nia Sara | 1900643F	Sara
Tan Yi Ching | 1902249J	yiching
Ye TingKai | 1901102B	Ye
Zachary Phoon Jun Ze | 1900353B	

Table of Contents

1 Introduction to Payment Card Industry

The Payment Card Industry Data Security Standard (PCI DSS) is required by the contract for those handling cardholder for both start-ups and global enterprises. Businesses must always be compliant and compliance must be validated annually.
Generally mandatory by credit card companies and discussed on credit card network agreements.

The PCI Security Standard Council (SSC) is responsible for the development of the standards for PCI compliance and to help secure and protect the entire payment card ecosystem. Merchants and Service Providers processing credit/debit card payment transactions are to comply to these standards.

Payment Card Industry (PCI) compliance is mandated by credit card companies to ensure the security of credit card transactions in the payment industry. PCI compliance refers to the technical and operational standards that businesses must follow to secure and protect credit card data provided by cardholders and transmitted through card processing transactions.

2 Introduction of PCI’s Standards / Regulations

The Payment Card Industry Security Standards Council (PCI SSC) was launched on 7 September 2006 by five major payment brands, American Express, Discover Financial Services, JCB International, MasterCard and Visa Inc, with the goal of managing a body of security standards known as **Payment Card Industry Data Security Standard (PCI DSS)**.

The PCI DSS consists of twelve main requirements including multiple sub-requirements which contain numerous information security standards and directives for organisations that handed credit cards.

Businesses may measure their own payment card security policies, procedures and guidelines against the PCI DSS to help develop a security process that incorporates preventive measures, detection and appropriate reaction to security incidents. *For more information regarding the twelve requirements of the PCI DSS, refer to* ***section 4.3*** *of this report documentation.*

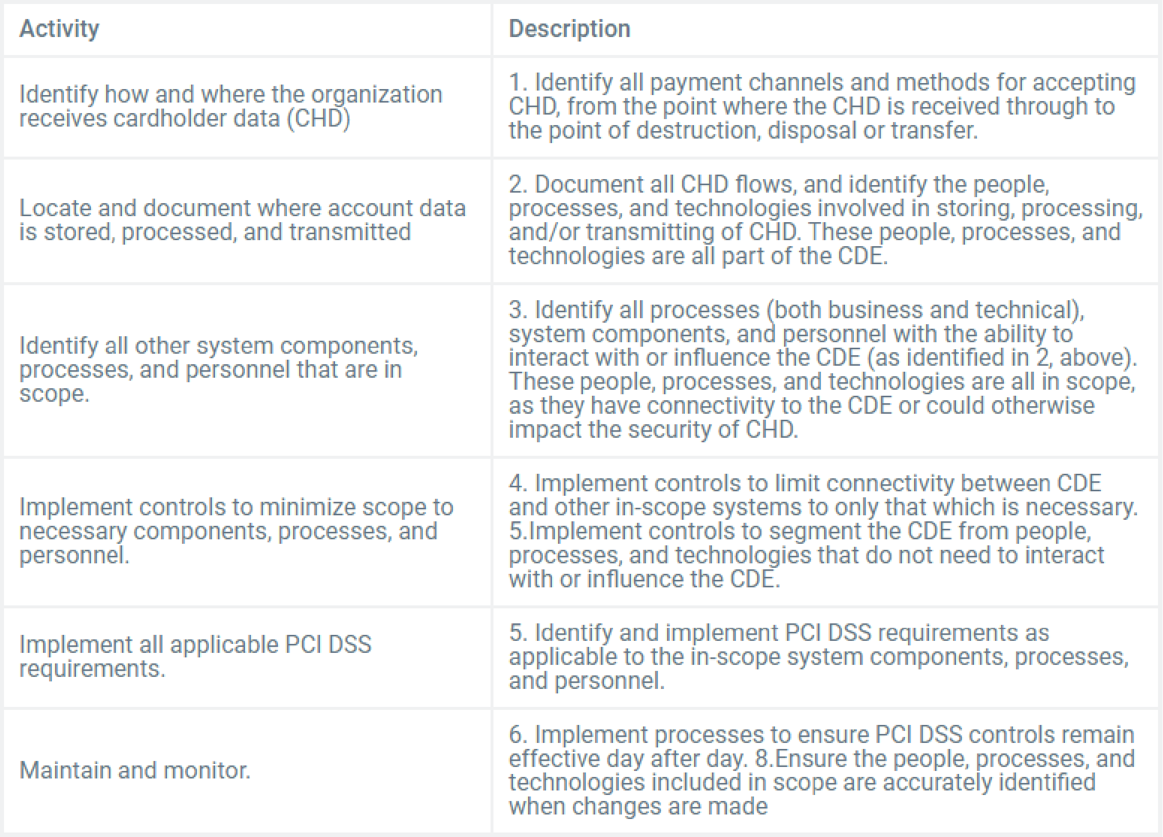
There are 12 requirements of PCI DSS, operational and technical, and the main focus of these rules are always to protect cardholder data.PCI DSS applies to all entities involved in the payment card process including merchants, processors, issuers and service providers.

2.1 Scope of Standard

PCI Scope is part of your environment that must meet the 12 requirements stated within the PCI Data Security Standards (DSS). The scope is the combination of people, processes and technologies that interact with or could otherwise impact the security of the cardholder data.

Internal systems and networks that are related to storing , processing or transmitting payment card data are considered to be within the scope for the PCI Compliance. While systems components that store or process or transmit payment card information are considered as part of the cardholder data environment (CDE).

All business partners, entities providing remote support service, and other services providers ,such as service providers and other third parties, connected to cardholder data environments (CDE) or may have risk of potentially compromising an entity’s CDE are also considered in PCI DSS scope. If an entity outsources in-scope functions or facilities to a third party, or utilizes a third-party service that impacts how it meets PCI DSS requirements, the entity will need to work with the third party to ensure the applicable aspects of the service are included in scope for PCI DSS.
PCI SCOPING EXERCISE:



Activity	Description
Identify how and where the organization receives cardholder data (CHD)	1. Identify all payment channels and methods for accepting CHD, from the point where the CHD is received through to the point of destruction, disposal or transfer.
Locate and document where account data is stored, processed, and transmitted	2. Document all CHD flows, and identify the people, processes, and technologies involved in storing, processing, and/or transmitting of CHD. These people, processes, and technologies are all part of the CDE.
Identify all other system components, processes, and personnel that are in scope.	3. Identify all processes (both business and technical), system components, and personnel with the ability to interact with or influence the CDE (as identified in 2, above). These people, processes, and technologies are all in scope, as they have connectivity to the CDE or could otherwise impact the security of CHD.
Implement controls to minimize scope to necessary components, processes, and personnel.	4. Implement controls to limit connectivity between CDE and other in-scope systems to only that which is necessary. 5.Implement controls to segment the CDE from people, processes, and technologies that do not need to interact with or influence the CDE.
Implement all applicable PCI DSS requirements.	5. Identify and implement PCI DSS requirements as applicable to the in-scope system components, processes, and personnel.
Maintain and monitor.	6. Implement processes to ensure PCI DSS controls remain effective day after day. 8.Ensure the people, processes, and technologies included in scope are accurately identified when changes are made

- System Components included under network devices, servers, computing devices and applications does not mean that all PCI DSS requirements apply to it. The applicable PCI DSS requirements depend on the function and/or location of the system components.
  The information supplement explains how system components can be categorized using three system category types and how scope applies to them. These categories are hierarchical.
- **CDE Systems**
  - These are in scope of PCI DSS.
  - These must be evaluated against all PCI DSS requirements to determine the applicability of each requirement.

- **Connected-to and/or Security-Impacting Systems**
  - Are in scope for PCI DSS. Even where a connection is limited to specific ports or services on specific systems, those systems are included in scope to verify that applicable security controls are in place.
  - Must be evaluated against PCI DSS requirements to determine the applicability of each requirement.
  - Must not provide an access path between CDE (cardholder data environment) systems and out-of-scope systems.

- **Out-of-scope Systems**
    - Are not in scope of PCI DSS;therefore, PCI DSS controls are not required,
    - Have no access to any CDE (cardholder data environment) systems; if there is any access, then systems are in scope.
    - Are considered untrusted (or ‘public’)- There is no assurance they have been properly secured.
    - If on the same network / subnet / VLANS or otherwise connectivity to, a connected to or security impacting systems, controls must be in place to prevent the out-of-scope systems from gaining access to the CDE via in-scope systems, These controls must be validated at least annually.
    - Not in scope but could still represent a risk to the CDE if not secured.

Ways to reduce the PCI DSS SCOPE cost for smaller managements/companies.

- Do not store information when not required to.
    - Do not store cardholder data unless it is absolutely necessary as running cardholder data discovery tools will find PANs (Personal Area Network) , processes and flows that some did not know even existed.

- Network Segmentation.
    - It is a method of separating systems that store, process or transmit cardholder data from those that do not. The adequacy of a specific implementation of network segmentation is highly variable and dependent upon several factors such as network configuration, the techniques deployed and other controls that may be implemented.
    - This reduces the scope and cost of the PCI DSS assessment, cost and difficulty of implementing and maintaining PCI DSS controls, as well as the risk to an organization by consolidating cardholder data in fewer, more controlled locations.
    - Segmentation may help to reduce the number of exposures areas to the cardholder data environment (CDE), but it isn't anyway 100% protected as it is not a replacement for a holistic approach to securing an organization’s infrastructure.

- Tokenization.
    - It is the process of converting sensitive data into non-sensitive data. It completely replaces the PAN in your environment by storing tokens in the database which is not considered as cardholder data. Once data is tokenized, it will be able to flow through the environment without bringing ant devices that store, process or transmit the token into scope of PCI compliance requirements.

- Using a PCI-listed P2PE Solution.
    - This leverages the use of a secure Point-of-interaction (POI) device to encrypt cardholder data. The data can only be decrypted by the solution provider and at no point does either the merchant or payment solution have access to unencrypted account data be it transit or other times. These entities are eligible

to complete a P2PE SAQ which provides the maximum scope reduction available.

- Outsourcing to a third-party service provider.
    - When done correctly, outsourcing certain aspects of the CDE (cardholder data environment) or cardholder data flow can reduce the scope and overall PCI burden for an entity. Examples will be Managed Firewall Service, Log Monitoring and Management, Server Hosting Facilities and Payment Solutions offered up as Software as a Service.
      When an entity outsources in-scope functions or facilities to a third party or utilizes a third-party service that impacts how it meets PCI DSS requirements, the entity will need to work with the third party to ensure the applicable aspects of the service are included in scope for PCI DSS—either for the entity or the service provider. It is also important for both parties to clearly understand which PCI DSS requirements are being provided by the service provider and which are the responsibility of the entity using the service.

2.2 Who Does It Apply To

PCI's Data Security Standards (PCI DSS) applies to any and all merchants or service providers that are involved in handling, storing, processing and/or transmitting credit card information and data. Following the PCI DSS' standards/regulations, it is the payment brands, acquirers and merchants who are the ones responsible for enforcing their compliance to the PCI DSS than the PCI DSS itself.

