Dissertation

« Payment Card Industry Data Security Standard - Readiness Project»

By

Vergetis M. Michail

MTE 1306

Submitted in partial fulfillment
of the requirements for the degree of
MSc [Techno-economic Management & Security of Digital Systems],

University of Piraeus,
Department of Digital Systems

Thesis Sponsor: Lamprinoudakis Konstantinos

Piraeus, *December 2015*

Declaration

I hereby declare that this paper is all my own work, that it has not previously been submitted for assessment and that I have not knowingly allowed it to be copied by another student. I understand that deceiving or attempting to deceive examiners by passing off the work of another writer, as one's own is plagiarism. I also understand that plagiarizing another's work or knowingly allowing another student to plagiarize from my work is against the University regulations and that doing so will result in loss of marks and possible disciplinary proceedings.

Abstract

This paper is my thesis as part of my studies at the Department of Informatics, at University of Piraeus for the Postgraduate Programme in “Techno-economic Management & Security of Digital Systems”. Scope of this paper is to introduce to the reader with the basics of PCI DSS and to guide and provide any sort of assistance to organizations willing to achieve compliance with the Payment Card Industry Data Security Standard (PCI DSS). As for its practical section, a PCI DSS readiness project has been delivered to a certain Organization willing to determine its level of compliance and get prepared for the PCI DSS assessment.

Acknowledgments

On the completion of my dissertation I would like to thank the following people for all the help and encouragement they have offered me throughout the Master's course. Many thanks to my supervisor Ioannis Friagkiadakis for his support during the entire project. I would also like to the thank the University of Piraeus and especially the lectures, staff of the department of Digital Systems for everything they have offered me during my postgraduate studies, and finally, my family for all their support.

Table of Contents

Chapter 1

PCI Fundamentals

1.1 History of PCI

The Payment Card Industry Data Security Standard has been developed significantly over the years, especially due to the enormous effort of the major card brands. As a matter of fact, this creation proved to be urgent. At the beginning, and more particular the time period between 1988 and 1998, the reported amount of credit card fraud losses were at 750 million dollars. Not that much, If you consider that the total amount of transactions processed annually valued at hundreds billions of dollars. However, this analogy would soon change with the technological evolution and the appearance of the Internet which introduced to the merchants the numerous abilities through the use of e-commerce. This motion towards the electronic features of online purchases, attracted several fraudsters who found ways to penetrate card processing systems and payment networks for illegal benefits taking advantage of the poorly security mechanisms.

This newly created danger, alerted the major credit card brands with the need to create a standard in order to stop the generation of cybercrime. That is why, on October of 1999 Visa developed the Cardholder Information Security Program (CISP), which was actually the "granddaddy" of PCI DSS and reached version 2.3 in March of 2004, a security standard for merchants performing online transactions. However, the creation of this standard was very difficult and its effectiveness was not the desired because of the differences between the North American and the international guidelines for security. Similar difficulties and failures appeared to other known card brands, including MasterCard, American Express, Discover and JCB which also tried to create their own security standards naming their programs MasterCard's Site Data Protection, American Express' Data Security Operating Policy and Discover's Information Security and Compliance. While having all those failures, the online lost revenue reached the enormous amount of $1.5 billion.

From that time until March 2004, the above mentioned audit programs went through several revisions and continued growing and developing in order to protect sensitive cardholder data. It was at that time, when Visa and MasterCard joined together in an attempt to protect those data. However, that relationship faced some problems because the list of approved vendors was not so well maintained and it was unclear of how a security vendor could get added to that list. As for the remaining card brands, as mentioned above, they all held programs on their own with little cooperation between them and the entire industry. This specific approach created a major problem: Since most of the merchants accepted at that time each one of these individual programs (credit cards), that meant that in order to be compliant each merchant and service provider had to undergo several audits so to prove compliance with each one of them, on a yearly basis, which was obviously costing too much money.

That gap in the creation of a unified security standard, for all these years, resulted in fraudulent online activity by attacks of newly created Trojans from personal computers to payment servers. So, all these would soon come to an end as on December 2004 all the major brands worked together and created PCI DSS 1.0, which

offered us the concept of PCI Compliance which was made mandatory for merchants and any other organization in the payment - processing lifecycle. On that union, VISA and MasterCard took on major duties, bigger than the other brands. More specifically, MasterCard was responsible for the certification of product and companies who are able of fulfilling scanning requirements whereas VISA was responsible for the training and certification of those able to perform the onsite audits.

Upon the creation of the standard, there was still something missing - the issue of the ownership. So, in order to solve the ownership's issue, the PCI Security Standards Council was founded which preserves the ownership, the approved vendor lists, the training programs and any other detail for the program. This council consisted of American Express, Discover Financial Services, JCB, MasterCard Worldwide and VISA International. At that time, all merchants processing at least 20.000 transactions annually had to be compliant with the newly published PCI DSS, but still a lot of them found it difficult to be fully compliant by the deadline. That meant, there was still work to do, so in October of 2006 PCI DSS 1.1 was released. The feature added was that every merchant to be complied should be tested by a professional company for possible security vulnerabilities, which are licensed by the Council. It is worth to mention that, apart from PCI DSS each card brand maintains its own security program regarding protection of sensitive cardholder data including actions like fraud prevention, as shown on the table below.

Card Brand	Additional Program Information
American Express	American Express CardBrand Info
Discover	Discover CardBrand Info
JCB	JCB CardBrand Info
MasterCard	MasterCard CardBrand Info
Visa USA	VISA USA CardBrand Info
Visa Canada	VISA Canada CardBrand Info

Table 1: Brand Security Programs

PCI Council, as mentioned later on, is a technically independent industry standards body providing an oversight to the development of the standard. The community including merchants and providers quickly felt the positive impact of the creation of the council due to the fact that they could finally play a more active role in the compliance procedure and the development of the standard. However, at the end of that year, the world economy faced one of the biggest data breaches, 45 million customer credit card and debit cards were stolen, with the victim being the company TJX which had later made to pay more than $40 million in fines and undergo an independent third party security audit every other year for a period of 20 years. For the next couple of years, professionals started criticizing PCI DSS due to a lack of flexibility in audits and the assessment processes. According to them, the requirements to be met are extremely difficult and demanding and for the most cases PCI compliance costs them about 40% more that the initial estimation. Luckily, at the end of 2007 the so called compensating tools came to save the day and ease the compliance procedure. Those tools are some loopholes that allow enterprises to avoid specific PCI DSS requirements that are proven to hard or costly to be achieved. In addition to that, at the early 2008 council created the PA DSS (Payment Application Data Security Standard). This new sister standard to the PCI DSS is designed to help software vendors and others develop secure applications that don't store sensitive card data such as full magnetic stripe, PIN and CVV2 data.

In October of 2008, PCI DSS 1.2 appears which includes new requirements regarding the 802.1x for wireless network protection and antivirus among other things. At that time, experts estimated that for those controls to be implemented several retailers would have to pay millions of dollars, questioning the entire PCI

specification and the included security procedures. By the next year, several serious data breaches occurred with the largest amount being that of Heartland Payment Systems which lost more than 130 million payment records, despite the fact that the company was fully compliant with the PCI DSS. At June 2010 the council decided to extend the Standard's refresh cycle to three years, in order to offer merchants more time comply between iterations. In fact, the actual lifecycle along with the different steps of the Standard that is being followed can be viewed on the figure below:

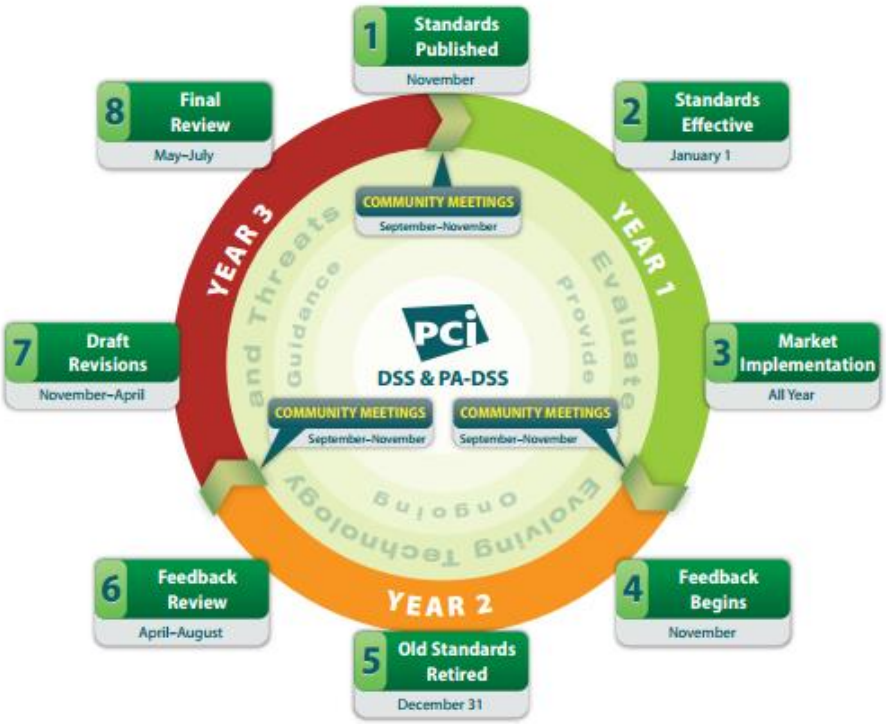


Figure 1: PCI DSS Lifecycle

So, upon update of the Standard's lifecycle, October of 2010 both brought a new version of the PCI DSS which represented a streamline of the assessment process which should ease the compliance stress. At the same time that the new version is released, Verizon releases its own PCI Industry Compliance Report taking advantage of the difficulties companies face to meet compliance with PCI DSS. During the next years, until the next version release, council reveals several guidelines such as new virtualization and tokenization guidelines and further on highlighted the need of encryption when using smartphones and tablets during transactions. According to VISA's report, compliance with PCI DSS reaches its record level with 97% of compliance among merchants of level 1 (explained later on, those who process more than 6 million transactions annually).

Finally, on November of 2013, the latest version of PCI DSS - version 3.0 - is released which points out the need for vulnerability assessments within the company, adds some level of flexibility to requirements regarding passwords and emphasizes on the need of compliance for provider among other things. The council's main target with the creation of that version is to assist companies combine compliance best practices with daily operations. Basically, what PCI compliance is all about is the need for properly securing sensitive data on a credit card. The importance is not only to achieve compliance but also to figure out why there is that need for compliance. Unfortunately, data breaches will still occur but it is crucial for the council and all the brands evolved to learn from each breach resulting into tighter and smarter measures in the upcoming versions of PCI

DSS, with the next coming on 2016. As for the time being, PCI Data Security Standard (PCI DSS) Version 3.1 has been published which includes minor updates and clarifications focusing on SSL vulnerabilities.

1.2 What is PCI DSS?

1.2.1 Electronic Transactions Basics

Before analyzing the standard, let's first understand the basics of a typical payment transaction along with all the needed information around payment cards. As mentioned, the primary goal of the PCI DSS is to protect cardholder data. But, what exactly is that data? Some cardholder data are printed on a card while others are located in digital format on a magnetic stripe or computer chip. The figure bellow, illustrates the types of sensitive information that can be located on such a payment card.

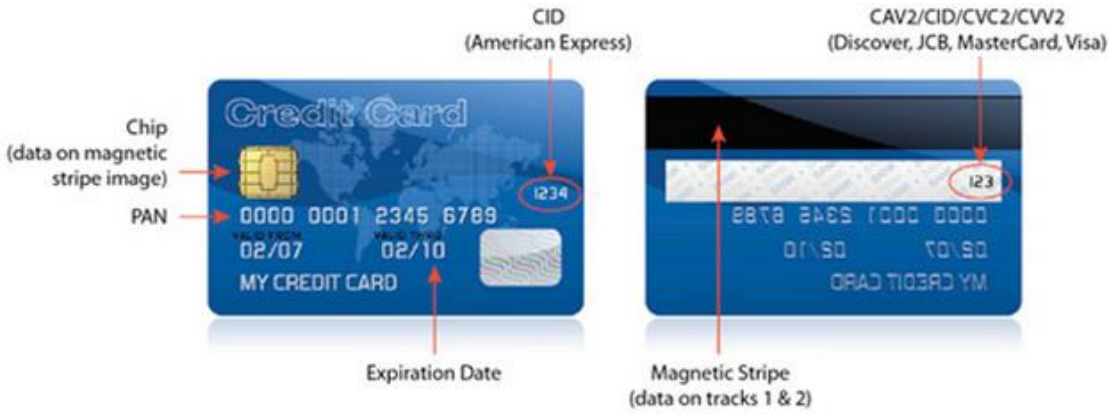


Figure 2: Types of data on a payment card

First of all, cardholder data refers to the primary account number (PAN) of a payment card owned by a specific cardholder, along with the following information:

- Cardholder Name: Obviously the name of the cardholder, to whom the payment card is issued
- Expiration Code: The date until which the payment card is valid
- Service Code: A three/four digit number coded into the magnetic stripe that specifies the acceptance requirements, the authorization processing and the range of services.

As a matter of fact, in order to be aligned and fully understand the process of electronic transactions and the role of PCI DSS, the table below contains some valuable definitions according to the standard's official glossary.

Term	Description
Account Number	The bank card number merely identifies the card, which is then electronically associated by the issuing organization with one of its customers and then to the customer's designated bank accounts. Also known as Primary Account Number (PAN). According to the Council, if PAN is not stored, processed or transmitted then PCI DSS does not apply.

Cardholder	Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.
Cardholder Data	Cardholder data consists of, except from the PAN, the following: cardholder name, expiration date and/or service code
Card Validation Value or Code	This term refers to either: (1) magnetic-stripe data, or (2) printed security features. 1. Data element on a card's magnetic stripe that uses secure cryptographic processes to protect data integrity on the stripe, and reveals any alteration or counterfeiting. • CAV - Card Authentication Value (JCB payment cards) • CVC - Card Validation Code (MasterCard payment cards) • CVV - Card Verification Value (Visa and Discover payment cards) • CSC - Card Security Code (American Express) 2. For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit un-embossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. • CID - Card Identification Number (American Express and Discover payment cards) • CAV2 - Card Authentication Value 2 (JCB payment cards) • CVC2 - Card Validation Code 2 (MasterCard payment cards) • CVV2 - Card Verification Value 2 (Visa payment cards)

Table 2: Payment Card Information

The following table, contains valuable definitions about terms usually used during electronic transactions.

Term	Description
Authentication	It is the act of confirming the truth of an attribute of a single piece of data or entity. Authentication typically occurs through the use of one or more authentication factors like a password, token or biometric.
Authorization	It defines what an individual or program can do after successful authentication.
Card Skimmer	It is a physical device designed to illegitimately capture and/or store the information of a payment card.
Closed Payment System	It is a system in which the card brand act as an acquirer.
Hosting Provider	Offers multiple services to merchants and other service providers and could be a shared hosting provider hosting multiple entities on a single server
Issuing Services	Include among others the authorization and card personalization.
Open Payment System	It is a system in which the card brand doesn't act as an acquirer.
Payment Gateway	It is a service provider that enables payment transactions which are located between the merchant and the processor.
PIN	It is the acronym for "personal identification number." It is a numeric password shared between a user and a system, that can be used to authenticate the user to the system
PIN Block	It is a block of data used that is used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed in order to retrieve the PIN.
POS	It is the acronym for "Point Of Sale"
Processing of Cardholder Data	Any manipulation of cardholder data by a computing resource or on physical premises.
Sensitive Authentication Data	They are those elements of a payment card transaction that are used to verify the identity of the cardholder such as card validation codes, full track data, PINs, and PIN blocks
Settlement	It is a process of transferring funds between an acquiring bank and an issuing bank.
Storage of Cardholder Data	Any retention of cardholder data on digital/ analog media.
Third Party Processor	It is a service provider that participates in any part of the transaction.
Track Data	It is the data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. It can be either the magnetic-stripe image on a

	chip or the data on the track 1 or track 2 portion of the magnetic stripe.
Transmission of Cardholder Data	Refers to any transfer of cardholder data through a part of the computer network or physical premises.
Transaction Data	It is the data related to electronic payment card transaction.

Table 3: Electronic Transaction's Information

At the same pace, the table below contains valuable definitions about terms usually used during electronic transactions concerning the organization.

Term	Description
Acquirer	Also referred to as "merchant bank" "acquiring bank" or "acquiring financial institution." Actually, it is the entity that initiates and maintains relationships with merchants for the acceptance of payment cards.
Issuer	It is the entity that issues payment cards or performs and/or supports issuing services including but not limited to issuing banks and issuing processors.
Merchant	An authorized acceptor of the payment card who receives payment for good and services.
Service Provider	It is a business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. It may also be a company that controls or influences the security of cardholder data. For example, it might be a company that provides managed firewalls, IDS and other services as well as hosting providers and other entities.

Table 4: Electronic Transaction's Information - Organization

In addition to the definitions tables above, the following table of applicability illustrates those commonly used cardholder's features along with the sensitive authentication data regarding PCI DSS's storage and protection demands of them.

Data Feature	Permission of Storage	Demand for Protection
Primary Account Number (PAN)	Yes	Yes
Cardholder Name	Yes	Yes
Service Code	Yes	Yes
Expiration Code	Yes	Yes
Full Magnetic Stripe	No	N/A
Card Validation Value	No	N/A
PIN/PIN Block	No	N/A

Table 5: PCI DSS Table of Applicability

Regarding the protection of cardholder's data and more specific the Cardholder name, the service code and the expiration code, it should be considered that the standard requests their protection as long as those data are stored along with the Primary Account Number. In fact, this protection has to be consistent with the requirements of the standard, as described later on. Apart from that, as easily understood by the table above, storage of the sensitive information available on the payment card is not allowed by the standard following the authorization.

Having analyzed the basic terms that are being used during an electronic transaction and are included in the PCI DSS, we can now review the electronic transaction's process in order to better understand the associated parties required to complete that transaction. So, in general the following diagrams illustrate the steps executed during an electronic transaction and the different parties that participate in it along with the requests according to the standard.

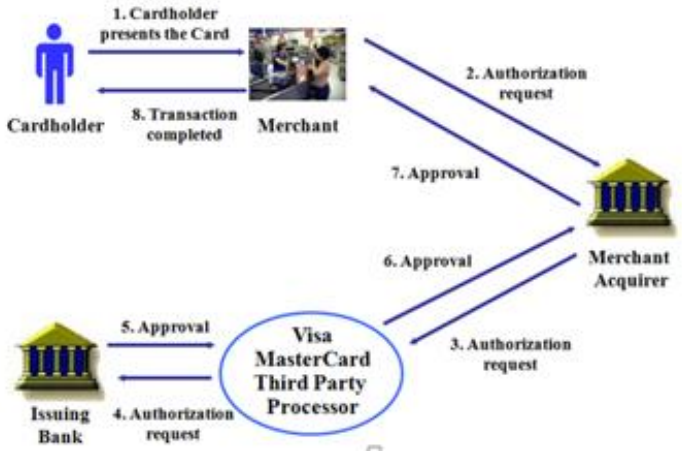


Figure 3: Credit Card Transaction Processing

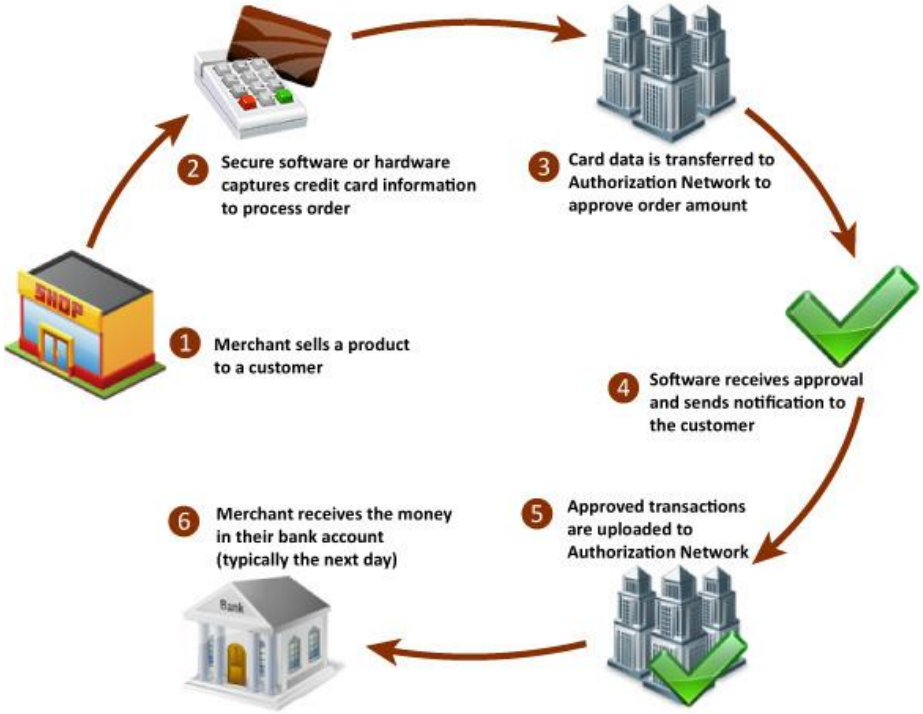


Figure 4: Requirements for Transactions

A typical payment card transaction consists of the following basic steps:

- In the beginning, a cardholder present the payment card to the Merchant starting the transaction process using a secure software or hardware in order to capture the credit card information and process the order.
- Next, the card data is transferred to the Authorization Network to approve the order amount.
- That Network, consists of the Merchant Acquirer through which the authorization requests goes to a Visa, MasterCard Third Party Processor and to the Issuing Bank which approves the transaction sending the approval back to the Merchant and more specifically to the software performing the transaction. Later on, a notification is sent to the customer about the successful transaction.
- All the approved transactions, are uploaded to the Authorization Network.
- Finally, the merchant receives the money in their bank account, usually within the next day.

Apart of the obvious authorization step that is being executed during the transaction, there are 3 further steps that are not quite obvious.

- Batching: Authorized transactions are stored in "batches", which are sent to the acquirer. Batches are typically submitted once per day at the end of the business day. If a transaction is not submitted in the batch, the authorization will stay valid for a period determined by the issuer, after which the held amount will be returned to the cardholder's available credit. Some transactions may be submitted in the batch without prior authorizations, these are either transactions falling under the merchant's floor limit or ones where the authorization was unsuccessful but the merchant still attempts to force the transaction through.

- Clearing: During this phase, the acquirer sends the batch transactions through the credit card association, which debits the issuers for payment and credits the acquirer. Essentially, the issuer pays the acquirer for the transaction.

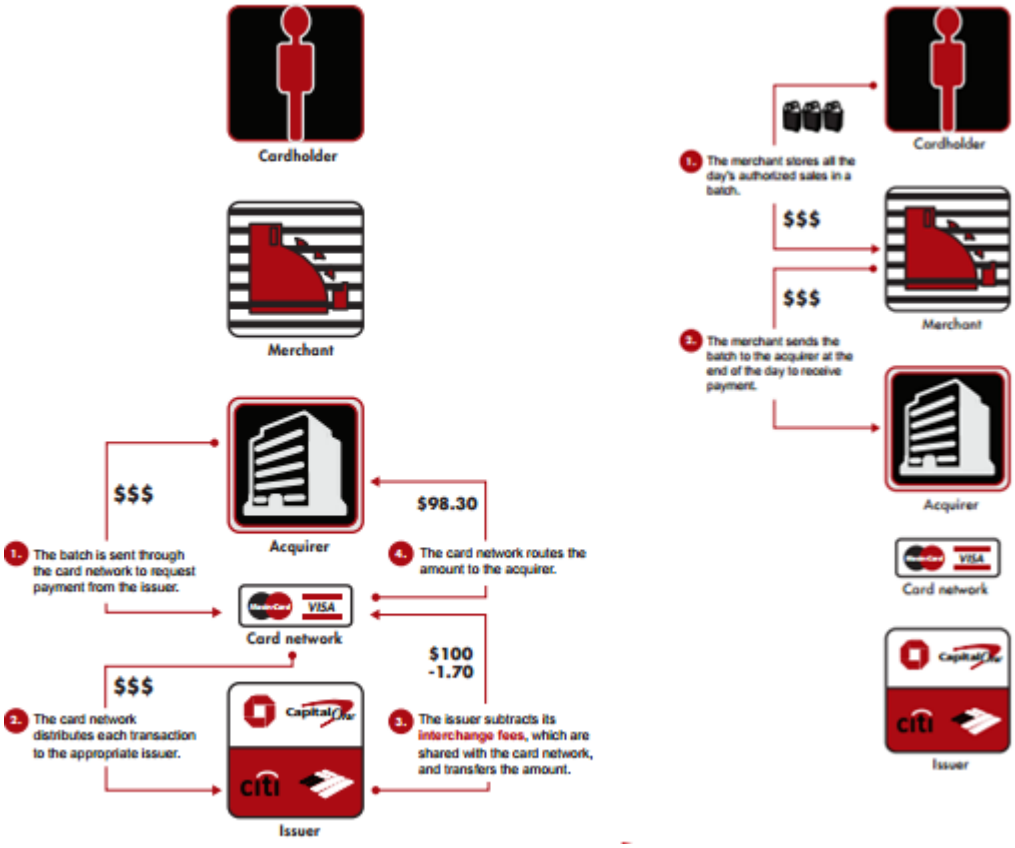


Figure 5: Batching - Clearing phases

- Funding: Once the acquirer has been paid, the acquirer pays the merchant, receives the amount totaling the funds in the batch minus either the "discount rate", "mid-qualified rate", or "non-qualified rate" which are tiers of fees the merchant pays the acquirer for processing the transactions.

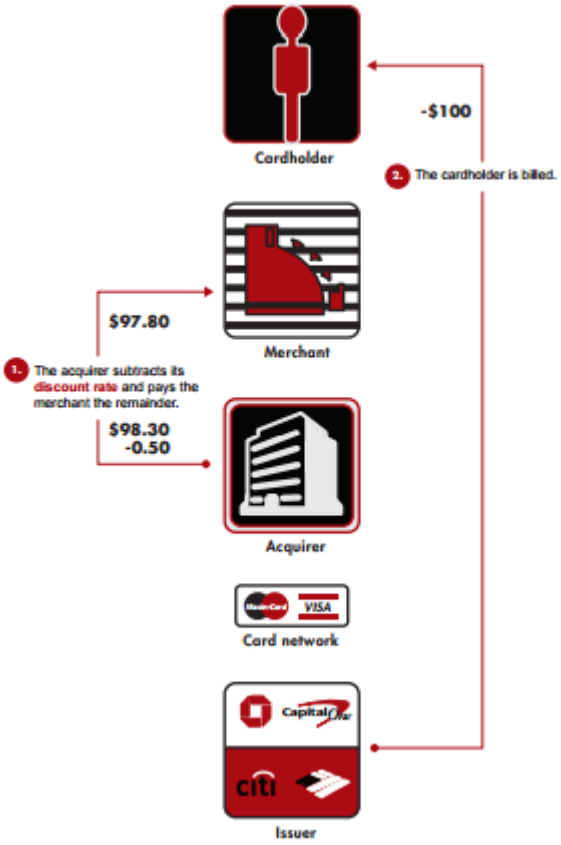


Figure 6: Funding Phase

1.2.2 Credit Card Fraud and Identity Theft

It is an undeniable fact that credit card fraud and identity theft are real and critical threats for merchants and consumers. Pretty much, for everyone involved in the storing, processing and transmitting of cardholder data. Apart from that, the evolution of payment technology through its various features such as online, mobile and wireless capabilities that it offers, has complicated the methods used by fraudsters who are willing to access sensitive information. As a matter of fact, those criminals have understood the enormous amounts of money that they could steal, without even being noticed. So, the capability of understanding and reacting to every attempt of credit card fraud and ID theft is crucial for the overall secure function of the organization.

First of all, let's discuss the terms mentioned and better understand the different types of those threats to cardholder data. In case that an unauthorized person accesses a consumer's personal information such as social security numbers, credit card numbers and account numbers (please refer to the previous section for the types of cardholder data) then it would be possible for him to identify who really the consumer is. With that kind of information in the fraudster's hands, he/she can proceed to several illegal actions pretending to be the actual owner of that information. The ways through which that person gets access to that kind of information varies including of course any possible data breach containing cardholder sensitive information. This kind of threat is an enormous problem for merchants and consumers which unfortunately grows year after year.

Unfortunately, as already mentioned, the rise of the technology has given attackers various methods for attacking cardholder data. That often makes the style of the attack more high tech and as a result more

effective. Those methods may include malicious software which is called *malware* and can access sensitive information when accessing the victim's computer. Another possible way a fraudster could use is through *phishing scams* which occur online and often through the use of emails sent to the consumer. Those emails are most of the times written to seem like coming from a trustworthy source, often someone familiar to the consumer. In that email, the victim is requested to provide account numbers, credentials and generally any sensitive information. In addition to that, those emails might contain links directing the victim to fake websites used to steal data on behalf of the identity thieves. Of course, consumers must not, at any time, provide such valuable information to anyone, especially via email unless they are sure about the source of the email.

After accessing sensitive cardholder data, by using several methods as described above, the thief might create *fake credit cards* using the stolen information. This particular threat is called *counterfeiting* and involves taking a real credit card and the information from the magnetic strip in order to create the fake one. That is why real credit cards have special features on them that are difficult to replicate like holograms and other characteristics.

Those several techniques used by malicious attackers in order to gain access to sensitive cardholder data and steal large amounts of money has resulted into millions of account records compromised. As mentioned in the history section of PCI DSS, those several data breaches resulted into millions of dollars losses for the companies being compromised along with several other enormous side effects as described later on in the section describing the benefits of PCI DSS compliance. So, as easily understood by the seriousness of the attacks that might harm a company and its stored or processed cardholder data, it is really crucial to take the appropriate steps in order to protect this data and any other sensitive information related to it.

1.2.3 Introduction to the Standard

As mentioned in the previous chapter of the roots of PCI DSS the technological evolution and the appearance of e-commerce has lead into the rapid use of credit cards in every day transactions worldwide. In fact, the average daily transaction's rate on a world scale is estimated around billions. As easily understood, those numbers attract plenty of fraudsters because the information available in the credit cards is very useful for such malicious causes giving them direct access to the victim's account without even being noticed. As described in the previous sector, several electronic frauds through hacking techniques have occurred causing the compromise of millions of debit and credit cards with enormous side effects both economical and to the reputation of card brands and the entire Payment Card Industry.

All the above incidents along with the resulted rise of information security, disclosure laws, privacy concerns, the mentioned impact of e-commerce in today's society and several other situations, addressed for a joint effort in order to handle and protect cards and cardholder data. In fact, it is undoubtedly that in the world of electronic transactions no risk is acceptable, so the need of protecting cardholder data cannot be overseen.

In today's world, every one of us as consumers benefit from the convenience and efficiency that electronic transactions offer us but we assume and demand those transactions to be made securely. For sure, if we are not happy with the level of security provided we can easily turn to another vendor to continue using those services. From the other side as well, businesses want to keep their customers satisfied and eventually increase their profits. To do so, they have to secure customer's data and protect them from potential payment card fraud and abuse. So all the above in addition with the pressure to the payment card industry from banks, service providers and merchants to improve their data security, resulted into the **Payment Cards Industry Data Security Standard (PCI DSS)**, commonly known as PCI compliance, creation. In fact, the PCI Security Council

which was formed by all the major card brands including VISA, American Express, Discover Financial Services, JCB and MasterCard developed the standard to help facilitate the broad acceptance of consistent data security rules on a global basis guarantying that credit card information is sufficiently protected and to protect the entire industry.

Going deeper into the standards characteristics, *PCI DSS* is a widely accepted set of policies, processes and internationally security requirements designed to improve the security of credit, debit and cash transactions. In fact, this standard is intended to help all companies that store, manage, transmit or process cardholder data, such as payment card numbers or primary account numbers. To make it clearer, if that company accepts even one card for payment, it has to comply with the PCI DSS standard. Regardless of its respective level it has to comply with the all the requirements of the standard as it is published. Most of the financial institutions, don't maintain a dedicated infrastructure to handle those card transactions and that is the reason that PCI DSS affects the entire technological infrastructure, strongly affecting the organizations determined to comply with it.

1.2.4 PCI DSS Overview

The *PCI Data Security Standard* is the key standard for protecting cardholder data while at the same time protects any merchant, service provider and financial institution that stores, processes or transmits those data. It is a widely accepted group of policies and procedures designed to enhance the security of credit, debit and cash card transactions and protect the cardholders from abuse of their personal sensitive information.

The standard describes the technical and operational system components that form or are connected to the cardholder data. More specifically, PCI DSS consists of six goals that include 12 relevant requirements which can be briefly viewed on this sector. A further analysis of those requirements is made in the next chapter.

Those 12 detailed control objectives can be grouped on the following six broader categories that consist of the goals that the standard has set:

1. Build and maintain a secure network
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

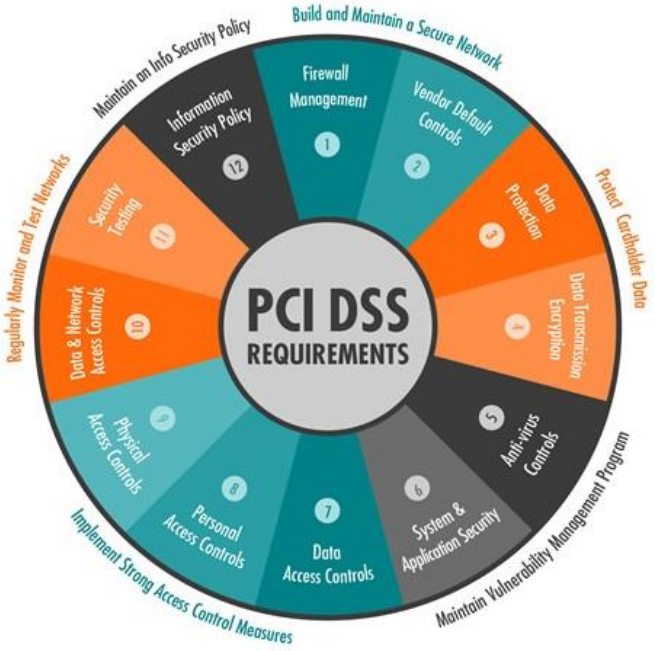


Figure 7: PCI DSS Requirements

First of all, the standard demands the existence of a secure network through which the electronic transactions can be executed. This particular requirement involves the probable use of *firewalls* that can be really efficient to secure the network without disturbing the overall function of the business processes. However, there are some things to consider for enhancing the security of the network such as not using the default authentication data (passwords) and easily change of those data according to the needs.

