PCI DSS case study: Impact in network design and security

Yudit María
PCI DSS Case Study: Impact in Network Design and Security

By

Yudit María

Thesis submitted in partial fulfillment of the requirements for the Degree of Master of Science in Networking and Systems Administration

Rochester Institute of Technology

B. Thomas Golisano College of Computing and Information Sciences

April, 2010
Rochester Institute of Technology
B. Thomas Golisano College
of Computing and Information Sciences

Master of Science in Networking and Systems Administration

Thesis Approval Form

Student Name: Yudit María

Thesis Title: PCI DSS Case Study: Impact on Network Design and Security

Thesis Committee

Name: Charles Border, Ph.D
Signature: 
Date: 
Chair

Name: Héctor Mora
Signature: 
Date: 
Committee Member

Name: Arlene Estévez
Signature: 
Date: 
Committee Member
PCI DSS Case Study: Impact in Network Design and Security

I, Yudit María hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.

Date: April, 2010  Signature of Author: __________________________
PCI DSS Case Study

Impact on Network Design and Security

Yudit María

Committee Members:

Héctor Mora
Charles Border
Arlene Estévez

Project Proposal submitted in partial fulfillment of the requirements for the Degree of Master of Science in Networking and Systems Administration

April, 2010
Abstract

The Payment Card Industry Data Security Standard is a set of twelve security requirements applicable to all institutions and systems handling, storing or transmitting cardholder information. It was created by the main card brands in a united effort to respond to the increasing number of attacks and data breaches cases targeted and linked to card and cardholder data. The standard considers points such as policies design, data security, network architecture, software design, application security, transmission encryption requirements and so on. Being compliant with the standard can be both expensive and traumatic for any business willing to do it. This research analyzes the impact that this compliance achievement process can have on an enterprise. This work is focused on the networking infrastructure and security and application security in general. This is a case study based on a real situation, where real current procedures and implementations were evaluated against the standard requirements regarding networking design, security and applications security. This will provide a benchmark of the situation towards getting the compliance validation in the company subject of this case study.
Table of Contents

Abstract ......................................................................................................................................... 1

Table of Contents .......................................................................................................................... 2

1. Introduction .................................................................................................................................. 4

2. Antecedents ................................................................................................................................... 7
    2.1. What is it about? ...................................................................................................................... 7
    2.2. Who is the target? ................................................................................................................... 9
    2.3. Some History ......................................................................................................................... 10
    2.4. PCI DSS Compliance Validation ......................................................................................... 12
    2.5. Network Design and PCI DSS Impact ................................................................................. 13

3. Motivation and Scope .................................................................................................................. 15

4. Methods, Materials and Procedures .......................................................................................... 16
    Procedure ...................................................................................................................................... 16

5. Case Study Scenario ..................................................................................................................... 18
    5.1. Regional Situation .................................................................................................................. 20
    5.2. Analysis ................................................................................................................................... 21

6. Network Diagrams Analysis ........................................................................................................ 22

7. Experience and Impact ................................................................................................................ 35
    7.1. Cardholder Environment: ..................................................................................................... 35
    7.2. Firewall Implementation ......................................................................................................... 36
    7.3. Network and Infrastructure .................................................................................................... 37
    7.4. Access Control ....................................................................................................................... 39
    Requirement 6: Developing and Maintaining Secure Applications and Systems ...................... 40
    Requirement 7: Restrict access to cardholder data by business need-to-know ......................... 42
    Requirement 10: Track and monitor all access to network resources and cardholder data .......... 43
    Requirement 11: Regularly test security systems and processes .................................................. 44
    7.5. Costs ....................................................................................................................................... 45

8. Findings and Results ..................................................................................................................... 47
9. Recommendations ................................................................. 53
10. Conclusions ............................................................................. 55
11. Glossary .................................................................................. 57
12. Bibliography .............................................................................. 58
Appendix A ................................................................................... 61
Appendix B ..................................................................................... 73
1. Introduction

Credit cards have become a very common way to handle money transactions around the globe. The amount of credit cards being issued keeps going up each year. We have gone a long way since the emission of the first credit card in 1958 (Woolsey & Schulz, 2010). In the USA by June 30, 2009 Visa had 309 million credit cards circulating; Master Card 211 million by September 30, 2009; American Express 54 million by December 31, 2008 and Discover 57.1 million by the same year (Woolsey & Schulz, 2010). From those numbers it can be inferred a total estimate of 631.1 million credit cards were spread all over the country by the end of 2009. Extending those numbers to the globe, and considering debit cards, probably we would be talking about billions of cards doing billions of transactions each day.