2.2.1 For Merchants,

Merchants who outsource the handling, storing and transmitting of credit card data to a service provider/third-party, they are **required** to make sure that their provider has been **validated** to be PCI DSS Compliant as well as ensuring that the credit card and/or account data is properly protected by the service provider/third-party as required by the PCI DSS requirements.

The PCI Security Standards Council has provided compliance validation tools in the form of questionnaires called Self Assessment Questionnaires (SAQs). The questionnaires were devised to accommodate different business types, ranging from restaurants ro ecommerce, and different business processing methods for both merchants who do or do not handle nor touch credit card information and data. However, for merchants who are processing millions of transactions per year, are required to additionally have an onsite audit conducted by a Qualified Security Assessor (QSA). *Please refer to section 4.2 to know more about QSA).*

2.2.2 For Service Providers/Third-Parties,

Any business that processes, handles, stores or transmits credit card data on behalf of a merchant is required to be compliant to the PCI DSS and ensuring that they are properly protecting the credit card and/or account data as per the PCI DSS requirements.. *Achieving the Level 1 compliance requires onsite audit by a Qualified Security Assessor. Please refer to section 4.2 to know more about QSA.*

Not complying to the PCI DSS can result in fines or loss of permission to accept credit card payments or both. The penalties depend on the overall percentage of clients, the amount of transactions made, the level of PCI-DSS that the company was assessed to be on, and the length of time the company has been non-compliant.

Some penalties include:

- **Loss of permission to accept credit card payment** - damages company’s reputation and gives a disadvantage in the financial revenue and market share,
- **Fines**, of up to four million Singapore dollars,
- **Mandatory forensic examination** - merchants/organisations are to undergo one when a suspected data breach has been identified,
- **Liability for fraud charges** - lawsuits, insurance claims, canceled accounts, payment card issuer and/or government fines. This penalty is liable following after a security breach as it is the organisation’s responsibility to keep customer’s sensitive card information secure.

To regain permission to process credit card payment and handle them, the company will need to undergo a PCI reassessment by an external Quality Security Assessor (QSA).

For more information on the requirements of PCI DSS and its compliances, please refer to section 4 of this report documentation.

2.3 What Kind of Information Does It Apply To

The PCI DSS aims to protect cardholder data and sensitive authentication data wherever it is processed, stored or transmitted. Any entities involved with payment card processing must never store sensitive authentication data after authorization. The following data are included below.

- Chip (Read Application Data)
- Primary Account Number (PAN)
- Cardholder Name
- Expiration Date
- CID(Amex)/CVC/CAV2/CVC2/CVV2
- Magnetic stripe or "Full track Data"

2.4 Enforcement of Standards

The PCI security standards are enforced by the council founders, namely:

- American Express
- Discover Financial Services
- JCB International
- MasterCard Worldwide
- Visa

Although the PCI Security Standards Council sets the standard, each payment card brand has its respective compliance programme. The standard is designed to enforce security controls affecting cardholder data environments to reduce fraud and cyber risks.

2.5 Background of Different Levels of Merchants

The PCI DSS merchant levels are different rankings of transactions made by merchants per year. These rankings are classified into four levels. Merchants levels are used to determine risk from fraud and verify the suitable level of security for their businesses. Merchant levels also determine the amount of assessment and security verification needed for the merchant to pass the PCI DSS assessment.

The four merchant levels of PCI DSS include:
Level 1 - Merchants that process **over 6 million** transactions yearly, **across all channels** OR any merchant that has **experienced data breach**
Level 2 - Merchants that process **between 1-6 million** transactions annually, **across all channels**
Level 3 - Merchants that process **between 20,000 to 1 million online** transactions every year
Level 4 - Merchants that process **fewer than 20,000 online** transactions annually OR any merchants processing **up to 1 million regular** transactions every year

3 History / Previous Versions of PCI

3.1 Differences between PCI Versions

PCI DSS Version 1.0 to 1.1 minor revision of topics and more clarity. Special consideration to ensure security of other entities that connect to internal networks; ensure they are PCI DSS compliant and have a way to segregate them. It also includes clarification that service providers comply with security requirements, and code to be independently reviewed for vulnerabilities. The version added supplementary use of other types of anti-malware.

PCI DSS Version 1.1 to 1.2 changed the title of the document and made corrections to terminology of the requirements accordingly. The version clarified mainly requirements and testing procedures of WiFi related technologies, data encryption and verification of sub-requirement standards for testing procedures and in-house application codes. It also defined the data types and procedures for security implementation. Further clarified OWASP requirements. The document now also includes methods of network segmentation and network encryption along with device configurations to further tighten security. The document also tightened requirements for in-house system code and logging processes.

PCI DSS Version 1.2 to 1.2.1 made minor grammar corrections and proofreading of the document layout to create consistency and more clarity.

PCI DSS Version 1.2.1 to 2.0 made significant clarifications of terminology used to various parts of requirements and testing procedures. It also added examples of a secure system or device for organisation reference. The clarifications mainly include access control, account management, network security and data storage policies. The version also updated requirements to align with testing procedures. The procedures and requirements were also updated to be more specific to dispel confusion of operating methods.

PCI DSS Version 2.0 to 3.0 made significant clarifications to the intent of the requirements and clarified operating procedures in detail. The new version clarified the management of accounts and security controls. It also split several sub-requirements to focus on necessary services, protocols and ports to secure them.
New requirements were made to; maintain inventory of system components to support configuration standards, to evaluate evolving malware threats for any systems not considered to be commonly affected, ensure that anti-virus solutions are actively running and cannot be disabled to altered unless authorized by management, adopt better coding practices to protect against broken authentication and session management, define access control for each role of users, have service providers with remote access to customer premises use unique

authentication credentials for each customer, have mechanisms for authentication be linked to an individual account and ensure only intended user access, have access control for physical access, implement a methodology for penetration testing, implement a process to respond to any alerts generated by change-detection mechanism, perform penetration testing on CDE to verify segmentation methods are effective, maintain information about which PCI DSS requirements are managed by each service providers and which are managed by entity, service providers are required to provide written acknowledgement to their customers.

PCI DSS Version 3.0 to 3.1 made some clarifications to the words used and language for consistency in various sections that are mainly for testing procedures, system files, techniques used for testing, account policies, sensitive data storage. It removed SSL as an example of secure technology and updated testing procedures to recognize all versions of SSL as examples of weak encryption. Set a deadline of 30 June 2016 for migration of updated TLS security protocol.

PCI DSS Version 3.1 to 3.2 extended the original deadline of migrating to an updated TLS security protocol from 30 June 2016 to 1 July 2018. Changed the two-factor authentication requirement to multi-factor. The requirement no longer applies to just employees working remotely, but anyone with non-console admin access to the cardholder data environment (CDE). It also clarifies that primary account numbers must be masked when displayed. New requirements are also made for service providers to do routine testing of systems and management processes.

PCI DSS Version 3.2 to 3.2.1 removed the various notes in each subsection and testing procedure for SSL/ early TLS migration efforts as the migration date has passed. Removed MFA from the compensating control example, as MFA is now required for all non-console administrative access. Requirements A2.1 – A2.3 are also updated to focus only on the allowance for POS POIs that are not susceptible to known exploits and their service provider termination points to continue using SSL/early TLS.

3.2 Changes between Versions (The Cause)

PCI DSS Version 1 to 1.1 made specified Clarification and minor revisions of standards.

PCI DSS Version 1.1 to 1.2 made enhanced clarity, improved flexibility, and addressed evolving risks and threats. One of the Data Breaches that caused this change was the Hannaford Data Breach of the Maine-based Hannaford Brothers grocery store chain announced that 4.2 million customer card transactions had been compromised by the hackers. More than 1800 credit card numbers were immediately used for fraudulent transactions. This caused the bank and credit cards to reissue the credit cards. Retailer claimed that the system was PCI compliant and had passed a PCI assessment the week before it was discovered. Hence PCI Security Council has decided that due to this case that the PCI requirements are found to be wanting light of the report hence required to be tightened.

PCI DSS Version 1.2 to 1.2.1 made minor corrections designated to create more clarity and consistency among the standards and supporting documents. No specified cause to trigger the swap.

PCI DSS Version 1.2.1 to 2.0 made additional clarifications, guidance and being more restrictive on the requirements. These changes were made to keep up to those days standard and making it more restrictive as The Verizon PCI DSS 2010 Compliance Report stated that only 22% of organizations were validated as compliant while most of the other organizations on average had 81 % of the test procedures in the PCI DSS Stage. The companies in the 22% were mainly the same companies that had been compliant in the past.

PCI DSS Version 2.0 to 3.0 change could have been due to Target Breach in 2014. The Target data breach stole track data, data contained in magnetic tape on the back of credit/debit cards, from the point of sales (POS) equipment using a strain of malware to capture the card credentials to a compromised central server within Targets internal Infrastructure.The stolen data was double encrypted was transmitted to the attacker, outside of the internal network, to obfuscate the details from any data leakage protection programmes. The analysis of the malware indicated that an admin grade credential was used in the attack. The PCI DSS covered the changing of default username and password for systems within the scope of the PCI DSS. The credentials were obtained via memory scraping which allowed data held in the RAM of the equipment to be analyzed. Requirements 4 in PCI DSS v2.0 covered the strong use of encryption from swiping the card and transmission however the device used when swiping the card was the weak link and caused the data to be stored in the memory in plain text. Requirement 6.5 in the PCI DSS also covered the application development and mentions memory scraping. Hence these specifications weren't specific enough which resulted in these data breaches.

3.3 Future Releases & Their Purposes

3.3.4 Why are these future releases planned? What are so important of them?

Currently, PCI DSS v4.0 is in development subject to completion by mid-2021. Since industrial feedback is more involved in the development as compared to past revisions, this timeframe may be extended. This allows for stakeholders to give more input in shaping the new revision. Once it is released, an 18-month transition period will be provided to update from the latest PCI DSS (v3.2.1) to PCI DSS v4.0

Although the 12 PCI DSS requirements will not drastically change with the upcoming version, the revised version will focus more on security and flexibility, as well as to accommodate changes in technology, risk mitigation techniques and threat landscape. The key goals for PCI DSS v4.0 is as follows:

- **Ensure the standard continues to meet the security needs of the payments industry**
  PCI DSS v4.0 hopes to make the scoping guidance more integral by providing more details for validation and ensuring that organizations and service providers follow their scope through additional requirements. Enhanced protection of cardholder data transmission and anti-phishing & social engineering treatment is also in discussion as they have been highlighted as big attack vectors in recent years. An update on risk assessment and authentication enhancement controls is expected due to the growing concern of its vagueness. Lastly, cloud technology may be applied in the standard with added requirements for shared hosting providers.
- **Add flexibility and support additional methodologies to achieve security**
  One of the main concerns with the PCI DSS is companies having their own security methods that may not align with traditional requirement fulfillments. With this in mind, the council is introducing a Customized Approach as a new security control validation. This allows organizations to present new benefits and alternate considerations.