Secondly, the next goal of the standard is that of protection for the cardholder data meaning that this information must be protected whenever it is stored. Wherever this information is saved, this must be done by a secure manner in order to avoid anyone unauthorized from getting access to it. In addition to that, encryption while transmitting this data is crucial for its protection.

According to the third goal of the standard, systems have to be protected against the activities of malicious hackers by using antivirus software, antispyware and any other antimalware software. Apart from that, any used application by the organization must be free of bugs and fully patched covering any potential vulnerability that might be exploited by anyone malicious.

Fourthly, according to the next objective of the standard, any access to information should be limited and controlled. Cardholders specially must not present any information to businesses that they don't have to and it is not needed for the electronic transaction. In addition, any user that has access to the system must have a unique identification name in order to be fully audited at any time. The suggested restriction to cardholder data might be either physical or electronic.

According to the fifth objective, networks must be regularly monitored and tested in order to guarantee that all the implemented security measure and operation functions as designed. As mentioned in the third goal, any antivirus used must be checked constantly to be sure that it is updated with the latest releases and must be used at a regular basis to scan the entire network.

Finally, an information security policy must be determined, maintained and implemented within the company and anyone involved, as designed. Scenarios for non-compliance might prove to be really helpful, such as audits and penalties.

All the above categories are the critical foundation for creating, protecting, maintaining and operating in a secure manner any cardholder data at any time. The mentioned objectives of the PCI DSS can be easily viewed on the following table.

Objective	Requirements
Build and maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
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
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Table 6: PCI DSS Objectives and Requirements

1.2.5 Standard's Scope

As already mentioned, PCI DSS applies to all system elements that participate, by any means, to the cardholder environment. Those elements vary from network devices to applications. Being more accurate, those elements might include among others, a server of any kind, a firewall, a virtual machine, an internal/external application and literally any device that is located into the cardholder environment or just participating with it at any possible way.

Determining the scope is actually a major success factor in achieving the desired compliance with the PCI DSS and as most people say, among the most challenging ones. That is why, the first step in any PCI assessment is

to determine the *extent* of the organization's environment. Within that determination, a key point is to identify who is responsible to identify and state the actual cardholder environment. Another question to be asked, is how the organization proves that the identified environment is the correct one. A hint for the organization to achieve this is to make and document a *data flow* in order to correctly identify all the components and eventually the cardholder environment. A final step, regarding the network segmentation is to identify the extent of the cardholder environment in order to confirm that cardholder data is not stored at any other point besides the cardholder environment.

Regarding the transmission of cardholder data, the Council is strict about its statements. Networks that are used for transmission of the data are always in the scope of PCI DSS. That applies to any instance, even if there is a Managed Service Provider responsible for that transmission between the endpoints. Encryption of the data is of course without doubt urgent retaining the confidentiality and integrity of the data but that does not take those endpoints out of scope. When it comes for wireless networks, according to the standard, the PCI DSS requirements and testing procedures apply and must be performed. However, the standard advices the use of wireless networks only after serious thoughts.

Another major component is obviously the applications that process, store or transmit cardholder data, which are of course within the scope of the standard. However, this is not so easy, the PA DSS standard described later on has made things easier, because most organizations find it impossible to determine the data flow within those applications. That happens, obviously because they are not the ones responsible for the development of those apps.

Having covered the basics of determining the standard's scope, it is really helpful to have in mind the following rules that describe what exactly must be in the scope of PCI compliance:

- The cardholder data environment consists of people, processes and technology that manage cardholder data
- The standard applies to all system components that are included or interact with the environment at any possible way
- The standard applies as well to all systems involved in managing the security of any other in-scope system

Concluding this particular section, an example to help determine the scope might prove to be really helpful: If there is a system on a network that does not store, process or transmits card data, but this system is able to communicate with another device that stores, processes or transmits cardholder data then that particular system should be in the scope of compliance. However, if there is a machine on that network that cannot connect or interact to any other system that stores, processes or transmits cardholder data nor it does it itself then that particular component is out of scope. Of course, that is a simplified example of determining what is in scope because there are a lot of complexities related to determining the scope of PCI DSS.

1.3 PCI Standards Combine

The PCI standards present technical and operational requirements for cardholder data protection which apply to anyone who stores, process or transmits them. These standards are focused on merchants and processors, software developers and manufactures (for definitions about that terms please refer to Electronic Transactions

Basics). All these different roles form the named 'ecosystem' of the retail payment devices, the applications, the card processing infrastructure and the organizations that perform all the related to them activities.

The core standard, is the PCI Data Security Standard (PCI DSS) which focuses mainly on merchants and processors. It is being analyzed throughout this current document, so any further analysis at this point on the standard is not needed. The other two main standards that all together form the Payment Card Industry Security Standards are analyzed on this section. The below figures represents all the standards combined together:

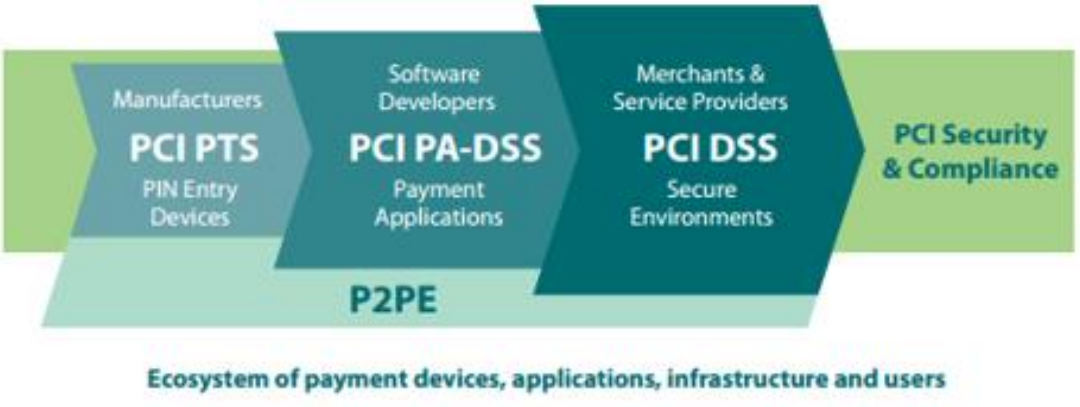


Figure 8: Payment Card Industry Security Standards

1.3.1 PIN Transaction (PTS) Security Requirements

Until 2004, each of the major card brands had their own PIN Entry Device (PED) requirements regarding security. But In 2004, Visa and MasterCard work together to come up with a unified standard and that is how PCI PED was born. The first release of PCI PED harmonized the requirements of both Visa and MasterCard and provided a baseline that worked as a minimum level of security required in any PIN accepting device. This particular standard tried to balance the cost of compliance with that of the expense that a criminal would need to invest in an attack on a Pin Entry Device.

Lately, attackers have begun focusing on Point Of Sale hardware and software in order to gain access to sensitive cardholder data. They took advantage of the fact that these devices do not offer encryption technology. Apart from that, they often automatically print the consumer's Primary Account Number (PAN) on the receipts and are not configured to clear information in memory on a regular basis. These vulnerabilities made those devices an easy target, and that is why PCI Pin Transaction Security (PTS) requirements focus on protecting them. Every merchant is obligated to use only approved PIN entry devices by the PCI Security Standards Council. For that reason, there is a specific list containing the approved devices uploaded on the official site Approved PTS Devices.

As mentioned in the beginning, security requirements for each type of device were covered separately. However on May 2010 the council announced the PTS requirements that according to the council: "restructures the existing security requirements, simplifying the evaluation process by combining the three

separate sets of Point of Interaction (POI) PIN acceptance product-type evaluation requirements into one, covering attended and unattended PIN entry devices along with encrypting PIN pad (EPP) requirements."

So, organizations were made to look after the physical security of devices first, and then focus on logical security, meaning that all the used devices must be physically secured in order to deter them from being stolen or replaced by phony devices. Apart from that, merchants have to use any latest updated device enhancing by that way the security of the device.

To make things clear, the goal of this PCI Standard is the following: PIN Entry Device (PED) standard was created in order to improve the security features and the management of point-of-sale (point-of-interaction) devices accepting the Personal Identification Number (PIN) during the execution of a transaction. Manufacturers have to provide a product with an uncompromised physical and logical security, either during the operation of manufacturing or the transportation to the merchant eventually using the device, as indicated in the diagram below:

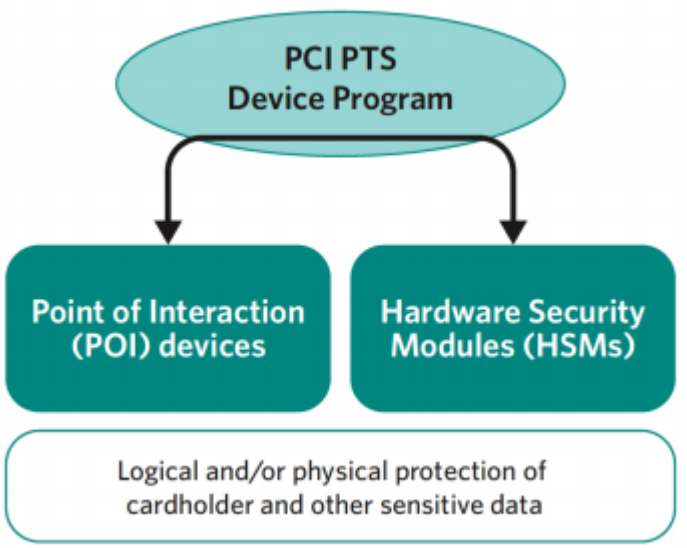


Figure 9: PCI PTS Device Program

Standard's Security Requirements focus mainly on the device characteristics impacting the security of the PIN Entry Device used by the cardholder. Those requirements also include management features for the PIN Entry Device until the initial key loading. However, the evaluation for this particular standard contains only checking for the device characteristics.

1. *Device characteristics* are those attributes of the device that define its physical and its logical characteristics. The physical security characteristics of the device are those that can defense a physical attack on the device. On the other hand, logical security characteristics include some functional capabilities such as allowing the device to print the PAN in cleartext on the receipt.
2. *Device management* considers how the device is produced, controlled, transported, stored, and used throughout its lifecycle. If the device is not properly managed, unauthorized modifications might be made to its physical and/or logical security features.

Undoubtingly, security is a never-ending race against potential attackers. As a result, it is necessary to regularly review, update, and improve the security requirements used to evaluate Point of Interaction devices and their

hardware security modules. That is why, the council has decided that all relevant security requirements and associated test requirements have to be updated every three years. The following diagram describes the three-year cycle of Security Requirements for this particular standard.

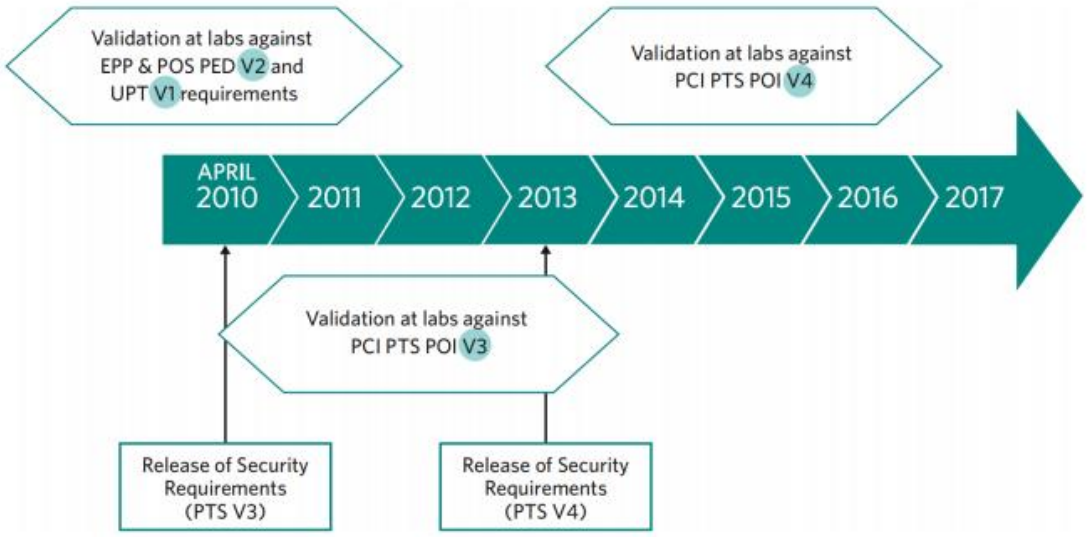


Figure 10: Lifecycle of PTS Requirements

1.3.2 Payment Application Data Security Standard (PA-DSS)

As with the others standards described, a certain point of potential attack addressed the need for a standard that would cover this certain vulnerability. This certain point is through the payment applications that are used to store, process or transmit cardholder data during authorization. The Payment Application Data Security Standard (PA-DSS) is a set of requirements that are intended to help software vendors develop secure payment applications that support PCI DSS compliance. This standard, applies to third-party applications that store, process or transmit payment cardholder data as part of an authorization of the user. As with the other described standards, the Payment Card Industry Security Standards Council maintains PA-DSS, which was published in 2008 as a replacement to Visa's Payment Application Best Practices (PABP) which was Visa's attempt to guide software vendors in creating secure applications.

PA DSS focuses mainly in preventing the compromise of full magnetic stripe data stored on the back of the payment card and the protection of the computer chip embedded on the front of some payment cards (please refer to Figure 2: Types of data on a payment card). So, merchants are obligated to use approved, by the council, payment applications that comply with the PA DSS standard (please refer to the uploaded list of the Validated Payment Applications).

More particularly, to achieve PA-DSS compliance, a software provider must have all the used applications audited by a PA-DSS Qualified Security Assessor. The standard's requirements include the following, as published on the standard itself:

- Do not retain full magnetic stripe, card validation code or value, or PIN block data.
- Provide secure password features.
- Protect stored cardholder data.
- Log application activity.

- Develop secure applications.
- Protect wireless transmissions.
- Test applications to address vulnerabilities.
- Facilitate secure network implementation.
- Do not store cardholder data on a server connected to the Internet.
- Facilitate secure remote software updates.
- Facilitate secure remote access to applications.
- Encrypt sensitive traffic over public networks.
- Encrypt all non-console administrative access.
- Maintain instructional documentation and training programs for customers, resellers and integrators.

Whereas, the scope of a PA-DSS assessment, should cover the following:

- All payment application functionalities, including but not limited to end-to-end payment functions, input and output, error conditions, interfaces and connections to other files, systems, payment applications and their components, all cardholder data flows and finally encryption and authentication mechanisms.
- Guidance to the payment application vendor in order to provide to customers and integrators/resellers the certainty that the customer knows how to implement the payment application in a PCI DSS-compliant manner and he/she was clearly told that certain payment application and environment settings may prohibit their PCI DSS compliance.
- All selected platforms for the reviewed payment application version.
- Tools used by or within the payment application to access and/or view cardholder data.
- All payment application related software components, including third-party software requirements and dependencies.
- Any other type of payment applications necessary for a full implementation.
- Vendor's versioning methodology.

Using a PA-DSS compliant application by itself does not make an entity PCI DSS compliant, because that application must be implemented into a PCI DSS compliant environment and according to the PA-DSS provided by the payment application vendor. The above mentioned requirements are extracted from the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures. As already mentioned, all the applications that store, process, or transmit cardholder data are within the scope of PCI DSS assessment, including those applications that have been validated to PA-DSS.

The PCI DSS assessment should confirm that this payment application is properly configured and securely implemented according to PCI DSS requirements. In case that the payment application has been customized, a more in-depth review will be required during the PCI DSS assessment, as the application may no longer characterize the application that was validated by the PA-DSS.

1.3.3 Point-to-Point Encryption (P2PE)

The PCI Point-to-Point Encryption (P2PE) Standard contains detailed security requirements and testing procedures for application vendors and providers of P2PE solutions to ensure that their solutions comply with the necessary requirements for the protection of cardholder data. But what is actually the point-to-point encryption solution? It is a blend of secure devices, applications and processes that have the ability to encrypt

data from the point of interaction (POI) until the data comes to the solution provider's decryption environment.

According to the council, each PCI P2PE solution must include: As already mentioned, secure encryption of payment card data at the point-of-interaction, validated applications for that cause at POI, management of the encryption and decryption device as far as security is concerned and finally, use of several encryption methodologies.

To make things clear, in a compliant Point-to-Point Encryption environment, sensitive cardholder data is encrypted from the point of interaction at the merchant and decrypted only within the secure boundary of a FIPS 140-2 Level 3 or PCI HSM validated hardware security module (HSM). So, by implementing P2PE, organizations can enhance their data security infrastructure while simultaneously reducing both the scope and the expenses for the PCI DSS compliance procedure. As happens, with QSA and ASV, P2PE assessors are qualified by the Council to evaluate P2PE solutions and applications.

1.4 Operation of Compliance

1.4.1 Basics of Compliance

As mentioned in previous sections, in order to achieve PCI DSS compliance, all acquirers, issuers, merchants and service providers who store, process or transmit cardholder data must adhere to PCI DSS requirements (please refer to PCI DSS Overview) set by the PCI Security Standards Council. By complying with this standard, all the above entities can protect both their business and their customers while advantaging the various benefits offered by that standard, in terms of security. However, the process of compliance to PCI DSS is not that easy-going (not easy at all) and demands a series of steps and accomplishments in order to finally achieve compliance with it.

In general, according to the organization's merchant or service provider level, the validation of compliance changes either to an annual on-site PCI audit or a Self-Assessment Questionnaire (SAQ). Apart from that, depending on that level, the organization should present the results of a quarterly network scan executed by an Approved Scanning Vendor (explained later on), present the results of internal vulnerability scans and results from application and penetration tests. All these mean that, in order for the company to achieve compliance, it must confirm to the card brands that all the intended by the standard actions have been implemented.

But let's take the different aspects of the procedure of compliance one at a time. First of all, according to the Standards Security Council the lifecycle of the PCI DSS compliance consist of three on-going steps (see Figure 11: PCI DSS Compliance Steps): First of all, at the stage of *assess*, the company has to identify all locations that contain cardholder data, writing down all the IT assets and procedures in order to find any possible vulnerability that could affect the cardholder data posing risks to the security of cardholder data that is transmitted, processed or stored by the business. Apart from that, the company should know that its liability for PCI compliance also extends to third parties involved with the process flow, so the company must also confirm that each one of these third party is compliant with PCI DSS. Moving on, after having identified every possible vulnerability the company has to *perform any action to remediate any of these vulnerabilities*. In

addition, any unnecessary cardholder data storage has to be removed and implement the business's processes in a secure manner. This particular step, may include several different actions such as scanning of the network with software tools that analyze infrastructure and find known vulnerabilities, classifying and ranking of the found vulnerabilities to help prioritize their remediation, applying patches, fixes, workarounds and any other possible action helping to remediate the discovered vulnerabilities. A possible re-scan of the network after performing any possible remediation action might be extremely useful. Finally, during the stage of *reporting*, the company shall proceed into documenting assessment and remediation details and submit any needed compliance report (according to its level – quarterly scan report) both to the acquiring bank and to the global card brand which must completed by an Approved Scanning Vendor or use SAQ for annual attestations.

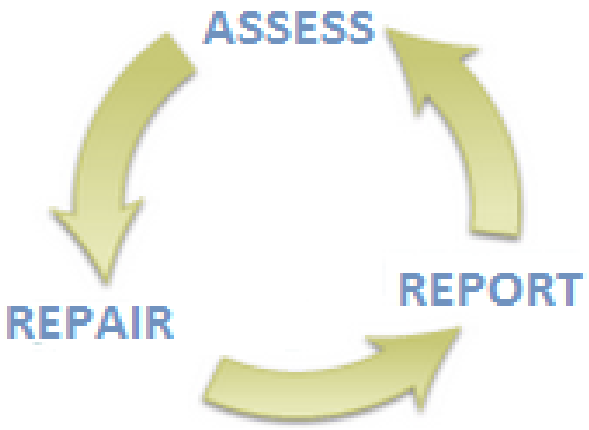


Figure 11: PCI DSS Compliance Steps

Let us see all the above in more detail. As already mentioned above, in order for a company to comply with the PCI DSS requirements it can hire a **Qualified Security Assessor** (QSA) who is a data security firm qualified by the council in order to perform on-site PCI DSS assessments and guidance to any company willing to comply with the standard. In general, QSA can verify all technological information supplied by the company, confirm that the company meets the standard's requirements (on-site when needed), validate the scope that the company has determined, evaluate the compensating controls (explained later on) and finally produce the **Report On Compliance** (ROC) which is a kind of assessment form that is created either for evaluation or to be provided to the legitimate authorities stating that the company is compliant with the standard and can of course be used at any point in the future. Another kind of report to validate compliance (stage 3 of the figure above) is the **Self-Assessment Questionnaire** (SAQ) which can be also used internally by the company because, in contrast with the ROC, it doesn't have to be validated by a third party. This validation tool contains a series of yes-no questions for each PCI DSS requirement and comes with different types according to the merchants environment. Finally as far as the QSA is concerned, choosing an appropriate one is not that easy and most of times costs serious money, but it is crucial for the PCI DSS compliance of the company. That is because, the compliance process is far more than just a project. It is actually a whole transformation process. So, an external help by a QSA is more than helpful, no matter how much it costs. Of course, the decision of hiring a QSA depends in a series of factors such as the amount of resources that the company has decided to spend on PCI DSS compliance. In the possibility, that the company decides that it can achieve the compliance by itself, there must be the certainty that the company's personnel is capable of that. Because in a possible failure, the costs might be even higher. So, that risk in addition to the overwhelming feeling that companies have when faced with the PCI DSS compliance procedure makes them seek for assistance.

Another crucial decision that the company willing to achieve compliance with the PCI DSS, is to choose an appropriate **Approved Scanning Vendor** (ASV) which is a security firm that validates compliance with the standard's external network scanning requirements. The ASV can either use its own software to perform those scans or use some of the approved software for that reason. Their responsibilities can include several actions such as different scanning procedures and tools, associated scanning reports and the process for exchanging information between the scanning vendor and the scan customer. In addition, an ASV can submit compliance reports to the acquiring institution on behalf of a merchant or service provider. However, its actions cannot result system reboot, DNS routing, switching and address resolution and in general any action with possible side-effects like DOS, buffer overflow, bottlenecks etc.

1.4.2 Levels of Compliance

As mentioned earlier before, the actual mechanism for PCI DSS compliance depends on the company's classification, meaning the actual level that the company needs to comply. This classification, is based on the amount of credit card transactions made. To help determine that level, please refer to the following tables for merchants and service providers:

LEVEL	VISA	AMEX	DISCOVER	JCB	MasterCard
1	Any merchant-regardless of acceptance channel-processing over 6,000,000 Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.	Merchants processing over 2.5 million American Express Card transactions annually or any merchant that American Express otherwise deems a Level 1	Merchants are currently not categorized into levels based on transaction volume. Discover takes a "risk based approach" for validating compliance.	Merchants processing over 1 million JCB transactions annually, or compromised merchants	Merchants processing over 6 million MasterCard transactions annually, identified by another payment card brand as Level 1, or merchants that have experienced an account data compromise
2	Any merchant-regardless of acceptance channel-processing 1,000,000 to 6,000,000 Visa transactions per year.	Merchants providing 50,000 to 2.5 million American Express transactions annually or any merchant that American Express		Merchants processing less than 1 million JCB transactions annually	Merchants processing 1 million to 6 million MasterCard transactions annually

		otherwise deems Level 2			
3	Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year.	Merchants processing less than 50,000 American Express transactions annually		N/A	Merchants processing 20,000 to 1 million MasterCard e-commerce transactions annually
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants- regardless of acceptance channel- processing up to 1,000,000 Visa transactions per year.	N/A		N/A	All other MasterCard Merchants

Table 7: Merchant Levels

As for the service providers, VISA categorizes the different levels of service providers for purposes of compliance, as shown on the table below:

Level	Canada, CEMEA, Europe, USA	Asia Pacific	Latin American/Caribbean
1	All VisaNet processors (member and non-member) and all payment gateways	Large: Service Providers processing over 600,000 Visa transactions annually	All VisaNet processors (member and non-member), payment gateways, and Internet Payment Service Providers regardless of transaction volume
2	Service Providers (agents) not in Level 1 that store, process, or transmit > 1 million accounts/transactions annually	Medium: Service providers processing between 120,000 and 600,000 Visa transactions annually	N/A
3	Service Providers (agents) not in Level 1 that store, process, or	Small-Service Providers processing less than 120,000	N/A

	transmit < 1 million accounts/transactions annually	transactions annually	

Table 8: VISA Service Provider Levels

All the remaining major card brands, define their service provider levels are shown on the below table.

Level	AMEX	Discover	JCB	MasterCard
1	All Third Party Processors (TPP) and Payment Service Providers (PSPs)			All Third Party Processors (TPP) and all DSE's that store, transmit, or process greater than 1,000,000 total combined MasterCard and Maestro transactions annually. Additionally, all "compromised TPPs and DSEs"
2				All DSE's that store, transmit or process less than 1,000,000 total combined MasterCard and Maestro transactions annually

Table 9: Cards Brands Service Provider Levels

Having determined the level of classification both for merchants and service providers, the following tables contain their validation requirements according to the different levels that they have. So, for merchants those different validation requirements are shown on the following table.

Level	AMEX	Discover	JCB	MasterCard	VISA
1	Annual onsite review by QSA (PCI DSS Assessment) and Quarterly Network Scan by ASV	Quarterly Network Scan by ASV AND one of the following: • Annual onsite review by QSA-PCI DSS Assessment • Annual Self-Assessment Questionnaire	Annual onsite review by QSA (PCI DSS Assessment) and Quarterly Network Scan by ASV		
2	Quarterly Network Scan by ASV	Annual Self-Assessment Questionnaire and Quarterly Network Scan by ASV			
3	Quarterly Network Scan by ASV	Quarterly Network Scan by ASV AND one of the following:	N/A	Annual Self-Assessment Questionnaire and Quarterly Network Scan by ASV	

		• Annual onsite review by QSA- PCI DSS Assessment • Annual Self-Assessment Questionnaire		
4	Quarterly Network Scan by ASV	N/A	N/A	Annual Self-Assessment Questionnaire and Quarterly Network Scan by ASV

Table 10: Card Brands Merchant Validation Requirements

As for the service providers, their validation requirements for the PCI DSS can be viewed on the two following tables. For the VISA, those requirements are the ones shown below.

Level	Canada, Europe and USA
1	Annual onsite review by QSA Quarterly network scan by ASV Annual Self-Assessment Questionnaire (Canada: SAQ required and must be reviewed by QSA)
2	Annual onsite review by QSA Quarterly network scan by ASV Annual Self-Assessment Questionnaire (Canada: Must be reviewed by QSA)
3	Annual onsite review by QSA Quarterly network scan by ASV Annual Self-Assessment Questionnaire (Canada: Must be reviewed by QSA)

Table 11: VISA Service Provider Validation Requirements

The remaining major card brands, have created the following validation requirements for the service providers willing to comply with PCI DSS.

Level	AMEX	Discover	JCB	MasterCard
1	Annual on-site review by QSA (or internal auditor if signed by officer of merchant company) Quarterly network scan by ASV	Quarterly network scans by ASV AND one of the following: Annual on-site review by QSA (or internal auditor if signed by officer of Service Provider) Annual self-assessment questionnaire	Quarterly network scans by ASV and Annual on-site review by QSA	Annual on-site review by QSA AND Quarterly network scan by ASV
2				Annual self-assessment questionnaire AND Quarterly network scan

Table 12: Card Brands Service Provider Validation Requirements

1.4.3 Compliance Walkthrough

As easily understood so far, compliance for a company to PCI DSS can proved to be a completely nightmare. Standard's requirements are chaotic for a company willing to comply with it. In this particular sector, there are several steps that every organization can easily follow and make compliance procedure an easier way to live.

In general, the initial step for a company to make is of course whether it really needs to comply with the standard. Having determined that it actually needs to meet compliance with PCI DSS there should be some thought about the level of compliance as thoroughly described in the previous section. After having determined that level, a useful tool that could be used in order to determine how many new policies and procedures should be created and put in action is the SAQ already mentioned. That way, the company can easily understand what percentage of compliance already the company meets.

After that, the thought should be if compliance with other different standards that the company has may overlap those of PCI DSS. So, by determining this the whole process of compliance might proceed in a more quick way because some of the already implemented requirements for other standards may be the same with those of PCI DSS. For example, both HIPAA and PCI DSS have some rules for encryption. So, by collecting all the information needed about the HIPAA compliance already met, the company might find out that nothing further needs to be implemented in order to meet this particular PCI DSS requirement.

Having a general idea of the initial steps for the PCI DSS compliance, let's have a closer look on the PCI DSS needed steps in order to comply with the standard. First of all, as already mentioned, the whole process of compliance is very demanding both in terms of time and more basic - money. This means that in order for the compliance process to be successful, there must be the appropriate corporate sponsorship. Apart from the financial terms, the senior management must support the whole process and fully understand the need for compliance with the standard and not just by regulations obligation. Another tip is that as many as senior staff is onboard with the process the better and more successful the whole process will be.

In general, this specific project of PCI DSS compliance has to be managed appropriately in terms of time and resources management. It is essential for the project to set expectations, goals and milestones, like any other project of the same significance value. Firstly, the compliance team must set the appropriate actual expectations and share those expectations to the management in order for everyone to be aligned to what to expect. In addition to that, it is really important to set any goal and milestone about anything to be implemented. Any goal - milestone, and their prerequisites, should be assigned to members of the compliance team moving the whole project towards the right direction.

Having now, the appropriate corporate sponsorship in our hands, we can proceed to forming the compliance team, meaning putting together the qualified employees that fit for the causes of the PCI DSS compliance procedure. Creating the compliance team is a very crucial point in the whole process and can result into successful/unsuccessful procedure of compliance. So, choosing the ones that would participate in the team should be given serious considerations. As far as the appropriate selection of the members, their workload should be taken under consideration, because the whole procedure of compliance is extremely time consuming for each member of the team. However, it is not just choosing the participants, it is also assigning the appropriate roles to each one of them. Each participant must have clear role in the process and must know what he/she is supposed to do. Among their actions may be setting the scope of the project, selecting leaders and any other possible assigned action resulting into compliance. Apart from recruiting the compliance team and assigning different roles to each one of them, the continuous training of it is really important. Of course,

all of them should be aware of the different aspects of PCI DSS and its requirements, a review of the project plan in order to have in their minds the goals and milestones. Overall, all members of the compliance team should be at the same level of PCI DSS awareness so that they can be successful in making the company compliant.

Moving on, and assuming that the company has already defined its *level of compliance* which determines the actual effort and requirements, a valuable step is to complete the *PCI DSS Self-Assessment Questionnaire*. The results of this report will help the organization determine the level of compliance. In other words, by completing the SAQ the company can understand how much compliant is with the standard having the ability to know the compliance status of your organization's data environment before a third-party assessment. For every requirement, that the company has answered that is not compliant with, there should be suggestions and actions on how to meet the specific requirement. On this specific task, a QSA might do the case and help achieve the 'no-answered' requirements. Of course, annual validation by a QSA is only mandate for merchant level 1 but at any case a QSA can help towards compliance process.

After determining, with the valuable use of SAQ, the percentage of compliance with the standard, the company might hire an Approved Scanning Vendor in order to have an external scan on the company's network (please refer to Basics of Compliance for further information). As shown, in the tables of the previous section, most of the card brands demand an external network scan (quarterly) and apart from that, all externally exposed IP addresses are required to be scanned for vulnerabilities. After that scan, the ASV can suggest and mitigation plan to the company for any found vulnerability.

Upon implementation of the steps mentioned above, the compliance team might perform a **GAP Analysis** which provides a holistic view of the organization's current compliance state and outlines the steps needed today to achieve compliance with the standard. More particular, this report contains each PCI DSS requirement and an answer indicating if there is compliance with the specific requirement or not, like the PCI GAP Analysis sample shown below.

Requirement	Question	OA Answers	GAP ANALYSIS	Gap Measurement
1.1.1	Is there a formal process for approving and testing all external network connections and changes to the firewall and router configurations?	NO	There is not a formal process for approving and testing external network connections, changes to the firewall, router configurations.	Not Compliant
1.1.6	(a) Do firewall and router configuration standards require review of firewall and router rule sets at least every six months? (b) Are firewall and router rule sets reviewed at least every six months?	YES, Router and FW configuration are checked frequently (more often than 6 months).	Procedure and report documentations of the review are missing.	Partial

Table 13: GAP Analysis sample

Having implemented all the mentioned steps, the company has all the needed information in order to proceed to the creation of the PCI DSS Compliance Plan. This plan might include among others any identified gap

resulted by the above reports and any suggested action in order for the company to keep compliance with the standard in the future ensuring the continuous compliance with PCI DSS.

Finally, as clearly stated on the following tables of Levels of Compliance, the company should get ready for the annual audit in order to validate its compliance with the standard. Actually, the steps mentioned until now in this section, can be summarized on the below figure containing the basic different steps needed towards PCI DSS compliance procedure.

Figure 12: PCI DSS Compliance Lifecycle

1.4.4 Benefits of Compliance

In most of the cases, compliance with PCI DSS is obligatory for companies because they store, process or transmit cardholder data. So, non-compliance with the standard would automatically result into several enormous fines that would cause significant harm to the organization. Actually, companies will be up against those financial punishments in case of a compromise. Because, if compromised but compliant with the PCI DSS no fines will be probably assessed to that company. Apart from that, it is really probable that the company will be taken to court because of that cardholder data compromise. On the other hand, companies that are PCI DSS compliant may receive additional rewards by the major card brands for being complying, like it happened on 2006 with VISA announcing its PCI Compliance Acceleration Program (CAP) for merchants complying with the standard.

Except from the financial benefits that a company can gain by PCI DSS compliance the most important, by far, advantage is the calmness knowing that the entire IT infrastructure of the company is secure and so as the cardholder data stored, transmitted or processed within it. Apart from the calmness and the confidence that PCI DSS compliance provides, it instantly affects the reputation of the company. That is because, PCI DSS compliance puts the company among the compliant companies by the standard and enhances the confidence

of the customers as far as the protection of their cardholder data. A probable data breach may have an enormous negative effect on the company's reputation. So, ensuring that all the needed actions and requirements according to the standard have been met eliminates the possibility of a data breach and so any side effect to the company's prestige.

The standard's nature implies that the overall security of the company is enhanced, because the scope of PCI DSS includes actually, general speaking, best practices regarding security which offer a lot of benefits regarding not only the protection of cardholder data but the overall protection of the company's network. Going back to the financial effects of PCI DSS compliance, one should consider the direct financial costs of a potential data breach. Because, when it comes to business the only that it seems to matter is the financial gain, each company must comply with the standard in order to reduce the risk and the costs associated with a data breach (containing sensitive cardholder data).