Card numbers have always been a temptation for delinquents; cardholder’s data (name, account number, pin) is very useful information for identity theft purposes and a cloned credit card can give a vandal immediate money to spend without being noticed for a while.

Credit card information and cardholder’s data can be illegally collected from several sources such as: garbage, mailboxes, personal records on a hospital or at your workplace, electronically stolen from e-commerce sites, through phishing or with the use of hacking techniques targeted to databases of any company that is known to handle credit card information (Obringer, 2002).

Early in the past decade electronic frauds and hacking techniques started giving serious headaches and represent big losses to companies of all sizes. In 2007 TJX Companies Inc. reported a data breach compromising more than 45 million credit and debit card data; at that moment it was considered the biggest data breach ever (Bosworth, 2007). Before that, in 2005, CardSystems Solutions a payment processor had an intrusion that was presumed having compromised about 40 million credit card
numbers (Krazit, 2005). More recently in 2009, Network Solutions had an incident where about 573,000 debit and credit cards accounts were compromised (Krebs, 2009) while HeartLand Payments Systems had a data breach case, also in 2009, even though they alleged no card data was compromised. It is possible to continue citing cases like these for another couple of paragraphs, but it is enough to illustrate the idea, that those incidents were part of the driving factors (along with disclosure laws and some other particular situations) on the development of enhanced security requirements and standards.

Some years ago before PCI DSS different card brands had made their individual efforts on security initiatives; Visa developed the Cardholder Information Security Program (CISP) and the Account Information Security (AIS) while MasterCard created the Site Data Protection Program (SDP)(Gorge, 2006); American Express had the (DSS) Data Security Standards and Discover Card –(DISC) the Discover Card Information Security and Compliance (Security Assessment, 2007).

Paradoxically, data breaches incidents like those mentioned above made the Payment Card Industry major representatives think that the security topic needed to be addressed as a joint effort in order to make it work. The idea was involving all stakeholders in the protection of their most important assets: cards and cardholder data. That is how the Payment Card Industry Data Security Standard (PCI DSS) was born. The main card brands (American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International) formed the PCI Security Standards Council that later would release the PCI DSS standard on its first version.

The standard attempts to be a guide on how to approach data security for companies handling credit card transactions in order to minimize the risks of data breaches, identity theft and frauds related to cardholders’ data. However getting stakeholders complying with the standard has not been an easy road, and actually represents a transforming process for every company affected by it, worth of a case study.
The following document contains documentation on a case of study about the PCI DSS compliance process for a Dominican financial institution and the impact it has had on its network designing and technological infrastructure security.
2. Antecedents

2.1. What is it about?

PCI DSS is a Security Standard. Its objective is to protect cardholder data. Its requirements should be applied on any system, server and/or network containing this type of data. Cardholder data includes: PAN: Principal Account Number or Card Number, Cardholder Name, Card Expiration Date, Service Code, Sensitive Authentication Data: Full magnetic stripe data, CAV2/CVC2/CVV2/CID¹ and PINs/PIN blocks. “The Primary Account Number (PAN) is the defining factor in the applicability of PCI DSS requirements and PA-DSS². If PAN is not stored, processed, or transmitted, PCI DSS and PA-DSS do not apply (PCI Security Standards Council LLC, 2008)”

The vast majority of financial institutions (or any institution affected by the standard) do not possess a whole infrastructure or resources exclusively dedicated to handle card transactions and cardholders’ data thus in most cases, not to say in all of them, PCI DSS requirements will affect the entire technological infrastructure and organization; that is the reason why this standard supposes such a big impact on the institutions willing to comply with it.

PCI DSS establishes the following twelve requirements:

**Build and Maintain a Secure Network**

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

---

¹ See Glossary
² Payment Application Data Security Standard
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

**Protect Cardholder Data**

Requirement 3: Protect stored cardholder data.

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

**Maintain a Vulnerability Management Program**

Requirement 5: Use and regularly update anti-virus software or programs

Requirement 6: Develop and maintain secure systems and applications

**Implement Strong Access Control Measures**

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

**Regularly Monitor and Test Networks**

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

Requirement 11: Regularly test security systems and processes

**Maintain an Information Security Policy**

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

But, how such common sense directives can be so difficult to achieve? Some of the problems come with the sizes of the companies and the comprehension of the standard as well. Sometimes, misconception of the requirements leads to major difficulties on implementations.
2.2. Who is the target?