SECURITY CONTROL	ENTITY	ASSESSOR
Defined Approach	● Implements and operates controls that meet the PCI DSS requirement	● Plans and conducts the assessment ● Follows PCI DSS testing procedures to access implemented controls ● Documents results of testing in the ROC
Customized Approach	● Implement controls that meet the intent of PCI DSS requirement ● Provide documentation describing customized implementation ○ Who, what, where, when, and how of the controls ○ Evidence proving controls meet stated intent ○ Evidence of how controls are maintained, and effectiveness is assured	● Plans and conducts the assessment ● Reviews information provided by entity ● Derives testing procedure based on information provided ● Documents details of testing procedures and results of testing in the ROC

Although this offers more validation flexibility, it also increases costs for assessment phases due to thorough documentation, testing and risk analysis effort needed for QSA presentation. Hence, this method should be used by organizations with mature security with robust assessment processes in place.

- **Promote security as a continuous process**
  Because PCI Data Security Standard is more of a security requirement guide rather than a law to abide by, some businesses may comply only during the assessment phases. Through PCI DSS v4.0, it aims to encourage security process continuity in organizations and increase the need to strengthen and enhance security controls.

- **Enhance validation methods and procedures**
  Although not much updates were given in the validation method procedure especially with the introduction of the Customized Approach, a concern was on how the previous versions did not accommodate for newer technologies. Some areas that may be focused on for this aspect is the NIST MFA/password guidance and increased frequency of testing of critical controls.

3.3.5 Why are they required to be released? Is there a problem in the current release?

The reason for the new release (i.e. PCI DSS version 4.0) is because many of the PCI security controls are over 10 years old and not many major changes have been occurring since 2015. This meant that the security, implementations, controls and such are now behind in the current technology and threats. The methods that attackers take to compromise and steal information and data stored in servers, or when the data is in transit, are being more sophisticated over the years. If the security controls are not up-to-date, it is vulnerable to attacks.

There is no problem in the current 3.2.1 version, but as explained in 3.3.4, the new revised version 4.0 will cover over the areas of security and flexibility, as well as accommodating to the changes in the current changes in technology and sophisticated threat landscape that the current version is unable to cover/stabilize. *Refer to section **3.3.4** to see the changes that version 4.0 will bring in the future.*

The release of PCI DSS version 4.0 is to focus on improving the security of cardholder data and enable solutions that disparage credit card data and remove the spots that give attackers chances to steal them.

PCI DSS version 3.2.1 has a series of security objectives with specific stringent requirements that determines how companies must achieve those requirements. However, this does not give the company any flexibility to improvise those security objectives into their own system environment. But, for the new PCI DSS version 4.0, not only does it keep the same stringent requirements from version 3.2.1, it replaces the compensating controls with the ability to customise the implementation, allowing companies to design their own security controls with other entities while keeping the same method for compliance.

Version 4.0 will set the bar higher and build on the assurance of the previous 3.2.1 version.

4 Sections of PCI’s Standards & Regulations

In this section of the report, documentation of the PCI DSS and their regulations will be documented here. The sub-sections includes the different compliance levels regarding the PCI DSS and the method of validating the organisation’s compliance, the twelve requirements under PCI DSS, and doubts on the trust of security that the requirements in the PCI DSS gives.

4.1 PCI DSS Compliance Levels

The criterion of the respective levels are as follows:

American Express:

Level	Definition	Validation Documentation
1	2.5 million transactions or more per year OR Any merchant that has had data breach OR Any merchant that American Express has deemed a Level 1 merchant	● Annual Onsite Security Assessment Report ● Quarterly Network Scan
2	50,000 to 2.5 million transactions per year	● Quarterly Network Scan ● Annual Self Assessment
3	Less than 50,000 transactions per year	● Quarterly Network Scan ● Annual Self Assessment

Discover Financial Services:

Level	Definition	Validation Documentation
1	6 million or more transactions per year OR Any merchant that Discover has deemed a Level 1 merchant OR All merchants required by another payment brand/acquirer to validate & report their compliance as a Level 1 merchant	● Onsite assessment using PCI DSS requirements and Security Assessment Procedures ● Quarterly external network vulnerability scans

2	Between 1-6 million transactions per year	● Self-assessment using applicable PCI DSS Self-Assessment Questionnaire (SAQ) ● Quarterly external network vulnerability scans
3	All other merchants	● Self-assessment using applicable SAQ ● Quarterly external network vulnerability scans

JCB International:
(JCB International does not classify merchants according to the official levels. As such, this is an estimation of the different merchant levels.)

Level	Definition	Validation Documentation
“1”	1 million or more transactions per year	● Quarterly Network Security Scan ● Annual Onsite Review
“2”	Less than 1 million transactions per year	● Annual Self-Assessment ● Quarterly Network Security Scan
“3”	Any other merchants	● Quarterly Network Security Scan ● Annual Onsite Review

Mastercard Worldwide:

Level	Definition	Validation Documentation
1	Any merchant that has suffered any data breach OR More than 6 million transactions (Mastercard and Maestro combined) annually OR Any merchant that meets the Level 1 criteria of Visa OR Any merchant deemed as Level 1	● Annual Onsite Assessment ● Quarterly Network Scan conducted by an Approved Scanning Vendor (ASV)

	merchant	
2	More than 1 million but less than OR equal to 6 million transactions (Mastercard and Maestro combined) annually OR Any merchant that meets the Level 2 criteria of Visa	● Annual Self-Assessment ● Onsite Assessment at Merchant Discretion ● Quarterly Network Scan by an ASV
3	More than 20,000 transactions (Mastercard and Maestro combined) annually BUT less than OR equal to 1 million e-commerce transactions (Mastercard and Maestro combined) annually OR Any merchant that meets Level 3 criteria of Visa	● Annual Self-Assessment ● Quarterly Network Scan by an ASV
4	All other merchants	● Annual Self-Assessment ● Quarterly Network Scan by an ASV

Visa Inc.:

Level	Definition	Validation Documentation
1	Over 6 million transactions annually OR Global merchants deemed as Level 1 merchants by any Visa region	● Annual Report on Compliance (ROC) by a Qualified Security Assessor (QSA) ● Annual Internal Auditor if signed by an officer of the company ● Annual Attestation of Compliance (AOC) Form ● Quarterly Network Scan by an ASV
2	1-6 million transactions annually	● Annual SAQ ● Annual AOC Form ● Quarterly Network Scan by an ASV
3	20,000 to 1 million e-commerce transactions annually	● Annual SAQ ● Annual AOC Form ● Quarterly Network Scan by an ASV

4	Less than 20,000 e-commerce transactions annually AND All other merchants processing up to 1 million transactions annually	● Annual SAQ ● Annual AOC Form ● Quarterly Network Scan by an ASV

4.2 Method of Validation of Compliance

PCI DSS requirements, security assessment and corresponding testing procedures jointly act as a security assessment tool which is used for compliance validation. This deals with the assessment and verification of the correct implementation of security controls, procedures and policies as per the requirements of PCI DSS. There are many tools and resources made available from PCI SSC.
Such tools and resources are:

- **Self Assessment Questionnaires (SAQ):**
  SAQ is a set of questions that banks require their service providers and merchants to fill and submit on a yearly basis. The SAQ is answered on the basis of the PCI DSS self-assessment that was carried out internally. The SAQ questions have to be answered with yes or no option. If a question has the answer “NO”, then the organisation must provide its respective implementation in future.
  SAQ normally consists of two components:
    - A Set of question corresponding to the PCI Data Security Standard requirements designed for service providers and merchants
    - An Attestation of Compliance or Certification that you are eligible to perform and have performed the appropriate self-assessment.

- **Qualified Security Assessors (QSAs):**
    - **Becoming a QSA:**
        - **The applicant must be with a firm for qualification in the program.**
        - **Provide documentation adhering to the Qualification Requirements for Qualified Security Assessors (QSA)v 3.1 as of 8 February 2021.**
            - The security company must first submit the required documentation, including certifications, business license, insurance certificates and the registration fee, which is credited against the initial enrollment fee if the firm becomes qualified. The Council will review these materials, and will communicate with the security company to address any issues or lack of information. When the materials are complete, the prospective Qualified Security Assessor Company (QSAC) will be invited to schedule training for its employees.
        - **Qualify individual employees, through training and testing, to perform the assessment.**

            - All individuals who will be involved in assessing security for the company's clients must undergo and pass the Council's QSA training course and receive official certification. A Council representative will schedule training for the prospective QSA's employees, and the company will be notified whether they pass or fail the test at the end of the course.
        - **Execute an agreement with the PCI Security Standards Council governing performance.**
            - If the PCI Security Standards Council has received the enrollment fee balance, the security company will receive a letter of acceptance from the Council and a certificate of qualification will be awarded to each of its employees who have passed the training course.
            - The new QSA firm will be listed on the website of the Council, the staff will be added to the certified staff database of the Council, and the company can now carry out audits for its customers.
            - The PCI Security Standards Council encourages payment brands and other entities to submit audit Quality Feedback Forms, which will be evaluated by the Technical Working Group of the Council, to ensure that security audits are carried out at the highest levels of quality and professionalism.

    - QSA is used for autonomous or self-governing security organizations that are certified by PCI SSC to validate and endorse the implementation and compliance of the PCI DSS requirements within organization workflow. This certification only designates that a QSA hash addressed all the respective requirements which are compulsory to carry out PCI DSS assessments. PCI SSC maintains a very detailed program for organizations to certify for QSA certification, which is valid for one year, and the organizations have to annually renew the QSA certification by addressing the requalification requirements.
      The requirements for QSA certification not only involve the company itself but also its employees. The employees of the QSA organization are referred to as QSA employees. PCI SSC enlists the QSAs on their website, which is updated on a regular basis.

- **Internal Security Assessors (ISA):**
  ISA is targeted for internal employees of an organization who receives a certification from PCI SSC for internal use in the company. The main aim of the Certification is to assist Level 2 Merchants for the compliance validation assessment. It enables an employee to carry out an internal assessment of their organization and suggest/commend security controls and solutions related to PCI DSS compliance.

- **Report Of Compliance (ROC):**

> ROC form is used for the verification of the merchant/client who was in the audit phase and has achieved compliance with PCI DSS. ROC affirms that the organization has developed and correctly implemented the procedures and policies for the protection of card-based transactions and protects cardholders against fraudulent charges and others.

It is mandatory for every level, excluding level 1, to complete a self-assessment questionnaire, as well as a quarterly external vulnerability scan using an Approved Scanning Vendor (ASV). Level 1 merchants are obligated to have onsite data security assessments.

To comply with the PCI DSS, Level 1 merchants are required to submit an Annual Report on Compliance (ROC) by a Qualified Security Assessor (QSA). This is also known as a Level 1 onsite assessment, or internal auditor if endorsed by an officer of the company. A quarterly network scan by ASV is also mandatory as it is an Attestation of Compliance form.

Some common compliance requirements for Levels 2,3 and 4 merchants include a submission of an Annual Self-Assessment Questionnaire (SAQ), a quarterly network scan by an ASV and an Attestation of Compliance form. However, merchants of Level 4 may not be subjected to all of the requirements stated above.

4.3 PCI DSS Requirements

The PCI DSS is a set of minimum requirements for protecting account data, which may be enhanced by additional controls and practices to further mitigate risks. It is important to note that the PCI DSS **does not oversee** local or regional laws, government regulations or other legal requirements.

PCI DSS requirements are considered **best practices for data security** and businesses that handle credit card/account data are **expected** to implement those security requirements into their system environment(s) to the latest update.