To make things even clearer, let's talk with accurate numbers: The average total cost per reporting company was more than $6.3 million per data breach and ranged between $225.000 and $35 million. In addition to this, a possible data breach has direct impact to the reputation of the company which results a cost of lost business averaging at $4.1 million. The percentage of lost business has been estimated at around 65%. Apart from the company's own data breaches, there are also costs created by third-party data breaches which average at about $231 per compromised data record. Concluding the financial effects of the company, the growing dissatisfaction and the needed action from a probable data breach results into plenty of money growing from year to year costs to the company for legal defense and public relations.

According to all the above mentioned benefits of PCI DSS compliance, focusing mainly to the financial sector which has direct impact to the company, we can clearly see the need of compliance with the standard for the protection of cardholder data and the overall secure functioning of the organization.

1.5 Debunking PCI Myths

There is an abundance of myths and misunderstandings concerning the world of PCI. These originate from the critics of PCI whose judgment however is primarily based on rumors they have heard from other people. But let us now have a closer look at those myths while debunking them at the same time.

The first misperception regarding PCI is associated with the compliance it requires. Critics support that it is impossible for a company to comply with PCI because it is an *infinite process*. The truth is that it is a complex process which requires a great deal of diligence. However, companies which already had vigorous security policies and technology do not face any trouble with PCI which leads to the conclusion that a company's difficulty in becoming PCI compliant reflects its overall approach to information security.

The second PCI myth regards its *non-compliance fines*. It is wrong and untruthful to state that the penalties involved with non-compliance and data breach are small. The non-compliance fines themselves might indeed be relatively small but the risk for credit card theft is where the real costs lie. It has been estimated that the cost for each compromised record could be up to $300 per company excluding other extra costs. Legal consequences may also arise bringing the total cost of TJX breach up to $250 million.

The third myth essentially questions the *effectiveness of PCI compliance*. It is true that companies with a Report of Compliance (ROC) on file have experienced a data breach. In the end, it was revealed that these companies

were not compliant at the time the data breach occurred. PCI compliance must be retained continuously while failures often result from PCI maintenance efforts. In a project-focused IT world long-term compliance can involve major efforts which mustn't be halted when the ROC is signed. Remaining PCI-compliant can be a strenuous process and as painful as the initial compliance efforts.

The three pillars of PCI compliance are compliance, validation, security. It is from these that the misunderstanding of PCI originated from. In fact, a helpful way to understand how PCI works would be to understand the following equation: the validation of compliance ≠ security. The meaning of this is that an organization may be validated as compliant but it isn't necessarily secure. PCI compliance is falsely considered by many organizations as their ultimate security goal. In fact, PCI should be the *minimum scale of security* should be aiming at. Once a company has built the PCI foundation, it should seek more security beyond PCI according to its needs. To make the most of your PCI efforts, it is essential to understand the interaction amongst the three pillars discussed above i.e. compliance, validation and security. Let us have a closer look at each of these.

Compliance in essence means meeting the terms of the PCI DSS. All organizations which accept credit cards today must be PCI-compliant. Because of this fact, PCI is in reality the world's biggest vertical. Even non-traditional retailers such as universities accept credit card payments bringing them in the scope of PCI. Organizations are bound by contract to be PCI-compliant, it is part of a business agreement, which brings us to the following conclusions:

PCI is not enforced by the card brands but each assumes self-enforcement. There is not really any necessity - and it actually is rather impossible - to review every single ROC for every single company. A merchant will be contacted by a card brand only if a data breach has taken place.

Merchants are expected to be 100% PCI-compliant at all times even though card brands know this hardly ever corresponds to reality. But the truth is companies are either compliant or not; there is no other alternative. PCI cannot be nullified. As mentioned above, PCI DSS compliance is part of a legal contract so organizations cannot ignore PCI. Even if they choose to do so, non-compliance is penalized by fines, fees and other costs.

The second pillar, validation, is about testing the truth of compliance and below are some of its key points. Attestations are believed to be honest and accurate. However, several organizations are tempted to answer self-assessment documents or QSAs dishonestly leading to the assumption that these organizations may have been hacked.

Moreover, a third-party assessor may be called on. This is usually somebody who has been certified by the PCI SSC to conduct the assessment and certify the company is indeed PCI-compliant. This is usually required by large merchants or companies that have had their systems hacked. A final point to be made regarding validation is that 'validation' and 'compliance validation' are not the same. The latter may mean that an organization has some type of attestation on file but it does not mean that it has done any type of validation. And it certainly does not guarantee it is PCI-compliant at any given time.

The third and most crucial pillar is security which does not only entail securing cardholder data but also preventing a company's network and data from being abused. Essentially, security should be in the foundation of every organization. Today, many companies are striving with PCI which shows that, even though PCI's controls are not new, companies were not at the desired level of security prior to PCI.

Compliance encourages security to the point that organizations can attract funding for security projects more easily compared to the past. Funding is almost guaranteed if these projects can be justified by PCI or other compliance initiatives. Finally, security is a company's duty since their customers entrust their private information to them. Abusing that data could be harmful to their customers and, in turn, the company itself. Protecting a customer's data and private information should essentially be the utmost corporate goal.

Chapter 2

Introduction to Security

The current chapter introduces to the individual, who is willing to understand and learn in depth the PCI DSS standard, with the information security basics that are related to the standard and as a result mentioned throughout the current document. Apart from introduction to the security fundamentals used by the PCI DSS standard, this chapter is really helpful as a review of this specific information for those already familiar with information security and participate -at any possible point- of the PCI DSS implementation.

In more particular, it is really important for any organization willing to accomplish PCI DSS compliance to obtain an, at least, basic knowledge of information security. That is because it would be extremely difficult not only to achieve PCI DSS compliance but also to maintain it since the PCI DSS compliance is a constant process and not a onetime accomplishment.

As far as the information security is concerned the key point to consider is that its main target is to protect the organization's important resources which can vary between physical assets and any kind of valuable information such as financial, legal and generally any kind of asset that is considered as valuable for the organization.

2.1 What is Information Security?

So, what are we actually implying when referring to Information Security is the need of protection when dealing with organizational risk. The base of information security are the security policies (for further information please refer to Information Security Policies) which in general contain specific security rules for the protection of the organization's technical and information resources. So, using the created policy as a baseline the organization has simply to enforce it by using a series of processes and technical mechanisms.

There are several different types of mechanisms that an organization could use to apply a security policy. At first, the organization must prevent any negative event from occurring by using specific protection measures. In addition, detection measures should be used in order for the organization to be alerted about those negative events and proceed with the appropriate response to each one of the negative event that has occurred. In the

end of the security measures used, the company should assess the effectiveness of all the measures used in the aim of protecting against any information security business risk.

Apart from the used protection measures, it is really important for the effectiveness of the overall protection against risks to perform audits to determine whether any additional actions should be implemented. As already mentioned about the PCI DSS compliance process, the use of the above mentioned detection, prevention and audit mechanisms should be continuously and properly used throughout the entire company's life cycle.

2.1.1 Risk Management

Having introduced with the Information Security it is extremely important to analyze the process of Information Risk Management. First of all, as easily understood the term 'risk' represents the possibility of a negative event occurring within the organization. Of course, every one of us is familiar with that term because we simple have to manage and deal with risk pretty much every day. In the same way, organizations have to manage risk by making the right decisions for analyzing risks, considering any alternative action and finally concluding into and implementing the best suitable action.

So, this is actually the purpose of *Information Risk Management*. To successfully identify, control and mitigate any kind of information risk by (typically) implementing a formal risk assessment, a cost benefit analysis and several appropriate safeguards. In addition, it is essential for the process of risk management that the senior management supports it and that all the related organization teams participate somehow in the process.

As thoroughly explained in the next section, the process of Risk Management can be divided into three different sub-processes. That is the *risk assessment, risk mitigation* and finally the process of *evaluation and assessment*. In general, the first sub-process contains the *identification*, the *evaluation* of risks along with their possible effects and finally the appropriate *measures* to deal with them. The next step is the *mitigation process* which includes all the appropriate actions for reducing the identified risks. The final step of the risk management process is that of *constant evaluating and assessing* in order for the whole management process to be successful.

Having created and implemented the information risk management plan it is crucial to keep in mind several key points. Firstly, whatever the organization might decide and implement one thing is inevitable. That is the complete protection against information risk meaning that whatever the action might be the risk in the organization's recourses always exists. In addition, as previously mentioned, Information Risk Management is a process which involves the constant implementation of actions due to the large number of factors that might affect the organization's security environment and the overall process of risk management. For further information about those sub-processes please refer to the following sections of the current chapter.

Another key factor to consider about the process of risk management is of course the *consideration of cost*. That is because, any part of that process that is proved to be too costly and/or unmanageable will be eventually abandoned and with drowned from the risk management process. However, this does not mean that the organization should not proceed with protective measures that are costly but that there must be a balanced situation between costs and the benefits achieved by them. As thoroughly explained in the next sections, the mentioned costs typically depends on three different factors which are the cost of risk management, the impact of ignoring the risk, and finally the benefit from mitigating or -if possible- eliminating the risk. So, at the end of the day organizations must decide the appropriate level of balance between the risk and the overall

mentioned cost as it would be impossible to deal with risk without cost or even worse without taking under consideration this extremely important factor. Although from a PCI DSS compliance perspective it seems as an easy decision (the company has to comply or face the consequences of noncompliance), the benefits of cost - benefit analysis can be used in creating the compliance strategy, the prioritization of compliance initiatives, and the selection of one common strategy for compliance.

2.1.2 Risk Assessment

As already mentioned, the first sub-process of the Risk Management process it that of *risk assessment*. In more particular, Risk Assessment is the process of analyzing and defining risk which contains three individual sub-processes as well concluding to the extent of a possible threat and its risk to the Information Technology system. The results of risk assessment process helps the organization decide about the implementation of the appropriate controls for the elimination of risks (mitigation process - thoroughly analyzed in the next section). In most of the situations, the overall target is the CIA protection of data. Which is actually a model designed to guide policies for information security within an organization and is combined by the confidentiality (privacy), integrity (consistency, accuracy, and trustworthiness of data) and availability of data. In order to better understand the term of risk and its assessment the below circle of risk is really useful.

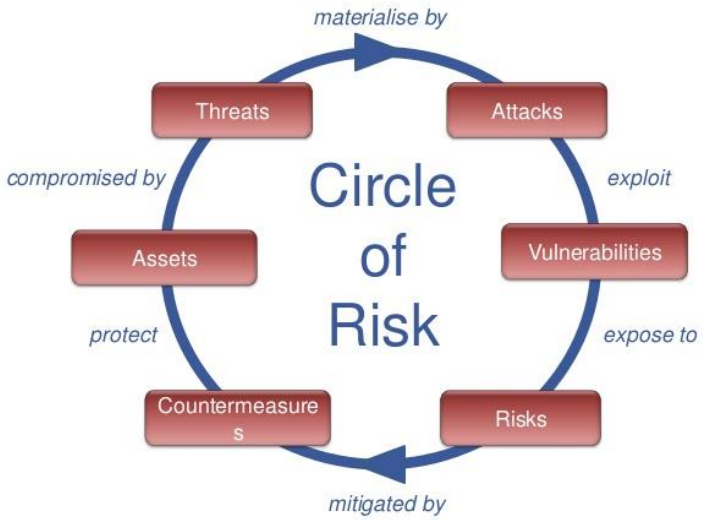


Figure 13: Risk Assessment Cycle

Overall, the process of Risk Assessment can be categorized into several different and interrelated procedures/steps which have to be executed during the assessment process. More specifically, this particular process is a combination of the following steps:

- System Characterization
- Threat Identification
- Vulnerability Identification
- Control Analysis
- Likelihood Determination
- Impact Analysis

- Risk Determination
- Control Recommendations
- Results Documentation

In more detail, as far as the process of risk assessment is concerned, we should state that the first sub-process of the Risk Assessment methodology is the ***determination of the scope of the assessment*** and the exact method that is going to be used. More particular, the team has to determine which specific component will be assessed and at what level. That's because there might be different needs about the different areas of the company and varying levels of detail and formality for each one of them. This specific approach, determining the exact scope, definitely results into a more successful and cost-less assessment.

The above mentioned approach can be influenced by a series of factors such as the exact position of the system component in the entire company's environment and its status (new/existing). In addition, the severity of the system being assessed plays a significant role on its risk assessment meaning that an important one should be thoroughly examined in contrast to a less important one. Finally, as already mentioned, this process involves constant actions which means that any change to the system environment results into a different scope that the initial one. As for the methodologies, we should keep in mind that there are many approaches with different characteristics according to the company's individual needs and that of course there is no single method that can fit on every single environment.

Following the scope and methodology determination we have the ***data collection and risk analysis*** stage. During this stage, all the needed information and data is being collected (screening of information might be needed), in order for the whole risk management process to focus on those - under threat - areas.

There are different stages and terms to be considered about this particular phase. In more detail, the *asset valuation* includes the determination of the assets' (might be software, hardware or physical) values along with the possible results of their compromise. Another stage is that of *consequence assessment* which contains estimation of the loss that might occur. This estimation includes both short and long term consequences which could vary between disclosure, deletion or modification of information to the more important long-term ones such as affection of the company's reputation, loss of privacy etc.

After those steps, an important process follows. That of *threat identification* which as one could easily understood contains actions for the identification, analysis and likelihood determination of any possible threat to the system. In addition to that, we should keep in mind that in order for the risk analysis to be more effective it is best to assess areas that are not too well examined (possible newly added) and documented and that have high possibility of being affected with important "damages" to the system.

Another step contains actions for reducing or eliminating any system vulnerability to a possible threat. This process is called *safeguard analysis* and contains apart from the mentioned actions the investigation of the effectiveness of those created and implemented security actions. In addition to the implementation of safeguards the company should implement *vulnerability analysis* in order to identify all the possible vulnerabilities that the system has in relation with any missing safeguard.

Lastly, one should consider the *likelihood* of a specific threat which is actually the possibility of this threat occurring. This possibility is influenced by several factors such as the characteristics of threats and the effectiveness of the previous mentioned implemented safeguards and needless to say that biggest the

likelihood greatest the risk of it. So, one could say that risk is a combination of the possibility for a threat occurring taking advantage of a specific vulnerability and results into a negative event for the organization.

The above analyzed process is in fact the needed, for the purposes of the risk assessment, risk analysis. We should keep in mind that this specific process is influenced by several factors that could be either quantitative such as value of assets, threats and vulnerabilities and of course qualitative such as the best practices generally used or others.

The final step in the risk assessment process is actually the output of the whole process in order for the organization to determine what is considered as really important in a way of **interpreting the risk analysis results**.

Concluding the current analysis of the risk assessment process, it is important once again to highlight that only if the organization decides to spend enough time and recourses to successfully develop a risk assessment strategy only then it would be wise to proceed with the overall risk management plan. In addition, as already mentioned, it is nearly impossible to achieve complete protection against any potential threat as it would be extremely costly to do so. This means that every organization should find the correct balance between time and money spent for protection and the acceptable level of risks.

2.1.3 Facing Risk

Following the process of risk assessment the company has to decide on how exactly is going to deal with the identified risk. As previously mentioned, the results of risk assessment process helps the organization decide about the defense against risks and the overall strategy that is going to be followed in order to deal with company's risks. So, the company must take the appropriate decision taking under consideration the results of all the sub-processes used during the security risk assessment process. This means that the organization must successfully decide about the upcoming protection measures that are going to be used according always to the cost - benefit decision previously made.

The different approaches that the company might follow are simply the following:

- Firstly, the organization might decide to deal with the risks by implementing the appropriate controls and safeguards in order to reduce - as much as possible - the possibility of the risk happening. This particular approach is known as **risk mitigation**. In more detail, this approach includes all the security actions (controls, safeguards) that have to be implemented in order to reduce or eliminate (if possible) the identified risks.
- Another different approaches are those of **avoiding the risk**. To do so, the company can avoid any action that could cause this particular risk. Similar to this, the company might decide simply to **transfer the risk** to another environment.
- Lastly, as one could easily understand, the remaining strategy is that of not dealing with the risk but deciding to **accept the risk** along with its consequences. This means that the company chooses not to mitigate or avoid the risk because, in most cases, choosing to deal with it costs more that the possible impacts of it.

2.2 Information Security Policies

Though out the current document, several references have been made regarding security policies. The intention of this particular section is to clearly define the term of policy along with its various and different characteristics. So, getting started we should mention that the term of security policy comes with several definitions. The most common deals with the term as the effort of the senior management to establish a security program along with its targets and the assigned responsibilities. In other documents, security policy refer to certain decisions that again the senior management is opt to make regarding several security issues of the organization and possibly needed security rules. Those decisions are influenced by several factors such as the needed resource distribution and the followed strategy for the protection of both the organization's information and assets.

An important factor related to security policies is the documentation as clearly stated and understood throughout the current document and especially during the PCI Breakdown chapter. Of course, policy can be treated at a broader level containing all of the above different aspects of security policy and it is up to the organization the exact approach that is going to be followed. It is undeniable that in order for the organization to succeed into the whole process of risk assessment/management and the overall methodology towards PCI DSS compliance to create and maintain a security policy addressing security of information for employees and contractors. In more detail, as for the security policy's concepts, we should consider several of them such as the needed written documents, document ownership, management structure, user of groups that the policy is for, audit trails, written exception policies and several others that are likely to be determined by the organization.

2.2.1 Policy Implementation

Regardless the decision that the organization might make regarding the information security policy to be implemented and followed there are certain "tools" that can be used to plan and apply that policy.

Firstly, security *organizational standards* can be developed specifying specific activities, technologies, procedures, rules and requirements that the organization is going to use and apply. Those standards are usually mandatory referring to hardware or software and their implementation helps the effective use of security controls within the organization.

In addition to organization standards, an establishment of a *baseline* is really helpful for the policy implementation. The baseline is that point of time that can be used as a reference time for upcoming changes within the organization for comparison purposes. In that way, the organization can better determine the improvement that every change offers by comparing to that time. Apart from that, the situation at that time can be used as a minimum requirement for the organization.

Another tool to be used is that of *guidelines* that are being used as recommendations at situations that the organization doesn't use specific standards because their implementation might prove to be inappropriate and cost-effective. Their use is to deal with individual operational situations and address actions according to certain circumstances assisting users and the company's personnel to successfully secure and protect their systems. Like standards, guidelines offer the ability to implement security controls according to the organization's nature in any possible way ensuring that there are not any measures ignored.

The final tool that helps towards the security policy implementation is those detailed step-by-step instructions, called *procedures*, which are being used by users and others in order to complete certain tasks and cover specific operational requirements.

It is important to consider that all the above mentioned methods and tools are all different and can be used all together in order to gain all the possible benefits that each one of them can offer. In that way, the organization gain a clearer approach to implement the security policy and accomplish its organizational goals. As for the policy implementation it should be applied throughout the organization in a steady manner and should be used for guidance but with attention to clearly distinguish between policy and its implementation. In that way, the organization is offered with the flexibility and cost-effectiveness needed to implement different approaches as desired.

2.2.2 System Development Life Cycle (SDLC)

The systems development life cycle (SDLC) is used in systems engineering, information systems and software engineering describing the variety of technologies, strategies, methodologies and tools that can be used in order to plan, create, implement and manage information systems within the cardholder data environment. The concept of this life-cycle applies to a wide scope of hardware and software configurations depending on each system.

It is an undeniable fact that security must and does play a significant role through the whole system development process no matter which exact development approach the organization chooses to follow. So proactive thinking, at the stage of system development, in terms of security has enormous benefits for the cardholder environment especially at the money and time spent and of course at its effectiveness. The exact phases of the systems development life cycle can be viewed in the below figure along with its stage analysis further on.

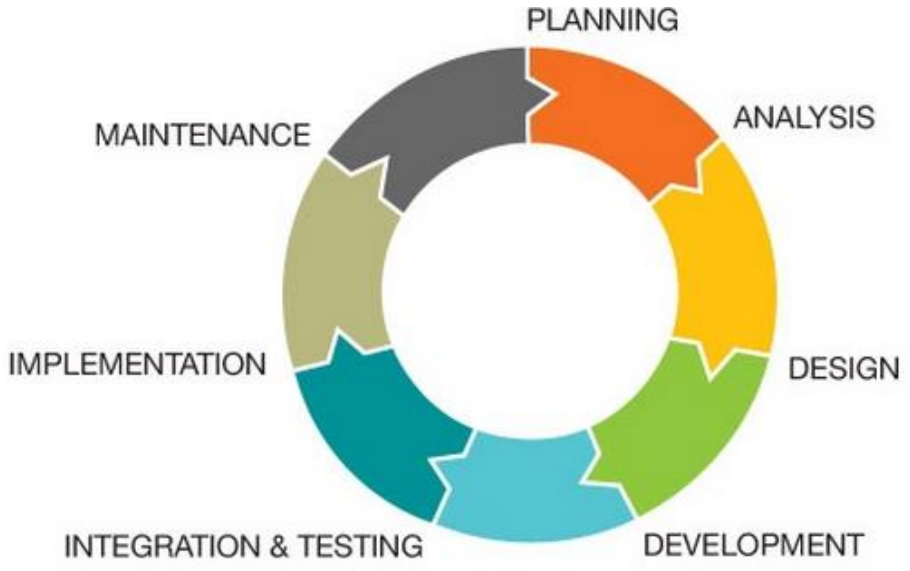


Figure 14: SDLC - Stages

As one could see from the above figure containing the general phases of the systems development life cycle (SDLC) all starts with the planning and analysis phase. During this initiation phase, the organization first determines the security categorization of the system that is going to be developed taking under consideration its impact to the organization in case of a compromise. In addition to that, an initial assessment should be implemented to provide a basic knowledge about the security needs in order to select those security controls that fit and better protect the cardholder data environment.

At the next phase of the life cycle we can actually find the development phase which can include several activities - regarding security - a lot of which have been already discussed and analyzed. The most important of them are the following:

- *Risk Assessment*, following the initial risk assessment during the initial phase there will be further and more enhanced assessment. For further information please refer to the section Risk Assessment.
- *Requirement Analysis*, this particular activity targets on determining the security requirements that are needed to be covered. In addition, the needed effort and assurance evidence needs to determined so to make sure that the security will work as planned.
- *Consideration about the cost and reporting*, contains though about the cost of security and reporting.
- *Security Planning,* ensures that all the security controls that have been selected are documented along with any other information that should also be documented.
- *Development of Controls,* ensures that the previously documented security controls are actually developed and implemented.
- *Security Testing and Evaluation,* contains the appropriate testing - if possible - of the implemented security controls.

Following the Development phase, is actually the Implementation phase of the life cycle. Having validated that all the designed security controls cover the security requirements then the appropriate organization team will proceed with the implementation of the system along with all the related controls and vulnerability identification.

The last phases of the development life cycle (SDLC) contains all the needed actions, especially monitoring, to validate that all the implemented security controls are effective even after changes to the system occur. Lastly, an important step is that of disposing information that lays in the system when it is no longer needed. In the scope of deletion might also be, apart from information, any software/hardware component depending always to the information security policy.

2.3 Information Security Awareness

During the PCI DSS analysis taking place at the PCI Breakdown chapter, at several of the requirements (mostly at the end of each one) one could find the need for making all affected parties aware about all the related to the requirement information. Keeping that in mind, it is obviously how important security awareness is for not only PCI DSS compliance process but for any security related procedure. In fact, there are three different methods/actions that can help towards that directions: *Security awareness, training* and *education*. All of these enhance security by improving security awareness for the system protection, obtaining knowledge on how to

perform any action in a secure manner and of course in terms of designing, implementing and maintaining security programs.

Overall, those three terms offer to security by simply improving each employee's behavior on security issues and of course by holding them accountable about their actions which is one of the best and most effective way to improve the organization's information security.

All of these approaches are thoroughly analyzed in the below sections:

2.3.1 Security Awareness

This specific approach contains actions in order to educate employees on security issues targeting on the protection of the cardholder environment by making them care about security and constant thinking about serious security practices. It is an undeniable fact, that security awareness can have significant impact on the protection of the cardholder environment against unauthorized actions. That happens, mainly, due to the fact that in cases that the employee understands and knows what will happen to the organization and to themselves if security fails they are going to take the security factor more seriously. In addition to that, always depending to the policy implemented, each employee knows that a possible violation might result into warning or even termination. So, they are not going just to forget and ignore security but instead might keep in their minds the security best practices. By using all these actions the organization manages to demonstrate to employees the importance of compliance and the seriousness of security for the organization.

Of course, there are different levels of security awareness that targets to different audiences according to the position of each employee and his/hers job responsibilities. However, we should keep in mind that in today's organizations most of the employees can have significant impact on it as access to system resources is part of their everyday activities.

As for the means that can be used to perform security awareness there can be several of them. The most common of them include videos, newsletters, posters, flyers, bulletin boards, general reminders on banners and warning messages and of course formal speeches at meetings. All of these techniques can be used in combination with a specific frequency and variety in order to increase awareness and the overall protection of the system. However, the organization should understand that those techniques should be creative and constantly changed so not to be ignored by employees.

2.3.2 Education

As in any other aspect of life, education plays an important role in our society. It is the formal process of learning where some people have the knowledge to teach while others adopt the role of learner and absorbing that knowledge. The same happens in our case regarding security knowledge and therefore education. In fact, security education's audience is mainly those security professionals and everyone else whose job demands a more in-depth knowledge of security. In contrast to security training that is being analyzed in the following subsection, this particular approach is most of the times out of the organization's security scope because it is a rather self-development approach. So, it is up to the employee to enhance his knowledge on security through educational choices such as college, graduate classes and other training programs.

2.3.3 Employee Training

Finally, perhaps the most important approach is that of training which aims to teach employees how to perform their job in a secure manner. It starts from the first day of someone's working in the organization as it should be considered as a fact that the recruiting process doesn't end at the moment of hiring but it should continue with the employee training in order for him/her to acknowledge the security responsibilities and duties.

In fact, security training is a more formal process than the security awareness described above with more focus in detail. It targets to develop certain security skill to employees teaching them how to use them to securely perform their jobs. It can extend to multiple levels of skills from the basic ones to more advanced and specialized. In addition, this approach can be more effective when targeting to specific audiences with common duties and background knowledge. Of course, finding that individual audience is not as easy as it seems. There are several methods to do so, such as looking at certain job categories, job functions or even looking for the products and technologies used.

So as easily understood, there is a significant connection of this approach with that of security awareness because the awareness level determines the needed effort for training. Overall, those two approaches should become part of the employee's daily activities and should be adopted as a routine by the organization. Of course as in most cases, the training programs have to be reviewed constantly to validate their effectiveness and adoption to changes.

2.4 Means of Protection

The current section contains the most common and available ways that an organization can use in order to protect information. However, we should have in mind that there is no single solution for information security. That is because the security controls that are appropriate for an organization will depend on several circumstances, so the approach to be followed will depend on this and the level of security that the organization needs.

2.4.1 Physical Security

The first of the protection measures that can be used by the organization concerns the protection against threats of the physical environment. It is usually the first layer of protection for the organization including security controls of three broad areas of it:

- Firstly, the physical controls aim to the protection of the organization's *physical components* such as the facilities (building) or any possible physical component of the network. Of course, their physical characteristics are the ones determining the actual level of threats such as fire, flood, earthquakes etc.
- Another important area to keep in mind is the geographic operating location of each component which again determines the actual level of threats.
- The last area to consider is the facilities that support the operations of the organization. Those facilities might be the electric power, heating and air-conditioning whose failure might result into significant damage to the organization's operations.

In more detail, physical security measures mainly target the restriction of entrance and exit of personnel from areas of the organization by using methods like controlled areas, barriers, entry points, and screening measures for entrance and exit of those areas. The needed physical protection should include not only areas containing hardware components but also locations of wiring that connect the facilities with the supporting facilities that were mentioned above. Of course, the effectiveness of those security controls should be regularly examined at any possible time and under various circumstances as it would depend on a wide range of factors such as the characteristics of the devices and the implementation and operation that is being delivered. At any point, the organization might proceed into corrective actions that should cover any weakness or threats that might still exist or arise in the future.

Those threats to the physical security of the organization might include: *Services Interruption* which might cause interruption of the operation of the organization's systems. *Physical damage* targeting mainly to hardware which might be destroyed or corrupted resulting into loss of information contained in that media. In addition to loss of information, *disclosure of information* might also occur making sensitive cardholder data available to unauthorized personnel. Apart from information disclosure, the *integrity of information* is also at stake.

As already mentioned, there is no single measure that can be used to cover the physical protection needs of the organization. Instead several controls could be used for better protection of the cardholder data environment which should, among others, include as a best practice the following:

- Physical Access Control
- Media Inventory Control
- Monitoring Tools
- Network Access Points Control
- Visitors Identification
- Storage of Media Backup
- Media Distribution Control
- Media Destruction

2.4.1.1 Security in the Perimeter

Regarding physical security of the organization as analyzed in the section above, one of the basic measures is that of firewall which protects the internal network and as a result the cardholder environment. In fact, firewalls are being used to control access between the Internet and the internal network and within the internal networks via *segments*. So, in that way authorized traffic (according always to specific firewall rules created) will have access to certain segments of the network but not to those that contain cardholder data. So, all the traffic entering or leaving the intranet has to pass through the established firewall, which determines whether the specific message has to pass or not and blocks those that do not meet the security criteria.

In more detail, there are different types of firewall techniques that can be used in order to protect the company's network. First of all the *packet filter,* which is really effective but difficult to be configured, can be used which examines each packet entering or leaving the network and accepts or rejects it accordingly. Next, by using the *application gateway* we can enforce security mechanisms to certain applications. Another mechanism is that of *Circuit-level Gateway* which also enforces security mechanisms when either a TCP or a UDP connection is established. After the successful establishment of the connection, packets can pass through

between the hosts without any further checking. Lastly, the *Proxy Server* can be used to intercept the traffic of the network.

Another important term to consider with the use of firewall is that of DMZ (Demilitarized Zone). In fact, it is a network segment that "sits" between two firewalls (external and internal) in order to create this trusted zone and to control traffic from that to the remaining internal network. So in that way, this zone is like a buffer between Internet and the internal network.

The figure below shows an example of firewalls use in a network:

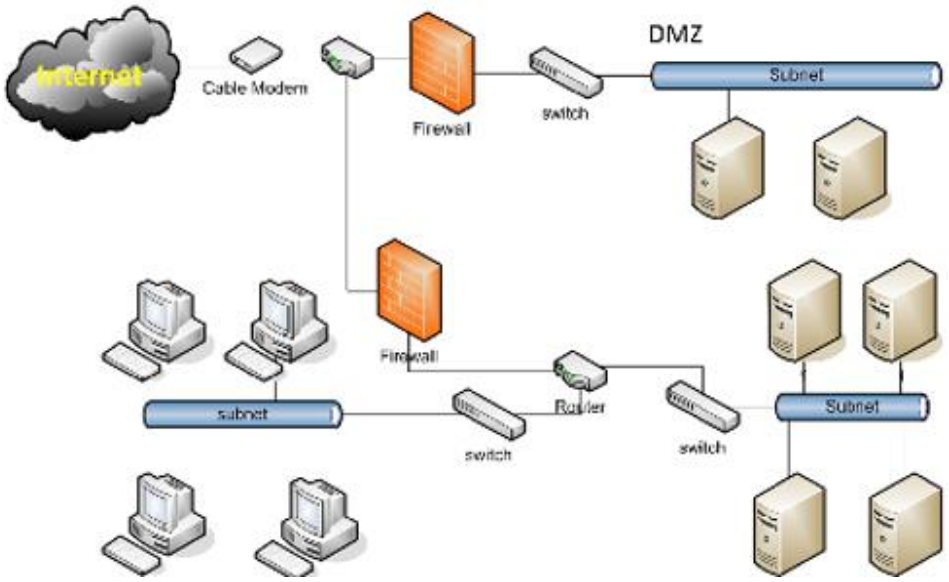


Figure 15: Use of Firewalls

2.4.2 Logical Security

The second of the protection measures that can be used by the organization ensures that only authorized users are able to perform actions or access information in the organization's network. The logic behind this specific category of measures is that the user should have access only to job-related information and so actions for denying access to all the remaining information should be forced. Apart from controlling access to resources, measures should be used in order to control the actions that the user should be allowed to perform on them.

The controls used in this particular protection category are called *logical access controls* and attend into enabling or restricting access to system resources by setting not only who has access to every system but also the kind of access. Those measures can be implemented on different levels from the application level and operating system to any other possible level through the use of specifically created add-ons. All these different components can work altogether to accomplish the restriction of user access to the organization's resources. The overall target is to protect the CIA of information by implementing those security logical controls to any asset of the organization by restricting access of the users and processes and by preventing sensitive information from being disclosed. Of course, we should keep in mind that, all the above requirements and measures for accessing and using organization's resources can differ on each situation.

In comparison to the previous mentioned set of controls - physical security controls - both have the same intention of securing information within the organization by restricting access to any component of the organization that needs to be protected. However, the controls being discussed in this particular section occur within the information system in terms of identification, authentication and authorization aspects through the implementation of specific, for each one of them, *control measures*. That is why, those kind of measures are being used for the perimeter protection as well, before a user gets further into the organization's environment.

As for the technical implementation mechanisms regarding logical access controls, the most important of them are being analyzed below.

- *Least Privileged Access Control*: By using this specific kind of mechanism a user can only access the job related information. It can be applied to employees by giving them the lowest level of user rights in order to still do their jobs. Apart from employees, those measures can also be applied to programs and processes.

- *Role Based Access Control (RBAC)*: This specific mechanism uses different levels of access depending on users' roles. So, the permissions to perform certain operations and perform particular computer-system functions are assigned to those specific roles.

2.4.2.1 Internal Access Controls

This category of logical security measures determines user's access to resources and what exactly any user can or cannot do with them.