PCI DSS applies to any merchants, service providers, and financial institutions that handle, store, process or transmit cardholder data (Bradley, et al., 2007). Merchants are defined as any company that receives a card payment in exchange of a good or service. Service Providers are companies that process, store or transmit cardholder data; they might serve merchants or other service providers (Bradley, et al., 2007).

The standard classifies members, merchants, and service providers into different levels according to the number of transactions they handle. The classification also defines diverse compliance validation procedures and who is responsible for validating the compliance.

Table 1 – Compliance validation summary Table for merchants (www.ncsu.edu, 2005)(Bitter, 2009) (PriceWaterHouseCoopers, 2009)

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>Description</th>
<th>Compliance Validation</th>
<th>Validated By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>More than 6,000,000 annual credit card transactions; Global Merchants identified as level 1 by any Visa region; or Any merchant that has suffered an attack causing account data to be compromised</td>
<td>Annual On-site data security audit; Quarterly Network Scan Annual external/internal Penetration tests</td>
<td>Qualified Independent security assessor; or Internal audit Approved Scanning vendor (ASV)</td>
</tr>
<tr>
<td>2</td>
<td>1,000,000 to 6,000,000 annual transactions</td>
<td>Annual self-assessment; Quarterly Network Scan Annual external/internal Penetration tests</td>
<td>Merchant; Approved Scanning Vendor (ASV)</td>
</tr>
<tr>
<td>3</td>
<td>20K to 1,000,000 transactions per year</td>
<td>Annual self-assessment; Quarterly Network Scan Annual external/internal Penetration tests</td>
<td>Merchant; Approved Scanning Vendor (ASV)</td>
</tr>
<tr>
<td>4</td>
<td>Less than 20K annual transaction (Visa Credit Card e-commerce transactions) Less than 1,000,000 traditional Visa credit card transactions.</td>
<td>Annual self-assessment (recommended); Quarterly Network Scan (recommended)</td>
<td>Merchant; Approved Scanning Vendor (ASV)</td>
</tr>
<tr>
<td>Service Provider Level</td>
<td>Description</td>
<td>Compliance Validation</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------</td>
<td>----------------------------------------</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>More than 300,000 annual transactions</td>
<td>Annual On-site data security audit; Quarterly Network Scan</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Less than 300,000 annual transactions</td>
<td>Annual self-assessment Questionnaire (SAQ); Quarterly Network Scan</td>
<td></td>
</tr>
</tbody>
</table>

2.3. Some History

PCI DSS was settled as mandatory back in 2004. The latest compliance dates were established for 2007. (Miller). In 2005 several USA major (and minor) retailers and card processors were victims of data breaches incidents that exposed millions of credit card numbers and cardholders confidential information.

According to data contained in the Chronology of Data Breaches (Privacy Rights Clearinghouse, 2010), provided by the privacy rights Clearinghouse from the United States with data compiled from incidents within that country, a total of 345,124,400 records containing sensitive personal information were affected by security breaches in the USA since January 2005 to February 2010. Those breaches occurred on several different entities: universities, hospitals, Stores, banks and other financial institutions.

According to the ITRC (Identity Theft Resource Center, 2008), who keeps statistics on data breaches cases, in 2005 there was a “total of 158 disclosed incidents, potentially affecting more than 64.8 million individuals plus 20 undisclosed victim group populations” (ITRC, 2006); While in 2006 (ITRC, 2007) “At least 312 incidents have been disclosed, potentially affecting more than 19 million individuals: 30% of disclosures involve governmental or military agencies; 28%, educational institutions; 21%, general business; 13%, health care facilities or companies; and 8%, banking, credit or financial services entities”.

In 2007 (ITRC, 2008) there were 446 incidents and 127,725,343 records were exposed (although a record does not necessarily mean an individual because multiple records might be bound to only one individual, this is still a high number). The incidents were
distributed under the following categories: Medical/Healthcare 14.6%, Government/Military 24.7%, Educational 24.9%, General Business 28.9%, Banking/Credit/Financial.

In 2009 (ITRC, 2010) a total of 498 breaches incidents were reported with 222,477,043 records exposed. The breaches corresponded to: Medical/Healthcare 13.7%, Government/Military 18.1%, Educational 15.7%, General Business 41.2%, Banking/Credit/Financial 11.4%. For 2010 so far there have been reported 35 breaches affecting 1,422,304 records.