It is composed of twelve specific requirements that are organised into six logically related groups called ‘control objectives’ which comprises the following groups, which could be seen in figure 2 below. *For more information on the control objectives, please refer to* ***section 4.3.1.***

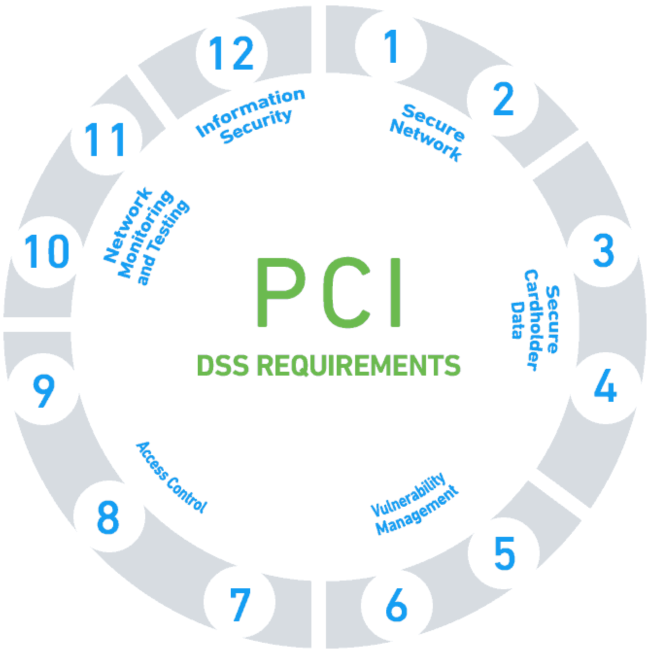


Fig 1. An image of the PCI DSS specified requirements

Although each version of PCI DSS has divided these six control objective requirements into a number of sub-requirements differently, the twelve main requirements have not been modified or changed since the inception of the standard. Each of the requirements are further broken down into multiple standards that helps to provide comprehensive details to improve your security systems and methods. By following the standards, you can mitigate risks to your security systems and protect cardholder information and data. *For more information on the twelve requirements, please refer to **section 4.3.2**.*

4.3.1 PCI DSS 6 Control Objectives

To be in compliance with the current PCI DSS requirements, businesses are required to implement controls that are focused on attaining the 12 requirements. Below is the list that identifies the six control objectives and the twelve respective related requirements;

(1) 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

(2) Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

(3) Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update antivirus software or programs
6. Develop and maintain secure systems and applications

(4) Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data

(5) Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

(6) Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel

4.3.2 PCI DSS 12 Requirements

Control Objective 1: Build and Maintain a Secure Network and Systems

The first control objective, build and maintain a secure network and systems, consists of the two requirements (numbered 1 & 2) as listed below. The two requirements under this objective cover over the data center and the network security.

It details how a firewall should be implemented, maintained and managed, and the merchant/vendor's security configurations should be.

Requirement 1: Install & maintain a firewall configuration to protect cardholder data

Firewalls are devices that control traffic in the network and/or computer systems, allowing and denying traffic between a system's internal network (internal) and untrusted external network (public), as well as traffic into and out of sensitive areas within an entity's trusted network (internal). It examines and blocks any traffic packets that do not meet the specified security criteria rules configured in itself.

In this requirement, it is required that all systems **must** be protected from unauthorised access from untrusted networks, especially for public networks, regardless of the method of entry. Some examples of the different methods of entry are: Internet e-commerce, business-to-business connections, employee email access, wireless networks and more.

On the other hand, other system components may provide firewall functionality, so long as they meet the minimum requirements for firewalls as defined in this **Requirement 1** and that the devices are included within the scope and assessment in this requirement.

Following this requirement, some steps that the company can take to be compliant are listed below. Firewalls are an important protection mechanism for any organisation’s network, no matter how big or small they are. Building and maintaining a secure network and systems with the proper firewall practices should be one of the priorities.

1. Implement a firewall that can **segment** the network into **three main security areas**:
    a. Allow of Internet access limited to the DMZ (i.e. communications to and from public to DMZ)
    b. Organisation’s internal network, where it must be secured
        i. All devices that store or process sensitive data in the internal network can only communicate with the **DMZ or other secure internal networks**, and **NEVER** communicate with the **public network**
    c. DMZ, where all devices that communicate between the Internet and the internal network are located.
        i. Some examples are Mail servers, Web servers, FTP servers and the above mentioned practice (i.e. organisation’s internal network)

Additionally, to make it more convenient to keep your environment secure, there should always be a base security configurations for your firewalls as it is the normal that the firewalls will have additional segments and changes made.

2. To keep a base security configurations, it is advisable for organisations to document down the following and constantly develop them:
    a. The configuration of each firewall parameters that verify PCI DSS compliance
    b. The organisation’s network and data flow diagram, and constantly update the documentation per every change made
    c. The network control changes process, where any changes made on the network must go through a process that controls and authorises the change
    d. The rule set review process. It is important to revise the rules and verify that all configurations of the device is part of the scope, and all changes on the firewall were made through the change control procedure verified via the network control change process
    e. The network policy that guarantees compliance with all principles on which PCI DSS is based on to maintain a secure network

Refer below for more specific details of each sub-requirements

1.1 Establish & implement firewall and router configuration standards that include the following:

1.1.1	**Process of approving and testing all network connections as well as changes made to the firewall and router configurations.**
	It is important that the network connections are tested and approved to be secured and configured according to site policy. Firewall and routers are the key components to keeping control over the entry and exit in and out of the network. If those points were not secured, it give the advantage to attackers to successfully hack into the network and steal sensitive data, violating the organisation’s compliancy.
1.1.2	**Current network diagram that identifies all connections between cardholder data environment and other networks, including any wireless networks**

1.1.3	**Current diagram that shows all cardholder data flows across systems and networks**
1.1.4	**Requirements for firewall at each Internet connection and between any DMZ and internal network zone**
	This allows the organisation to monitor the traffic coming in and out of the network (including the DMZ and internal network traffics). On top of monitoring, they are able to control and deny any suspicious or malicious traffic with the use of the firewall and prevent the chances of an unauthorised access from a malicious individual outside of the organisation's network via an unprotected connection.
1.1.5	**Description of groups, roles and responsibilities for management of network components**
	This is to ensure that all personnel are aware of who is **responsible** for the security of all network components. - It gets the organisation on the same page, reduce risks and incidents, helping the entire workforce protect their organisation and themselves. Those who are assigned to manage components are aware of their responsibilities. If roles and responsibilities are not formally assigned, devices could be left unmanaged.
1.1.6	**Document down business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.**
	The sub-requirement involves both firewall and router configurations. Compromises often happen due to unused or insecure service and ports. Since these often have known vulnerabilities and there are organisations that do not patch their systems/ports/services they don't use but still kept them switched on/installed in their network. By clearly defining and documenting them, organisations can refer to the logs and ensure that all unnecessary services, protocols and ports are disabled/removed.
1.1.7	**Requirements to review firewall and router rulesets at least every six months:** (a) Verify that firewall and router configuration standards require review of firewall and router rulesets, (b) Examine documentation relating to ruleset reviews and interview responsible personnel to verify that the rulesets are reviewed
	It is important to clean up every few months to remove the unnecessary, outdated, incorrect rules etc. to make the organisation of the rules neater and easier to see/understand. Additionally, it is important that the company examine and verify their rulesets to allow only authorised services and ports that match the documented business justifications. *Firewall and router rulesets are complex. Extra, unnecessary and outdated rulesets will cause more complexity and time wasted, which could be used for other important matters.*

1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment	
1.2.1	**Restrict inbound and outbound traffic to a level necessary for the cardholder data environment, and specially deny all other traffic**
	This sub-requirement prevents unfiltered access between untrusted and trusted environments and traffics, which helps to prevent malicious individuals from accessing the entity’s network via unauthorised IP addresses or from using services, protocols or ports in an unauthorised manner. Eg. sending data they have obtained from within the entity’s network out to an untrusted server
1.2.2	**Secure and synchronise router configuration files**
1.2.3	**Install perimeter firewalls between all wireless networks and the cardholder data environment. Configure those firewalls to deny all traffic and only permit authorised traffic between the wireless environment and cardholder data environment (permitted traffic includes business purposes traffic).**
1.3	**Prohibit public access between Internet and any system component in the cardholder data environment by following the requirements below:** **(1.3.1) Implement a DMZ to limit inbound traffic to only system components that provide authorised publicly accessible services, protocols and ports** **(1.3.2) Limit inbound Internet traffic to IP addresses within the DMZ** **(1.3.3) Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network** - ***Eg. Block traffic originating from Internet with internal source address*** **(1.3.4) Do not allow unauthorised outbound traffic from the cardholder data environment to the Internet** **(1.3.5) Permit ONLY “established” connections into the network** **(1.3.6) Place system components that store cardholder data (i.e. database and servers) in an internal network zone, SEGREGATED from the DMZ and other untrusted network (i.e. public network)** **(1.3.7) Do not disclose private IP addresses and routing information to unauthorised parties.**
	There may be legitimate reasons for untrusted connections to be permitted to DMZ systems like allowing public access to a web server, however such connections should never be granted to systems in the internal network. It is important that a firewall’s intent is to control and manage all connections between public and internal networks, especially for those who store, process or transmit sensitive card data. If direct access if allowed between public and the sensitive information, the firewall protection

	will be bypassed and the system storing the sensitive card data will be compromised and exposed for anyone to see and steal.
1.4	**Install personal firewall software or equivalent functionality on any portable computing devices (including company/employee-owned) that connect to the Internet when outside the network (eg. laptops used by employees) and which re also used to access the CDE. Firewall or equivalent configurations must include:** - **Specific configuration settings are defined** - **Personal firewall or equivalent functionality is actively running and protecting** - **Personal firewall or equivalent functionality is not modified by users of the portable computing devices (i.e. laptop)**
	It is important for everyone to know that portable computers/devices that are allowed to connect to the Internet from outside the corporate firewall are more vulnerable to Internet-based threats.
1.5	**Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties**

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

If vendor-supplied default passwords were used, it increases the attack surface of the system since most vendor-supplied passwords could be guessed and cracked easily through brute forcing and/or dictionary attack. Thus it is critically important to change vendor-supplied default password and settings once the equipment is properly installed into your organisation’s environment. Additionally, it is recommended to remove and/or disable unnecessary default accounts before introducing the new equipment/system into your environment for your company people to use.

These are all considered under system hardening.

Best practices for the implementation of security configuration on your systems is important, especially for practices to harden your system. Following this requirement, some steps that the company can take to be compliant are listed below.

1. Standard configuration settings for devices connected to stored cardholder data network which includes:
    a. Changing of ALL default settings provided upon first boot or usage of that device

2. Organisations are to only have one function per server
    a. Please refer to reference number 2.2.1 under this requirement

3. Create and write hardening configuration standards documentations that are tailored to own organisation’s networks and systems, and make sure that the documentations are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include;
    a. Center for Internet Security (CIS)
    b. International Organisation for Standardisation (ISO)

c. SysAdmin Audit Network Security (SANS) Institute
d. National Institute of Standards Technology (NIST)

4. Keep hardening documentation guide up-to-date. It is recommended to review those guides when your organisation had done a software update/upgrade or whenever a vulnerability that involves a configuration change is made.

Refer below for more specific details of each sub-requirements

2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.