2.4.2.1.1 Passwords

Passwords are used for data and application protection on a great variety of systems. In more detail, a password is actually a word or string of characters used for user authentication in order to prove his/hers identity or access approval to gain access to a specific resource. This measure's implementation is rather easy but a lot of users find it difficult to remember all the different passwords being used especially due to the demand for enhanced complexity. Some of the needed characteristics and a thing to consider about passwords used are the following:

- Rate at which an attacker can try guessed passwords
- Limits on the number of password guesses
- Form of stored passwords
- Number of users per password
- Password reuse
- Password longevity

2.4.2.1.2 Cryptography

Cryptography protects information by using advanced mathematics in order to transform data towards its protection. In more detail, cryptography provides the following:

- *Authentication*: A way to prove someone's identity
- *Privacy/confidentiality*: A way to ensure a message is being read only by the validated receiver

- *Integrity*: A way to ensure that the content of the message has not been altered in any way from the original one
- *Non-repudiation*: A way to prove that the sender that claims to have sent the message is the right one

Because the context of this particular chapter is to introduce the user with the basic of security - always regarding PCI DSS - the thing to keep in mind is that cryptography lies on two basic components. Those are the *cryptographic algorithm* being used and the *key*. There are several ways of classifying cryptographic algorithms. In most of the cases, they are categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The types of cryptography are the following:

- *Secret Key Cryptography* (SKC): In this particular type, a single key is being used both for encryption and decryption. It is really important to keep this key secret and protect it from modification as a possible compromise of it would result into elimination of the cryptography. The most known algorithm for this category of encryption is DES.
- *Public Key Cryptography* (PKC): In this particular type, two keys are being used. One key for encryption and another for decryption. The first one is called *public* key and can be known to other parties whereas the other is called private must be *secret* and used only by its owner. This type of cryptography is useful when the parties willing to communicate cannot seem to share a common key or simply cannot rely to each other with the DSS being an example of public key cryptography.
- *Hybrid Cryptography*: This particular type is actually a combination of the above two types of cryptography. It uses the advantages of both types of cryptography for different purposes.

But what are exactly the uses of all the above types of cryptography and functions. The main target of it is to protect data when in transit and no longer under the protection of its creator/owner. The most basic uses of it are the ones below:

2.4.2.1.2.1 Encryption

Encryption is another protection measure that can be used as a cost effective way to protect data's confidentiality. It simply converts the so called plaintext into ciphertext and can be reversed with the method called decryption. The overall complexity of the algorithm being used is the one that determines the strength of the encryption and as a result more difficult for the attacker to decrypt the message. As mentioned above, according to the exact type of cryptography the encryption is either symmetric (secret) or asymmetric (public).

It is really important to keep in mind that the strength of the encryption depends on the strength of the key being used for it. So, as easily understood it is vital for the effectiveness to manage the key properly. This contains plan and actions for its secure creation, storage, distribution and overall for protection against exposure and modification.

2.4.2.1.2.2 Integrity

Another use of cryptography is that of identification of any modification to the original message sent. As it could be difficult or even impossible for a person to identify any change to the original message. So, by using cryptography (secret or public) it is possible to automatically identify those changes but not prevent them.

What is actually happening is that a particular value is created (from the original message) by using a secure hash algorithm and it is then attached to the message to be sent. This "value" which is called *message authentication code* (MAC) ensures that the message is original as at any time a comparison of the original mac

with a newly created one verifies whether the message has been changes or not. So, anyone that has access to the key used can validate by recalculating that value (hash) and comparing it with the sent one.

2.4.2.1.2.3 Electronic Signatures

Apart from the previously mentioned purposes, cryptography can also be used for non-repudiation (and also integrity) via the implementation and use of electronic signatures. Those are in fact the electronic equivalent of the written signatures with the exact equal legal status. By using electronic signatures we achieve into proving that the sender that claims to have sent the message is the right one and that the message has not been change because only the sender can electronically sign that document.

In comparison to written signatures which could easily be copied from one electronic document to another without being able to determine whether it is legitimate or not. Electronic signatures, are unique to the message that is being signed and won't verify if they are copied to another document. However, electronic signatures should and cannot fully protect an electronic document and overall data. So, electronic signatures should only be used as an extra layer of protection for electronic documents.

2.4.2.1.3 Control Lists

Another internal measure that can be used by a company is that of an access control list (ACL) which is a list of permissions that can be applied to a specific object defining which exactly users (groups, machines) or system processes are allowed to have access to those objects in addition to what is the allowed action on them.

Of course, those lists can differ according to each situation offering different capabilities and flexibility. So, some of them can only allow certain actions on specific predefined groups while others can be used to allow actions in a more flexible way determined by the user. This specific measure can also be used to cover a great series of situations such as clearly denying access to certain objects (individuals or groups) or can depend on the implemented security controls. Of course, as in any asset of the organization, these lists must also have a certain owner which will be probably its creator or any other user or group assigned to it.

In general, access control lists can be implemented using the following types:

- *Filesystem lists,* which is in fact the type of list that has been analyzed above containing specific entries/rules that specify individual user or group rights to certain system objects such as programs, processes, files and machines.
- *Networking lists*, which contain rules that are applied to ports and IP Addresses that can be found on each host determining specific allowed services.
- *SQL implementations lists*, which use specifically designed algorithms for SQL and relational database systems.

The above mentioned lists can be used in combination with the so called user interfaces which can be used to restrict user access to specific functions which prevent them from requesting any information that should not be allowed to access simulating in a way the organization's operations. In more detail, there are three different types of user interfaces:

- *Menus,* which allow the administrators to successfully restrict user's access on operating system resources
- *Database views*, which is a method used to restrict access to data (or a portion of it) that is being saved in a database

- *Physically constrained user interfaces,* which is a physical method of constraining access

2.4.2.1.4 Security Labels

This specific security access control uses anti-tamper seals for organization's resources such as files, doors, windows, boxes, and literally any other component of the organization that needs designation. In that way, those labels can be used to control access, protect products and equipment and provide indications about tampering or pilfering.

As far as the control access in concerned, labels can be used for user sessions meaning that users can only start and use those sessions that are labeled in a certain way. In that way, the organization prevents not only unauthorized access and use of resources but also protection of information throughout its life in the organization's system. This happens due to the fact that they are permanently linked with this specific data and so it cannot be disclosed by a certain malicious user by coping it or simply altering the access to the file/container.

However, this specific measure's disadvantage is that they are usually inflexible and sometimes expensive because it is difficult to be changed on a regular basis - unlike to most of the previously mentioned measures.

2.4.3 Monitoring and Logging

As one could easily understood through the PCI DSS breakdown occurring in the following chapter of PCI Breakdown the processes of information security monitoring and log management are highly important for the protection of information and the PCI DSS compliance process. Those two activities can have multiple impacts to the organization towards the protection of cardholder data either as a detective control of malicious activity or as an investigation method for incident response procedures and any other legal identification process.

Of course, those two activities demand a lot of attention and effort to successfully protect the organization as they require the implementation of specific safeguards for the protection of captured logs within the cardholder data environment. There are different sub-processes that have to be executed in order for the log management and logging to be effective. Among them the most important ones are those of *log collection*, *centralized aggregation* of logs in a central location, *long-term retention, log rotation, log analysis* and lastly that of *log search and reporting*. As already mentioned, the process of log management and monitoring can prove to be really demanding and tricky as the process of analyzing really large volumes of various logs can pose many challenges. First of all, we are talking about huge log-volumes even hundreds of gigabytes per day. In addition, logs are characterized by a log-format diversity and last but not least the presence of false log records in some types of logs could be another challenge.

As a best practice NIST recommends that, most of the organizations should perform a baseline of operations regarding logs:

- First of all, the integrity of logs should be protected. To do so, *access* to log files should be controlled along with the appropriate actions permitted (read, write, delete).

- Next, sensitive information should be protected. To achieve that, it is best not to record any information that might contain sensitive data and that is not really needed to be recorded. An attacker gaining access to logs containing this kind of information gets also access to sensitive information.
- Other mechanisms that should be used are those of protection regarding those log files that have been archived and of course the protection of the processes that result into the creation of logs. Several different approaches could be used to achieve the needed protection such as encryption and physical protection for any archived log file and access control for using log creation processes.
- Lastly, another important mechanism to be implemented regarding the log protection is that of ensuring their secure transportation to where might be needed. To do so, further security characteristics might be needed in addition to measures protecting the channels used for log transferring such as Internet Protocol Security (IPsec) protocol, Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.

2.4.4 Classification of Information

During the data collection and risk analysis stage of the risk assessment process, it was clearly stated that one of the sub-process it that of asset valuation and characterization. This is a really important step in order for the risk assessment to be successfully with the minimum possible costs. This particular step, is known as classification of the organization's information and related assets and it should not be ignored by any company. That is because only after knowing what is characterized as important for the company and eventually what is considered with less value, the chances are that the organization can successfully proceed with the risk assessment process and finally protect its assets against risks.

The mentioned classification can and should include not only data, systems and users but also literally everything within the organization that could be categorized in order for the company to implement the appropriate safeguards to the systems to be protected. So, as a result, having different categories of assets would be easily manageable and effective to protect assets according to their category. As for the classification itself, there are different ways to classify information and data and it is up to the organization on the exact way that is going to be used for the needed classification of information. In most of the cases, it is preferable to follow the hierarchical structure of information so to categorize and prioritize it. To better understand the classification of information that the company is opt to make for the risk assessment process let us review some typical categorization of information:

- *Top Secret*, is actually the highest possible level of information classification and usually specifies important information and possible reveal of it will most likely cause inevitable damage to the organization. In most cases, a secret code is used for its protection.
- *Secret*, is the next level of possible classification and could also cause serious damage to the company if revealed.
- *Confidential*, is actually the type of information that is shared with only certain people in order to fulfill certain purposes. In addition, the receiver of this kind of information is generally prohibited from using it to take advantage of it.
- *Restricted*, is the type of information that need to notify people if there has been unauthorized access or disclosure of this information. Leaks of this type of information can lead to identity theft, news coverage/publicity, and reputational damage and costs to the university.

- *Unclassified*, is the kind of information that is obviously lacking of a particular classification. This lack of classification characterizes information that is of low-impact and doesn't demand any special protection.

Concluding this particular section regarding the information classification process we should highlight the importance of this step during the risk assessment and management process. Not paying attention to this step and its results is really irresponsible during the PCI DSS compliance process and could result into spending time and money to protect information that might not require protection (up to a certain level).

Chapter 3

PCI Breakdown

3.1 Build and Maintain a Secure Network and Systems

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

This particular requirement addresses the need of the use of a firewall in order to protect all the systems of the organization from unauthorized access. Firewall is that network security system that can control the traffic, both incoming and outcoming, based on created and applied rules. So, that system component can establish a barrier between the trusted internal network of the organization and any other network which might be a threat for the company's systems. In our particular situation, firewall can protect sensitive cardholder data from unauthorized access by an undefined network providing a basic protection mechanism for that computer network. According to the standard, there might be used other system components as well, as long as they can provide the same functionalities with those of a firewall.

1.1 Establish firewall configuration standards that include the following:

First of all, those firewall configurations must include a formal process for approving and testing all external network connections and changes. This means that a change control methodology must be in place, no matter how much effort this might take, in order to make sure that those changes have no negative impact to the company. The company must understand the significant value of a firewall to its systems security and make sure that the implemented configurations are the appropriate ones.

In addition, the organization must make sure that an *accurate network diagram* has been created and documented describing the above mentioned configurations and the position of any device within the network in order to assure that all the devices of the network are being included in the scope of PCI DSS. This diagram must be kept as current as possible, interviews might be needed, and must show the actual flow of cardholder

data within the network. That would help the compliance team to identify all the locations that cardholder might be stored, processed or transmitted between the network's different systems devices.

The implemented firewall, must be used on every connection between the company's network and the internet, so we are talking about both incoming and outcoming traffic, and apart from that the firewall must control any connection between the network and any DMZ used by the company in order to control at a maximum possible level the connections established and protect the internal network from any unauthorized access that could harm the sensitive cardholder data. As already mentioned above, all these configurations must be documented and accurately described on the up to date diagram.

Another important thing to be taken under consideration is the creation of purely described roles and responsibilities between the company's personnel in order for each one of them to understand his/her responsibilities regarding the protection of the assigned to them assets. This assignment is really important for the process of compliance, in order to minimize the possibility of any device/asset left unmanaged and unprotected. The standard addresses that a series of interviews should be performed to validate the requirement of role and responsibilities assignment.

Going back to the necessary documentation, the company must keep in mind that all the used services, protocols and ports must be thoroughly listed and described in order to ensure that any unused service, protocol or port is disabled. In addition, the compliance team by documenting this information can understand the risk that of any one of them poses. This is really important for the protection of the network, because attackers might take advantage of any unused but "open", and unpatched when talking for services, hole in the system. So, by documenting the above configurations for the firewall and all the included devices the company can verify that the suggested configurations have been implemented.

Concluding this specific requirement, the standard forces the company to review the rule sets regarding the firewall and router at least every six months giving the ability to the company to accumulate any unneeded rule set. The frequency of this review might change according to the company's specific needs and the validation that this review is being carried out correctly can be performed by several interviews.

1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment

This particular requirement extends the scope of the previous one focusing on what is called untrusted network. As already mentioned, it is crucial for the protection of cardholder data to create and apply rules for denying any kind of traffic to and from the network that it is not needed and might be proved harmful. To that direction, all the firewall and router configuration should be examined in order to validate that only the absolutely needed connections are allowed and on the opposite all the unneeded traffic is denied.

Another important thing to consider is the examination of the router configuration files to validate that these files are secured from unauthorized access. The team must also examine the start-up files as well to ensure, what is actually called *synchronization*, that these files address the same configurations as the current/running ones in order to prevent the appliance of any weaker rule by mistake.

The implementation of firewall rules must also include connections between all wireless networks and the cardholder environment, and as mentioned before, apply deny/permit rules whether the intended connection is needed for the company or not. So, the standard according to this particular requirement, implies that the

use of firewall rules must be applied to any connection between the company's cardholder environment and the wireless connected.

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment

As already mentioned in the previous requirement, the use of firewall offers the ability to control all connections, to and from the systems of the company that store, process or transmit cardholder data. This specific ability, must be used in order to prevent any direct access to those systems, from any possible source through the Internet. There are many possible ways to achieve this. First of all, according to the standard the company should implement a **Demilitarized Zone (DMZ)** which acts as a buffer to control traffic and prohibit inbound and outbound connections. In addition, as far as the inbound connections are concerned, the created and applied firewall configurations should be examined so to verify that they are limited to IP addresses within the designed DMZ.

In general, all inbound and outbound connections possibly established should be examined in order to verify that there is no direct access within the systems of the DMZ. This can be achieved by creating rules based on the source and destination address of the packets to be send or received. In addition, these rules might check and block unwanted content. Apart from this, an implementation of an anti-spoofing control can provide the ability to avoid any attacker who might spoof the sending address with a trusted one. Having set rules for *inbound traffic*, the team must create appropriate rules for *outbound traffic* as well, from the cardholder data environment to the Internet to ensure that only authorized communication is permitted. Another important measure, is to implement what is known as stateful inspection (dynamic packet filtering), meaning that the firewall maintains the status of each connection trying to pass through the network.

Another sub-requirement is to maintain all those network's components that store the cardholder data - not the temporary ones - , like a database, into a segregated internal subnet in order to prevent any attacker from getting access to the data if saved somewhere into the DMZ.

For the next requirement, it is really important to understand the value that an attacker can gain in his or hers attempt to access the cardholder data environment when knowing the IP addresses of the company's network. The company can use a variation of methods and assure that these methods are effective to achieve this non-disclosure of the internal/private IP addresses such as using Network Address Translation (NAT), proxies, RFC1918 and any other possible way to keep that anonymity.

1.4 Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include:
- Specific configuration settings are defined for personal firewall software.
- Personal firewall software is actively running.
- Personal firewall software is not alterable by users of mobile and/or employee-owned devices.

This particular requirement, addresses the threat of personal portable computing devices that employees use to gain access to the cardholder data from outside of the network. The company must assure the security of those devices by implementing personal firewall software on those devices and periodically checking a sample of them to validate that the appropriate firewall software is up and running. The importance of this

requirement is really high because any left and unmanaged device is a weak point for the network's security providing the chance to any attacker and malicious user to access the sensitive cardholder data.

1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties

Concluding this particular set of requirements concerning the first requirement of the creation and maintenance of a secure network for cardholder data, it is really important to ensure that all the created security policies and configurations are *documented* and of course, used for the continuous protection of cardholder data from unauthorized access. Finally, the company must ensure that all the affected parties are being *informed* about those procedures. A really useful way for the company to assure that the above mentioned requirements are fulfilled is for the company to perform a series of *interviews* with its personnel.

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

This particular requirement addresses the necessity for merchants to use *strong passwords* in order to protect the cardholder data. More particular, hackers and internal malicious users often use the default passwords and other default settings provided by each vendor to gain access to systems containing valuable information. So, sticking with the default passwords is a common mistake that merchants often make and which should be given the appropriate attention by the compliance team.

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

This particular requirement addresses the need for protection against accessing cardholder data by using the default (by vendor) passwords. Most of the vendors use standard passwords and configurations which are commonly known to anyone willing to penetrate such a system. So, the standard by setting this requirement forces the company to change all those default passwords and configurations so to prevent attackers from gaining access by using those credentials. In addition, the company is forced to disable or remove any of the un-used default accounts. In case of deactivating it is suggested first to change the default password and then deactivate that account, to prevent the malicious user from using the account after enabling it.

The described need for altering the default passwords also extends for wireless environments including among others default wireless encryption keys, passwords and default SNMP community strings. This would prevent any attacker from using sniffing techniques for wireless environments and access the cardholder environment. Of course, like the previous requirements, a series of interviews is needed in order to verify that default passwords and any other vendor supplied setting has been changed and that all the wireless devices have the latest firmware covering any security hole regarding the vendor defaults.

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

Unfortunately, a lot of the used operating systems, databases and applications are prone to a series of security vulnerabilities. So, the need for fixing all these vulnerabilities is extremely high and critical for the protection of the cardholder data. To achieve this, some security organizations, such as the Center for Internet Security,

International Organization for Standardizations and National Institute of Standards Technology, have created guidelines and proposals that help companies protect their valuable assets.

According to this particular requirement the company must first examine the system configuration standards (like the ones mentioned above) and confirm that those standards are consistent with the accepted by the industry hardening standards. In addition, the company must ensure that these system configuration standards are up-to-date to protect against newly discovered vulnerabilities and that are applied whenever a new system is configured and installed on the network.

The system configuration standards must include, according to this requirement, a number of procedures such as: altering all the defaults by the vendor and deletion of any unneeded account as mentioned on the 2.1 and implementing only one primary function to each server in order to avoid different multiple levels of security for each of these functions (independent of virtual of physical servers). Another important procedure is to enable only the needed services, protocols and generally only features that the company really needs and that are documented by configuration standards. For those features (protocols, services etc.) that are being used by the company and are recognized as vulnerable, implementation of additional security must be performed. This action, prevents malicious users from taking advantage of security holes on used protocols and services.

Another important action that the company must perform is to configure the parameters of the system so to prevent misuse. More particular, administrators and managers related to company's security have to know about common security parameter settings for each system that is being used. Apart from this, the compliance team has to remove all the unneeded functionalities, like mentioned before, preventing any attacker from taking advantage of this unused function to gain access to the cardholder data environment.

2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access

This requirement address the need for secure authentication and encrypted communications to prevent any malicious user to eavesdrop the communication to retrieve in plain text passwords and ID'S. The technology used by the company such as HTTP, telnet and others, often transmits sensitive information in clear text. So, the standard forces the use of strong cryptography to protect administrators' passwords and IDS during non-console administrative access.

2.4 Maintain an inventory of system components that are in scope for PCI DSS

This requirement focuses on determining the scope for PCI DSS in the most accurate way possible, by maintaining and examining a system inventory listing all the hardware and software components along with their intended use by the company. This prevents from "forgetting" any system component and leaving it out of scope of PCI DSS and as a result unprotected. Like in other cases, interviews can help the organization to validate that this inventory of components is up-do-date and accurate.

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

According to this requirement, all the created security policies and the operational procedures for the managing of default passwords and configurations must be *documented*, *in use* and of course *known* to all the related personnel to better be prepared and prevent insecure configurations.

2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

This particular requirement focuses on shared hosting providers that provide services to multiple users on the same server. More particular, in such situations clients often alter the configurations or add insecure ones influencing the security of all the other hosted environments. So, according to the standard's Appendix the company must perform testing procedures in order to validate that providers effectively protect their users.

3.2 Protect Cardholder Data

3.2.1 Requirement 3: Protect stored cardholder data

This particular requirement addresses the need of preserving the confidentiality of sensitive cardholder information via the use of encryption, truncation, masking, and hashing. So, even when an intruder gets access to cardholder data, without access to the proper encryption keys, he or she cannot read it and therefore use it. That is why, the PCI standard forces the use of such methods for the preservation of the confidentiality of cardholder data but also allows the use of compensating controls in order to mitigate the risk if the team is unable to meet this specific requirement.

3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements
- Processes for secure deletion of data when no longer needed
- Specific retention requirements for cardholder data
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.

This particular requirement forces the company to use a retention policy in order to identify the data that has to be retained and so to destroy or delete the remaining unneeded data. For this specific requirement, it is highly important to know where exactly each cardholder data is stored so to easily decide and implement the needed deletion. Overall, the company must keep the storage of this data at a minimum in order to reduce the risk of a possible data compromise.

A series of interviews is needed to understand the exact location of cardholder data storage and that all these locations are successfully included in the mentioned retention and disposal process. In addition, this process has to include quarterly automatic or manual features to effectively delete any unneeded information. As in most cases already described, a sample of system components might be needed to investigate whether this specific requirement is covered and that any unneeded data is deleted effectively.

3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process

This specific requirement forces the company not to store any sensitive authentication data after the process of authorization even if the data is encrypted. In more particular, storage of sensitive cardholder data, which has been already described in previous chapters, after the process of authorization is prohibited because in any case that an attacker gets access to that information the company might be at risk of several attacks as described on the Credit Card Fraud and Identity Theft.

Any company and issuer that store sensitive cardholder information and support issuing services is obliged not to store this kind of information except from the cases that the business needs this kind of information to operate. For any other entity, it is crucial to delete any sensitive cardholder data after authorization. In more detail, according to the standard the company is obliged not to store the full contents of any track (magnetic stripe, chip etc). However, as mentioned earlier, the company or issuer might retain cardholder data such as the cardholder's name, the PAN, expiration date and service code as long as those are needed for the core business. Apart from that, another crucial sensitive cardholder data which must not be retained after authorization is the card verification code (please refer to Electronic Transactions Basics) which is used to protect the so called card-not-present transactions. In the same way, the PIN information must also be deleted after authorization preventing any fraudulent PIN-based transaction in case of PIN compromise.

3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN

According to this requirement, the Primary Account Number (PAN) has to be masked in order to prevent its disclosure to anyone unauthorized. To achieve this, there must be a number of policies and procedures implemented for the PAN masking assuring that only specified authorized personnel can access the full PAN whereas anyone else sees only the masked PAN.

3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:

- One-way hashes based on strong cryptography (hash must be of the entire PAN)
- Truncation (hashing cannot be used to replace the truncated segment of PAN)
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures.

This particular requirement is based on the fact that it is extremely difficult for malicious individuals to retrieve the original PAN assuming that he or she has gained access to the hashed and truncated version of it. So, as it can be understood form the requirement itself there are different approaches of protecting the PAN confidentiality. First of all, strong encryption, with the possible use of one-way hashes, can be used to make this kind of information unreadable by attackers. In addition, another method that can be used is that of truncating the PAN stored by the company, meaning to store only a portion of it. Finally, index tokes and pans can be used to replace the PAN and therefore protect it from unauthorized access.

The compliance team must perform several examination actions to validate that the PAN is not stored in plain-text. Those actions must extend to any location that this sensitive information might be stored including any removable media such as back-up tapes and might also include the examination of logs.

Another method that could be used, according to the standard, is the disk encryption which encrypts the entire disk possibly containing sensitive cardholder information. In that possibility, the requirement forces to use a

different account authenticator for the disk level encryption and the host operating system and a use of a decryption key that cannot be derived from any possible source. Of course, as any other case, a series of interviews and a lot of observation is needed to validate that all the above are effectively implemented. Concluding this particular requirement, the standard pays some additional attention for removable media and the need of also protecting its content, by using the techniques mentioned above.

3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse

In addition to the requirement above, according to this requirement, the cryptographic keys used for the encryption of sensitive cardholder data must be kept securely from anyone unauthorized. Because, any access to that information gives the attacker the ability to use reverse engineering and obtain the original information. In order to achieve this, the company must have in mind that the fewer people having access to those keys, the better. Those people must be authorized, and having key access must be necessary to do their jobs. So having understood the value of protection of those keys there must be a number of actions assuring that the keys used are stored in a secure way to prevent any unauthorized access to them.

In more particular, the requirement addresses the storage of the cryptographic keys used in specific formats. Either encrypted, stored in a secure cryptographic device or as key components or key shares. In whatever format the keys are stored, the company must ensure that those keys are stored in the fewest locations offering the company the ability to better handle them minimizing the risk of compromise.

3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data

As already understood the key management is a crucial factor for the protection of the sensitive cardholder information. This particular requirement examines all the cryptographic keys related processes and procedures which must be documented, in use and known to all the affected personnel.

Those procedures must include actions which perform first of all generation of strong cryptographic keys which increase the security level. In addition, the actions must include a secure distribution of those keys meaning that those keys are only distributed to authorized personnel and never in clear-text. Apart from that, as already mentioned, the cryptographic keys must be stored securely, by encrypting them with an appropriate key-encrypting key, preventing any unauthorized disclosure of them.

Having clearly stated the importance of the protection of the cryptographic keys, it is vital to also state the importance of changes to those keys when it is needed. For example, cryptographic keys might have a specific period until when are valid and so there must be specific procedures for their retirement and/or renewal. Furthermore, keys that are suspected to be compromised should be revoked and replaced by new stronger ones.

Another control forced by this requirement is that of knowledge and control splitting when it comes to manual key-management operations in order to prevent one person from gaining access to the whole encryption key. Apart from that, the requirement addresses the prevention of any substitution of the cryptographic keys without the proper authorization. That is because, if an unauthorized user has the ability to substitute an encryption key, the user can maliciously subvert the organization's encryption key safeguards and pose

substantial risk to the cardholder data environment. Further on, it is really important for the authorized personnel to understand their roles and responsibilities towards the management of the cryptographic keys.

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

Like described in the previous requirement of protecting stored data, the most reliable and efficient way to ensure that the transmitted cardholder data is not compromised and that the confidentiality and integrity is preserved, is to *encrypt* the data during transmission. The current requirement includes some specific details related to procedures for the cardholder data protection during communication.

4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) 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.

This first sub-requirement addresses the need for encryption of the sensitive cardholder information during transmission over open public networks. To achieve this, strong cryptography and a number of secure network protocols (such as SSL/TLS, IPSEC, SSH, etc.) have to be used in order to maximize the security during the transmission of that data. However, only the use of protocols for secure communications is not enough because some of them might be vulnerable to a series of attacks. So, it must be assured that the version of the protocols used are the latest ones and configured appropriately.

In order to achieve this, first of all the team has to recognize all the locations through which cardholder data is being transferred over open public networks. As with all other situations, all the related documented policies must be reviewed to verify that only trusted keys and certificates are being accepted and that the used protocol is secure and the proper encryption configurations are being used. As far as the wireless networks are concerned, the standard addresses the use of strong encryption for authentication and transmission of the cardholder data as well.

4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.)

According to this specific requirement, at any time that Primary Account Number (PAN) is being transferred by using several means such as email, instant messaging and chatting, it must never be transmitted in plain text but always encrypted. All the related policies have to be reviewed so to confirm that this kind of information is never sent unprotected.

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

This particular requirement addresses the need of examination that all the related policies and procedures for the encryption of the cardholder data during transmission is being documented, in use and known to all the affected parties.

3.3 Maintain a Vulnerability Management Program

3.3.1 Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

As already mentioned, the technology improvement has introduced a number of new threats and vulnerabilities which have to be defended in order to protect cardholder data. There are several different methods, tools and techniques to achieve protection against all these threats and vulnerabilities and generally protect the cardholder environment. During this particular requirement, the technique described is that of antivirus software and security patching.

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

As discussed in previous chapters, zero-day attacks take advantage of the cardholder's environment vulnerabilities by using widely known exploits. In order to defend against such attacks, this requirement addresses that *anti-virus software* has to be used. This kind of software has to protect from all kind of malicious software including viruses, worms, spyware and rootkits.

The company team, must be aware of the malicious software and their industry trends, so to be better prepared against them. It is really important to monitor any system within the environment even if those systems are not theoretically prone to vulnerabilities and threats.

5.2 Ensure that all anti-virus mechanisms are maintained as follows:

- Are kept current
- Perform periodic scans
- Generate audit logs which are retained per PCI DSS Requirement 10.7.

In addition to the previous requirement, it is not enough just to obtain and maintain an antivirus software. It is also important to assure that the software is correctly maintained and up-to-date. In addition, a series of configurations must be performed in order to enhance the software's effectiveness such as performing automatic updates and periodic scans as well as producing and maintaining the appropriate audit logs.

5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period

Another important factor about the use of antivirus software, is to assure that this service is always running and that it cannot be disabled or modified by users unless authorized to do so for technical reasons. In such cases, of temporarily disabling the antivirus software, several other measures might be needed to substitute the AV for the time that the service is down.

5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties

Concluding this series of requirements concerning the use of antivirus software, it is really important to keep the created policies and procedures documented and in use. In addition, the personnel has to know about all these in order to better prepare and defend against such attacks.

3.3.2 Requirement 6: Develop and maintain secure systems and applications

This particular requirement addresses the need of covering security vulnerabilities in order to be protected against malicious individuals. The sub-requirements of accomplishing the development and maintenance of secure systems and applications are the following:

6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities

The current sub-requirement addresses the need for the companies to be up to date against new vulnerabilities that may exist. This requires a specific process through which all the industry will be monitored for such vulnerabilities. In order for this procedures to be successful, the company must ensure that all the vulnerabilities - related information is reliable which might mean that several sources should be used, including vendor websites, industry news groups, mailing list or RSS feeds. Apart from that, having identified any possible hole in the system, the company must proceed into evaluating and ranking each one of them (high - critical). This will help companies to better and more effectively identify and deal with threats that might occur.

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

This requirement forces once again the company to cover any possible vulnerability that might be exploited by malicious users who are willing to take into their hands valuable cardholder data. To achieve this, a needed procedure is to ensure that security patches (software releases by vendors covering particular security holes) are installed at the time that those releases are published. In more particular, according to the standard, the company must apply those security patches within *30 days* of their release for critical or at-risk systems and within two or *three months* (or the appropriate time frame) for lower risk vulnerabilities.

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:

- In accordance with PCI DSS (for example, secure authentication and logging)
- Based on industry standards and/or best practices.
- Incorporating information security throughout the software-development life cycle

Covering the vulnerabilities that might exist within the company's different systems is crucial for the protection of cardholder data. To do so, it is really important to pay attention to the applications being used by the company. In more detail, the company must ensure that information security is included throughout the application's life cycle so to better understand and eventually deal with vulnerabilities that come from the applications. In addition, applications should be developed in accordance with the PCI DSS.

Going deeper to this specific requirement, specific sensitive information such as user IDs and passwords should not be included into the application's code in order to prevent any malicious user from accessing this kind of information. This means that firstly the development team and afterwards the team responsible for the application's security should review the code of the application to verify that there aren't vulnerabilities within it and that the application is being developed according to secure coding guidelines. Of course, any finding should result to the appropriate fix prior to the application's release authorized by the management.

6.4 Follow change control processes and procedures for all changes to system components

This particular requirement addresses the need of a change control process containing procedures and policies for all changes to system components. Those policies, first of all, will ensure that test environments are separate from the production one. In addition, the personnel responsible for the test environment has different duties that the team for the production environment. Another important factor to be considered is that production data won't be used for test purposes and that all the test data and account should be removed before going to the production. As far as implementation of security patches and software modification are concerned, there should be documented change control for the impact of those changes, for the authorization of that change making sure that those changes won't have an adverse effect on the system's security and lastly documentation for all the back-out procedures in case the change fails or has adverse effects.

The environments used by the company must be separated to build and maintain secure systems and applications. It is really important for the security risk of cardholder data, not to use data among the different phases of system and application development nor promote an environment instead of another. In addition, by keeping the three environments (development, test and production) separate is that, if the need for any system arise, the system can be developed and tested in environments that mirror the production environment without even interrupting it.

As mentioned above, it is really important to separate and segregate the personnel's duties between that development/test environment and the production. The intention of this requirement is to have an appropriate level of control over the company's different cardholder data environments. Apart from that, as mentioned in previous requirement for the least privileged access control, users must have access to information that is necessary for their jobs. So, sensitive cardholder data, including live PANs must not be used for testing or development purposes. In addition, users testing a production environment should not have the ability to use the same test accounts and IDs for the production environment as they did with the testing one.

6.5 Address common coding vulnerabilities in software-development processes as follows:

- Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.
- Develop applications based on secure coding guidelines.

These particular vulnerabilities along with its sub-requirements focuses on the protection of the application layer which has been recognized as high-risk by both external and internal attackers. So, the standard provides a baseline of measures to implement into their secure coding practices in order to be protected against known coding vulnerabilities. Of course, training is needed for the developing team in order to be in line with those security code best practices.

The company has to examine the policies and procedures for software development and as in any other case interview its personnel to verify that the coding vulnerabilities mentioned below are being addressed. The mentioned minimum baseline of protection includes protection for the following common coding attacks: (For more information about different kinds of attacks please refer to chapter 2.)

- *Injection flaws, particularly SQL injection*: This measure includes input validation for the data by the user and utilization of parameterized queries.
- *Buffer overflows*: This measure includes validation of buffer boundaries and truncation of input strings.
- *Insecure cryptographic storage*: This measure includes prevention of cryptographic flaws and use of strong cryptographic algorithms and keys.
- *Insecure communications*: This measure includes policies and procedures to ensure that the insecure communications are being handled by coding techniques which include authentication and encryption, as already mentioned previously.
- *Improper error handling*: This measure includes policies and procedures to ensure that there is no leakage of information through error messages.
- *Cross-site scripting* (XSS): This measure includes validation of all parameters before inclusion and utilization of escaping for sensitive content.
- *Improper Access Control*: This measure includes proper authentication of users, sanitization of users, avoidance of exposing internal object references to users and blocking access to unauthorized functions.
- *Cross-site request forgery* (CSRF): This measure includes coding techniques to verify that the applications used don't rely on authorization credentials and tokens that are automatically submitted by browsers.
- *Broken authentication and session management*: This measure includes the flagging of session tokens as secure, prevention of IDs session exposure in the URL and use of appropriate timeouts and rotation of session IDs after a successful login.

6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:

- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes
- Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.

This particular requirement addresses the need of protection against new threats and vulnerabilities on an ongoing basis when dealing with web applications on the public. In more particular, the company must review those applications by using manual or automated tools covering specific requirements or methods *annually* (at least) and installing solutions like firewall to effectively protect public facing applications.

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

Concluding this series of requirements concerning the development and maintenance of secure systems and applications, it is really important to keep the created policies and procedures documented and in use. In addition, the personnel has to know about all these in order to better prepare and defend against such attacks.