According to Tech//404 Data Loss Calculator (Allied World Assurance Company, 2006) a security incident where 1000 records are compromised can cost a company an average of US$ 199,526.00. Imagine cases as the ones contained in the reports mentioned above with numbers of records compromised as large as 2,900,000 records have been compromised (ITRC, 2007).

Credit card brands are aware of the fact that compromised data can cost a lot of money; this is especially true for card/cardholders data. They are also conscious that data breaches can turn into identity theft cases affecting the reputation of their industry. This is especially harmful since the industry could lose plenty of its gains if people start thinking that credit cards are not a safe way to handle their finances.

In order to minimize the risk of having card/cardholder data compromised, losing a lot of money and damaging a reputation, it is necessary to implement comprehensive security measures on the systems and environment where this data resides. It is also necessary to make everybody in the card payment business knowing of the need for collaboration and engagement with security on the infrastructure handling card/cardholder information. That is how PCI DSS came into the scenario.
2.4. PCI DSS Compliance Validation

In order to complete PCI DSS requirements companies can hire a Qualified Security Assessor (QSA) who is authorized to provide both assessment and guidance to institutions willing to comply with the standard. VISA certifies that QSAs are well trained and can assist a business on their road toward compliance. However hiring a QSA is not as easy as just thinking you need one and calling asking for their services.

Having a QSA can cost you a lot of money depending on the size of the company and the range of services you are requiring from this QSA. Those services can include several things such as: an initial assessment to evaluate in which stage the institution is positioned on the road to compliance, or how much will be needed to change, evaluate or invest in order to achieve the compliance. Also, this QSA might be the person responsible of completing your Report On Compliance (ROC).

The Report On Compliance is sort of an assessment form that is completed either for evaluation purposes or to be sent to the proper authorities stating that your business is considered to be in compliance with the standard and can be evaluated at any moment. There is another type of assessment filled out to validate compliance the Self-Assessment Questionnaire (SAC).

The difference between Report On Compliance and a Self-Assessment Questionnaire is that while the Report On Compliance is a document filled by institutions that must be validated by the brands, the Self-Assessment Questionnaire (valid to certify compliance of level 3 merchants) is an evaluation that does not need to be validated by any third party.

Why would it be necessary to hire a QSA in order to receive guidance to be compliant with this standard? Getting PCI DSS compliance is more than just a project. It is a whole transformation process, and as any process there could be resistance to start
working on it. This resistance might be due to several reasons such as: an insufficiency of resources, including money, time and personnel to complete the tasks that are supposed to be executed in order to be compliant with the standard. That is why some help from an outsider is not only welcomed but also required, even if it costs you a lot.

Another factor considered is that setting down PCI DSS compliance in any company is not only about reading the documents provided by VISA, and filling a checklist. It is more about adapting the statements settled by the standard to the reality of the enterprise in a manner that allows evaluating accurately the technological infrastructure status and changes required to achieve compliance.

The decision from a company of having a QSA or a QSAC to help them during the procedure or to do it by themselves will strongly depend on the amount of resources the company can destine to achieve PCI DSS compliance. If a company understands that it has capable personnel that can complete the requirements and is willing to assign PCI DSS as an internal project to that personnel under complete assurance that they can lead the project and execute all the required activities, it is fine designate that personnel with the task of getting each PCI DSS requirement revised and done omitting the assistance of a QSA (or QSAC). This is not the most common approach, but it might be successful as well and even cheaper. Almost every company seeks for assistance, because they find themselves overwhelmed with all the things that come up from a process of this magnitude.

2.5. Network Design and PCI DSS Impact

As we know a company does not necessarily emerge with an understandable idea on how their technological infrastructure will be implemented, at least in this country (Dominican Republic). Even when they do have clear network design in mind, they eventually grow and have major or minor changes that affect their initial designing.
An organization might completes all the steps since the initial phase in order to create their technological platform or they can just accommodate to the situation and recycle or reuse existing elements if it comes that they are getting part or their total installations from somebody else.

The financial Institution selected for this case study is a relatively young one. It is an organization which network and infrastructure deployment was not previously designed and conceived from scratch. They inherited their physical installations and part of its technological infrastructure from other financial institutions that used to run their operations in the same physical place where this latest institution currently works. This means that the networking designing process has not been actually a “designing process”. It has been more an adaptation process. Their implementations were created responding to necessities and evolved precisely because of those necessities.