- ***This applies to ALL default passwords, including but not limited to those used by OS, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) etc.***

2.1.1

For wireless environments connected to the cardholder data environment or transmitting cardholder data, they are needed to change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords and SNMP community strings.

If wireless networks are not implemented with sufficient security configurations including changing default settings, attackers can sniff and eavesdrop on the wireless traffic, easily capturing data and passwords as well as entering the network.

Note: The key-exchange protocol for older version of 802.11x encryption has been broek and cna render the encryption useless. Thus organisation should make sure that their devices firmware are updated to the latest version to support more secure protocols.

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.
Source of industry-accepted system hardening standards may include, but are not limited to

- **CIS, ISO, SANS Institute, NIST**

2.2.1

Implement only 1 primary function per server to prevent functions that require different security levels from co-existing on the same server (Eg. Web servers, database servers, DNS etc should be implemented on separate servers)

The security level of functions with higher security needs would be reduced due to the presence of the lower-security functions.
Server functions with lower security level may introduce security weaknesses to other functions on the same server, which will then increase that server's attack surface and vulnerabilities.

2.2.2

Enable only necessary services, protocols, daemons etc as required for the function of the system

2.2.3	**Implement additional security features for any required services, protocols or daemons that are considered to be insecure.**
	Enabling security features before new servers are deployed will prevent servers being installed into an environment with in secure configurations. It is also important to ensure that all insecure services, protocols and daemons are adequately secured with appropriate security features. This decreases the chance for malicious individuals to take advantage of commonly used points of compromise within a network.
2.2.4	**Configure system security parameters to present misuse**
	In order for systems to be configured securely, system administrators are responsible for configurations and must be knowledgeable in the specific security parameters and settings that apply to the system environments
2.2.5	**Remove all unnecessary functionality such as scripts, drivers, features, subsystems, file systems unnecessary web servers**
	Unnecessary functions can provide additional opportunities for malicious individuals to gain access to a system. Removing unnecessary functionality can help reduce the risk of unknown vulnerable functions to be exploited.
2.3 Encrypt all non-console administrative access using strong cryptography	
2.4 Maintain an inventory of system components that are in scope for PCI DSS	
-	Without an inventory, some system components could be forgotten and may be excluded from organisation’s own configuration standards. Maintaining a current list of all system components helps tp accurately and efficiently define how and what their organisation can implement the PCI DSS controls into their environment.
2.5	**Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use and known to all affected parties**

Control Objective 2: Protect Cardholder Data

The second control objective, protect cardholder data, consists of the two requirements (number 3 & 4) as listed below. The two requirements under this objective covers over the protection of cardholder data during its transmission from customer side to the data center across the public network and stored data inside the data center’s servers.

It details how cardholder data should be stored, the restrictions on what data can be stored, and most importantly the encryption standards used when transmitting cardholder data across public network and the restrictions against unencrypted transmission of cardholder data over public network.

Requirement 3: Protect stored cardholder data

To protect cardholder data, there are many methods of doing so, and they include: encryption, truncation, masking and hashing. It is the organisation's responsibility to protect the customers' data to prevent unauthorised use of those data and thwart theft.

Another critical method/good habit to take to protect stored cardholder data is to not store them unless necessary. Remove any unnecessary data and don't keep any old data in the server.

Following this requirement, some steps that the company can take to be compliant are listed below.

1. Document the data retention and eliminating policy. Make sure the following are clear:
    a. The type of data that **can be kept**
    b. Reason why the data is stored
    c. How long should the data be stored
    d. The place where the data is stored
    e. When should the data be deleted
    f. How the data should be eliminated securely

2. The organisation needs to keep in mind that PCI DSS only allows storing of those listed below:
    a. Main account number (PAN) *(please refer to the list numbered 3.4 for more information on this sub-requirement)*
    b. The expiration date
    c. Customer's Cardholder name
    d. The service code

Once the authorisation process is finished, it is a **MUST** that the organisation remove all other data immediately after the process.

3. The organisation must keep the PAN unreadable any where it is stored by implementing one of the below methods that is mentioned in **3.4** below for this sub-requirement

Card data is one of the most important and world-wide used assets of the payment industry, thus it is important that we need to keep it secure in the database(s). **Those data are valuable to attackers as it allows them to generate counterfeit payment cards and create fraudulent transactions.** For these reasons, developing detailed documentation and taking proper steps and implementing best practices will help reduce the risk(s).

4. Define a procedure to identify and securely delete the stored card data that had exceeded the retention period established in the data retention and deletion policy.
    a. It is recommended to delete unnecessary data or outdated data

5. Document and implement procedures that protect encryption keys against their possible disclosure or misuse *(please refer to number 3.5 for more information on this sub-requirement)*
    a. The documentation must detail **all** algorithms, protocols, keys used and definition of its

<table>
<tr><td colspan="2">encryption period.

It is the organisation’s responsibility to protect the card data that they store in their database servers. However, even if it’s secure enough, there are always risks of the data being stolen, thus one of the sub-requirement is to have a data analysis to define which and what data is really necessary to store.

6. All the data retentions and elimination definitions/documentations depend exclusively on the needs of the business and local legal regulations that apply into your industry or on the type of data that is retained

<b><i>Refer below for more specific details of each sub-requirements.</i></b></td></tr>
<tr><td colspan="2"><b>3.1 Keep cardholder data storage ot a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all servers/storages that stores cardholder data
(1) Limiting data storage amount and retention time to that which is required for legal, regulatory and/or business requirements
(2) Specific retention requirements for cardholder data
(3) Processes for secure deletion off data when no longer needed
(4) A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention</b></td></tr>
<tr><td>-</td><td>A formal data retention policy helps to identify and understand what kind and where should the data be retained so that it can be securely destroyed or deleted as soon as when its no longer needed.
The only cardholder data that may be stored after authorisation is the primary account number or unreadable PAN, expiration date, cardholder name and service code.</td></tr>
<tr><td colspan="2"><b>3.2 Do not store sensitive authentication data after authorisation, even if encrypted. If sensitive authentication data is received, render all data unrecoverable upon completion of the authorisation process.
(Sensitive authentication data includes the data as cited in the following sub-requirements 3.2.1 to 3.2.3)
- Sensitive authentication data consists of full track data, card validation code or value and PIN data.
- <i>These are valuable to attackers as it allows them to generate counterfeit payment cards and create fraudulent transactions.</i></b></td></tr>
<tr><td><b>3.2.1</b></td><td><b>Do not store the full contents of any track after authorisation. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data
- Eg of track: from magnetic stripe located on the back of a card, equivalent data contained on a chip or else where.</b></td></tr>
<tr><td rowspan="2"><b>3.2.2</b></td><td><b>Do not store the card verification code or value (3 or 4 digit number printed on the front of back of card to verify card-not-present transactions) after authorisation</b></td></tr>
<tr><td><i>Purpose of the card validation code is to protect “card-not-present” transactions made on the Internet or mail/telephone order where the card is not shown to the</i></td></tr>
</table>

	sender/seller *If these numbers were stolen, malicious individuals can execute fraudulent transactions*
3.2.3	**Do not store the personal identification number (PIN) or the encrypted PIN block after authorisation** - **These data should only be known to card owner or bank that issued the card.**
3.3 Mask PAN when displayed (1st six and last four digits are the maximum number of digits to be displayed), such that only personnel with legitimate business can see more than the first six/last four digits of the PAN.	
-	Ensuring that full PAN is only displayed for those with legitimate business minimises the risk of unauthorised persons gaining access to PAN data. Organisation should always ensure that the masking approach only display the minimum number of digits to perform a specific business function. - *Eg 1. if only the last 4 digits are needed to perform a business function, mask the PAN so that individuals performing that function can view only the last 4 digits.* - *Eg 2. If function needs access to the bank identification number (BIN) for routing purposes, unmask only the BIN digits (first six digits) during that function*
3.4 Render PAN unreadable anywhere it is stored by using any of the follow approaches: - **One-way hashes based on strong cryptography in which the entire PAN must be hashed** - **Truncation, which stores a segment of the PAN (not exceed the 1st six and last four digit)** - **Tokenisation, which stores a substitute or proxy for the PAN rather than the PAN itself** - **Strong cryptography underpinned by key management processes and security procedures**	
3.4.1	**If disk encryption is used, logical access must be managed separately and independently of native OS authentication and access control mechanisms. Also decryption keys must not be associated with user accounts.**
	For example, it is advisable for the company to not use local user account databases or general network login credentials. *On top of that, the cryptographic keys must be stored and secured in a separate place.*
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.	
3.5.1	**[For Service Provider ONLY] Main a documented description of the cryptographic architecture that includes:** **(a) Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date** **(b) Description of key usage for each key** **(c) Inventory of any HSMs and other SCDs used for key management**

3.5.2	**Restrict access to cryptographic keys to the fewest number of custodians necessary**
3.5.3	**Store secure and private keys used to encrypt/decrypt cardholder data in one or more of the following forms at all times:** **(1) Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key** **(2) Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device)** **(3) At least two full-length key components or key shares, in accordance with an industry-accepted method**
	Cryptographic keys must be stored securely to prevent unauthorised access that could result in the exposure of cardholder data to malicious individuals. *[If key-encrypting keys are used] Storing the key-encrypting keys in physically or logically separate locations from the data-encrypting keys reduces the risk of unauthorised access to both keys.*
3.5.4	**Store cryptographic keys in the fewest possible locations**
	Storing the keys in fewest locations helps the organisation to keep track and monitor the locations; minimising the chance for the keys to be known and exposed to unauthorised people
3.6	**Fully document and implement all key-management processes and procedures for cryptographic keys used for encrypting of cardholder data, including the following sub-requirements from 3.6.1 to 3.6.8:**
3.6.1	**Generation of strong cryptographic keys**
3.6.2	**Secure cryptographic key distribution**
3.6.3	**Secure cryptographic key storage**
3.6.4	**Conduct cryptographic key changes for keys that have reached the end of their period as defined by the associated application vendor or key owner, and based on industry best practices and guidelines**
	The period is the time span during which a particular cryptographic key can be used for defined purpose. To calculate the period include, but not limited to, the strength of the algorithm, size or length of key, risk of key compromise and sensitivity of the data being encrypted. Periodic changing off encryption keys when the keys have reached the end of their period is to minimise risk of someone else obtaining the encryption keys and using them to decrypt data

3.6.5	**Retirement or replacement of keys (eg. archiving, destruction), as deemed necessary, when the integrity of key has been weakened (eg. departure of an employee with knowledge of the key in clear-text) or keys are suspected of being compromised.**
3.6.6	**If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control**
3.6.7	**Prevention of unauthorised substitution of cryptographic keys**
3.6.8	**Requirement of cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities**
3.7	**Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use and known to all affected parties** - **Personnel(s) needs to be aware of and ALWAYS follow security policies as well as document operational procedures for managing the secured storage of cardholder data.**

Requirement 4: Encrypt transmission of cardholder data across open public networks

It is important that the organisation encrypt the sensitive data and authenticate information during the transmission of the data across client and the server because these networks are usually targeted by individuals who exploit the open, visible nature of the network to exploit and gain unauthorised access into the network's system.