3.4 Implement Strong Access Control

3.4.1 Requirement 7: Restrict access to cardholder data by business need to know

This particular requirement addresses the need of implementing strong access control in order to restrict access to cardholder data to only authorized personnel. The sub-requirements of controlling who, how, and why cardholder data is accessed are the following:

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access

The specific requirement focuses on the access restriction to both system components and cardholder data to only personnel who really needs to have access to them so to effectively complete their job requirements. To do so, first of all the company has to define to each role the appropriate access rights and privileges to system components and data resources. Having determined the different access rights for each role, the company has simply to assign those rights to the appropriate groups and hence to the users. Finally, it is really important that all these assignments have to be performed with the appropriate documented approvals performed by authorized parties.

7.2 Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed

Following the previous requirement, the company has to create and implement an access control system for system components in order to automate the process of access restriction and assignment of privileges. In addition, as far as the restrictions are concerned, by default should be set to *"deny all",* unless intended to be allowed.

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

Concluding this series of requirements concerning the restriction of access to cardholder data by business need to know, it is really important to keep the created policies and procedures documented and in use. In addition, the personnel has to know about all these in order to better prepare and protect cardholder data.

3.4.2 Requirement 8: Identify and authenticate access to system components

This particular requirement enhances the need of Strong Access Control implementation by assigning unique identification (ID) to the personnel in order to successfully track all the actions performed by each one of them on critical data and systems. The requirements bellow apply to all accounts having administrative capabilities and all the accounts used to view or access cardholder data or to access systems with cardholder data.

However, some of them are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction.

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:

As described in the introduction of the requirement, the company has to assign to all users that access system components or cardholder data a unique ID. Apart from that assignment, there must be a specific process for the ID management including any possible action to it such as deletion and modification. In addition, every time an employee leaves the company his or hers access rights should be revoked to prevent any unauthorized access to cardholder data and other sensitive information. This also extends to the return of any physical authentication method the employee used including smart cards, tokens etc. The needed management of the IDs has to be also performed for remote access situations.

In addition, even if the employee hasn't left the company, any account that hasn't been used for at least *ninety (90) days* should be removed or disabled. Furthermore, the standard requires a limitation on the *repeated access attempts for the same user ID to maximum six (6) and a reactivation of minimum thirty (30) minutes* to prevent a malicious user for continuously trying to guess a password. Another needed configuration for the accounts requires the re-authentication of the user whenever the account session stays idle for more that fifteen (15) minutes.

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.

This particular requirement enhances the security of the systems as it requires an authentication method to be used in addition to unique IDs described above. In more detail, to prevent sniffing of authentication credentials like passwords, strong cryptography should be used during transmission of this information. In cases of altering authentication credentials the user should be validated first in order to prevent the so called *social engineering*.

The requirement also includes guidance for credentials complexity and strength used according to which passwords and phrases must have at *least seven (7) characters* and contain *both numeric and alphabetic characters*. In addition, system configuration settings must force users to *change their passwords and passphrases at least every ninety (90) days* and when this change occurs there must be *check for the last four (4)* to prevent the same credential to be used over and over again. Apart from that, first-time passwords for new users, and reset passwords for existing users have to be set to a unique value for every user and must be changed after the initial use.

8.3 Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance)

This particular requirement focuses on high-risk connections like remote network access from outside of the corporate network. It addresses the use of a two factor authentication for such connections which means that in order to successfully connect and authenticate one should provide two forms of authentications meaning something he or she knows, has or is. This specific requirement applies only to situations that the user is able to connect to or impact with the cardholder environment.

8.4 Document and communicate authentication procedures and policies 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.

As with all other similar situations, the users of the company must be aware about the authentication procedures and policies. So, this information must get to their hands in order for all of them to be aware and in line with the authentication requirements. In order to further help users, policies must include guidance on how to select and use the needed authentication methods and fulfill the authentication requirements.

8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:

- Generic user IDs are disabled or removed.
- Shared user IDs do not exist for system administration and other critical functions.
- Shared and generic user IDs are not used to administer any system components.

This particular requirement helps the whole process of tracking users' actions. Meaning that it prevents users from using the same authentication credentials in order to successfully track and identify any user's action. In addition, this specific requirement contains a specific good practice, which is intended to *become a requirement on June 30, 2015*. This good practice, mentions that the particular requirement also applies to service providers using remote access to customer premises.

8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:

- 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.

Continuing the previous requirement and the need of identifying and tracking user's actions, this particular requirement addresses that each authentication mechanism should be used by unique accounts and not by any means by multiple accounts which might result to hardly identify each action. In addition, to accomplish this, possible physical and logical methods should be in place to prevent the multiple assignment of authentication mechanisms to individuals.

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).

This requirement contains measures to protect databases containing sensitive cardholder data. In more detail, access to databases must be performed through *user authentication* in order for the authenticated user to be successfully tracked after being identified. In addition, only the database administrators should have the ability to directly log in to databases. By any means, access to the database through queries and not directly, should be performed only by programmatic methods.

8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties

Concluding this series of requirements concerning the identification and authentication of access to system components, it is really important to keep the created policies and procedures documented and in use. In addition, the personnel has to know about all these in order to better prepare and protect cardholder data.

3.4.3 Requirement 9: Restrict physical access to cardholder data

This particular requirement introduces the need of physical security as the first layer of defense for the cardholder environment. However, a series of controls should be in place in order for this defense to be effective and everyone involved should have in mind that this control is only as effective as its weakest link. Overall, companies have to design, implement, and manage physical security controls that are appropriate to their specific needs and complement logical and administrative security controls.

9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment

The first of the requirements, addresses the need of physical security controls for each area within the cardholder environment. Companies have to verify that each access is controlled with badge readers and other devices. In addition, for a random number of systems, attempts to log into systems by system administrator should be examined.

It is really usual for malicious individuals attempting to break into cardholder environments to try bypass monitoring controls that are being implemented. To protect against such actions, companies can use video cameras to monitor individual physical access to such sensitive areas. Of course, the cameras used and any other access control mechanism should be protected from tampering or being disabled because we really need their 24/7 functionality. In addition, the data captured from those devices must be kept for at least a three month period.

Further on, this requirement protects against attackers from trying to connect into the network by compromising a network jack or port. The last point of this requirement is the protection of physical access to wireless components and devices by securing networking and communications from *traffic interception*.

9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include:

- Identifying new onsite personnel or visitors (for example, assigning badges)
- Changes to access requirements

- Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).

This particular requirement addresses the need of easily and effectively distinguishing onsite personnel and visitors in order to prevent the unauthorized ones from gaining access to sensitive cardholder data. To further help with this need, the company should examine and implement *identification methods* so to clearly distinguish the visitors from the onsite personnel.

9.3 Control physical access for onsite personnel to the 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.

Continuing the need of controlling the physical access to the cardholder environment the onsite personnel must be granted access upon authorization and based on individual job function. Furthermore, any time that any employee leaves the company he or she must return or disable their personal physical access mechanisms to prevent any unauthorized access in the future by those individuals.

9.4 Implement procedures to identify and authorize visitors

As with the previous requirements, this specific is used for identifying and authorizing visitors. This will help the company's personnel to better and more effectively monitor visitors' actions while being inside the cardholder environment. More particularly, visitors should be escorted at all times while onsite (in areas maintaining or processing cardholder data) while at the same time observing the use of visitor badges (that expires) to verify that the requirement for escorting through the cardholder environment is fulfilled.

Another important action is that of logging the visitor's actions inside the cardholder environment. Furthermore, those logs must contain specific information such as the visitor's name, the firm represented and the onsite personnel that authorizes the visitor's physical access. Those logs, must be again maintained for of period of three months.

9.5 Physically secure all media

This particular requirement addresses the need of physical protection of all media in order to prevent any unauthorized access to it and prevention of any action on it such as viewing, editing and printing.

Apart from the protection of the media it is really important to keep backups of the media in secure locations, preferable away from the original ones.

9.6 Maintain strict control over the internal or external distribution of any kind of media

It is crucial for the media protection to maintain procedures and policies for the distribution of this data. In more detail, classification of the media should be contacted in order to determine and distinguish sensitive information contained in that media. In addition, in many cases, organizations may have to transport media containing cardholder data. This practice should be avoided as much as possible and only performed when necessary for critical business operations. In such cases, the organizations has to ensure that a secured courier is used or any other delivery method is used that can be accurately tracked. This tracking capability enables the organization to monitor data when it is not in their immediate possession. Finally, in cases that the media

has to be transported from a secured area, it is really important to ensure that the appropriate management approvement is obtained.

9.7 Maintain strict control over the storage and accessibility of media

Continuing the previous requirements, it is really important to create and use policy for storage and maintenance of media. This kind of media inventory can help against situations of stealing or just missing media without even noticing it.

9.8 Destroy media when it is no longer needed for business or legal reasons

Regarding the periodic destruction of media storing information there should a policy for this specific requirement. More specifically, this requirement addresses the need of deterring any malicious from reconstructing media and gaining access to the information included. To do so, the organization should proceed to the destruction of hard-copy materials containing information using any possible method of destruction. When dealing with electronic media the organization must ensure that the information stored on it remains unrecoverable.

9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution

Protecting card-reading devices is highly crucial for the protection of cardholder data during transactions against attacks such as *skimming* which has been already described in the first Chapter of the current document. These particular instructions are treated as best practices until June 30, 2015, after which they become requirements.

Those best practices, among others, include the following: First of all, it is necessary to maintain an up-to-date list containing all the related POS devices with all the needed information such as model, location and device serial number. As with all other similar situations, the company has to ensure that the list is kept safe from alterations and up-to-date. In addition, in order to be protected against possible fraudulent devices the company has to use procedures for device inspections to protect against tampering and/or substitution.

Another important factor, is the level of awareness of the personnel regarding attempts of tampering and replacement of POS devices by attackers. In more detail, the personnel has to learn to verify the identity of anyone trying to physically access the device, not to install - replace - return those devices without any verification. In addition, the personnel has to be aware of any suspicious behavior regarding the physical protection of the devices and moreover report this behavior to the appropriate authorities.

9.10 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties

Concluding this series of requirements concerning the identification and authentication of access to system components, it is really important to keep the created policies and procedures documented and in use. In addition, the personnel has to know about all these in order to better prepare and protect cardholder data.

3.5 Regularly Monitor and Test Networks

3.5.1 Requirement 10: Track and monitor all access to network resources and cardholder data

This particular series of requirements addresses the need of logging mechanisms, the importance of which has already been mentioned throughout the requirements so far. Once more, system activity logs through constant monitoring is crucial for the protection of cardholder data and compliance with the PCI DSS. By regularly testing all the critical network components of the cardholder data environment, organizations can identify and correct any vulnerabilities found before their exploitation. In more detail, requirements regarding the monitoring and testing of networks are being discussed, including how the networks must be monitored and tested, how often must be monitored and tested, and what kind of audit trails have to be established in order to be compliant with the standard.

10.1 Implement audit trails to link all access to system components to each individual user

As already mentioned, it is really important to keep track of user access to any component of the cardholder data. To do so, it is crucial to keep audit trails of these accesses for each individual user of the cardholder environment.

10.2 Implement automated audit trails for all system components to reconstruct the following events:

- All individual user accesses to cardholder data

  This kind of event covers any user access to any system component of the cardholder environment to proactively identify whether an user account has been compromised.

- All actions taken by any individual with root or administrative privileges

  This kind of event covers any action performed by an account with increased privileges.

- Access to all audit trails

  This kind of event covers any access to the audit trails being held by the company for the purposes of the current requirement.

- Invalid logical access attempts

  This kind of event covers any illogical access attempt to system component in order to detect irregular attempts by malicious to access those components including multiple invalid login attempts performed by a *brute force attack*.

- 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

This kind of event covers logging of the identification and authentication mechanisms. This concerns the use of those mechanisms, the elevation of privileges and any other change, addition or deletion of any account with root or administrative privileges.

- Initialization, stopping, or pausing of the audit logs

This kind of event covers any possible action on the audit logs such as initialization, stopping and pausing. Because it is really often for attackers to try disable audit logging in order to perform their malicious actions.

- Creation and deletion of system-level objects

Lastly, this kind of event includes actions of creation and deletion for the system-level components which might indicate any attempt by the attacker to control a function or operation of that system.

10.3 Record at least the following audit trail entries for all system components for each event:

- 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

This particular requirement contains the necessary information that must be included in an audit trail in order for the team to quickly identify a potential compromise along with the need information about that compromise including the person who performs attack, the exact time and the location. So, when the information derived from the individual components of this requirement is properly aggregated, it offers the details required for incident response and investigation.

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

This particular requirement address the need of time synchronization between the systems of the cardholder environment to make it easier for the team to inspect the logs produced by those systems. So, the company must ensure that critical systems have the correct and consistent time and the configurations related to time are properly protected to prevent any modification by unauthorized personnel. In addition to that, it must be verified that any alteration to those settings is logged and constantly monitored.

10.5 Secure audit trails so they cannot be altered

Of course, since the information provided by audit trails is required to validate the findings of an incident response investigation, the integrity of the audit trails must also be protected as stated before. That is because, if audit trails are not maintained in a secure environment, then an attacker can easily modificate this data in an attempt to hide malicious behavior. To achieve this, *access control mechanisms, physical segregation, and network segregation* must be implemented in order to protect audit trails. Furthermore, file containing that information must be regularly backed-up and last but not least file-integrity monitoring (FIM) or change-

detection software on logs can be used to ensure that existing log data cannot be altered without generating alerts.

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity

This requirement implies the logic of the series of requirement 10 according to which it is really important to review logs in order to identify any anomaly or suspicious activity through either a manual or automating (by using specific tools) process. In more detail, first of all, daily review of the logs minimizes the appearance of a potential breach. To be more accurate, the logs should contain all security events, logs of all system and critical system components and logs of all servers and system components that perform security functions. Apart from those logs, any other system component logs must be periodically reviewed according to the organization's policies and risk management strategy with significant attention to exceptions and anomalies during the investigation.

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)

It is really important not only to log events for further analysis but also to keep a log history for at *least one year* and at a minimum of *three months* for online data (immediately available) to quickly identify and minimize the impact of a potential data breach.

10.8 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

Concluding this series of requirements concerning the monitoring and testing of networks, it is really important to keep the created policies and procedures documented and in use. In addition, the personnel has to know about all these in order to better prepare and protect cardholder data.

3.5.2 Requirement 11: Regularly test security systems and processes

As already mentioned, the regular testing of the organization's systems is crucial for the compliance with PCI DSS. However difficult this process might appear, it is indeed the best way to validate PCI DSS compliance of the organization's network. That is because, testing confirms the appropriate level of protection within the infrastructure, but it also helps the organization determine and identify any vulnerability during the completion of the company's routine security practices and daily operations. As far as the current requirement is concerned, the intention of such tests is to validate the security posture of the system and identify any possible weaknesses that are likely to be exploited by attackers. So, having fulfilled the current requirement, organizations can get a comprehensive picture of their cardholder data environment. Furthermore, it is really important to state that there are many different strategies, techniques, tactics, and tools that can be utilized to accomplish the needed security testing of the requirement 11.

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

This particular requirement focuses on wireless technology and more particular on wireless access points within the cardholder data environment. So, the requirement addresses the need of *quarterly* examining the

created policies and procedures regarding the detection and identification of all the wireless access points whether authorized or unauthorized. Apart from the access points it is really important to examine WLAN cards inserted into system components, any portable or mobile device used for wireless access point creation and finally any wireless device attached to ports or other devices.

In addition, results from wireless scans must be examined to verify that all the access points have been identified. These scans must be performed to all system components and facilities at a *quarterly*, at least, basis. In situation of automatic monitoring, the company should use alerting in order to be properly notified.

As in several other similar situations, it is really important to keep an inventory of authorized wireless access points and use incident response procedures for any case that an unauthorized wireless access point is detected.

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)

This particular requirement demands the execution of internal and external network vulnerability scans at least once a *quarter* or after any significant change in the network. The first important note from this requirement is that the standard requires both internal and external scans. The scan must be performed both by internal and external aspect because each of the vulnerability scans examines vulnerabilities from a different perspective.

The other important factor from the current requirement is that internal and external scans must be performed after any significant changes occur in the cardholder environment. These changes might include, among others, changes to network topology, firewalls and product upgrades. So, network vulnerability scanning will identify any new vulnerability to be quickly and successfully remediated in order to protect the integrity and security of the cardholder data.

Going deeper to the needed vulnerability scans, it is important to note that those quarterly internal vulnerability scans/rescans have to be conducted until all high-risk vulnerabilities (please refer to Requirement 6: Develop and maintain secure systems and applications) are covered. In addition, it is really important those scans to be performed either by qualified internal personnel or qualified external third party.

For the external vulnerability scans, it is necessary to be conducted by an Approved Scanning Vendor (please refer to Operation of Compliance). In any case, the scan results have to be reviewed to verify that requirements for a passing scan have been met and of course that an authorized ASV performed the scans.

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

First of all, as easily understood from the above, there are some particular requirements concerning the penetration testing. External and internal penetration testing must be performed at least at *a yearly basis* after any significant infrastructure or application upgrade or modification. Like mentioned in the previous requirement, the pentest has to be performed by a qualified internal resource or qualified external third party. Finally, penetration testing is an important and useful method to confirm that any segmentation in place to isolate the cardholder data environment from other networks is effective which again must be performed at least *annually* and after any changes.

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

This particular requirement addresses the need of IDS/IPS use in order to successfully monitor all the traffic at the perimeter of the cardholder data environment and at all the critical points of the environment. These technologies can be utilized to alert the organization to a potential breach in the cardholder data environment. In addition, this particular requirement states that the used techniques are properly maintained and kept up to date. Similar to antivirus definitions and engines, these components are critical to the proper functioning of these tools. This means that, these technologies are only effective at identifying and preventing incidents based on the information stored in the engine. So, if the engine is not kept up to date, organizations run the risk of not being able to properly identify the latest threats.

11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly

This particular requirement addresses the need of detection of any change on critical system files, configuration files or content files. To do so, a change-detection mechanism such as File Integrity Monitoring (FIM) should be implemented to monitor critical files and notify any time that a change on those files occur. As for the notification, an alert should be automatically created every time a change is detected to successfully and proactively notify authorized users.

11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties

Concluding this series of requirements concerning the regular testing of security systems and processes, it is really important to keep the created policies and procedures documented and in use. In addition, the personnel has to know about all these in order to better prepare and protect cardholder data.

3.6 Maintain an Information Security Policy

3.6.1 Requirement 12: Maintain a policy that addresses information security for all personnel

The base of an effective information security program is as already stated an information security policy. That is because this particular document holds the organization's strategic security objectives in an organized and fully documented format. In addition, the information security policy acts as a roadmap towards the organization's process of PCI DSS compliance. Apart from that, an effective policy helps employees to make better decisions by choosing alternatives that will add value and in overall strengthen the organization's security posture. The thing is that, without having and complying with an information security policy, employees of the organization cannot be held accountable when it comes to compliance with the entity's information security program and protection of the cardholder data environment. This particular last requirement, addresses the need of developing, maintaining, and distributing an information security policy towards the PCI DSS compliance.

12.1 Establish, publish, maintain, and disseminate a security policy

The first requirement, of course addresses the need of examination of the information security policy to verify that it is published and spread to all the company's related personnel. Furthermore, the policy must be reviewed at *least annually* and changed accordingly to any update needed.

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 risk assessment.

The role of a risk-assessment process has already been mentioned regarding the identification of threats and vulnerabilities. This particular process must have specific characteristics as mentioned in the bullets of the requirement. Furthermore, it is really important to keep the process documented (formal risk assessment) and of course review the risk-assessment documentation.

12.3 Develop usage policies for critical technologies and define proper use of these technologies

This particular requirement addresses the need of development and examination of usage policies regarding critical technologies. In more detail, usage policies must first have processes for explicit approval from authorized parties in order to use the technologies and include processes for all technologies used for the user authentication with user ID and password or any other authentication item.

In addition, the usage policies have to define a list of devices and personnel who are authorized to use those devices. Another important factor, is to maintain a method in those usage policies to successfully identify the owner, contact information and purpose to prevent any unauthorized user from creating a back door on the network.

Apart from the above, it is necessary for the usage policy to define acceptable uses and network locations for the technologies in order for the company to better manage and control any misconfiguration and prevent any back door. In addition, the usage policies have to include a list of company-approved products. Another important factor of this requirement is to automatically disconnect sessions for remote-access technologies after specific time period being inactive. Apart from that, regarding the remote-access technologies it is crucial for them to be activated to vendors and business partners only when necessary and of course deactivated afterwards. Lastly, personnel using remote-access technologies to access cardholder data should be prohibited actions like copy and move on local hard drives and any removable media without the appropriate authorization.

12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel

This particular requirement addresses the need of identifying the security responsibilities and roles of all the related personnel of the organization to prevent unsecured and outdated implementation of technologies.

12.5 Assign to an individual or team the following information security management responsibilities:

- 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

This particular requirement contains a series of sub-requirements regarding the responsibilities that are assigned to individuals or a specific team for the information security management. First of all, the *establishment, documentation and distribution* of security policies must be formally assigned. In addition, results of monitoring process as described previously (alerts and information) have to be *distributed* to the appropriate personnel including the incident response and escalation procedures which must also be established, documented and distributed to the appropriate personnel. Another important requirement is the administration of user accounts and authentication mechanisms which have to be appropriately and formally assigned. Lastly, all access to data has to be formally monitored and controlled.

12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security

This particular requirement addresses the need of awareness as it has been already described as last sub-requirement in each requirement of the PCI DSS. It is really important, for the personnel to be fully aware of the importance of security of the cardholder data in order for the protection to be more effective without errors. In more detail, every employee must be trained when hired and at *least annually* for cardholder data security and again annually demand from the personnel to acknowledge that they have read and understood security policies and procedures.

12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources

The intention of this requirement is to "check" the background of the person to be hired to reduce the possibilities of cardholder data being used for malicious purposes by the personnel. These checks might include previous employment history, criminal records, and other 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

This particular requirement focuses on service providers with whom cardholder data is shared or generally that affect the security of it. First of all, the standard forces the company to keep an updated list of service providers keeping track of anyone using the cardholder data. In addition, it is important to maintain a written agreement as an acknowledgement of the service providers which evidences their commitment of maintaining proper security of cardholder data that it obtains from its clients. Apart from that, the company must ensure that there is an established process for engaging service providers prior to establishing a formal relationship with the service provider.

Another important factor of this specific requirement concerning service provider is to monitor their PCI DSS compliance status at least *annually*. Lastly, information should be maintained about the specific PCI DSS requirements that are managed by service providers and by the company.

12.9 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 (best practice until June 30, 2015)

This specific requirement is quite clear and focuses again on service providers. It requires once again a level of commitment and acknowledgement towards the proper security of cardholder data that they obtain from the companies that cooperate.

12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.

This last requirement of the PCI DSS addresses a very important demand that of an incident response plan which must be thorough and contain some, according to the requirement, key elements. So, this plan must include *roles, responsibilities, communication and contact strategies* in the event of a compromise including, at a minimum, *notification of the payment brands, specific incident response procedures, business recovery and continuity procedures, data backup processes and analysis of legal requirements for reporting compromises*. In addition, there should be coverage and responses of all critical system components and finally reference or inclusion of incident response procedures from the payment brands.

Apart from the existence of the incident response plan the company must ensure that the plan is tested at least annually and that specific personnel is available on a 24/7 basis to respond to alerts. For better results, the personnel that has any kind of responsibility regarding the cardholder data should be properly trained. Finally, a process should be developed to modify and evolve the incident response plan according to lessons learned.

Chapter 4

Pentesting

As mentioned in the Operation of Compliance section, depending on the level, the organization should present the results of a quarterly network scan executed by an Approved Scanning Vendor and present the results of internal vulnerability scans and results from application and penetration tests. In addition to that, according to the requirement 11.3 of PCI DSS, there are some particular requirements concerning the **penetration testing**. External and internal penetration testing must be performed at *least at a yearly basis* after any significant infrastructure or application upgrade or modification. Furthermore, the pentest has to be performed by a qualified internal resource or qualified external third party. Finally, penetration testing is an important and useful method to confirm that any segmentation is in place to isolate the cardholder data environment from other networks which again must be performed at least annually and after any change.

Throughout several points of the PCI Payment Card Industry Data Security Standard as mentioned above, the process of Penetration Test is being required for the compliance with the standard. During the current chapter, the basics of this needed process are analyzed along with the general principles and best practices applied to the latest version of the standard.

4.1 Basics of Penetration Test

The process of *penetration test* (also known as pentest) targets into identifying the systems under investigation in order to achieve a certain goal. In addition to that, review of available information in addition to the needed means to achieve that goal has to be performed and collected.

In more detail, a penetration test mostly likely targets into the following: First of all, the pentest aims to determine whether a particular set of attacking scenarios through which the attacker can gain unauthorized access to cardholder data might occur. So, to achieve that all the vulnerabilities that the system might have should be identified via a series of different tools that could be used during the security assessment.

Having identified the possible threats and vulnerabilities the penetration test should ensure that all the applicable controls, such as *scope, vulnerability management, methodology, and segmentation* that are required by the PCI DSS exist in order to detect and respond to attacks. All those results of the pentest can be used to prove that further actions are needed including increased investments in security personnel and technology.

As for the different types of penetration tests that exist there are three of them. First, the *white box* type includes those pentests that are being contacted having complete knowledge and background of the network and/or applications to be assessed. On the opposite side, *black box* penetration tests provides only basic or even no knowledge at all about the component under investigation. In between, during *grey box* penetration tests the company might provide some basic knowledge to the pentester about the target systems. For the purposes of the PCI DSS, most of the required penetration tests are being contacted as either white or grey box in order for those tests to be more efficient in terms of time and resources spent.

Concluding the basics of penetration tests, we should clear things out about the differences with *vulnerability scans* that must also performed according to PCI DSS. First of all, their purposes are different because vulnerability scans target on identifying vulnerabilities that might cause harm to the company whereas pentests' goal is to find certain ways of exploiting those vulnerabilities. Apart from that, the time period of execution differs as vulnerability scans should be performed quarterly or after a significant change occurs and for a very short period (usually within seconds or minutes per host) whereas pentests must be contacted at least annually and after significant changes for longer period of times such as days or even weeks. Of course, we should keep in mind that the standard cannot clearly define significant change for each organization but overall as significant change we can consider any change that could affect the organization's security. Lastly, vulnerability's scan report includes potential risks that have been identified ranked according to known base scores for each vulnerability. In contrast, reports of penetration tests should include description for each vulnerability that was verified during the assessment along with methods of exploiting.

Finally, another thing to consider is the person who will be responsible to perform the penetration test. That person, could be internal personnel properly trained for that purpose or an external third party, must be independent of the organization's systems to be assessed. In more detail, there are certain best practices and guidelines that the organization should follow in order for the pentest to be successful. First of all, the person mentioned above that will be responsible to perform the test should hold some specific certifications indicating some level of skills and certain abilities. There are several kinds of certifications such as the Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH), CREST Penetration Testing Certifications and several others. Of course, certifications are not enough to prove someone's knowledge regarding pentests. Previous experience, not only in penetration tests but also in technologies of the target environment, is also an important factor to consider in order to choose the appropriate Pentesting team. It can be measured in years of pentesting experience while references from other companies might also help decide.

4.2 Fitting into PCI DSS

According to the standard, external (public facing) and internal (LAN) penetration testing must be performed at least at a yearly basis after any significant infrastructure or application upgrade or modification. These testings can be executed in several locations of the organization's environment focusing on several different components of it apart from data such as *applications, processes, network connections, resources, assets and any other element of the cardholder data environment*. As already mentioned, the pentest has to be performed by a qualified internal resource or qualified external third party. Of course, penetration testing is an important and useful method to confirm that any segmentation in place to isolate the cardholder data environment from other networks is effective which again must be performed at least annually and after any changes. But how exactly is the cardholder data environment is defined and what is the exact scope of the pentest?

First of all, as far as the *external penetration tests* are concerned the scope is the external perimeter of the organization and any critical system that is connected to it (with any possible way such as VPN and dial-up connections) or it can be accessed through public networks by using both application and network layer testing. On the opposite, *internal penetration tests* target into assessing the internal network of the cardholder environment including again any critical component that may affect the environment's security. Another key factor affecting the assessment's scope is that of the implementation of *segmentation controls* which must be assessed via segmentation checks in order to verify their effectiveness to separate non cardholder data environments from the cardholder data environments.

In order for a component to be considered as out of scope of the PCI DSS compliance process it must be separated from the environment in that way that possible compromise of it would not affect the cardholder environment. In order to prove this statement and to make sure that possible compromise of them is not affecting the overall security, the pentest should include those components in the assessment process.

4.3 Clearing Definitions

Having analyzed penetration tests' scope concerning PCI DSS it would be really useful to define some of the basic terms that have been mentioned during the previous paragraphs. First of all, PCI DSS considers as *critical systems* those that are part of the cardholder's data process or protection but it is always up to each organization to decide their criticality. Of course, as already mentioned there might be components outside of the environment that affect its overall security and as a result recognized also as critical systems.

In addition, in the previous section *application and network layer* testing has been mentioned as one of the actions in scope of each pentest. These actions target into identifying any security weakness due to faults/bugs in applications or any other possible mistake (application code, configuration, usage etc) in order afterwards to cover any recognized vulnerability by *reconfiguring, rewriting or updating the affected software*. There are some certain use cases for this specific plan of actions regarding the exact scope of the pentests. In more detail, in case that the application is being used for *user authentication* the pentest should include -among others - testing with any possible role (such as the customer itself) and type of access to the api even for those who should not be authorized to use and access the appropriate cardholder data. As mentioned in the Payment Application Data Security Standard (PA-DSS) section, there are certain payment applications that comply with the PA DSS standard (please refer to the uploaded list of the Validated Payment Applications). For those applications, pentests should not target into assessing their functionality but only operating system and any involved process.

Another important component to consider is that of *web applications* which are being used by the organization for several purposes. For this certain use case, the organization is not responsible for assessing its *source code* but only ensure that the implementation, configuration and maintenance are proper for securing cardholder data. Continuing, an important "tip" for penetration tests is to execute them in exact similar environments (testing) properly designed and configured for such purposes. In that way, the organization could easily proceed with the everyday procedures without any disruption to its production systems. Of course, any discovered vulnerability must be corrected in the production environment and tested once again.

According to Requirement 11: Regularly test security systems and processes, testing to validate any segmentation and scope-reduction controls is required including but not limited to actions to identify paths between the outside of the environment and the inside in terms of assessing each segmentation method used. In such scenarios, the team contacting the penetration test might use several methodologies in order to successfully assess all the possible types of segments within the organization. For better results, the pentester must gain complete knowledge prior to the assessment.

An important threat that an organization might face and that an attacker might use to get access to sensitive cardholder data is that of *social engineering* through which people might make wrong decisions which result into reveal of information or performing actions without even willing to. One of the goals of penetration testing, but not a requirement, is to discover such forms of attacks that might have arisen to the organization.

Of course, there are different methods of performing such a social engineering test and can vary depending on the size and complexity of the organization including among others *one-to-one interviews* in order to interact with the personnel and any logical action to achieve manipulation. It is up to the organization to include such tests in the penetration testing procedure and decide about its characteristics such as frequency, details etc. In order to remediate this specific vulnerability, if decided to perform such tests, the organization might consider to enhance its training and education programs.

4.4 Penetration Testing Process

4.4.1 Preparation

As with any other activity described so far, it is really important to get prepared and perform some sort of prework in order for the actions to become successful and get the desired results. This also occurs for the penetration test activities described so far and which also have to be contacted through different phases each one of which are equally important. So first of all, during the first phase of the *Pre-Engagement*, all the participants of the PCI DSS compliance process of the organization must obtain *knowledge* about the upcoming penetration test including any kind of detail. Next, the organization should proceed with defining the exact *scope* of the pentest which should be cross checked by both the organization and the pentester in order not to forget any system and exclude it - by mistake - from the assessment.

In addition to that, an important category of prerequisites to consider is the detailed *documentation* containing among others details of the assets within the scope, configuration and implementation guides, network topology, details regarding the cardholder environment, etc in order for the pentester to fully understand the scope and the actions that should be followed during the assessment.

Having defined the *scope* of the penetration test and *documented* all the needed details of the project it is really important to agree upon all these prerequisites (including the level of detail of the exploitation, the exact time of the assessment, how the assessment will be contacted, use of automated tools, tools to be used - whether they affect the environment, presentation of results - constant or only final ones, sensitive information disclosure etc.) of the preliminary phase. Of course, in order to determine whether the assessment is successful or not the team should decide (early in the preliminary phase) some *success criteria* setting at the same time the limits and expectations of the assessment. Another thing to be considered and agreed is the actions to be taken when a third party is engaged during the penetration testing. This means that, as already mentioned, within the scope of the pentest will not be included systems that are being provided by an external third party and that an approval should be provided by that party in cases that the assessment needs to include those systems.

Another helpful approach that the pentester might use is that of *reviewing threats and vulnerabilities* that were identified during previous assessments while paying attention to upgrades taking place, possible data breaches, and validation of previous findings and of course review of reports. All these would help the pentester to better identify and validate those vulnerabilities and gain some time while trying to identify new ones. Lastly, the pentester should avoid assessing systems that are being used for security purposes such as intrusion prevention systems (IPS) and web application firewalls (WAF).

4.4.2 Assessment

Following the prework that is really necessary for the penetration testing procedure the organization has to proceed of course with actions for the pentest itself. There are different approaches, methods and tools that can be used depending on each environment and the methodologies that the pentester uses. However, there are also some best practices regarding the actions to be contacted. First of all, it is highly important for the pentester to have complete unrestricted network access to the system under investigation in order to prevent any disruption or access blocking to those systems.

As previously mentioned, when assessing *applications* the pentester should be provided with accounts and credentials of different roles of the application so to validate that each role is limited to execute only the predefined actions. Apart from the existing accounts, the organization might decide to create new accounts only for the pentester to use them. In such situations, it must be ensured that those accounts offer the ability to test all the needed features of the application without any interruption. Continuing, when assessing the *network* layer of the organization it is more suitable to use automated tools such as *Metasploit, the Nessus Vulnerability Scanner, Nmap, Burp Suite, OWASP ZAP, SQLmap, Kali Linux, and Jawfish*. Using the results of those tools the pentester can then proceed with the manual exploitation of the identified vulnerabilities in order to validate them and ensure that no false positives are included in those results.

During the analysis of the penetration testing procedure it was mentioned that it is an important and useful method to confirm that any segmentation is in place to isolate the cardholder data environment from other networks which again must be performed at least annually and after any changes. So, by contacting the appropriate segmentation checks - either to each of the segment part or to a representative number of them - the pentester should be able to validate that all the isolated LANs of the organization's network are really isolated from the cardholder environment and that there is no possible way of getting into the environment from that isolated segment.