As any adaptation/evolution process it is understandable that several things are not actually on the place they should be. However, it is the responsibility of the team handling equipments, applications and installations to either improve the things they have inherited or just completely change them and turn it into what they need them to be. This is pretty much the process that this company is currently going through. And not only to introduce enhancements on the infrastructure they got from the past, but also to introduce a well planned security schema suitable to achieve PCI DSS compliance status.
3. Motivation and Scope

The objective of this case study is to evaluate how the adoption of a security Standard can impact the network design and the security infrastructure. The entire Dominican Market is facing the experience of getting PCI DSS Compliance. This standard was created back in 2004, by that time there was not a real attention or interest to respond to the standard requirements from the affected business in Dominican Republic (neither in USA or Europe). Also, since the standard was new, brands were not in the position of pushing that hard to make organizations compliant. Last years the story has changed. More and more card industry stakeholders including banks, merchants, service providers and issuers are working to get the compliance.

September 30th 2010 is the latest date globally (except for Europe) to achieve compliance for any enterprise handling, storing or processing card transactions. If decide not to be compliant with the standard they can be fined and eventually lose the right to do business with card brands. The Security Standard Council and the brands themselves are pushing hard to get everybody to be in compliant status.

The current Case study is related to PCI DSS and this standard covers different areas such as policies design, security approach, network architecture, software Design, application security, transmission encryption requirements and so on. This work will be focused only in the network designing activities and changes and the security schema for applications. Of course, if this activities are related to cards or cardholder environment, because PCI DSS its only applicable to those cases.
4. Methods, Materials and Procedures

The information presented on the following report was gathered by performing interviews with people working in the technology and security areas. Names of the participants of the interviews had been hidden for confidentiality purposes. During those interviews questions regarding to the design of the network and the original infrastructure diagrams from a couple of years ago were made.

There was a recompilation of existent documentation to know which things were already implemented and established regarding documentation requirements. Tests\(^3\) on the field were also performed to validate the truthfulness of the information provided by the interviewed personnel.

<table>
<thead>
<tr>
<th>Participants</th>
<th>Materials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking Administrators Level 1 and Level 2(^4)</td>
<td>Policies</td>
</tr>
<tr>
<td>Security Administrators Level 1 and Level 2</td>
<td>Network diagrams</td>
</tr>
<tr>
<td>Application Developers</td>
<td>Configuration procedures</td>
</tr>
<tr>
<td>System Users</td>
<td>Application development documentation</td>
</tr>
<tr>
<td></td>
<td>PCI DSS project complete documentation</td>
</tr>
<tr>
<td></td>
<td>Configuration Files</td>
</tr>
</tbody>
</table>

Procedure

Review Network Designs and configuration files.
Discuss information with personnel of the networking and security areas.
Execute activities to prove the affirmations of participants.
Policies revision and discussion with affected users.

---

3 Details on this activities has been omitted as required for confidentiality purposes
4 A higher number level means technical positions, while a lower number means a management position
Answer for the following questions were found along the development of this research for the company subject of the case study (it will be called Company X in the following paragraphs):

- Complete inventory of the changes made in the last years.
- The driving factors leading to those changes. Which of them were actually made because of PCI DSS.
- Which of them contribute to PCI DSS even if they were not initially made to comply with the standard.
- What is the effect of those changes/new implementations to make the infrastructure PCI DSS compliant?
- Analysis whether the changes can be accepted as well implementations for PCI DSS by a QSA /QSAC or by the brands.
5. Case Study Scenario

The organization featured on this case study is a national financial institution offering multiple services for customers of different categories: single individuals, small and medium enterprises, government, and so on.

The vast majority of its technological resources are located on a main site, there are seventy-five branch offices making use of those centralized resources. For example, users of remote offices access applications kept on servers located on the main site. Sometimes local users become distance clients accessing servers and facilities remotely using VPN connections. Also, third party vendors who are either collaborators or a special type of client accessing services from an extranet on the main site either through VPN tunnels or using dedicated connections. Web services are offered to allow any customer with an Internet connection to make use of different facilities for handling online banking activities.

Many of the services are offered within a specified office schedule while some others are offered on 24/7 basis such as online payments and accounts consulting. Annually they handle about six million eighty three thousand and five hundred forty seven (6,083,547) card transactions. This activity moves amounts of twenty millions three hundred twelve four hundred and sixty six millions dollars (US$ 20,312,466.76) monthly.