Malicious individuals can exploit the vulnerabilities of public or wireless networks that are misconfigured to gain privileged access to card data. There are many attacks were they intercept the traffic in between and listen in on the communication, thereafter getting sensitive data. Some attacks include man-in-the-middle (MitM) and packet-sniffing.

Following this requirement, some steps that the company can take to be compliant are listed below.

1. Implement only strong cryptography and security protocols and safeguards sensitive card data during transmission over open, public networks
    a. *! It is recommended that organisations disable the old/early versions and insecure protocols of TLS and SSL as they are no longer safe.*

2. Implement strong cryptography for authentication and transmission of card data over wireless networks and/or over other internal networks or internal data that has access to the sensitive card data. Additionally, organisations will need to apply the following or have knowledge over the following;
    a. Hardening of wireless networks
    b. Have knowledge of all best practices of industry-accepted system hardening standard like Center for Internet Security (CIS), International Organisation for Standardisation (ISO), SysAdmin Audit Network Security (SANS) Institute and National Institute of Standards

<table>
<tr><td colspan="2">Technology (NIST) and not limited to these few.
c. Include the recommendation of all technology providers.

3. Never send unprotected PANs by end-user messaging technologies such as email, instant messaging, SMS, chats and so on, unless they are configured to provide strong encryption.
a. These technologies can be easily intercepted by packet-sniffing during transmission on both internal and public networks.

It is important to keep informed about the new vulnerabilities that affect those protocols that were considered safe in the past and have ceased to be so.

Refer below for more specific details of each sub-requirements.</td></tr>
<tr><td colspan="2">**4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open public networks, including the following:**
- **Only trusted keys and certificates are accepted**
- **The protocol in use only supports secure versions or configurations**
- **The encryption strength is appropriate for the encryption methodology in use**</td></tr>
<tr><td>**4.1.1**</td><td>**Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission**</td></tr>
<tr><td colspan="2">**4.2 Never send unprotected PANs by end-user messaging technologies (eg. e-mail, instant messaging, SMS, chat etc.)**</td></tr>
<tr><td>-</td><td>E-mail, instant messaging, SMS etc can be easily intercepted by malicious individuals who can do MitM attacks or use packet-sniffing tools to listen in on the delivery across internal and public networks.
Do not utilise those messaging tools to send PAN unless configured to provide strong encryption to protect the PANs or render PANs unreadable before transmission.</td></tr>
<tr><td colspan="2">**4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties**</td></tr>
</table>

Control Objective 3: Maintain a Vulnerability Management Program

The third control objective, maintain a vulnerability management program, consists of the two requirements (number 5 & 6) as listed below. The two requirements under this objective covers over the usage of antivirus softwares, developing and maintaining a vulnerability management plan to secure payment systems and remediate any existing vulnerabilities.

It details how the programs will include the requirements that antivirus softwares needs (i.e. installations, capabilities, functionalities and more), and how you can secure systems and/or applications by constantly patching systems' security, being aware of vulnerabilities and developing on the security.

Requirement 5: Protect all systems against malware and regularly update antivirus software or programs

This requirement is important to follow through as malware is malicious and can bring harm to your systems and information data if not protected properly. Malware can be introduced into your network and systems through any methods including email, internet, personal employee computers, USB drive and more.

New attacks continually emerge in order to exploit system vulnerabilities against secure systems, where the attacks are often zero-day attacks. Without an anti-virus software/program, the evolved malwares can attack systems, causing disruptions and data stolen from them.

To prevent and decrease the attack surface as well as keeping up to the latest trend of malware and keep zero-days attacks at bay, it is advisable that anti-virus softwares are installed and regularly patched to the latest version, and properly configured and managed.

Following this requirement, some steps that the company can take to be compliant are listed below.

1. [For organisation] If a PCI DSS scope for anti-virus technology exists, **all** of those components **MUST** be implemented.

2. The anti-virus solution(s) must be able to detect, remove and protect against all types of malicious softwares and malwares.
    a. This sub-requirement includes all anti-virus entities installed in the organisation’s network and/or computer systems under the organisation
    b. Malicious softwares and malwares include virus, trojans, adware, spyware, rootkits etc.

3. The anti-virus solution must be updated to the latest security patch and signature files

4. The anti-virus solution must provide the ability to monitor viruses and malware activities through its audit logs.
    a. The audit logs must be administrated according to **PCI DSS requirement 10**

Although the organisation have up-to-date anti-virus softwares/programs, but it is recommended that organisations do not be lenient and hesitate on the thoughts about further strengthening their security as malwares are being more sophisticated, always changing to be harder to pick up, and prevent them from compromising your systems.

Refer below for more specific details of each sub-requirements.

5.1 Deploy anti-virus software on all systems commonly affected by malicious software, particularly personal computers and servers

5.1.1	**Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software**
5.1.2	**For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software**

	Malicious softwares can change quickly, so it is important for organisations to be aware of new malware that might affect their systems. (eg. monitoring vendor security notices and anti-virus groups to determine whether their systems might be coming under threat from new and evolving malware) Trends in malware should be included in the identification of new security vulnerabilities, and methods to address new trends should be incorporated into the company's configuration standards and protection mechanisms as needed.
5.2 Ensure that all anti-virus mechanisms are maintained as follows: - **Kept current,** - **Perform periodic scans** - **Generate audit logs which are retained per *PCI DSS requirement 10.7***	
-	Even the best anti-virus solutions are not fully effective in protecting against all malwares. Audit logs provide the ability to monitor virus and malware activity and anti-malware reactions. Thus it is recommended that anti-malware solutions be configured to generate audit logs, where they need to be managed in accordance to PCI DSS requirement 10
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorised by management on a case-by-case basis for a limited time period	
-	Use of policy-based controls on all systems to ensure anti-malware protections cannot be altered or disabled will help prevent system weaknesses from being shown and exploited by malicious individuals/softwares.
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties	

Requirement 6: Develop & maintain secure systems and applications
Attackers often use security vulnerabilities to gain unauthorised privilege access to your system. These security vulnerabilities are typically remediated through the application of security patches and must be installed by whoever manages those systems. However, there is still the problem of the entities that manage the system being the ones responsible for installing the security patches. Additionally, the security vulnerabilities that are introduced inadvertently inside custom software codes could also be exploited to gain access to a network and compromise the data of the cardholder. It is important that the system administrator ensure that all applications and systems to have appropriate, current software patches to protect against the exploitation and compromise of cardholder data
Following this requirement, some steps that the company can take to be compliant are listed below. To mitigate the risk, protect and secure the environment and card data, it is important to implement best practices for secure configurations, maintain up-to-date software and secure development.

1. **Update the organisation's systems regularly**
    a. Security patches & security settings update

2. **Identify the vulnerabilities continuously** through information provided by vendors, industry-accepted security sites and scanning tools.

3. **Classify the risk and set priorities**
    a. It is important to quickly address the elements of greater risk and **reduce the probability of exploiting** the vulnerabilities

4. **Remediate** vulnerabilities of the **highest risk**
    a. This has to be done **within 30 days** after finding the vulnerability
    b. Lower risk vulnerabilities are advisable to be remediated before the next scheduled data of the next security scan.

5. **Perform a security scan test again** to confirm that the vulnerability have been **remediated**; that the attack surface have decreased and the security hole is gone

6. **Perform objective and independent reviews**
    a. This should be done by someone NOT part of the development sector in charge of coding the site. **This is to prevent sabotage and inaccurate reviews**.

7. Keep the development environment **clean** and **separate the production environment** both physically and logically.
    a. Do not implement new codes with testing data such as user IDs and passwords that were used in the test phase,
    b. This is to **prevent unauthorised access** to the system in the event that those testing account's credentials were stolen before or were password cracked (dictionary attack) if the testing account's credentials were easy to crack.

Refer below for more specific details of each sub-requirements

6.1	**Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking to newly discovered security vulnerabilities**
6.2	**Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release**
6.3	**Develop internal and external software applications, including web-based administrative access to applications, securely**
6.3.1	**Remove development, test and/or custom application accounts, user IDs and passwords before applications become active or are released to customers.**
6.3.2	**Review custom code prior to release to production or customers in order to identify any potential coding vulnerability**
6.4	**Follow change control processes and procedures for all changes to system**

	components
6.5	**Address common coding vulnerabilities in software-development processes like:** **(6.5.1) Protected from injection flaws, particularly SQL injection attacks. Also consider OS command injection, LDAP, XPath injection flaws as well as other injection flaws** **(6.5.2) Protection from buffer overflow** **(6.5.3) Do not allow insecure cryptographic storage** **(6.5.4) Do not allow insecure communications** **(6.5.5) Protect applications from improper error handling** **(6.5.6) Manage all “high risk” vulnerabilities identified in the vulnerability identification process** **(6.5.7) Protect all web applications and application interfaces from cross-site scripting (XSS)** **(6.5.8) Do not allow improper access control, such as insecure direct object references, failure to restrict URL access, directory traversal and failure to restrict user access to functions** **(6.5.9) Do not allow cross-site request forgery (CSRF)**
	One way to be compliant for the above mentioned sub-requirements, it is advisable that the organisation constantly test and evaluate their network and company website and server for any security vulnerabilities like CSRF, XSS, injection attacks, in secure communication and such and exploits. Any problems found are to be reported and remediated immediately as well as sending out alerts to the organisation’s customers.
6.6	**For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these application are protected against known attacks**
6.7	**Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties**

Control Objective 4: Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data to business need to know	
7.1	**Limit access to system components and cardholder data to only those individuals whose job requires such access.**

7.1.1	Define access needs for each role, including: ● System components and data resources that each role needs to access for their job function ● Level of privilege required (for example, user, administrator, etc.) for accessing resources
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.
7.1.3	Assign access based on individual personnel's job classification and function
7.1.4	Require documented approval by authorized parties specifying required privileges
7.2	**Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed**
7.2.1	Coverage of all system components
7.2.2	Assignment of privileges to individuals based on job classification and function
7.2.3	Default "deny-all" setting
7.3	**Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties**

Requirement 8: **Identify and authenticate access to system components**	
8.1	**Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:**
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects
8.1.3	Immediately revoke access for any terminated users
8.1.4	Remove/disable inactive user accounts within 90 days
8.1.5	Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:

	Enabled only during the time period needed and disabled when not in use. Monitored when in use
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID
8.1.8	If a session has been idle for more than 15 minutes, require the user to reauthenticate to re-activate the terminal or session
8.2	**In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:** **Something you know, such as a password or passphrase** **Something you have, such as a token device or smart card** **Something you are, such as a biometric**
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components
8.2.2	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys
8.2.3	Passwords/passphrases must meet the following: Require a minimum length of at least seven characters. Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above
8.2.4	Change user passwords/passphrases at least once every 90 days
8.2.5	Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used
8.2.6	Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use
8.3	**Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication** **Note: Multi-factor authentication requires a minimum of two of the three authentication methods. Using one factor twice (e.g. using two separate passwords)**

	is not considered multi-factor authentication
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access
8.3.2	Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity’s network
8.4	**Develop, implement and communicate authentication policies and procedures to all users including:** **Guidance on selecting strong authentication credentials** **Guidance for how users should protect their authentication credentials** **Instructions not to reuse previously used passwords** **Instructions to change passwords if there is any suspicion the password could be compromised**
8.5	**Do not use group, shared, or generic IDs, or other authentication methods. Service providers with access to customer environments must use a unique authentication credential (such as a password/passphrase) for each customer environment**
8.6	**Use of other authentication mechanisms such as physical security tokens, smart cards, and certificates must be assigned to an individual account** **Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.** **Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.**
8.7	**All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:** **All user access to, user queries of, and user actions on databases are through programmatic methods** **Only database administrators have the ability to directly access or query databases** **Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes)**
8.8	**Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties**