4.4.3 Following the Pentest

After contacting the initial penetration test there are some actions to be performed by both the organization and the pentester in order for the assessment to have positive impact to the PCI DSS compliance process. First of all, all the identified vulnerabilities resulted from the penetration test must be investigated so to validate and remediate the initial cause of the problem. Apart from that, it must be examined whether the identified vulnerabilities may exist in other instances of the systems. This means that the needed remediation must include those forms as well. After having executed all the decided and suggested actions to remediate the discovered and cross-checked vulnerabilities, the organization should proceed with the *retesting* activities only on the identified vulnerabilities of the initial assessment to check whether the implemented controls successfully mitigate them. An important thing to keep in mind is that the time period of the retest should not be too long because in those situations penetration test might also be needed again.

In addition to the execution of a retest it is important to proceed with the necessary actions of leaving the organization's environment to its initial state as well as reporting and documentation including first of all any change that occurred to the environment from the pentester during both the initial and the retesting activity

and details about the contacted pentest. In more detail, those reports have to include details about the findings - either validated or not - that were identified and need to be mitigated. In addition, mentioning and analyzing those findings, Industry Standards references give the pentester the ability to assign severity score to each of the finding indicating their risk in order to prioritize their remediation as shown in the Figure 17: Findings Matrix. There are different references such as the *National Vulnerability Database (NVD), Common Vulnerability Scoring System (CVSS), Common Vulnerabilities and Exposure (CVE)* etc.

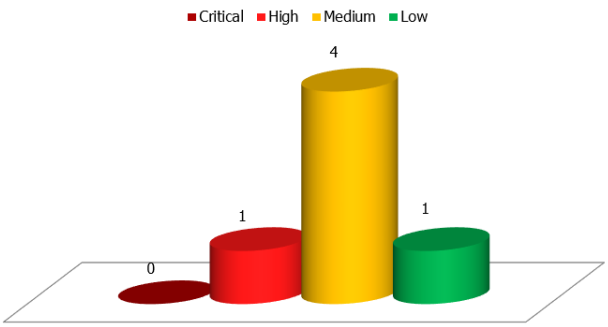


Figure 16: Graphical Representation of Findings

#	Finding	Vulnerable Point	Overall Rating/CVSS/ CWSS Score (Beta)	Remediation Cost	Ease of Detection	Consequences	Remediation	Reference
1.	**Reflected Cross-Site Scripting Attack** Web server vulnerability to Cross-Site Scripting attacks		High / CVSS Base Score : 7.6	Low	Easy	**Confidentiality loss, Denial of Service**	It is recommended to filter and escape for XSS	For more information please refer to Subsection **3.2.1**
2.	**Unencrypted Viewstate Parameter** The __VIEWSTATE parameter is not encrypted		Medium / CVSS Base Score : 5	Low	Easy	**Denial of Service**	It is recommended to encrypt the ViewState parameter	For more information please refer to Subsection **3.2.2** **CVE-2005-1665**
3.	**Internal Error (500)** Several 500 Internal Server Errors are presented, possibly disclosing sensitive information about the web application		Medium / CVSS Base Score: 5	Low	Easy	**Man -in-the middle attacks, Confidentiality loss**	This error can only be resolved by fixes to the Web server software	For more information please refer to Subsection **3.2.3**
4.	**Dom-based Open Redirection** Possible redirection to arbitrary third-party domain, resulting in many vulnerabilities, such as users' phishing		Medium / CVSS Base Score: 5	Low	Easy	**Man -in-the middle attacks, Confidentiality loss**	It is recommended to filter and escape for XSS	For more information please refer to Subsection **3.2.4**

Figure 17: Findings Matrix

Overall, the penetration testing report should include as a baseline the following:

- Executive Summary
- Overview of Findings
- Scope
- Rules of Engagement
- Methodology Overview
- Attack Scenarios
- Findings and Recommendations
    - Findings Matrix
    - Findings Details

Whereas, a retesting report should include as a baseline the following:

- Executive Summary
- Date of Initial Test
- Date of Retest
- Overview of initial Findings and testing ones

Chapter 5

Roles and Responsibilities

The current chapter analyzes the applied roles and responsibilities for the organization regarding the PCI DSS compliance process and the overall protection of cardholder data. Of course, anyone involved in that process is responsible for the protection of cardholder data. That is the reason that each organization should clearly define and share its employees' responsibilities regardless their position in the hierarchy. In order to better understand the roles and responsibilities analyzed during the next sections, a typical organizational chart is presented in the following figure containing among others the basic roles mentioned below.

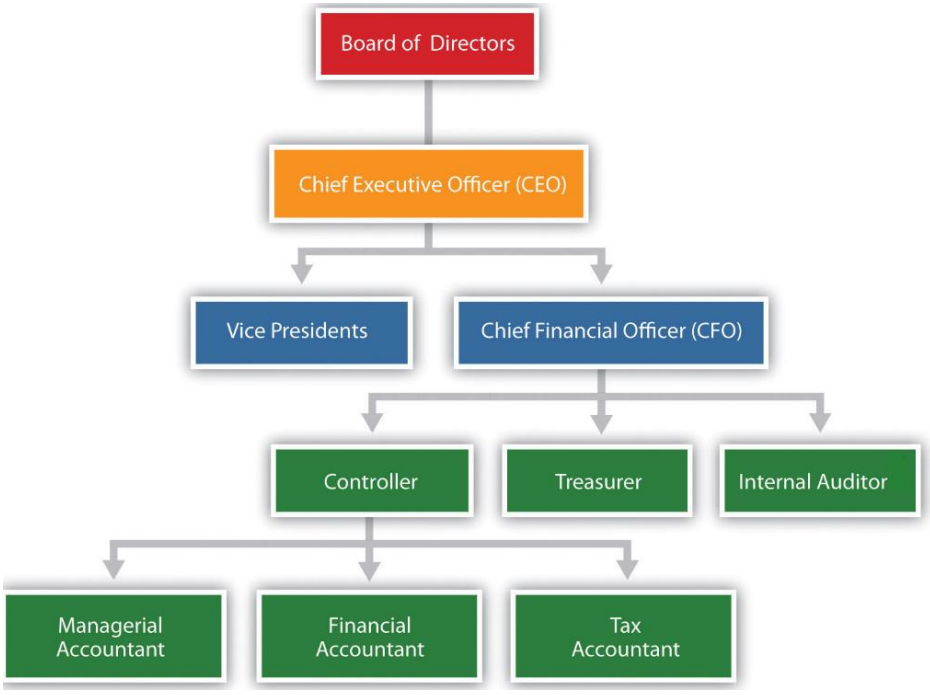


Figure 18: Typical Organizational Chart

However, there are certain roles within the organization that have greater responsibilities towards the security of cardholder data via means that are thoroughly analyzed in the Introduction to Security chapter focusing

mainly on daily incidents that might occur. This does not mean that the responsibilities related to security only affects those roles. It is important to have in mind that security tasks and duties extend among the whole organization as each member of it should be compliant with the created and implemented security policies while making sure that sensitive cardholder data will not be compromised to unauthorized people. Of course, to accomplish all these the personnel must be properly trained to react in case of a compromise or a security incident according to the created incident security plans of the organization.

5.1 Organizational Pyramid of Duties

Starting the organization's pyramid top to bottom, apart of course from the owner or group of owners of the organization, we most likely find the *chief executive officer* (CEO) or *managing director* (MD) who is the most senior corporate officer responsible for management (profit or nonprofit) of the organization reporting at the same time to the board of directors. In most cases, the CEO is responsible for running the organization and ensure its good and prosper standing. Among those duties really important are the support of the established security policies in order to ensure their effectiveness (for more information please refer to Information Security Policies section) along with the responsibility that the CEO has to pass through the organization's employees the awareness about their responsibilities and duties towards the protection of cardholder data. Having ensured that information security policies are in place and fully understood and so are the security controls by anyone involved another important task of the CEO is to provide the appropriate mitigation (for more information please refer to Facing Risk section) and means of recovering from security incidents (process known as *Incident Response*). In addition to that, as already mentioned in the previous chapters, PCI compliance also extends to third parties involved with the process flow, so the company must also confirm that each one of these third parties is compliant with PCI DSS. So, the CEO is responsible to ensure that all the contracts with those parties contain specific actions for protecting CD. Lastly, the chief executive officer is in charge of the training which aims to teach employees how to perform their jobs in a secure manner.

As easily understood, the duties and responsibilities of the chief executive officer or managing director can vary from organization to organization but overall they are extremely pressured and overloaded. So, that is exactly the reason that each organization has a dedicated senior-level executive responsible to ensure information assets and technologies are adequately protected. This executive, called *Chief Information Security Officer* (CISO), aims to reduce information technology risks by having of course the appropriate staff to perform all the necessary actions. Among their duties is to establish appropriate standards and controls - helping the CEO - manage security technologies, and organize the creation and implementation of information security policies, procedures and security controls always with focus on information and physical security of the organization.

In most cases, the responsibilities that the CISO has can vary from case to case. Overall, the CISO has to focus on establishing and maintaining Security Incident Response Team, Cybersecurity, planning and ensuring the effectiveness of Disaster recovery and business continuity, Identity and access management reviewing access rights to applications and systems, Information privacy, Information regulatory compliance (such as in our case in PCI DSS compliance process), Information risk management monitoring and dealing with potential new threats, Information security and information assurance, network monitoring including actions such as reviewing firewall/IDS/User activities/Audit/AV reports and managing inventory of all the HW/SW assets of the organization, monitoring of password files to effectively detect any potential compromise, Information technology controls, IT investigations, forensics, planning the organization's Security Architecture. In addition,

as previously mentioned, it is really important to keep the personnel of the organization aware and up to data about its responsibilities regarding the protection of cardholder data. So, the CISO should consult and assist the personnel regarding security policies, procedures and security controls and ensure that all these are acknowledged by every employee.

As mentioned above, the role of the CISO is to contribute and help the CEO to ensure the organization's good and prosper standing in terms of information security. So, those two should work together and cooperate with the CISO being the subordinate obliged to report to the CEO about any security related issue, consult on security procedures and review any needed change to information security policies.

Another important information security related position within the organization is the *Chief Information Officer* (CIO), a position again given to one of the most senior executive in the organization being responsible for the information technology as head of the Information Technology group. As for the responsibilities, the CIO has first of all to play the role of business leader by making executive decisions regarding IT issues. It is important to keep in mind that the CIO is the key factor into planning and establishing the strategic goals of the organization while being aware for any security related issue within the organization. All these responsibilities and actions must be performed in balance and cooperation with both the CEO and the CISO in order to achieve a competitive advantage and offer to the organization's employees. Another important task of the Chief Information Officer is that of recruiting, which is really important as the best employees have to be chosen in order perform the tasks assigned to them. As with CISO the CIO has also the obligation to report to the chief executive officer but of course it is up to each organization to establish and assign these responsibilities to each one of these PCI DSS related positions. In the figure below, the above mentioned connections between the three positions described so far are clearly shown.

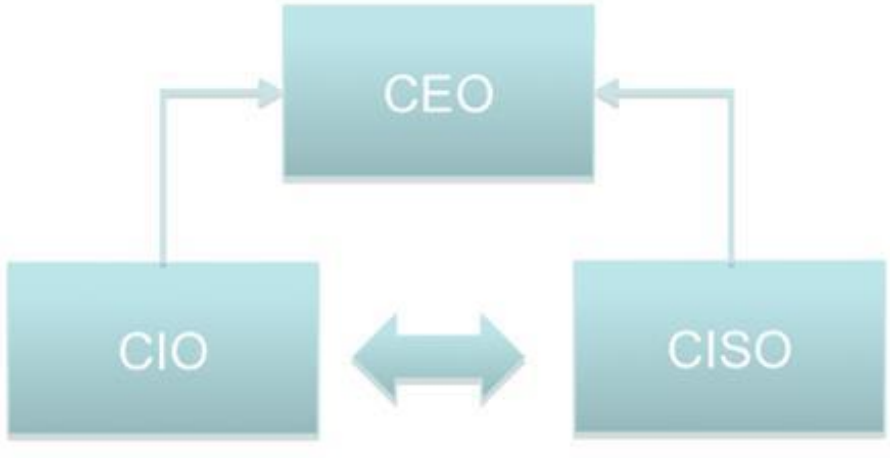


Figure 19: Relationships between Senior Management

Finally, at the bottom of the hierarchy of the organizational chart one can find the *system and security administrators*. Those employees are the ones implementing the security policies and the actions ordered by the three persons holding the positions described above (CEO, CISO and CIO). In more detail, the *System Administrator* (SYS Admin) is the employee responsible for the configuration and maintenance of the normal operation of IT systems mainly focusing of keeping all the operations and functionalities up and running. Apart

from that, it is important to ensure that the performance, resources, and security of the systems are maintained at the desired levels while following the instructions and recommendations of the higher levels.

To do so, the system administrator should use those components and features that offer the needed automation, help them maintain the established security policies, fix any issue and train and educate personnel. In most cases, the sysadmins are often assigned to the following different but related to each other areas:

- Database
- Network
- Security
- Web
- Mail
- Storage

The third of the above mentioned position, the *Security administrator*, is another important role regarding the PCI DSS compliance procedure. This employee is exclusively dedicated to daily information security actions on the organization's systems (servers, hosts, networks etc). To be able to successfully perform the assigned responsibilities that person might need to have access to sensitive information and cooperate with the system administrators in order to perform all the needed security features on the different systems of the organization while always having to report back to the Chief Information Security Officer.

Chapter 6

PCI Readiness Project

6.1 Executive Summary

The present section is one of the formal deliverables of the PCI Readiness project that has been delivered on behalf of the Organization. The scope of this section is to provide a high level overview of the findings and the respective analysis regarding the PCI Readiness of the organization.

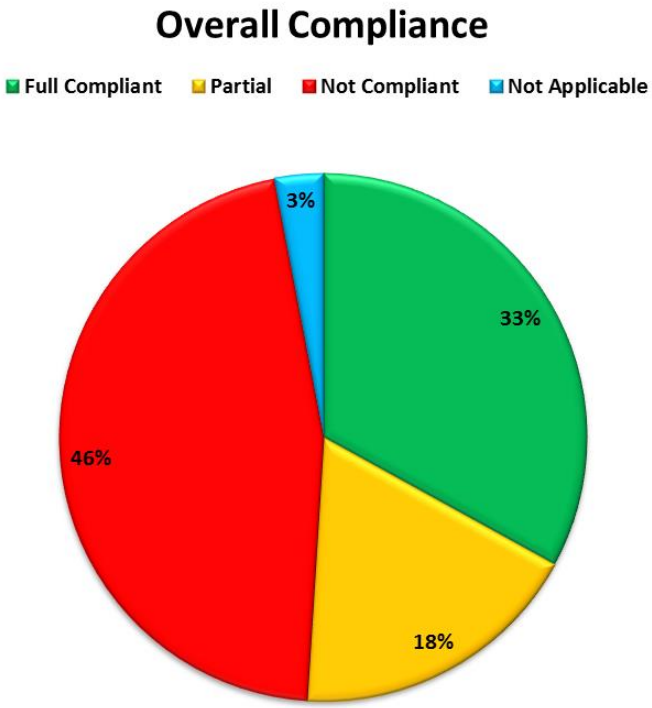


Figure 20: Overall Compliance

In this context and based on the analysis, the Organization was found to be **33% Fully Compliant, 18% Partial Compliant, 46% Not Compliant** and **3% Not Applicable** in the total requirements and subrequirements of PCI DSS v.3, as presented in the figure above.

In order for the Organization to get compliant with PCI DSS v.3 requirements a number of measures must be taken. In the following figure the percentage of the requirements fulfilled by each proposed measure is presented.

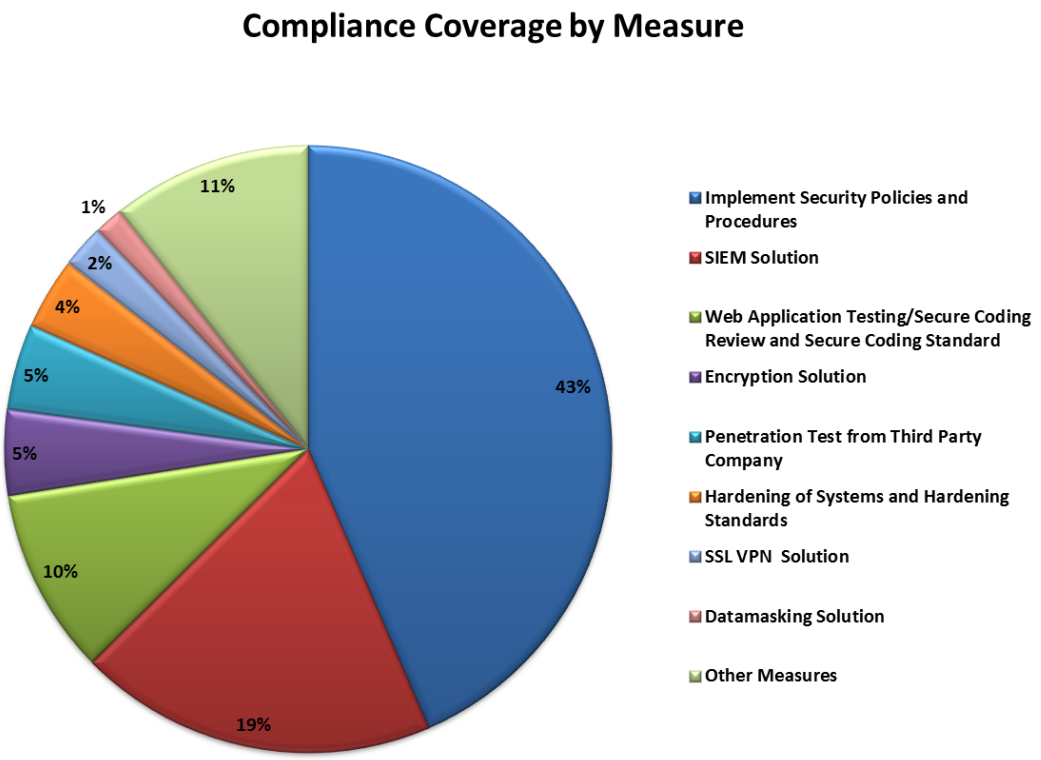


Figure 21: Compliance Coverage by Measure

- **NOT APPLICABLE**. The requirement of PCI DSS does not apply to the Organization (e.g. is not a hosting provider consequently the specific requirement is out of PCI DSS scope, wireless networks are also out of scope).
- **NOT COMPLIANT**. The requirement is not implemented to the Organization infrastructure (e.g. procedures that are not implemented or there are in schedule to be implemented).
- **PARTIAL**. The procedure exists in the Organization but it does not fully cover the requirement of PCI DSS (e.g. the Organization implements procedures but is in need of documentation).
- **FULLY**. The procedure has been identified in the Organization and fully covers the requirement of PCI DSS (e.g. the Organization implements PCI requirements and the evidence are presented).

Based on this graph the first actions that must take place is the implementation of Security Policies and Procedures and the SIEM solution, after this the next think that must take place is the Web Application Testing/Secure Coding Review and Secure Coding Standard following by an encryption Solution, Penetration Testing from Third Party Company and Hardening of Systems along with the appropriate Hardening Standards.

6.2 Methodology

In order to provide the PCI Readiness professional services a structured methodology, as described in the following image, has been followed:

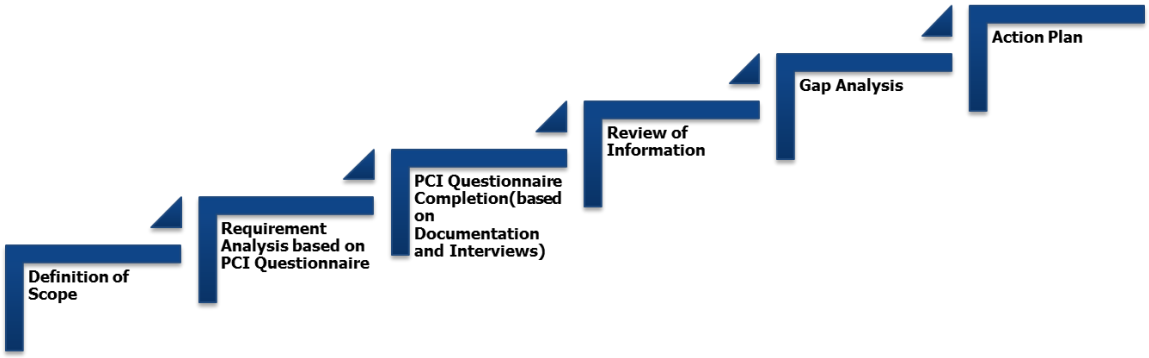


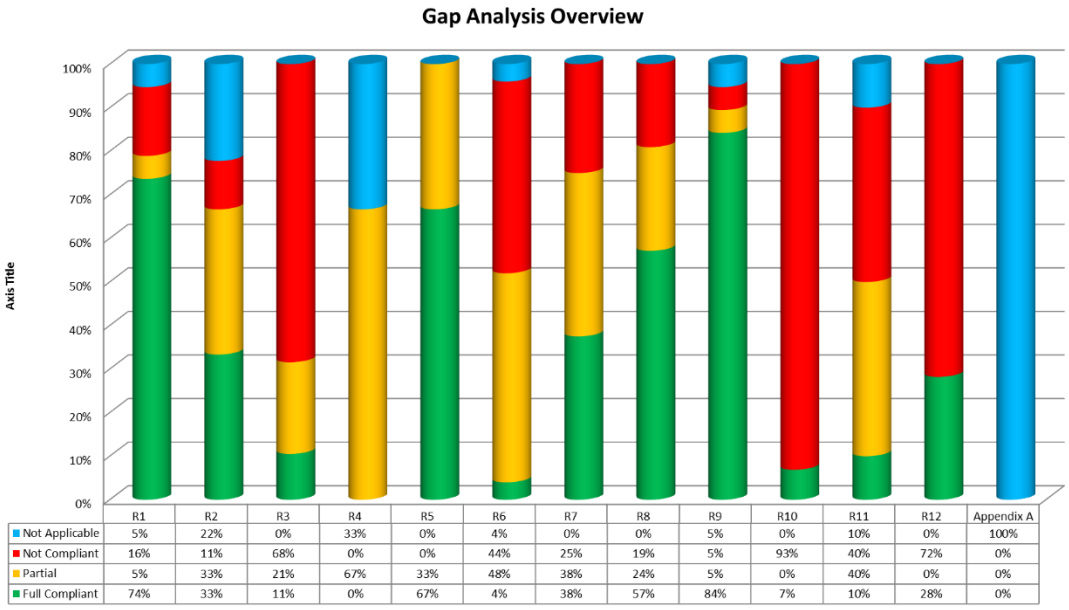
Figure 22: Methodology

6.3 Gap Analysis Overview

The categories of PCI where the Organization was assessed are:

- Requirement 1 - Install and maintain a firewall configuration to protect cardholder data
- Requirement 2 - Do not use vendor-supplied defaults for system passwords and other security parameters
- Requirement 3 - Protect stored cardholder data
- Requirement 4 - Encrypt transmission of cardholder data across open, public networks
- Requirement 5 - Use and regularly update anti-virus software or programs
- Requirement 6 - Develop and maintain secure systems and applications
- Requirement 7 - Restrict access to cardholder data by business need to know
- Requirement 8 - Assign a unique ID to each person with computer access
- Requirement 9 - Restrict physical access to cardholder data
- Requirement 10 - Track and monitor all access to network resources and cardholder data
- Requirement 11 - Regularly test security systems and processes
- Requirement 12 - Maintain a policy that addresses information security for all personnel.
- Additional PCI DSS Requirements for Shared Hosting Providers

In the following figure a gap analysis overview is presented.



	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	Appendix A
Not Applicable	5%	22%	0%	33%	0%	4%	0%	0%	5%	0%	10%	0%	100%
Not Compliant	16%	11%	68%	0%	0%	44%	25%	19%	5%	93%	40%	72%	0%
Partial	5%	33%	21%	67%	33%	48%	38%	24%	5%	0%	40%	0%	0%
Full Compliant	74%	33%	11%	0%	67%	4%	38%	57%	84%	7%	10%	28%	0%

Figure 23: Gap Analysis Overview

Based on the analysis that was based on the Organization's input the most compliant Requirements are 1,5,8,9 that concern Firewall Configuration, Update of antivirus programs, Assignment of Unique ID and the Physical Access Restriction accordingly. The most non -compliant requirement is the Requirement 10 and 12 that concern Monitoring and Tracking of access and the Maintenance of Security Policy accordingly.

According to requirements for wireless environment, in the Organization infrastructure there is an isolated wireless network, out of DMZ with no access to the internal network. According to that reason the wireless connection for the Organization is out of PCI scope.

Regarding PCI requirement for shared hosting providers, the Organization is not a hosting provider. According to that reason the requirement about hosting provider as well as Appendix A are out of PCI scope.

6.4 Action Plan Overview

The necessary actions in order to succeed PCI compliance are divided in missing Documentation, Tools/Systems, Configuration and Services and presented in detail in Action Plan Deliverable and summarized in the following table:

Requirement	Subject	Description of Gap	Necessary Measure	Type of Measure
1.	Install and maintain a firewall configuration to protect cardholder data	• Not a formal process for approving and testing external network connections, changes to the firewall, router, configurations. • Missing lists of groups, roles	• Network Security Policy • Change Management Procedure for Network Changes • Unified Threat Management System	Documentation, Product

Requirement	Subject	Description of Gap	Necessary Measure	Type of Measure
		and responsibilities. • Missing Personal Firewalls.	• Personal Firewall	
2.	Do not use vendor-supplied defaults for system passwords and other security parameters	• Missing Hardening of Systems • Missing Documentation and Implementation for Security Features • Proper Encryption Missing	• Hardening of Systems and Hardening Standards • Security policies and procedures for sensitive data storage and transmition • SSL VPN Solution	Documentation/Configuration/ Product
3.	Protect stored cardholder data	• Missing Security Policies and Procedures for Data Retention • Not sufficient masking for PAN • No use of cryptography and encryption	• Deploy Encryption Solution • Key-management Process and Procedure	Documentation/ Product
4.	Encrypt transmissio n of cardholder data across open, public networks	• Encryption Mechanisms applied are not documented	• SSL VPN Solution • Encryption Solution	Product
5.	Protect all systems against malware and regularly update anti-virus software or programs	• Internal Logging Capabilities on antivirus software not enabled.	• Enable Internal Logging Capabilities	Configuration

Requirement	Subject	Description of Gap	Necessary Measure	Type of Measure
6.	Develop and maintain secure systems and applications	• Web Application Testing is missing • Formal Procedure for Patch Management is missing • Secure Code Review along with Secure Coding Documented Practices Missing • Data Masking is missing	• Web Application Testing • Secure Coding Review and Secure Coding Standard • Hardening of Systems and Hardening Standards • Datamasking Tool • Test Environment • Change and Patch Management Procedure • Versioning Control	Service/Documentation/ Product
7.	Restrict access to cardholder data by business need to know	• Missing role access to certain systems • Missing formal Security Policies and Procedures related to logical and network access to the systems	• Role Management Document • Access Control Procedure	Documentation
8.	Identify and authenticate access to system components	• Missing Formal Policies and Procedures for Logical Access • Missing two factor authentication technologies for remote access to PCI-related systems • Missing Encryption for secure storage and transmission of passwords	• Token for strong Authentication • Encryption Solution • Authentication Procedures and Policies • Password Management Policies • Hardening of Systems and Hardening Standards	Product/Documentation
9.	Restrict physical access to	• Formal Procedures for handling	• Procedures for distinguishing personnel and visitors	Documentation

Requirement	Subject	Description of Gap	Necessary Measure	Type of Measure
	cardholder data	visitors are missing	• Audit of Backup Procedure	
10.	Track and monitor all access to network resources and cardholder data	• There is not an automated trail for all systems	• Access Management Procedure • SIEM solution	Documentation/ Product
11.	Regularly test security systems and processes	• No Penetration Testing Activities for third party company have taken place • There are not file-integrity monitoring tools deployed within the cardholder data environment	• Penetration Testing from Third Party Company Required • UTM Solution • File-Intergity Tool	Services/ Product
12.	Maintain a policy that addresses information security for all personnel	• Missing Security Policies and Procedures	• Security Policies and Procedures based on PCI DSS required	Documentation
Appendix A	Additional PCI DSS Requirements for Shared Hosting Providers	Not Applicable	Not Applicable	Not Applicable

Table 14: Summary of Action Plan

6.4.1 Measures

The measures that the Organization must take in order to be compliant with PCI DSS requirements are divided in Documentation that must be developed, Services and Products that must be acquired and Configuration Changes or Internal Issues. Some of the required measures fulfilled more than one requirement, so some of the necessary measures must be taken before others.

Concerning the documentation needs, in order for the Organization to be fully compliant with PCI DSS at least the below documentation must be developed:

- Develop Security Policies and Procedures based on PCI DSS requirements that cover(at least) the below areas:
  - Network Security
  - Change Management
  - Sensitive Data Storage and Transmition
  - Key Management
  - Patch Management
  - Logical and Network Access
  - Physical Acccess
  - Log and Audit Management
- Develop and Deploy Hardening Standards
- Secure Coding Documented Practices

Since there are a lot of Policies and Procedures to be deployed and need for Hardening Standards and Hardening a Control Compliance Solution with Both Procedural and Technical Controls in place is highly advisable.

From products point of view the below products must be supplied:

- SIEM
- Encryption Solution
- Tokens for Two Factor Authentication
- Unified Threat Management System
- Data Masking tool
- SIEM Solution
- File-Integrity Monitoring Tools
- Personal Firewall
- Versioning Control Tool

Also along with the tools and the documentation that missing. The below configuration/internal issues must be arranged:

- Enable Internal Logging Capabilities
- Create Test Environment
- Restrict Access to cryptographic keys

Concerning services that the Organization must implement these are presented in the list below:

- System Hardening
- Web Application Testing
- Secure Code Review
- Penetration Testing from Third Party Company Required

6.4.2 Prioritization

Based on the number of requirements each one of the proposed measure fulfills the below order is proposed to the Organization:

1. Implement Necessary Security Policies and Procedures
2. SIEM solution
3. Web Application Testing/Secure Coding Review and Secure Coding Standard
4. PGP Solution
5. An external partner must be used for penetration tests
6. Hardening of Systems and Hardening Standards
7. SSL VPN Solution
8. Datamasking
9. Test Environment
10. Audit of Backup Procedure
11. Enable Internal Logging Capabilities
12. File Integrity Monitoring Tool/Critical System Protection
13. Personal Firewall
14. Restrict access to cryptographic keys
15. Token
16. UTM Solution
17. Versioning Control

6.5 GAP Analysis – Requirements

6.5.1 Requirement 1- Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

In the below figure**,** a graphical representation of Requirement 1 is given.

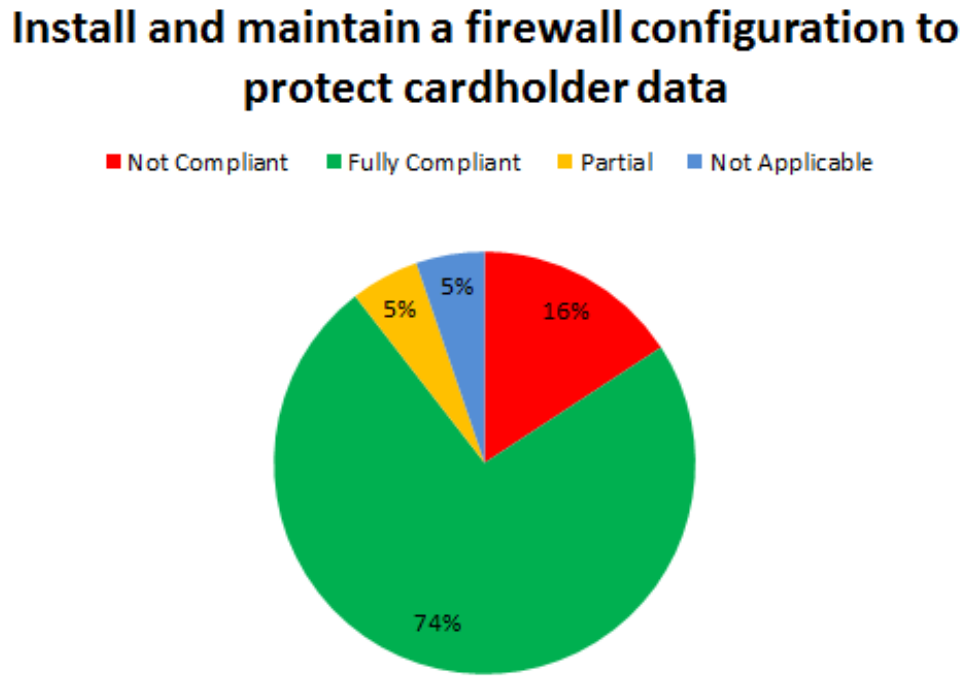


Figure 24: R1 Compliance Analysis

The detailed gap analysis is presented in the following table:

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
1.1 Establish firewall configuration standards that include the following:				
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	**Not Compliant**	No Formal Process Provided	There is not a formal process for approving and testing external network connections, changes to the firewall, router configurations.
1.1.2	Current network diagram with all connections to cardholder data, including any wireless networks	**Fully Compliant**	Network diagram has been provided	No Gap Identified

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
1.1.3	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**Fully Compliant**	As depicted from the network diagram, there is one INTERNET connection and traffic must pass through the firewall. (Network diagram has been provided)	No Gap Identified
1.1.4	Description of groups, roles, and responsibilities for logical management of network components	**Partial**	Each device serves particular role. Router is used for routing, fw is used for firewalling etc. Regarding management there is a network engineer with config privileges and IT helpdesk with view only in routers.	There is no documentation that has the lists of groups, roles and responsibilities.
1.1.5	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure	**Fully Compliant**	As depicted from the network diagram, INTERNET traffic cannot pass to servers directly. It must pass through the firewall. From INTERNET zone traffic goes to another zone e.g. PARTNERS (depending the location of the destination server)	No Gap Identified
1.1.6	Requirement to review firewall and router rule sets at least every six months	**Fully Compliant**	Router and FW configuration are checked frequently (more often than 6 months).	It is highly advisable to have documented the procedure and report of the review.
1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage				
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder	**Fully Compliant**	OUTBOUND traffic is through proxy (with the exception of airisa1-2)	No Gap Identified

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	data environment			
1.2.2	Secure and synchronize router configuration files	**Fully Compliant**	Each time when the configuration changes, the "wr mem" command is issued in order to save the running configuration. Besides that, every day the "sh run" command is taken from all network devices.	No Gap Identified
1.2.3	Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment	Not Applicable	Not Applicable	Not Applicable
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment	Fully Compliant	Please refer to 1.1.3 & 1.1.5	
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	**Fully Compliant**	There are DMZs. see 1.1.3 & 1.1.5 NO HOST FW	No Gap Identified
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ	**Fully Compliant**	Please refer to 1.1.3 & 1.1.5	No Gap Identified

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
1.3.3	Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment	**Fully Compliant**	Default route on whole network. All traffic goes through firewall.	Schedule d
1.3.4	Do not allow internal addresses to pass from the Internet into the DMZ	**Fully Compliant**	No default route on whole network. User access INTERNET only through proxy server	No Gap Identified
1.3.5	Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ	**Fully Compliant**	No default route on whole network. Server access to INTERNET only through proxy server (with the exception of airisa1-2)	No Gap Identified
1.3.6	Implement stateful inspection, also known as dynamic packet filtering. (That is, only established connections are allowed into the network.)	**Fully Compliant**	This is how firewall (Cisco ASA 5525) works (http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/intro_intro.html)	No Gap Identified
1.3.7	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	**Not Compliant**	SIRAX and BW are in MED and not managed by Organization. No host based firewall on servers with ISA exception	It is highly advisable to have the components that store cardholder data in an internal network.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
1.3.8	Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to: § Network Address Translation (NAT) § Placing servers containing cardholder data behind proxy servers/firewalls or content caches, § Removal or filtering of route advertisements for private networks that employ registered addressing, § Internal use of RFC1918 address space instead of registered addresses.	**Fully Compliant**	a) All servers are behind firewall and using NAT. Internal addressing is based on RFC 1918, b) No advertising of private addresses is made to the INTERNET. see 1.1.3 & 1.1.5	No Gap Identified
1.4	Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network	**Not Compliant**	No personal firewall on any employee owned device	Personal firewalls are missing.