Number one requirement on this institution is to have the entire infrastructure available almost all the time. “Almost” because they have not measured their availability necessities thus they are not able to specify it in terms of a percentage. It is assumed that for some services the availability needs to be of 99.999 percent and for some others a 90.00 percent is enough to cover the required time to keep their

---

5 According to card transactions data from 2009 and first quarter of 2010
6 This number correspond to a monthly average month from 2009 however there are peaks on the card activity both high and low.
services. This sentence synthesizes the business objective: to be always available for their clients with the minimum costs.

Even though the availability is not the topic of this case study, it was brought to the stage because security is part of that precious availability that many enterprises seek to have permanently, as the one under study for this work. In order to have this permanent availability it is necessary to invest on the right infrastructure to provide and secure that infrastructure from viruses and internal/external attacks that can disrupt their operations as well. The main topic of this case study is network design and security focused on PCI DSS.

They handle more than 6,000,000 card transactions annually thus they fall under the category of Level 1 merchants for PCI DSS. They use web servers, application servers and have multiple databases to run their operations.

As it was mentioned before this organization needs multiple incumbents to access the data and applications they store and handle: Third-party vendors, customers, business associates, internal users, etc. This situation creates special requirements for security, especially because the cardholder environment is not completely isolated from the rest of the data.

A couple of years ago a transformation process was started for the whole infrastructure of this organization. This change was not motivated because of PCI DSS, indeed it started as an effort to reorganize their assets because they inherited an infrastructure not so well implemented and several issues were occurring due to that particular situation.

The first step to achieve an optimal network implementation is to study the necessities on the enterprise environment. This way it is possible to get enough foundation to make the right decisions about the procedure to follow. Sometimes the reality is that you are not part of the network-designing project since the very beginning making impossible that first analyzing step.
However, analyzing business particularities and constraints if you are part of a network-redesigning project is also good practice. The original infrastructure of this organization showed a lack of good analysis for its initial implementation.

Good Network Designing is not a step-by-step generic and well-defined process applicable to each and every single enterprise or situation even though there are ways to make network designing a successful project by following the correct steps (Oppenheimer, 2004), such as:

1. Analyze requirements
2. Develop a logical design
3. Develop the physical design
4. Test, optimize, and document the design

An optimal network design should provide mechanisms to have the necessary performance that does not affect the business operations continuity and allows having a satisfactory service level, it should also scale properly when the business grows and fit the necessities of the business (Oppenheimer, 2004).

The network in study lacked of the previously mentioned characteristics. Even so, it has changed dramatically to improve the security and to be more PCI DSS compliant.

### 5.1. Regional Situation

Dominican Republic is a country located in the Caribbean. Its economy is highly dependent on both tourism and remittances. “During the last 12 years remittances almost triplicate, going from US$1,088.9 millions to US$3,110.7 millions in 2008, with an average annual growing of 15.5% during that period” (Tinta Criolla, 2009).
Tourism however still has a leading role on the economy. Each year thousands (near four millions in 2009 (Iglesias, 2010) tourists decide to spend their vacations on the Island.

If people sending remittances and tourists can feel confident about handling their transactions in Dominican financial institutions revenues of those activity can keep a larger growth rhythm, which at the end will benefit not only the financial sector but also the entire country economy.

Given the fact that PCI DSS is a global data security standard, saying that an institution is compliant with it, will be captivated by all the customers of that institution, either national or internationally. This can be considered as an added value of the PCI DSS compliance and a reason to work continuously into keeping that compliance.

5.2. Analysis

A process took place in which all retrieved network diagrams were evaluated against the real configurations of the network in order to determine the veracity if evolution of the network presented in the set of diagrams. This analysis was made considering selected PCI DSS Requirements that are directly related to network designing and security. In the following Section there is a discussion of what was found.
6. Network Diagrams Analysis

This diagram dates back from a couple of years ago. It is the first one found in the set of documentation collected for this case of study and it will be explained in the following lines. Later on, we will see other diagrams showing the changes that the network has gone through. This is an attempt to examine and in some cases question those changes thinking of PCI DSS requirements. The current status of the network will be presented in the last diagram to evaluate the network status towards achieving PCI DSS compliance.

Starting from upper left corner the server farm can be seen connected to a core switch where all users were also connected. Different network segments separate users and
servers. The access control between them was implemented at the application and databases level. There was neither a firewall implementation to protect servers from user access or an Intrusion Prevention System (IPS) to analyze traffic flowing between them. Implementation of Intrusion Prevention Systems is not only a good security practice but also part of PCI DSS requirements.