Requirement 9: **Restrict physical access to cardholder data**	
9.1	**Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment**
9.1.1	Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law “Sensitive areas” refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as cashier areas.
9.1.2	Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines
9.2	2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: ● Identifying onsite personnel and visitors (for example, assigning badges) ● Changes to access requirements ● Revoking or terminating onsite personnel and expired visitor identification (such as ID badges)
9.3	Control physical access for onsite personnel to sensitive areas as follows: ● Access must be authorized and based on individual job function. ● Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled
9.4	Implement procedures to identify and authorize visitors Procedures to follow as below:
9.4.1	Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained

9.4.2	Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel
9.4.3	Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration
9.4.4	A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law
9.5	Physically secure all media
9.5.1	Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location’s security at least annually
9.6	Maintain strict control over the internal or external distribution of any kind of media, including the following:
9.6.1	Classify media so the sensitivity of the data can be determined
9.6.2	Send the media by secured courier or other delivery method that can be accurately tracked
9.6.3	Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals)
9.7	Maintain strict control over the storage and accessibility of media
9.7.1	Properly maintain inventory logs of all media and conduct media inventories at least annually
9.8	Destroy media when it is no longer needed for business or legal reasons as follows:
9.8.1	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed
9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale
9.9.1	Maintain an up-to-date list of devices. The list should include the following:

	● Make, model of device ● Location of device (for example, the address of the site or facility where the device is located) ● Device serial number or other method of unique identification
9.9.2	Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings
9.9.3	Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: ● Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. ● Do not install, replace, or return devices without verification. ● Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). ● Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer)
9.10	Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties

Control Objective 5: Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data	
10.1	Implement audit trails to link all access to system components to each individual user
10.2	Implement automated audit trails for all system components to reconstruct the following events:
10.2.1 to 10.2.7	● All individual user accesses to cardholder data

	● All actions taken by any individual with root or administrative privileges ● Access to all audit trails ● Invalid logical access attempts ● Use of and changes to identification and authentication mechanisms— including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges ● Initialization, stopping, or pausing of the audit logs ● Creation and deletion of system-level objects
10.3	Record at least the following audit trail entries for all system components for each event:
10.3.1 to 10.3.6	● User identification ● Type of event ● Date and time ● Success or failure indication ● Origination of event ● Identity or name of affected data, system component, or resource
10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. One example of time synchronization technology is Network Time Protocol (NTP)
10.4.1 to 10.4.3	● Critical systems have the correct and consistent time ● Time data is protected ● Time settings are received from industry-accepted time sources
10.5	Secure audit trails so they cannot be altered
10.5.1 to 10.5.5	● Limit viewing of audit trails to those with a job-related need ● Protect audit trail files from unauthorized modifications ● Promptly back up audit trail files to a centralized log server or media that is difficult to alter ● Write logs for external-facing technologies onto a secure, centralized, internal log server or media device

	● Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity Log harvesting, parsing, and alerting tools may be used to meet this Requirement
10.6.1	Review the following at least daily: ● All security events ● Logs of all system components that store, process, or transmit CHD and/or SAD ● Logs of all critical system components ● Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)
10.6.2	Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment
10.6.3	Follow up exceptions and anomalies identified during the review process
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup)
10.8	Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: ● Firewalls ● IDS/IPS ● FIM ● Anti-virus ● Physical access controls ● Logical access controls ● Audit logging mechanisms ● Segmentation controls

10.8.1	Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: ● Restoring security functions Identifying and documenting the duration (date and time start to end) of the security failure ● Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause ● Identifying and addressing any security issues that arose during the failure ● Performing a risk assessment to determine whether further actions are required as a result of the security failure ● Implementing controls to prevent cause of failure from reoccurring ● Resuming monitoring of security controls
10.9	Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties

Requirement 11: **Regularly test security systems and processes**	
11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis
11.1.1	Maintain an inventory of authorized wireless access points including a documented business justification
11.1.2	Maintain an inventory of authorized wireless access points including a documented business justification
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)
11.2.1	Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel
11.2.2	Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform

	rescans as needed, until passing scans are achieved
11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel
11.3	Implement a methodology for penetration testing that includes the following: ● Is based on industry-accepted penetration testing approaches (for example, NIST SP800- 115) ● Includes coverage for the entire CDE perimeter and critical systems ● Includes testing from both inside and outside the network ● Includes testing to validate any segmentation and scope-reduction controls ● Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 ● Defines network-layer penetration tests to include components that support network functions as well as operating systems ● Includes review and consideration of threats and vulnerabilities experienced in the last 12 months ● Specifies retention of penetration testing results and remediation activities results
11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment)
11.3.2	Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment)
11.3.3	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections
11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/ methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE
11.3.4.1	Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data

	environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly
11.5.1	Implement a process to respond to any alerts generated by the change-detection solution
11.6	Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties

Control Objective 6: Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel	
12.1	Establish, publish, maintain, and disseminate a security policy
12.1.1	Review the security policy at least annually and update the policy when the environment changes
12.2	Implement a risk-assessment process that: ● Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), ● Identifies critical assets, threats, and vulnerabilities, and ● Results in a formal, documented analysis of risk. Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30
12.3	Develop usage policies for critical technologies and define proper use of these technologies. Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage
12.3.1 to 12.3.10	● Explicit approval by authorized parties ● Authentication for use of the technology

	● A list of all such devices and personnel with access ● A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices) ● Acceptable uses of the technology ● Acceptable network locations for the technologies ● List of company-approved products ● Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity ● Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use ● For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel
12.4.1	Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: ● Overall accountability for maintaining PCI DSS compliance ● Defining a charter for a PCI DSS compliance program and communication to executive management
12.5	Assign to an individual or team the following information security management responsibilities:
12.5.1 to 12.5.5	● Establish, document, and distribute security policies and procedures ● Monitor and analyze security alerts and information, and distribute to appropriate personnel ● Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations

	● Administer user accounts, including additions, deletions, and modifications ● Monitor and control all access to data
12.6	Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures
12.6.1	Educate personnel upon hire and at least annually. Methods can vary depending on the role of the personnel and their level of access to the cardholder data
12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures
12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)
12.8	Maintain and implement policies and procedures to manage service providers, with whom cardholder data is shared, or that could affect the security of cardholder data, as follows
12.8.1 to 12.8.5	● Maintain a list of service providers including a description of the service provided ● Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. ● Ensure there is an established process for engaging service providers including proper due diligence prior to engagement ● Maintain a program to monitor service providers' PCI DSS compliance status at least annually ● Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity
12.9	Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach
12.10.1	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:

	● Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum ● Specific incident response procedures ● Business recovery and continuity procedures ● Data backup processes ● Analysis of legal requirements for reporting compromises ● Coverage and responses of all critical system components ● Reference or inclusion of incident response procedures from the payment brands
12.10.2 to 12.10.6	● Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually ● Designate specific personnel to be available on a 24/7 basis to respond to alerts ● Provide appropriate training to staff with security breach response responsibilities ● Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems ● Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments
12.11	Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: ● Daily log reviews ● Firewall rule-set reviews ● Applying configuration standards to new systems ● Responding to security alerts ● Change management processes
12.11.2	Additional requirement for service providers only: Maintain documentation of quarterly review process to include: ● Documenting results of the reviews ● Review and sign off of results by personnel assigned responsibility for the PCI DSS

	compliance program

4.4 Controversies and Criticisms

One of the biggest complaints regarding the PCI Data Security Standard is its penalty for non-compliance. This system is implemented to establish consequence on security control negligence. However, PCI DSS has been known to be vague with its requirements, making it easier to claim non-compliance. Furthermore, many organizations have found issues with the fining penalty, claiming this gives opportunities for merchants to impose unnecessary fines. A case highlighting this is the Cisero’s alleged data breach case, where Elavon and Visa claimed that the company has caused $1.26 million in fraud due to negligence. Multiple forensic investigators confirmed that despite certain PCI DSS violations being found in the assessment, no concrete evidence of suspicious activity was found to be significant enough to be considered a data breach. Even then, Elavon and U.S. Bank did not give them an opportunity to appeal and the fines were imposed anyways. This raises the concern on the authority of payment card brands forcefully imposing fines despite lack of proof supplied by the merchant regarding major security concerns.

Another criticism is that PCI DSS does not guarantee protection against data breaches. Many organisations have suffered significant breaches despite being PCI DSS compliant, such as the 2008 Heartland Payment Systems data breach with more than 100,000,000 compromised card numbers and the 2011 Sony attack, compromising over twenty million of Sony’s Playstation Network users cardholders and other personally identifiable information. This emphasises the need of implementing other frameworks and standards as well to achieve data security, since PCI DSS does not require to protect every PII data possible.

To add on, some have argued that there is not much use in achieving the PCI DSS compliance goal as other information such as bank account details, addresses and other PII data are left unsecure. This is because rather than focusing on the risks that your company may face, PCI DSS is more of a checklist of requirements that needed to be fulfilled regardless. A more risk-based standard and framework that companies are more likely to implement is ISO27001 or NIST, as it requires them to properly assess and evaluate the different risks before implementing. Due to PCI's strict guidelines, it is difficult for some organizations to implement security measures without hitting non-compliance. For example, an organization may choose to implement a third-party application to manage their security system. However, this can cause non-compliance because it requires an approval from the council. Thus, PCI DSS as it is right now does not allow companies to be flexible with their needs.

5 Is PCI DSS Good?

Since the start of breaches having been reported over the years, there have been discussions and opinions about whether being compliant to the PCI DSS means they are completely safe. It is important that merchants, service providers and organisations should know and understand that being compliant to PCI DSS **does not mean** that they will be secured enough.

PCI DSS standards only provide the minimum set of security controls that should be implemented as part of the organisation's responsibility and commitment to keep customers' cardholder data safe and secure. More can be done to secure customers' cardholder data than just implementing the controls that PCI DSS stressed to implement and meet its requirements. Security is not just about adhering to the laws. It is about really protecting your systems and keeping up with the sophisticated evolving malwares and preventing them from compromising the network and stealing data.

With reference to section 4.4, you can see that there are many past breaches of the payment companies.

PCI DSS is a good guideline to start off the merchants, service providers and organisations on keeping cardholder data secure, however, it should only be viewed as a starting point and one should not stop there to secure the network environment.

5.1 Good enough to be enforced over other data?

Although PCI DSS is a set of compliance framework standards designed for the industry intended to keep consumers' card data and information safe when used with merchants and service providers, there are thoughts that maybe PCI DSS can be used and extended as a security standards for other things that had nothing to do with cardholder data; in this case, any sensitive data that are not related to credit card information.

As explained above in section 5, PCI DSS is good enough to be viewed as a starting point, but one should not stop there and instead, find other methods to further improve the organisation's network security. But PCI DSS can be used as a reference to enforce other data as it covers over some requirements that every organisation, even if it is not related to cardholder data, can use globally to protect other sensitive data. Some requirements in the PCI DSS covers over some security hardening, which other organisations can follow through to strengthen their security networks.