Table 15: R1 Gap Analysis

The main issue concerning the gap analysis of the Requirement 1 is the missing documentation of all the applied measures. Also it is highly advisable to have the components that store cardholder data in an internal network. Regarding wireless environment is out of PCI scope because there is an isolated wireless network, out of DMZ with no access to the internal network.

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

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

In the figure below**,** a graphical representation of Requirement 2 is given.

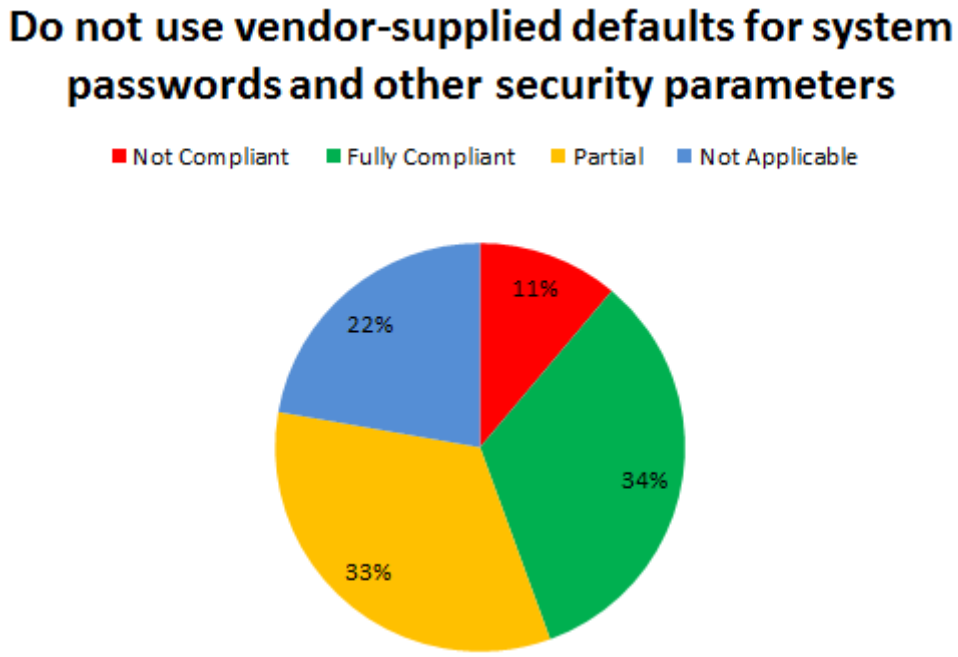


Figure 25: R2 Compliance Analysis

The detail gap analysis is presented in the following table:

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
2.1	Always change vendor-supplied defaults before installing a system on the network - for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts	Fully Compliant	IT Administrators locks and expires default accounts and passwords during installation. All Passwords for administration accounts are strong, complex and secure.	No Gap Identified

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	Not Applicable	Not Applicable	Not Applicable
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. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST)	Not Compliant	We should check out our approach. Next month we will implement hardening procedures on our servers with Microsoft partner	Hardening of Systems Required along with the necessary documented Standards
2.2.1	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.	**Partial**	Backup server, storage server, application server, ftp server are separate servers. The only servers that have more than the primary functions are: airisa1 & airisa2 servers. Services that run on this server are presented below: server1 - 21/TCP - ftp 22/TCP - ssh 80/TCP - http 1080/TCP - socks 1745/TCP - remote-winsock 8080/TCP - http	Each server must have one role based on its main functionality. The use of virtual servers could be an efficient solution.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
			server2 - 22/TCP - ssh 80/TCP - http 1080/TCP - socks 1080/TCP - socks 1745/TCP - remote-winsock 8080/TCP - http b) Will use Virtualization in order to separate roles	
2.2.2	Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure - for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	**Partial**	(a) Yes only necessary services, protocols, daemons are enabled as required for the function of the system (b) No, security features are not documented and implemented.	Documented Hardening Standards Required
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure - for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	Partial	SFTP is used for file transfer (with the exception of airisa1 which uses FTP besides SFTP	Additional security features must be used for all components
2.2.4	Configure system security parameters to prevent misuse	**Fully Compliant**	IT systems Administrators manage not to expose the organization to risk. The infrastructure is properly designed, security failures could not compromise the systems and the security parameters settings included in the system configuration standards.	No Gap Identified
2.2.5	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**Fully Compliant**	With our HIAB Outpost24 system, we have Inventory the running services, remove anything unrelated or auxiliary.	No Gap Identified

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web based management and other non-console administrative access	Partial	We use IPSec in order to encrypt connection between admins pcs and server	Encryption must be implemented.
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	**Fully Compliant**	With our HIAB Outpost24 system, we have Inventory the running services, remove anything unrelated or auxiliary.	No Gap Identified
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.	Not Compliant	Haven't documented any of these	Documentation for policies and operational procedures for managing vendor defaults and other security parameters are missing
2.6	Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers	Not Applicable	Not Aplicable	Not Applicable

Table 16: R2 Gap Analysis

The main issue concerning the gap analysis of the Requirement 2 is that there are no documented Hardening Standards for the systems in scope. Regarding shared hosting providers requirement this is out of scope since the organizations is not a shared hosting provider.

6.5.3 Requirement 3 - Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

In the below figure**,** a graphical representation of Requirement 3 is given.

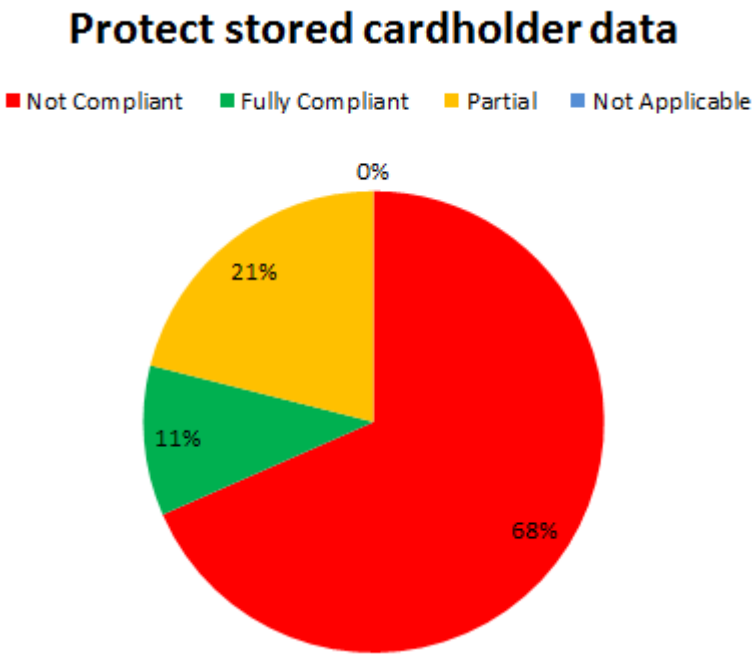


Figure 26: R3 Compliance Analysis

The detail gap analysis is presented in the following table:

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:	**Not Compliant**	There is no such policy in place.	Missing specific security policies and procedures regarding the data retention issues. Data storage time period should be in accordance with legal obligations and should be retained in accordance with the time needed.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	• Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements • Processes for secure deletion of data when no longer needed • Specific retention requirements for cardholder data • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.			
3.2	Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: Note: It is permissible for issuers and companies that support issuing services to store sensitive	Fully Compliant	No sensitive authentication data stored.	No Gap Identified

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	authentication data if there is a business justification and the data is stored securely.			
3.2.1	Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained: § The cardholder's name § Primary account number (PAN) § Expiration date § Service code To minimize risk, store only these data elements as needed for business.	**Fully Compliant**	No use of any magnetic stripe card reader.	No Gap Identified
3.2.2	Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a	**Partial**	None application stores verification code data. However call center conversations where this information is told are stored.	Consider to store encrypted the call center conversations.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	payment card) used to verify card-not-present transactions.			
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block	**Partial**	None application stores verification code data. However call center conversations where this information is told are stored.	Consider to store encrypted the call center conversations.
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). Notes: § This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN. § This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.	Partial	SIRAX does not. OPAT once entered PAN is tokenized.	PAN has to be masked when displayed.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: § One-way hashes based on strong cryptography (hash must be of the entire PAN) § Truncation (hashing cannot be used to replace the truncated segment of PAN) § Index tokens and pads (pads must be securely stored) § Strong cryptography with associated key-management processes and procedures	Partial	Only for transactions via B2C (website)	Strong cryptography for Pan should be implemented
3.4.1	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases).	**Not Compliant**	No use of cryptography and encryption	There is not implementation of cryptography and encryption

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	Decryption keys must not be tied to user accounts.			
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:			
3.5.1	Restrict access to cryptographic keys to the fewest number of custodians necessary	**Not Compliant**	No use of cryptography and encryption	There is a need of restricted access to cryptographic keys.
3.5.2	Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components	**Not Compliant**	No use of cryptography and encryption	a) Key stored in encrypted format b) Keys stored in the fewest possible locations and forms

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	or key shares, in accordance with an industry-accepted method			
3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.			
3.6.1	Generation of strong cryptographic keys	**Not Compliant**	No use of cryptography and encryption	Generation of cryptographic keys.
3.6.2	Secure cryptographic key distribution	**Not Compliant**	No use of cryptography and encryption	Key distribution.
3.6.3	Secure cryptographic key storage	**Not Compliant**	No use of cryptography and encryption	Procedures for key storage.
3.6.4	Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special	**Not Compliant**	No use of cryptography and encryption	No procedures for cryptographic key changes.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	Publication 800-57).			
3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.	**Not Compliant**	No use of cryptography and encryption	a) No cryptographic key procedures include retirement or replacement. B) No procedures including replacement of known or suspected compromised keys. C) No cryptographic keys are retained for decryption/verification purposes.
3.6.6	If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or	**Not Compliant**	No use of cryptography and encryption	Procedures in place of split knowledge and dual control of cryptographic keys.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	three people, each knowing only their own key component, to reconstruct the whole key). Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.			
3.6.7	Prevention of unauthorized substitution of cryptographic keys	**Not Compliant**	No use of cryptography and encryption	Procedures for prevention of unauthorized substitution.
3.6.8	Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key-custodian responsibilities	**Not Compliant**	No use of cryptography and encryption	Form stating tha they understand and accept the responsibilities of key-custodian.
3.7	Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	**Not Compliant**	Documentation is missing	Security policies and operational procedures for protecting stored cardholder data are not documented - have not been created at all.

Table 17: R3 Gap Analysis

Concerning Requirement 3 the Gap Analysis identified that there is no encryption in place for data stored and there is no documented procedure for that.

6.5.4 Requirement 4 - Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols

continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

In the below figure**,** a graphical representation of Requirement 4 is given.

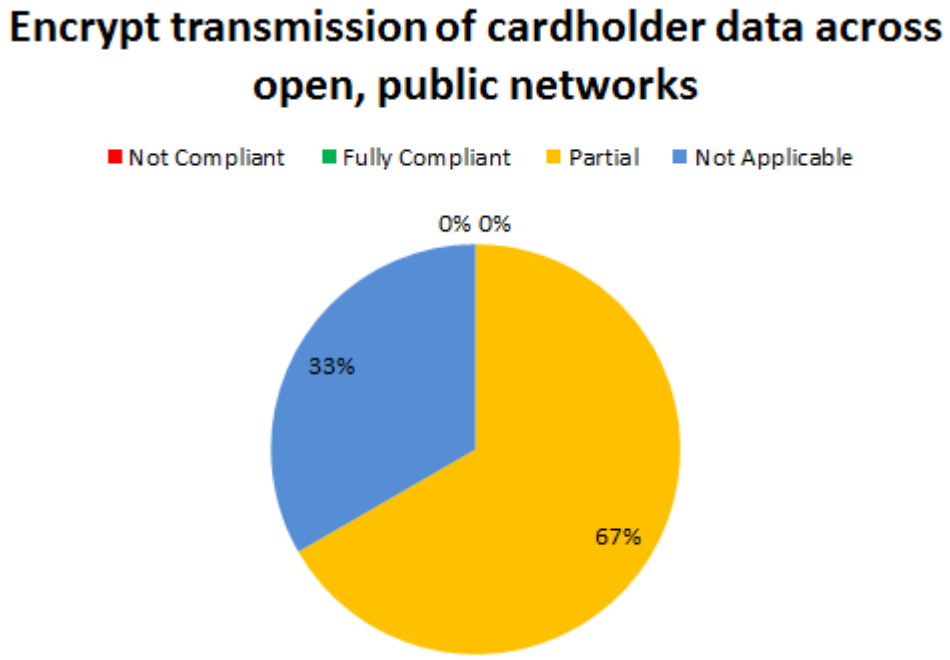


Figure 27: R4 Compliance Analysis

The detail gap analysis is presented in the following table:

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
4.1	Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to: • The Internet • Wireless technologies, • Global System for Mobile communications (GSM) • General Packet Radio Service (GPRS).	Partial	SFTP is used for file transfer (with the exception of airisa1 which uses FTP besides SFTP	Documentation is missing. All partners must switch to SFTP - Secure Ftp Analysis.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.	**Not Applicable**	**Not Applicable**	**Not Applicable**
4.2	Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	Partial	No we use only FTP, SFTP connections	Documentation is missing. No policies to state that unprotected PANs are not to be sent via end-user messaging technologies

Table 18: R4 Gap Analysis

In general, the R4 is partially completed. The most important issue is the fact that not all partners use SFTP connection.

6.5.5 Requirement 5 - Protect all systems against malware and regularly update anti-virus software or programs

Malicious software, commonly referred to as - malware - including viruses, worms, and Trojans - enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

In the below figure**,** a graphical representation of Requirement 5 is given.

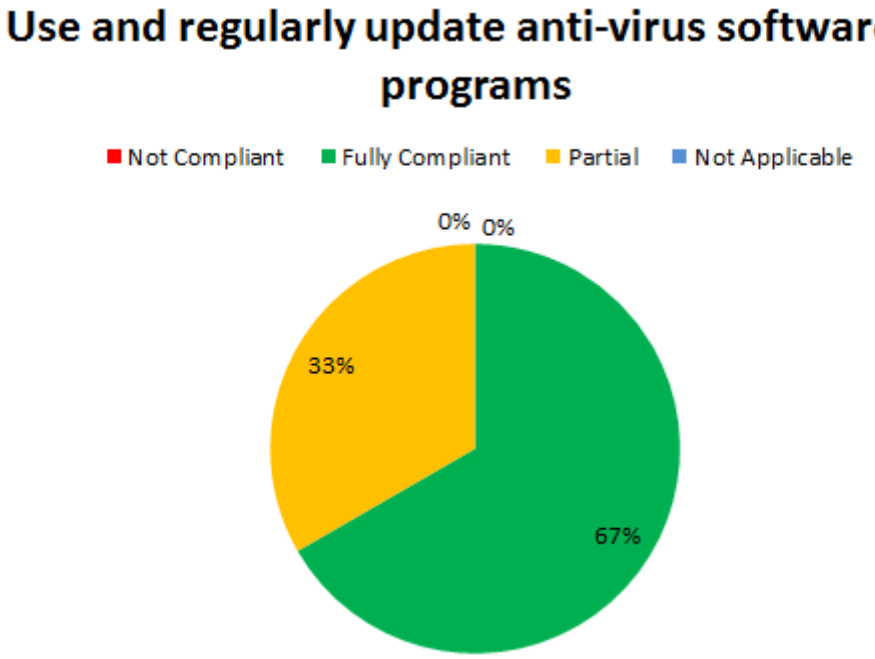


Figure 28: R5 Compliance Analysis

The detail gap analysis is presented in the following table:

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)	**Fully Compliant**	All systems that is part of Cardholder Environment have Antivirus, Antimalware and network inspection module installed. http://technet.microsoft.com/library/hh508836.aspx	No Gap Identified
5.1.1	Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software	**Fully Compliant**	The Endpoint Protection client has the following capabilities: •Malware and Spyware detection and remediation. •Rootkit detection and remediation. •Critical vulnerability assessment and automatic definition and engine updates. •Network vulnerability detection via Network Inspection System. •Integration with Microsoft Active Protection Services to report malware to Microsoft. When you join this service, the Endpoint Protection client can download the latest definitions from the Malware Protection Center when unidentified malware is detected on a computer.	No Gap Identified

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.	**Fully Compliant**	Periodic evaluations are being contacted	No Gap Identified
5.2	Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	**Partial**	5.2 (a) - Yes it does. There is a policy that all clients need to be updated every morning at 10:00 am, if some clients lost this time window then retrying every one hour. 5.2 (b) - Yes. Tasks for automatic update running at 3:00am every night and scan every Thursday at 2:00 pm 5.2 (c) - Yes. Automatic Updates run every day at 10:00 am and scan every Thursday at 2:00 pm. 5.2 (d) - The product supports audit logs and is PCI DSS compliant but this feature is not implemented on the company.	Internal Logging Capabilities on antivirus software not enabled.
5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period	**Fully Compliant**	AV being used cannot be disabled or altered by anyone but the AV admin.	No Gap Identified

Table 19 - R5 Gap Analysis

The most important issues in this requirement is that the organization must enable the internal logging capabilities on antivirus software.

6.5.6 Requirement 6 - Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

In the below figure**,** a graphical representation of Requirement 6 is given.

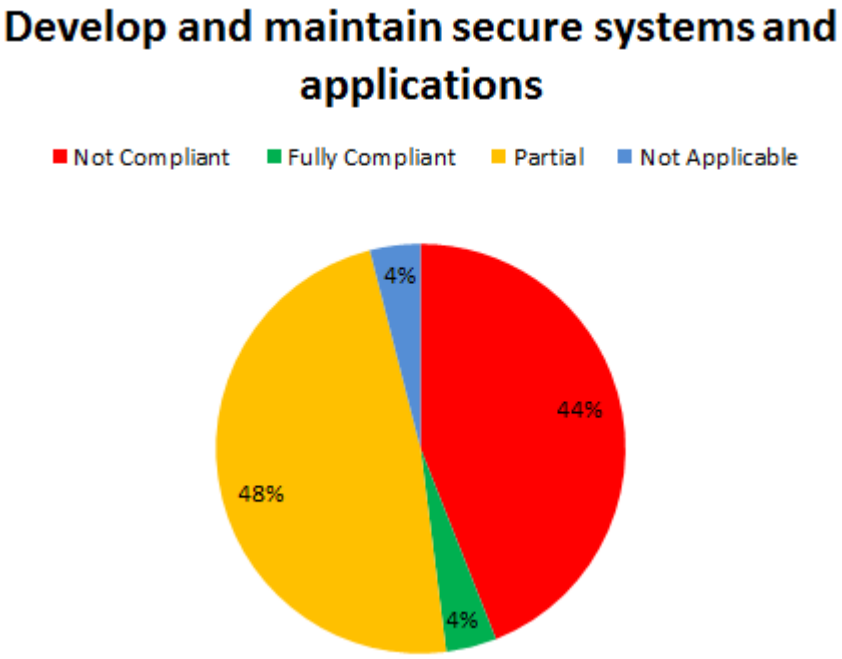


Figure 29: R6 Compliance Analysis

The detail gap analysis is presented in the following table:

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly	Partial	Squid: (a) We scan the application in regular basis with Outpost. (b) Outpost receives daily updates with most recent security vulnerabilities information. Shark: (a) We scan the application in regular basis with Outpost. (b) Outpost receives daily updates with most recent security vulnerabilities information.	Documentation is missing.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	discovered security vulnerabilities.		Q-Admin: (a) We scan the application in regular basis with Outpost. (b) Outpost receives daily updates with most recent security vulnerabilities information. axs.res: (a) HP information needed (b) HP information needed.	
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.	Fully Compliant	Microsoft SCCM is used for patch management	It is highly advisable to have a formal procedure for Patch Management
6.3	Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle	Partial	Squid: (a) No. (b) No. (c) Code reviews are performed every 3 months but not by external partners. (d) No. Shark: (a) No. (b) No. (c) Code reviews are performed every 3 months but not by external partners. (d) No. Q-Admin: (a) No. (b) No. (c) Code reviews are performed every 3 months but not by external partners. (d) No axs.res: (a) HP information needed (b) HP information needed. (c) HP information needed. (d) HP information needed. SAP-Sirax: (a)Yes , LSY develops its applications based on industry standards (b) Yes , LSY develops its applications based on industry standards (c) Yes , LSY develops its applications based on industry standards (d) Yes , LSY develops its applications based on industry standards	There are not following standards and best practices for Squid, shark, qadmin. Documentation for code review is missing.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
6.3.1	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	Partial	**Squid:** For database connectivity we use SQL Server Authentication. Credentials used by users (role: db_datareader) are different than those of the core automation (role: db_datareader, db_datawriter). For web UI, we use LDAP through PHP. For the core, we use LDAP authentication to retrieve files from the FTP. **Shark:** For downloading HOT files through FTP the application uses LDAP authentication. For downloading and uploading files to Weblink through SFTP we use credentials provided by Weblink. **Q-Admin**: **Core to database:** Custom username, mySQL authentication, INSERT only, limited to specific tables. **Web to database:** Custom username for SELECT only, custom username for INSERT only. The INSERT username has permissions only in tables without CC details. **axs.res: (a)** HP information needed **(b)** HP information needed. **SAP-Sirax:** In the production system only live and valid accounts exist.	
6.3.2	Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life	Partial	**Squid: (a)** Code changes are reviewed only by the code author. **(b)** No **(c)** Yes, all corrections are first released in development environment, and if they are considered safe, they are released in production. **(d)** No, management authorizes the launch of a new release but does not perform code reviews. **Shark: (a)** Code changes are reviewed only by the code author. **(b)** No **(c)**	It is not good practice to be reviewed by the author. Policy is missing.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.		Yes, all corrections are first released in development environment, and if they are considered safe, they are released in production. **(d)** No, management authorizes the launch of a new release but does not perform code reviews. **Q-Admin: (a)** Code changes are reviewed only by the code author. **(b)** No **(c)** Yes, all corrections are first released in development environment, and if they are considered safe, they are released in production. **(d)** No, management authorizes the launch of a new release but does not perform code reviews. **axs.res: (a)** HP information needed **(b)** HP information needed. **(c)** HP information needed. **(d)** HP information needed. **SAP-Sirax:** Code changes are done only by the provider LSY.	
6.4	Follow change control processes and procedures for all changes to system components. The processes must include the following:			
6.4.1	Separate development/test and production environments	**Partial**	**Squid:** Web UI, Core are different. Database is common. **Shark:** Development is made in administrator's computer. Data used for development are same with those of production. **Q-Admin:** Development environment does not exist. **axs.res:** HP offers production and test environment, but the data are the same. We only manage who has access to the development environment. ITP2 data are actually an image of RESA data.	Database should not be common for Squid. At axs.res the data should not be the same.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
			SAP-Sirax: Development and Production environments reside in 2 different servers. Project is still not fully implemented, so accounts are not cleaned up from the test server.	
6.4.2	Separation of duties between development/test and production environments	**Partial**	**Squid:** Yes, we have production and development environment. **Shark:** No, we only have production environment. Development is made in administrator's computer. **Q-Admin:** The systems core, offers the option to switch between ITP2 and RESA. We don't have development environment. **axs.res:** HP offers production and test environment, but the data are the same. We only manage who has access to the development environment. **SAP-Sirax:** No	No separation of duties between assigned at SAP-Sirax.
6.4.3	Production data (live PANs) are not used for testing or development	**Not Compliant**	**Squid:** No, we use production data for development. **Shark:** No, we use production data for development. **Q-Admin:** No, we use production data for development. **axs.res:** No, data are the same in ITP2 and RESA. **SAP-Sirax:** No, we use production data for testing.	There are used production data for testing and development
6.4.4	Removal of test data and accounts before production systems become active	**Not Compliant**	**Squid:** No, accounts are the same, but users do not have physical access to the development environment. **Shark:** No, accounts are the same, but users do not have physical access to the development environment. **Q-Admin:** We don't have development environment. **axs.res:** No, accounts are the same for RESA and ITP2, but only some	There are not test data and accounts removed before production systems become active.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
			specific users have access to the ITP2 environment. **SAP-Sirax:** In the production system only live and valid accounts exist. We do not use test data.	
6.4.5	Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:	**Not Compliant**	**Squid: (a)** No, **(b)** No **Shark: (a)** No, **(b)** No **Q-Admin: (a)** No, **(b)** No **axs.res: (a)** No, **(b)** No. **SAP-Sirax:** No	There are not change control procedures for implementing security patched and software.
6.4.5.1	Documentation of impact.	**Partial**	**Squid:** No **Shark:** No **Q-Admin:** No **axs.res:** No **SAP-Sirax:** Yes, LSY provides documentation of every new transport (system update) through our SIRAX Customer Portal.	There is not documentation of impact.
6.4.5.2	Documented change approval by authorized parties.	**Partial**	**Squid:** No **Shark:** No **Q-Admin:** No **axs.res:** No **SAP-Sirax:** Every transport we import is pre-approved by LSY and organization management.	There is not documented approval by authorized parties.
6.4.5.3	Functionality testing to verify that the change does not adversely impact the security of the system.	**Partial**	**Squid: (a)** No, **(b)** No **Shark: (a)** No, **(b)** No **Q-Admin: (a)** No, **(b)** No **axs.res: (a)** No, **(b)** No. **SAP-Sirax: a)** LSY tests functionality before releasing a new transport. **b)** LSY information needed	There is no such functionality
6.4.5.4	Back-out procedures.	**Partial**	**Squid:** Yes, through versioning but not included in a procedure. If something goes wrong, we can fallback to the latest stable release. **Shark:** Yes, through versioning but not included in a procedure. If something goes wrong, we can fallback to the latest stable release. **Q-Admin:** Yes, through	There are not back-out procedures.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
			versioning but not included in a procedure. If something goes wrong, we can fallback to the latest stable release. **axs.res:** HP information needed. **Sap-Sirax:** NO, Sap, Sirax Support code versioning through reguests. Before deploying a new version of a custom application, we keep backups, notify users and store the previous version of the application in order to restore it if something does not work as expected.	
6.5	Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines.	**Not Compliant**	Squid: (a) No, (b) No, (c) No. Shark: (a) No, (b) No, (c) No. Q-Admin: (a) No, (b) No, (c) No. axs.res: (a) No, (b) No, (c) No. SAP-Sirax: LSY confirmation needed	Do not develop according to secure coding guidelines
6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	**Partial**	**Squid:** SQL Server injections, scenario needs further research. Xpath values are passed through multiple error handlers and if something does not work as expected the application stops. LDAP injections scenario needs further research development. **Shark:** The application does not use database. Xpath values are passed	

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
			through multiple error handlers and if something does not work as expected the application stops. LDAP injections scenario needs further research development. **Q-Admin:** SQL injections on web UI level prevented by mysql_real_escape_string. Xpath values are passed through multiple error handlers and if something does not work as expected the application stops. LDAP injections scenario needs further research development. **axs.res:** SQL injections, LDAP injections, XPATH injections are technically impossible. **SAP-Sirax:** LSY confirmation needed	
6.5.2	Buffer overflow	**Partial**	**Squid:** Yes for core, through multiple validations. Web needs further research. **Shark:** Yes for core, through multiple validations. **Q-Admin:** Yes for core, through multiple validations. **SAP-Sirax:** LSY confirmation needed	
6.5.3	Insecure cryptographic storage	**Not Compliant**	**Squid:** No, data are not encrypted. **Shark:** No, data are not encrypted. **Q-Admin:** No, data are not encrypted. **axs.res:** HP information needed. **SAP-Sirax:** LSY confirmation needed	There are not cryptographic procedures.
6.5.4	Insecure communications	**Not Compliant**	**Squid:** No, data are not encrypted. **Shark:** Partial. SFTP is only used for uploading and downloading files from Accelya SFTP (Weblink). Files are retrieved via the	Squid has not encrypted data.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
			Organization FTP. **Q-Admin:** No, data are retrieved via the Organization FTP. **axs.res:** HP information needed - Organization Network team information needed. **SAP-Sirax:** LSY confirmation needed	
6.5.5	Improper error handling	**Partial**	**Squid:** Multiple error handlers, with log. Possible review needed. **Shark:** Multiple error handlers, with log. Possible review needed. **Q-Admin:** Multiple error handlers, with log. Possible review needed. **axs.res:** HP information needed. **SAP-Sirax:** LSY confirmation needed	There are not policy-procedures.
6.5.6	All —High‖ vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2).	**Not Compliant**	**Squid:** Not implemented yet. We need to discuss with Systems Team. **Shark:** Not implemented yet. We need to discuss with Systems Team. **Q-Admin:** Not implemented yet. We need to discuss with Systems Team. **axs.res:** HP information needed. **SAP-Sirax:** LSY confirmation needed	Not implemented yet.
Note: Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external):				
6.5.7	Cross-site scripting (XSS)	**Not Compliant**	**Squid:** Cross side scripting not found. **Shark:** Web interface does not exist. **Q-Admin:** Cross side scripting not found. **axs.res:** Web interface does not exist. **SAP-Sirax:** Does not apply	No Web Application Testing has taken place.
6.5.8	Improper Access Control (such as insecure direct	**Not Compliant**	**Squid:** Web interface does not display any credit card related information.	No Web Application Testing has taken place.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	object references, failure to restrict URL access, and directory traversal)		**Shark:** Web interface does not exist. **Q-Admin:** Web interface displays the last 4 digits of credit cards. Users are authenticated through LDAP, and internal object references, are not exposed to users. **axs.res:** Web interface does not exist. **SAP-Sirax:** Does not apply	
6.5.9	Cross-site request forgery (CSRF)	**Not Compliant**	**Squid:** Web interface does not display any credit card related information. **Shark:** Web interface does not exist. **Q-Admin:** Web interface works with sessions but CSRF scenario needs further research ($_SESSION_ID implementation). **axs.res:** Web interface does not exist. **SAP-Sirax:** Does not apply	No Web Application Testing has taken place.
6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: § Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes § Installing a web-application firewall in front of public-facing web applications	Not Applicable	Squid: Web interface does not display any credit card related information. Shark: Web interface does not exist. Q-Admin: The application is not exposed to web. It is only accessible via the Organization Internal network. axs.res: Web interface does not exist. SAP-Sirax: Does not apply.	Not Applicable

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
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.	**Not Compliant**	Documentation is missing	security policies and operational procedures for developing and maintaining secure systems and applications are not documented

Table 20 - R6 Gap Analysis

There is clear need for Web Application Testing and Secure Code Review. Also it is highly recommended to have Secure Coding Standards in place.

6.5.7 Requirement 7 - Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

In the below figure**,** a graphical representation of Requirement 7 is given.