In front of the core switch there was an IPS (IPS 1) to monitor traffic going in and out the most internal part of the network containing servers and users inside. This IPS seems to be strategically located to inspect every packet going to and coming from those internal segments, but the truth is that the proxy server they had to control Internet navigation was connected straight to the Internet (See connector 1). The traffic going to Internet from any of the segments behind the IPS went directly to the content switch H3 not passing through the IPS before leaving or entering the internal segments in that part of the network thus not being monitored.

However, there were two other IPSs (IPS 2 and IPS 3) in each of the ISP connections, so traffic entering the network was being analyzed in that point anyhow IPSs analyze traffic based on policies, signatures and traffic patterns learned and configured through a period of tuning and customization for the intended traffic they will be monitoring. Thus the policies you have on one IPS might not be effective monitoring certain type of traffic. In this case, the internal traffic was being analyzed by Internet IPSs and this could be highly ineffective monitoring.

Web and VPN Servers were behind the firewall it looks like any traffic from the Internet had to go through the firewall to access them and databases serving web applications were separated on a DMZ (See DMZ DB). All of these are PCI DSS Requirements. H3 and H4 (content switches) were being used as DNS servers and so were H1 and H2 providing redundancy for DNS Services. Even though H3 and H4 had an interface connected directly to the segment of web servers. If any of them was compromised there was an open entry to that segment that was supposedly protected by the firewall.
Both ISP lines entered to the network going to a hub (See HU1 and HU2). A hub is a device that repeats received packets into all its ports thus a host connected to the hub can see traffic that does not necessarily have anything to do with the communication it is maintaining at a moment. This might allow an intruder “listening” on the channel to get enough information about a communication session to be able to perform either a spoofing or a “man in the middle” attack.

There are different connections third party vendors (see Square A, B and C). One of these connections (See Square C) came from a router directly connected to the same switch that web servers were connected. There was not an IPS in the middle of this connection. Traffic coming in and out from that external company was not being monitored. Firewalls were controlling third party connections to the internal network (including the one depicted in square C). However there was still the issue that the switch where that third party was connected had an interface linked to H4 that also was connected straight to the internal network.

They had two ISP connections, but this facility was not being used for high availability purposes only one of them was functional for navigation and web services publishing. This did not work because it was not correctly configured on the equipments and by that time their availability requirements were not so strict.

There was an interface of FW2 dedicated for a connection of a third party and there was a server there in that segment also. Lamentably accurate information could not be retrieved on the purpose of this server. But it was connected in the same switch that the router connecting the third party vendor (Square B).
In this diagram we can see that the third party vendor previously seen in square C was now connected to the switch that the rest of the external companies were connected to (Square A). This was a good move because all the connections of third parties were separated on a segment of the network just for them (it will be called an extranet from now on). The traffic from that third party was controlled by the firewall (FW2) but traffic could not be monitored, because it was connected to a switch located “before” the IPS (See box C). Not other considerable changes were made in comparison to the first diagram.
A new firewall was added to control access from the internal segments to the DMZ. PCI DSS requires a firewall between any demilitarized zone and the internal network but this is not the reason why this firewall was added. Actually the reason was that some of the firewall implementations were made because it was necessary to have other interfaces to protect other network segments and the appliances in use did not provide them.

Other servers were added in the DMZ with the purpose of publishing the web site. Those servers had three interfaces connected to three different VLANs one in the segment of the databases; another in the content switch H4 for a connection to the public network and the 3rd one was used for synchronization among those servers.
A fourth firewall was added to the infrastructure. This one had two interfaces connected to the public networks of both ISPs. Another interface was connected to the internal network. The purpose of adding this firewall is not clear (none of the contacted personnel had a clear idea on the driving factors for this decision). There is different information about the reason for this movement but many coincide saying that it was added because they needed to protect other segments and no interfaces were available as with the FW3.

Others say it was added to establish a VPN tunnel with a third party vendor. This tunnel was going to be used for monitoring some specific services from an external company hired for this. This last affirmation seems more realistic, if we notice that the firewall had two interfaces into each of the ISP lines and one interface in the internal network.
Eventually two of the existent firewalls (FW1 and FW2) were configured in a cluster configuration for a high availability (failover).