Following requirement 1, the organisation can follow the requirement where they can implement the following:

- Install and maintain firewall configurations
- Segregating the organisation’s network into three main security areas
    - External (Public), DMZ, Internal
- Keep a baseline configurations and constantly develop them

Following requirement 2, the organisation can follow the requirement where they can implement the following:

- Changing ALL default settings provided upon first boot or usage of that device.
- Only have one function per server
    - Web server, database server, DNS, FTP server, are all one server each in the DMZ
- Create hardening configuration standards documentations that are tailored to own organisation’s networks and systems
    - Make sure the documentations are consistent with industry-accepted system hardening standards.
- Implement strong cryptography for all passwords. Do not store plain-text passwords in the database server.

Following requirement 3, the organisation can follow the requirement where they can implement the following:

- Only necessary data should be kept in the servers
- Delete any customers’ data that are old and/or outdated

Following requirement 5, the organisation can follow the requirement where they can implement the following:

- Install anti-virus and regularly update them to the latest security patch and signature files
- Anti-virus solution must provide the ability to monitor viruses and malware activities through audit logs.

Following requirement 6, the organisation can follow the requirement where they can implement the following:

- Update organisation’s system regularly
- Identify vulnerabilities continuously
- Classify the risk and remediate the vulnerabilities with priority and perform security scan tests to check if the vulnerabilities have been remediated
- Address common coding vulnerabilities in software-development processes
    - Protect server from injection flaws, particularly SQL injection.
    - Protection from buffer overflow, CSRF, XSS and other web attacks

Conclusion

In the time that we have worked on PCI DSS standards, what particularly stands out is the lack of procedures and guidance to sanitize the company system after a breach. The standard itself covers as much of the basics of starting out from zero in implementing an effective policy and control, but will not suffice in the aftermath of an incident.

One should understand that being compliant to PCI DSS does not mean one is fully protected from being compromised.

Merchants, organisations and service providers should not stop after getting PCI DSS compliance. More can be done to secure the network environment and data than just implementing the effective policies and controls. Security is not just about adhering to the laws. It is about really protecting your systems and keeping up with the sophisticated evolving malwares and preventing them from compromising the network and stealing data.

As a merchant or service provider that processes card payment transactions, the goal is to ensure that the cardholder data is kept as secure as possible. Any company can attain PCI compliance by achieving the minimum security requirements set by PCI Security Standards Council and the PCI DSS. Identifying risk associated with any card data collection or malicious activity is the first step towards security. Security in turn mitigates risks and helps organisations achieve and maintain compliance on top of having protection.

Compliance to the PCI DSS should not be the end goal for any organisation processing and handling card data. Risk management and ensuring the total security of the systems and networks should be the end goal.

Appendices

1 Comparison against ISO 27001

1.1 Type of Standards

PCI DSS is a set of compliance framework standards designed for the industry intended to keep consumers' card data and information safe when used with merchants and service providers. This set of standards places more focus on organizations that deal with e-commerce. There are four different compliance levels of merchants (please refer to sections 2.5 and 4.1 for more information on merchant levels). There are 6 goals and 12 requirements in this standard. These requirements have been discussed at a high level in ISO/IEC 27001:2013 standard, established by the ISO and IEC. Companies are required to be audited by qualified security assessors (QSA) and approved scanning vendors (ASV) to validate their compliance with the PCI DSS. Adding on, Internal Security Assessors (ISA) can perform assessments with self-assessments questionnaires (SAQs), depending on the capacity and level of the merchants *(please refer to section 4.2 for more information on methods of validation of compliance)*.

ISO/IEC 27001 is an international standard on how to manage information security and its systems. This set of standards is appropriate for every type of organization. ISO/IEC 27001 includes 7 main titles within the sphere of annex SL, which is a new management system format that aids in streamline establishment of new standards and make implementing multiple standards within one organization simpler. It was formed by ISO Technical Management Board's (TMB) Joint Technical Coordination Group (JTCG).

It is recommended to combine both PCI DSS and ISO/IEC 27001 as this combination provides better solutions for information security for organizations. Since the controls of ISO/IEC 27001 are written at a higher level, the flexibility of ISO/IEC 27001 is much higher than that of PCI DSS *(please refer to the section below for more information)*. This means that it is much easier to comply with ISO/IEC 27001 standards.

When comparing both standards, the scope selection of ISO/IEC 27001 depends on the company, while PCI DSS' scope is exactly the credit cardholder information. Controls in ISO/IEC 27001 are just recommendations while the controls in PCI DSS are compulsory. Revalidation auditing of ISO/IEC 27001 is performed in cycles of three years and a small auditing scope is carried out annually. Adding on, surveillance audits are performed at least once a year. For PCI DSS, there are four network scanning audits and also an onsite audit for level 1 merchants *(please refer to section 4.2 for more information on methods of validation of compliance)*.

1.2 Compliance & Flexibility

What makes ISO/IEC 27001 different from PCI DSS is its compliance. Compliance for ISO/IEC 27001 is voluntary for non-regulated organisations. However, it is compulsory for organisations falling under the requirements of PCI DSS (i.e. organisations who store, transmits and processes card data) to be compliant to the standards--PCI DSS--as part of the merchant/service provider agreement to keep cardholder data safe.

As explained in the section 1.1 above, the scope of the ISO/IEC 27001 is more all-rounded, but for PCI DSS, it is centered around credit cardholder data and information. Moreover, ISO/IEC 27001 flexibility is higher than that of PCI DSS because its controls have been written at a high level and that it is not compulsory that all controls in the ISO 27001 must be followed, but it is a recommendation to be followed. A “should”, not a “must” unlike PCI DSS.

1.3 Cost

The cost of establishing information security management system (ISMS) and completing the PDCA cycle for ISO/IEC 27001 takes about approximately US $150,000 in a typical organisation, where it includes the costs;

- For managing information security and things related to information security measures
- Of capital that are induced by information security risk
- That are caused by information security incidents

The cost of being compliant to PCI DSS is approximately US$120,000 to US$700,000 due to the differences among the four levels of merchants *(please refer to section 2.5 and 4.1 for more information for the merchant levels)*.

Additionally, PCI DSS is widely available for everyone and the requirement files are free to download, however, one would need to pay fees to get the ISO 27001 standards.

1.4 Other Thoughts/Opinions

Although there are similarities and differences between these two standards, it is recommended to have both standards applied into your organisation, especially if your organisation is a payment processor. It is said that most of the controls and risk assessment methodology in ISO 27001 complement and support PCI DSS, which is why both standards have requirements that are very easy to integrate.

In this case, the PCI DSS requirements can be viewed as a subsection of the information security management pertaining to cardholder data, which aligned with the recommended controls in the ISO 27001 standards, or in some other organisation that implements both standards, ISO 27001 can be the beginning point for PCI DSS implementation.

References

Eg. [the section number] website link.

[Overall]
https://www.pcicomplianceguide.org/faq/
https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard
https://digitalguardian.com/blog/what-pci-compliance

[2] https://en.wikipedia.org/wiki/Payment_Card_Industry_Security_Standards_Council

[2.2]
https://www.braintreepayments.com/blog/who-needs-to-be-pci-compliant/
https://www.exabeam.com/siem-guide/siem-concepts/pci-compliance/
https://www.solarwindsmsp.com/content/pci-dss-requirements-checklist

[2.5]
https://www.imperva.com/learn/data-security/pci-dss-certification/
https://semafone.com/blog/a-comprehensive-guide-to-pci-dss-merchant-levels/

[4.1]
American Express:
https://www.americanexpress.com/content/dam/amex/uk/staticassets/merchant/pdf/support-and-services/American_Express_Data_Security_Operating_Principles.pdf
Discover Financial Services:
https://www.discoverglobalnetwork.com/en-us/business-resources/fraud-security/pci-rules-regulations/determining-validation-reporting-requirements
JCB International:
https://www.global.jcb/en/products/security/data-security-program/
Mastercard:
https://www.mastercard.com.sg/en-sg/business/large-enterprise/safety-and-security/security-recommendations/merchants-need-to-know.html
Visa Inc.:
https://www.visa.com.sg/support/small-business/security-compliance.html#3

[2.2 and 4.3] https://www.exabeam.com/siem-guide/siem-concepts/pci-compliance/

[3.1]
http://ewingoil.com/sites/ewingoil.com/files/Summary%20of%20Changes%20from%20PCI%20DSS%20Version%202.0%20to%203.0.pdf
https://www.pcisecuritystandards.org/minisite/en/docs/PCI_DSS_v3.pdf
https://www.pcisecuritystandards.org/minisite/en/docs/PCI_DSS_v2.pdf
https://www.pcisecuritystandards.org/pdfs/pci_pa-dss_summary_changes_%20v1%201_%20v12.pdf

https://www.itprotoday.com/security/pci-dss-11
https://www.qualys.com/docs/PCI_DSS_1-2_Summary.pdf

[3.3.4]
https://www.ispartnersllc.com/blog/pci-dss-version-4-0-launching-2020/
https://www.securitymetrics.com/blog/PCI-DSS-v4-payment-card-industry-security-standard
https://blog.pcisecuritystandards.org/pci-dss-looking-ahead-to-version-4.0
https://blog.pcisecuritystandards.org/pci-dss-v4-0-anticipated-timelines-and-latest-updates

[3.3.5]
https://blog.pcisecuritystandards.org/3-things-to-know-about-pci-dss-v4-0-development
https://blog.pcisecuritystandards.org/pci-dss-now-and-looking-ahead
https://www.ispartnersllc.com/blog/pci-dss-version-4-0-launching-2020/
https://www.securitymetrics.com/blog/PCI-DSS-v4-payment-card-industry-security-standard

[4.2]
https://www.pcisecuritystandards.org/assessors_and_solutions/become_qsa

[4.3]
https://www.exabeam.com/siem-guide/siem-concepts/pci-compliance/
https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard
https://www.netsparker.com/blog/web-security/definitive-pci-dss-compliance-guide-web-application-security/

[4.3.2]
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1611672074208
https://www.solarwindsmsp.com/content/pci-dss-requirements-checklist
https://www.otava.com/blog/principles-of-pci-compliance/
https://www.compassitc.com/blog/pci-requirements-explained-pci-requirement-2-change-your-defaults (requirement 2)
https://help.globalscape.com/help/archive/eft6-2/mergedprojects/hsm/requirement6.htm
(requirement 6 - company example)

[4.4] https://constantinecannon.com/wp-content/uploads/2018/10/Hospitality-Law-Article-Cisero_s-Feb-2012.pdf
https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard
https://www.netsparker.com/blog/web-security/all-about-pci-compliance-pci-dss-good-bad-insecure/
https://www.information-age.com/pci-dss-assessment-wrong-and-outdated-why-its-time-change-123461536/

[Appendices]
http://www.brokencipher.org/iso27001-and-pcidss/

https://www.riskmanagementstudio.com/why-you-should-integrate-the-pci-dss-and-iso-27001-standards-for-your-data-protection/

https://www.isaca.org/resources/isaca-journal/issues/2016/volume-1/comparison-of-pci-dss-and-isoiec-27001-standards