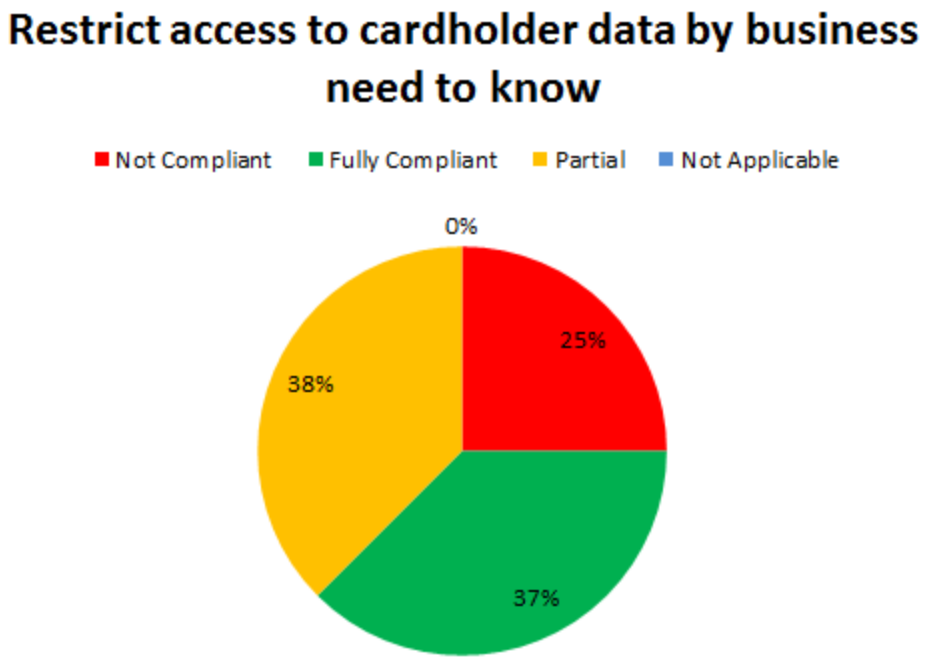


Figure 30: R7 Compliance Analysis

The detail gap analysis is presented in the following table:

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	Partial	Role based access by using active directory technology. There are IDs for physical access. IT admins are using a single key for access to computer room. Access to cardholder system components and data is limited to only those individuals whose jobs require such access. **Squid:** LDAP authentication. **Shark:** Runs as a scheduled task. **Q-Admin:** LDAP authentication. **axs.res:** a specific team is responsible for Access Control. Account is created only upon request via email. It is mandatory that at least a supervisor is copied (depending on the job duties and access level) **SAP-Sirax:** No, SIRAX is still not fully implemented and no strict access review has taken place. The answer is **NO.** We need to create separate accounts for every single end of our applications. E.g. Squid shares the same username with Q-Admin and BW automations.	Missing role based access and restrictions for part of the systems. No policies-procedures for (network access control).
7.1.1	Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	Partial	Access rights for privileged user IDs are restricted to the least privileges necessary to perform job responsibilities (Access permissions are given through AD With Groups & User Rights) The answer is **NO** **SAP-Sirax**: No, SIRAX is still not fully implemented and no strict access review has taken place.	Sirax has not restricted privileges.
7.1.2	Assignment of privileges is based on individual personnel's job classification and function	Partial	Privileges are assigned to individuals based on job classification and function Role-based access control given through organizational chart & Job description analysis. **NO**. **SAP-Sirax**: No, SIRAX is still not fully implemented and no strict access review has taken place.	No implementation at Sirax.
7.1.3	Requirement for a documented approval by authorized parties specifying	Not Compliant	No documented approval by authorized parties that specifies required privileges.	No documented approval by authorized parties that specifies required privileges.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	required privileges.			
7.1.4	Implementation of an automated access control system	Not Compliant	There is not an automated access control system.	There is not an automated access control system.
7.2. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to —deny all|| unless specifically allowed. This access control system must include the following:				
7.2.1	Coverage of all system components	Fully Compliant	**Squid:** Yes. We have two levels of access. **Shark:** Not applicable. It runs as a scheduled task. **Q-Admin:** Yes. We have two levels of access. **axs.res:** Yes, in partition, city code, application, duty code level. **SAP-Sirax:** Yes, Sirax environment is accessible only through our LAN and uses credentials authentication	No Gap Identified
7.2.2	Assignment of privileges to individuals based on job classification and function	Fully Compliant	**Squid:** Yes. We have two levels of access. **Shark:** Not applicable. It runs as a scheduled task. **Q-Admin:** Yes. We have two levels of access. **axs.res:** Yes, in partition, city code, application, duty code level. **SAP-Sirax:** No, SIRAX is still not fully implemented and no strict access review has taken place.	No Gap Identified
7.2.3	Default —deny-all|| setting Note: Some access control systems are set by default to —allow-all,|| thereby permitting access unless/until a rule is written to specifically deny it.	Fully Compliant	**Squid:** Yes. **Shark:** Not applicable. It runs as a scheduled task. **Q-Admin:** Yes. **axs.res:** Yes, in partition, city code, application, duty code level. **SAP-Sirax:** Yes, all SAP accounts require at least one role to have access to minimum screens.	No Gap Identified
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	Not Compliant	Documentation is missing	Security policies and operational procedures for restricting access to cardholder data are not documented - documented approval by authorized parties that specifies

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
				required privileges is missing

Table 21: R7 Gap Analysis

Generally, the R7 is partially completed. The organization has systems and processes in place to limit access based on need to know and according to job responsibilities. However it is highly advisable to keep the role management procedure documented.

6.5.8 Requirement 8 - Identify and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

In the below figure**,** a graphical representation of Requirement 8 is given.

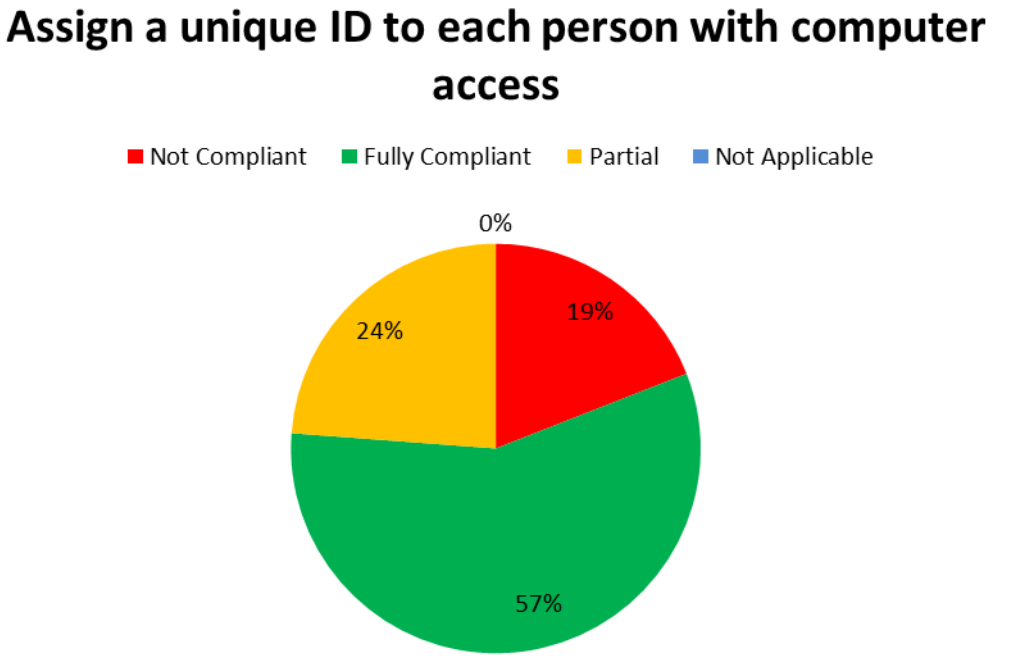


Figure 31: R8 Compliance Analysis

The detail gap analysis is presented in the following table:

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
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:	**Fully Compliant**	Yes	Define and adopt formal policies and procedures for the logical access.
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	**Fully Compliant**	Yes	No Gap identified
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**Fully Compliant**	Yes	No Gap identified
8.1.3	Immediately revoke access for any terminated users.	**Fully Compliant**	Yes immediately. Terminations are communicated by HR	No Gap identified
8.1.4	Remove/disable inactive user accounts at least every 90 days.	**Fully Compliant**	OPAT: TheUCF is automatically set to status inactive when not used for more than 80 days. The next time the user tries to log on, access will be denied. A message is displayed to say that the UCF is inactive and an administrator has to reactivate it. The password is valid for 40 days only. Once expired, the user is forced to change it. The UCF is automatically purged with all related	No Gap identified

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
			data (such as Message libraries, UET) if it has not been used during the last 240 days.	
8.1.5	Manage IDs used by vendors 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.	**Fully Compliant**	Yes	No Gap identified
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.	**Fully Compliant**	YES a) SAP/SIRAX (5 attempts) / OPAT: 3	No Gap identified
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	**Fully Compliant**	YES SAP/SIRAX/OPAT : Until the admin enables the user-ID	No Gap identified
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**Not Compliant**	NO	SAP/SIRAX currently do not have this policy, OPAT:30 min
8.2	In addition to assigning a unique ID, employ at least one of the following	**Fully Compliant**	We use passwords for all apps/systems	Define and adopt formal policies and procedures for the logical access.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	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 component.	Not Compliant	Not Compliant	Encryption is not used.
8.2.2	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	**Fully Compliant**	YES, Only via email	No Gap identified
8.2.3	Passwords/phrases must meet the following: • Require a minimum length of at least seven characters.	**Not Compliant**	NO, SAP/SIRAX currently do not have this policy a) OPAT : NO (min 4) b) Same as a	The current passwords have at least 6 characters. SAP/SIRAX don't have a password policy.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	• Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.			
8.2.4	Change user passwords/passphrases at least every 90 days.	**Partial**	YES,SAP/SIRAX currently do not have this policy a) OPAT:TheUCF is automatically set to status inactive when not used for more than 80 days. The next time the user tries to log on, access will be denied. A message is displayed to say that the UCF is	SAP/SIRAX policy is missing.
8.2.5	Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	**Fully Compliant**	YES OPAT : Last 10 / SAP-SIRAX : Last 5	No Gap identified
8.2.6	Set passwords/phrases for first time use and upon reset to a unique value for each user, and change immediately after the first use.	**Fully Compliant**	YES, for SAP/SIRAX/OPAT	No Gap identified

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
8.3	Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) Note: Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two	Not Compliant	Not Compliant	Define and adopt formal policies and procedures for the logical access. Adopt two factor authentication technologies for remote access to PCI-related systems

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	separate passwords) is not considered two-factor authentication.			
8.4	Document and communicate authentication procedures and policies 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	**Not Compliant**	No	Authentication procedures and policies have to be established
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for	**Partial**	We need to revise our group accounts in SAP/SIRAX	Revision of group accounts in SAP/SIRAX is necessary

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components			
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: •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	**Not Compliant**	No	Multiple accounts use the same authentication mechanisms

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
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)	**Fully Compliant**	YES	No Gap identified
8.8	Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all	**Not Compliant**	Documentation is missing	Define and adopt formal policies and procedures for the logical access

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	affected parties			

Table 22: R8 Gap Analysis

Although most of the requirements are fulfilled it is necessary for the organization to define and adopt formal policies and procedures for the logical access.

6.5.9 Requirement 9 - Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, - onsite personnel refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A visitor refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. Media refers to all paper and electronic media containing cardholder data.

In the below figure**,** a graphical representation of Requirement 9 is given.

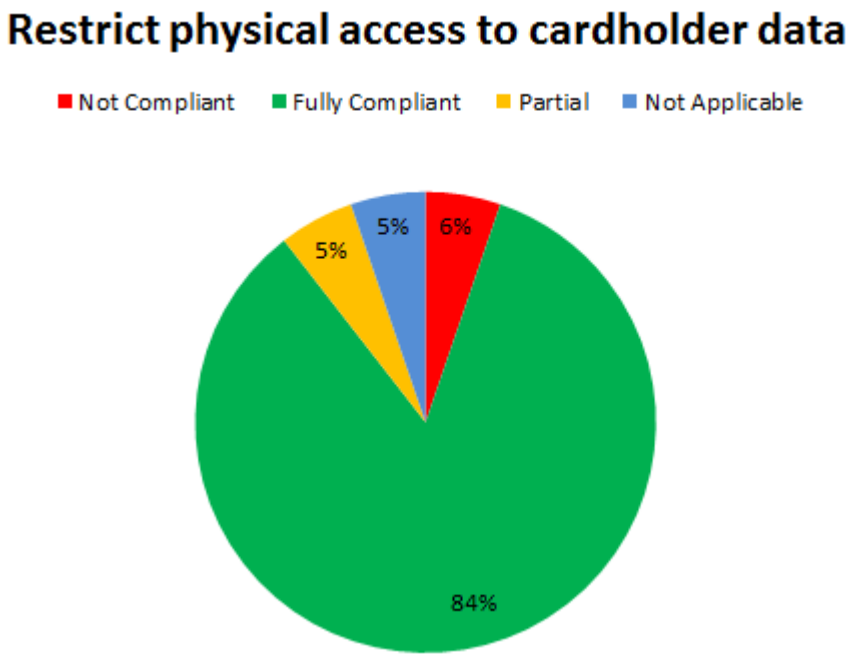


Figure 32: R9 Compliance Analysis

The detailed gap analysis is presented in the following table:

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	Fully Compliant	YES, There are IDs for physical access	No GAP identified
9.1.1	Use video cameras and/or access control mechanisms 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. Note: —Sensitive areas‖ refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.	**Fully Compliant**	YES, Video Cameras	Sample of records from sensitive 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. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in n areas with active network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is specifically authorized.	**Fully Compliant**	YES, Network jacks are activated upon request	No GAP identified
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	**Fully Compliant**	YES	No GAP identified
9.2	Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.	Not Compliant	NO, changes to access requirements are missing	Procedures for distinguishing personnel and visitors are missing.
9.3	Control physical access for onsite personnel to the sensitive areas as follows:	Fully Compliant	YES	No GAP identified

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	• 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 should include the following:			
9.4.1	Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	**Fully Compliant**	YES	No GAP identified
9.4.2	Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	**Fully Compliant**	YES	No GAP identified
9.4.3	Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	**Fully Compliant**	YES	No GAP identified
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 and 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 the law.	**Not Compliant**	NO	Visitor logs containing physical audit trails are not maintained.
9.5	Physically secure all media.	Fully Compliant	YES	No GAP identified
9.5.1	Store media backup in a secure location, preferable an off-site facility, such as an alternate of backup site, or a commercial storage facility. Review the location's security at least annually.	Fully Compliant	YES, backups are stored in a secure location away from the original site	No GAP identified
9.6	Maintain strict control over the internal or external distribution of any kind of media			

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
9.6.1	Classify media so the sensitivity of the data can be determined.	**Fully Compliant**	YES	It is highly advisable to implement policy for sensitive data.
9.6.2	Send the media by secured courier or other delivery method that can be accurately tracked.	**Fully Compliant**	YES	No Gap Identified
9.6.3	Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	**Fully Compliant**	YES	No Gap Identified
9.7	Maintain strict control over the storage and accessibility of media.	Fully Compliant	YES	It is highly advisable to create policy for controlling storage and maintenance of all media.
9.7.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.	**Fully Compliant**	YES	No Gap Identified
9.8	Destroy media when it is no longer needed for business or legal reasons as follows:	Fully Compliant	YES	It is highly advisable to create procedures for destroy media properly.
9.8.1	Shared, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	**Fully Compliant**	YES	No Gap Identified
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	**Fully Compliant**	YES	No Gap Identified
9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution- Best practices	Not Applicable	Not Applicable	Not Applicable
9.10	Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties	Not Compliant	NO	Procedures for physical measures, for distinguishing personnel and visitors, network jacks, are missing. Distinguishing personnel and

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
				visitors, network jacks are missing.

Table 23: R9 Gap Analysis

It is highly advisable for the organization to define, deploy and adopt specific physical access policies, procedures and controls.

6.5.10 Requirement 10 - Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

In the below figure**,** a graphical representation of Requirement 10 is given.

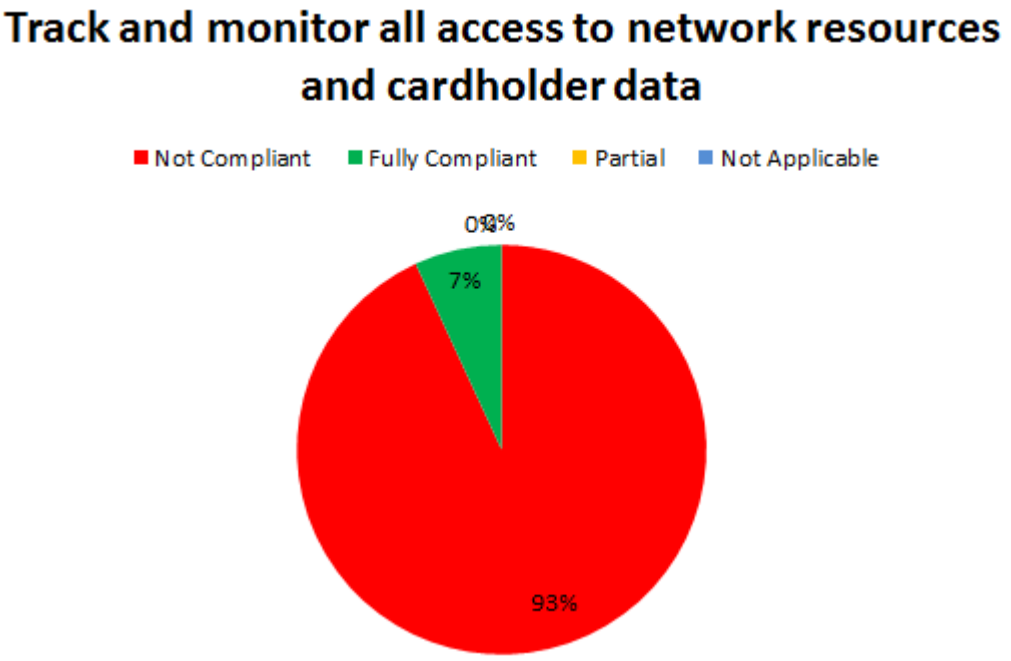


Figure 33: R10 Compliance Analysis

The detail gap analysis is presented in the following table:

Requirement #	Requirement	Compliance Status	Answers/Evidence	GAP ANALYSIS
10.1	Implement audit trails to link all access to system	Not Compliant	NO	There is not process in place to link all access to system components.

Requirement #	Requirement	Compliance Status	Answers/Evidence	GAP ANALYSIS
	components to each individual user			
10.2	Implement automated audit trails for all system components to reconstruct the following events:	Not Compliant	NO	There are not automated audit trails implemented for all system components
10.2.1	All individual accesses to cardholder data	**Not Compliant**	NO	There are not automated audit trails implemented for all system components
10.2.2	All actions taken by any individual with root or administrative privileges	**Not Compliant**	NO	There are not automated audit trails implemented for all system components
10.2.3	Access to all audit trails	**Not Compliant**	NO	There are not automated audit trails implemented for all system components
10.2.4	Invalid logical access attempts	**Not Compliant**	NO	There are not automated audit trails implemented for all system components
10.2.5	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.	**Not Compliant**	NO	There are not automated audit trails implemented for all system components
10.2.6	Initialization of the audit logs	**Not Compliant**	NO	There are not automated audit trails implemented for all system components
10.2.7	Creation and deletion of system-level objects	**Not Compliant**	NO	There are not automated audit trails implemented for all system components
10.3	Record at least the following audit trail entries for all system components for each event:	Not Compliant	NO	There are not audit trail entries recorded for all system components in place.
10.3.1	User identification	**Not Compliant**	NO	There are not audit trail entries recorded for all system components in place.

Requirement #	Requirement	Compliance Status	Answers/Evidence	GAP ANALYSIS
10.3.2	Type of event	**Not Compliant**	NO	There are not audit trail entries recorded for all system components in place.
10.3.3	Date and time	**Not Compliant**	NO	There are not audit trail entries recorded for all system components in place.
10.3.4	Success or failure indication	**Not Compliant**	NO	There are not audit trail entries recorded for all system components in place.
10.3.5	Origination of event	**Not Compliant**	NO	There are not audit trail entries recorded for all system components in place.
10.3.6	Identity or name of affected data, system component, or resource.	**Not Compliant**	NO	There are not audit trail entries recorded for all system components in place.
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. Note: One example of time synchronization technology is Network Time Protocol (NTP).	Fully Compliant	Domain controllers use Microsoft w32time Synchronize Clocks template which uses NTP to synchronize clocks on all discovered Windows servers and clients NTP.	No Gap Identified
10.4.1	Critical systems have the correct and consistent time.	**Fully Compliant**	(a) Servers receive time signals from internal sources (our DC) and all critical systems have the correct and consistent time, based on International Atomic Time or UTC (b) Only our Domain Controllers DC1 & Dc2 handle the time and peer with each other to keep accurate time. These 2 servers only send	No Gap Identified

Requirement #	Requirement	Compliance Status	Answers/Evidence	GAP ANALYSIS
			the accurate time to our servers & clients	
10.4.2	Time data is protected.	**Not Compliant**	NO	There is not time data protection in place.
10.4.3	Time settings are received from industry-accepted time sources.	**Not Compliant**	NO	Time settings are not received from a specific time source
10.5	Secure audit trails so they cannot be altered.	Not Compliant	NO	Audit Trails are not Secure
10.5.1	Limit viewing of audit trails to those with a job-related need.	**Not Compliant**	NO	Audit Trails are not Secure
10.5.2	Protect audit trail files from unauthorized modifications.	**Not Compliant**	NO	Audit Trails are not Secure
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	**Not Compliant**	NO	Audit Trails are not Secure
10.5.4	Write logs for external-facing technologies onto a log server on the internal LAN.	**Not Compliant**	NO	Audit Trails are not Secure
10.5.5	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).	**Not Compliant**	NO	Audit Trails are not Secure

Requirement #	Requirement	Compliance Status	Answers/Evidence	GAP ANALYSIS
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity	Not Compliant	NO	There is not policy for daily review of logs.
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, or that could impact the security of 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.)	**Not Compliant**	NO	No review/collection of logs performed
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.	**Not Compliant**	NO	No review/collection of logs performed
10.6.3	Follow up exceptions and anomalies	**Not Compliant**	NO	No review/collection of logs performed

Requirement #	Requirement	Compliance Status	Answers/Evidence	GAP ANALYSIS
	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 back-up).	Not Compliant	NO	There are not audit log retention policies and procedures in place.
10.8	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	Not Compliant	NO	There are not audit log retention, daily review and audit trails policies and procedures in place.

Table 24: R10 Gap Analysis

The organization has not logging mechanisms. It is highly advisable to define and deploy policies and procedures related to log and audit management. Also it is highly advisable to deploy a SIEM solution especially for PCI-related systems.

6.5.11 Requirement 11 - Regularly test security systems and processes

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

In the below figure**,** a graphical representation of Requirement 11 is given.

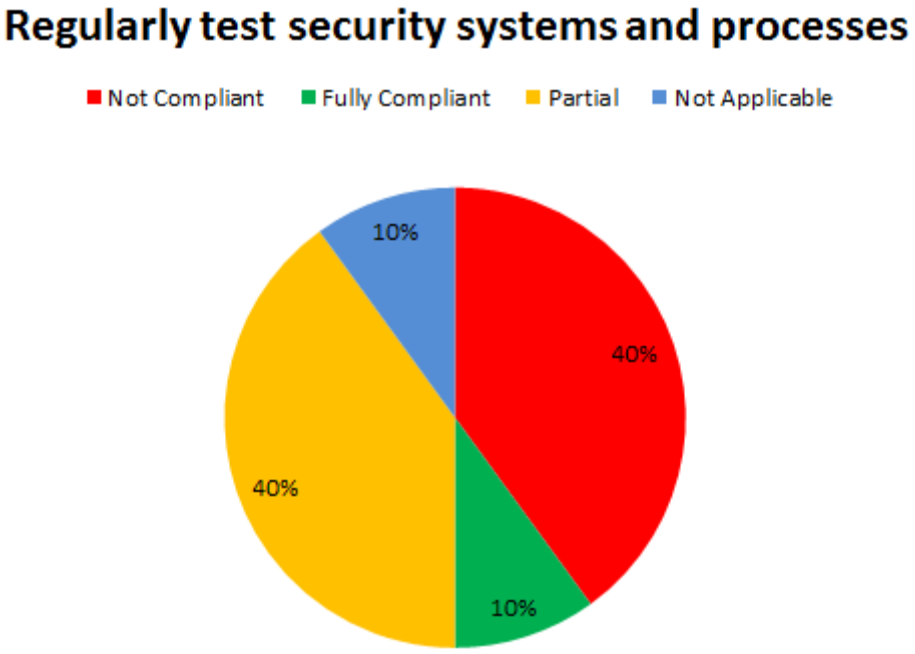


Figure 34: R11 Compliance Analysis

The detail gap analysis is presented in the following table:

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
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	Not Applicable	Not Applicable	Not Applicable
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	Partial	Already complete a vulnerability scan. internal and external network vulnerability scans at least quarterly and after any significant change in the network	Policy-procedures for internal & external vulnerability scans are missing.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	topology, firewall rule modifications, product upgrades). Note: It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.			
11.2.1	Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities are resolved. Scan must be performed by qualified personnel.	**Partial**	YES, (a) Internal network vulnerability scans at least quarterly and after any significant change in the network. (b) Yes, include rescans until passing results are obtained, or until all High vulnerabilities are resolved (c) All scans performed from qualified personnel from IT Department – no organizational independence	All scans performed from qualified personnel from IT Department – no organizational independence

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
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). Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by internal staff.	**Partial**	YES, (a) External network vulnerability scans at least quarterly and after any significant change in the network.(b) Yes, scan results satisfy the ASV Program Guide requirements (c) No, all scans performed inside our company with our qualified personnel from IT Department	An external partner must be used for vulnerability scans.
11.2.3	Perform internal and external scans after any significant change. Scan must be performed by qualified personnel.	**Partial**	YES, (a) Yes, Perform external and internal penetration testing after any significant infrastructure or application upgrade or modification, (b) c) Yes, all scans performed inside our company with our qualified personnel from IT Department	All scans performed from qualified personnel from IT Department – no organizational independence

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
11.3	Perform external and internal penetration testing at least once a year 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). These penetration tests must include the following:	Partial	YES, (a)Yes, Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification, (b) Yes, the scan process for exploitable vulnerabilities corrected and testing repeated (c) No, all scans performed inside our company with our personnel form IT Department	An external partner must be used for vulnerability scans.
11.3.1	Network-layer penetration tests	Not Compliant	No, Perform external penetration testing at least once a year and after any significant infrastructure or application upgrade or modification	No network-layer penetration test took place
11.3.2	Application-layer penetration tests	Not Compliant	No, Perform internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification	No application-layer penetration test took place
11.4	Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder	Not Compliant	NO, IDS/IPS is used for INTERNET traffic only right now	IDS/IPS is not used to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.			data environment
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly	Not Compliant	NO	There are not change-detection tools deployed within the cardholder data environment
11.5.1	Implement a process to respond to any alerts generated by the change detection mechanism	Not Compliant	NO	There are not tools configured to alert personnel to unauthorized modification of critical system files

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
11.6	Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties	Not Compliant	NO	There are not security policies established for security monitoring and testing

Table 25: R11 Gap Analysis

The main issues identified from this requirement is that the organization needs to do Both Network Layer and Application Layer Penetration Tests along with the vulnerability scans and it is highly advisable to use third company for the implementation of the testing. Also file-integrity monitoring tools are necessary.

6.5.12 Requirement 12 - Maintain a policy that addresses information security for all personnel

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, - personnel refers to full-time and part-time employees, temporary employees, contractors and consultants who are - resident on the entity's site or otherwise have access to the cardholder data environment.

In the below figure**,** a graphical representation of Requirement 12 is given.

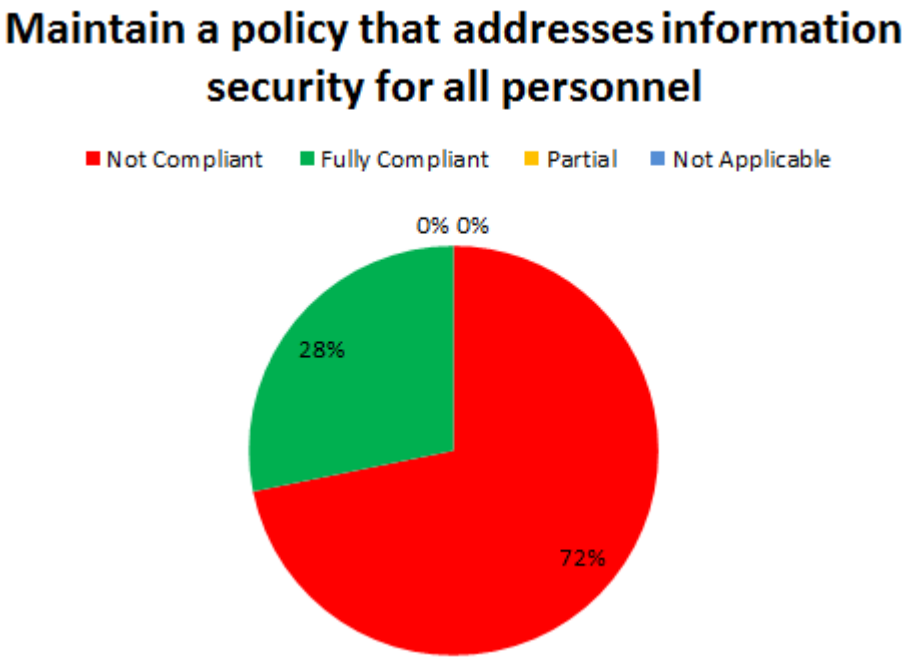


Figure 35: R12 Compliance Analysis

The detail gap analysis is presented in the following table:

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
12.1	Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	**Not Compliant**	NO	There is not security policy in place.
12.1.1	Review the security policy at least annually and update the policy when the environment changes.	**Not Compliant**	NO	There is not security policy in place.
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 risk assessment.	**Not Compliant**	NO	There is not risk assessment process in place.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
12.3	Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following:	**Not Compliant**	NO	There is not security policy in place.
12.3.1	Explicit approval by authorized parties	**Not Compliant**	NO	There is not security policy in place.
12.3.2	Authentication for use of the technology	**Not Compliant**	NO	There is not security policy in place.
12.3.3	A list of all such devices and personnel with access	**Not Compliant**	NO	There is not security policy in place.
12.3.4	A method to accurately and readily determine owner, contact information and purpose (for example labeling, coding, and/or inventorying of devices)	**Not Compliant**	NO	There is not security policy in place.
12.3.5	Acceptable uses of the technology	**Not Compliant**	NO	There is not security policy in place.
12.3.6	Acceptable network locations for the technologies	**Not Compliant**	NO	There is not security policy in place.
12.3.7	List of company-approved products	**Not Compliant**	NO	There is not security policy in place.
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	**Fully Compliant**	YES	No GAP identified
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	**Fully Compliant**	YES	No GAP identified
12.3.10	For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly	**Fully Compliant**	YES	No GAP identified

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	authorized for a defined business need.			
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	**Not Compliant**	NO	There is not security policy in place.
12.5	Assign to an individual or team the following information security management responsibilities:	**Not Compliant**	NO	There is not security policy in place.
12.5.1	Establish, document, and distribute security policies and procedures.	**Not Compliant**	NO	There is not security policy in place.
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel.	**Not Compliant**	NO	There is not security policy in place.
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	**Not Compliant**	NO	There is not security policy in place.
12.5.4	Administer user accounts, including additions, deletions, and modifications	**Fully Compliant**	YES	No Gap Identified
12.5.5	Monitor and control all access to data.	**Not Compliant**	NO	There is not security policy in place.
12.6	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	**Not Compliant**	NO	There is not an awareness program in place
12.6.1	Educate personnel upon hire and at least annually. Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.	**Fully Compliant**	YES	No Gap Identified
12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	**Not Compliant**	NO	There is no procedure for personnel to submit for the policies.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
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.) Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	**Fully Compliant**	YES	There is not documentation in place.
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:	**Fully Compliant**	YES	There is not documentation in place.
12.8.1	Maintain a list of service providers.	**Fully Compliant**	YES	No Gap Identified
12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	**Fully Compliant**	YES	No Gap Identified
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	**Fully Compliant**	YES	No Gap Identified
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	**Fully Compliant**	YES	No Gap Identified
12.8.5	Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity	**Fully Compliant**	YES	No Gap Identified

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
12.9	Additional requirement for service providers: 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. **Note:** This requirement is a best practice until June 30, 2015, after which it becomes a requirement. **Note:** The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	**Not Applicable**	**Not Applicable**	**Not Applicable**
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 back-up processes § Analysis of legal requirements for reporting compromises	**Not Compliant**	NO	There is not documentation in place.

Requirement #	Requirement	Compliance Status	Answers/Evidence	Gap Analysis
	§ Coverage and responses of all critical system components § Reference or inclusion of incident response procedures from the payment brands			
12.10.2	Test the plan at least annually.	**Not Compliant**	NO	There is not documentation in place.
12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.	**Not Compliant**	NO	There is not documentation in place.
12.10.4	Provide appropriate training to staff with security breach response responsibilities.	**Not Compliant**	NO	There is not documentation in place.
12.10.5	Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.	**Not Compliant**	NO	There is not documentation in place.
12.10.6	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**Not Compliant**	NO	There is not documentation in place.

Table 26: R12 Gap Analysis

References

1. The PCI Security Standards Council, available at http://www.pcisecuritystandards.org
2. PCI DSS, http://www.pcisecuritystandards.org/tech/index.htm
3. Glossary of Terms, Abbreviations, and
4. Acronyms, available at https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-1.pdf
5. PCI Cyber Crime, available at https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf
6. Merchant POS Security, available at https://www.pcisecuritystandards.org/pdfs/Merchant%20POS%20Security%20EMV%20chip%20and%20PCI.pdf
7. PCI SSC New Self - Assessment Questionnaire (SAQ), available at http://www.pcisecuritystandards.org/tech/saq.htm
8. PIN Entry Devices, available at http://www.pcisecuritystandards.org/pin
9. Migrating from SSL and Early TLS, available at https://www.pcisecuritystandards.org/pdfs/Migrating_from_SSL_and_Early_TLS_-v12.pdf
10. SAQ Documents, available at https://www.pcisecuritystandards.org/document_library?category=saqs#results
11. Qualified Security Assessors (QSAs), available at http://www.pcisecuritystandards.org/resources/qualified_security_
12. Approved Scanning Vendors (ASVs), available at http://www.pcisecuritystandards.org/resources/approved_scanning_
13. PCI DSS Supporting Documents, available at http://www.pcisecuritystandards.org/tech/supporting_documents.htm
14. PCI DSS Overview, available at https://www.pcisecuritystandards.org/documents/PCI_SSC_Overview.pdf
15. Getting Started with PCI DSS, available at https://www.pcisecuritystandards.org/documents/PCI_SSC_Getting_Started_with_PCI_DSS.pdf
16. Ten Common Myths of PCI, available at https://www.pcisecuritystandards.org/documents/PCI%20SSC%20-%20Ten%20Common%20Myths.pdf
17. Penetration Testing Guidance, available at https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf
18. Visa Cardholder Information Security Program, available at http://www.usa.visa.com/merchants/risk_management/cisp.
19. MasterCard, available at http://www.mastercard.com/us/merchant/security/index.html
20. American Express, available at https://www.americanexpress.com/
21. Discover, available at www.discovernetwork.com/resources/data/data_security.html
22. JCB International Credit Card Co., Ltd., available at http://www.jcbusa.com
23. NIST Special Publication 800 - 115 (DRAFT): Technical Guide to Information Security Testing, available at csrc.nist.gov/publications/PubsDrafts.html#SP - 800 - 115
24. NIST Special Publication 800 - 92: Guide to Computer Security Log Management, available at csrc.nist.gov/publications/nistpubs/800 - 92/SP800 - 92.pdf
25. NIST Special Publication 800 - 50: Building an Information Technology Security Awareness and Training Program, available at csrc.nist.gov/publications/nistpubs/800 - 50/NIST - SP800 - 50.pdf
26. NIST Special Publication 800 - 111: Guide to Storage Encryption Technologies for End User Devices, available at csrc.nist.gov/publications/nistpubs/800 - 111/SP800 - 111.pdf

27. NIST Special Publication 800 - 30: Risk Management Guide for Information Technology Systems, available at csrc.nist.gov/publications/nistpubs/800 - 30/sp800 - 30.pdf
28. NIST Special Publication 800 - 94: Guide to Intrusion Detection and Prevention Systems (IDPS), available at csrc.nist.gov/publications/nistpubs/800 - 94/SP800 - 94.pdf
29. National Vulnerability Database (NVD), available at nvd.nist.gov/nvd.cfm
30. Microsoft TechNet Security Center, available at http://www.microsoft.com/technet/security/default.mspx
31. Open Web Application Security Project (OWASP), available at http://www.owasp.org/index.php/Main_Page