On the two interfaces of the firewall connecting the extranet there was only one IPS. This IPS worked for the active line. If a problem occurred in that line, the traffic monitoring was not performed. This IPS could have been located right after the switch and before the router (See arrow) to monitor all the traffic, even though this would leave one of the external companies traffic with no monitoring at all (See Square A). The workaround to solve that was the creation of two different VLANs on that same switch, one of the IPS interfaces connected to one of those VLANs and all the routers for third parties also connected to that VLAN and the other interface of the IPS connected to the second VLAN were both lines (active and standby) were also
connected. That way it was possible to monitor any of the lines. Remember the reason of this workaround is that the IPS only had two interfaces.

At this point the network was becoming too complex and it was too hard to troubleshoot any issue (a big or an insignificant one) according to the interviewed personnel.
One of the content switches used for DNS is not here anymore. This equipment failed and was taken out from the network at that moment. A mail server was connected to the DMZ and to the public network. Two other VPN Boxes were connected to both ISPs to establish a VPN tunnel with another third party. These VPN Connections offered the possibility of having dedicated connection at a much lower cost than a “dedicated line” for example (as it was maintained with other third parties, see extranet).

Web Services were published only through the connection of the ISP 2. One of the hubs was disconnected and a switch was left on its place. At this point there was not a separation between users and servers other than the network segmentation. After this moment the network dramatically changed to a new configuration considering PCI DSS requirements.
Two new firewalls implementation can be seen on this diagram. One of the firewalls was placed (A) between the Internet and the internal network (PCI DSS Requirement 1.3) and another (B) between the DMZ and the internal zone. This one (B) was also protecting server’s access from internal users. One of these servers segments protected by the firewall contained all the equipments that were identified as containers of cardholder data.

The extranet segment was protected by another cluster of firewalls and an IPS was located in front of the connection to monitor all traffic coming in and out of that segment. Another stand-alone firewall stood to keep the VPN tunnel with the monitoring service because of compatibility issues (the VPN could not be configured on external firewalls because those had an ISP Redundancy configuration and the
other end equipments did not support this feature). Both firewalls (the cluster and the stand alone) also protected the internal network of an Internet connection kept with an ISP. Internal users came either from the main office buildings or from remote sites connected through a fiber connection or radio transmission. On the line connecting those remote users two IPSs were placed.

An appliance for analyzing outgoing mail was between two internal servers, this could be a security vulnerability since this box handles traffic going out to the internet and any security flaw could be used to compromise it and gain access to the internal network. Web servers were located in a DMZ and databases in another separated segment (PCI DSS Requirement 1.3.7). Besides the firewall, a proxy server controlled access to those web servers, from the internal networks. Those proxy servers security was hardened by closing all ports not required for its correct operation, disabling unnecessary services and prohibiting access from not authorized parties, because it works as a firewall too. Plus the VLAN on the core switch were they connect was a separate one, created only for them.
This is the current network status. It has evolved amazingly and the difference since its initial implementations is tangible. At this point, it seems to be a PCI Compliant network. It has two firewall implementations protecting the internal network from the DMZ and the DMZ protected from the Internet. It has IPSs implementations on each Internet connection and on the connection where remote offices traffic arrives. Public accessible servers are located in the DMZ and databases accessible by those servers are located on a separate network segment.

The appliance for analyzing outgoing mail is now located between the DMZ and an internal segment controlled by the firewalls. A stand-alone firewall implementation stood to keep a VPN tunnel because of the compatibility issue mentioned before.
7. Experience and Impact

After analyzing network diagrams and having personnel interviewed several facts can be discussed in here:

7.1. Cardholder Environment:

As in any enterprise this company had different environments: Production, Development and Testing. However, those environments were neither separated nor controlled. Any server on development and/or testing segment could easily access any other server from production and vice versa. There were controls at the database level but not at the network level. An insecure testing or development segment can be the wide open door through which intruders access your systems.

In the configuration of the network seen on Figure 1, there is not a clear separation of the cardholder environment from the rest of the applications. For example servers use to handle card transactions were mixed with the rest of the servers, probably on a common LAN segment, meaning the access to almost anywhere in the network also implied access to the cardholder environment.

Servers in production stored, handled and transmitted credit card data, and since there was not a clear limit on which of those servers in fact handled cardholder data there was a big issue about the protection of those servers. However, it was also an issue trying to secure all servers to comply with PCI DSS because there was not a firewall that could do it at that moment. Eventually all servers were secured with a new firewall implementation and those handling credit card data were separated on a network segment only for them.

Any of the collected diagrams described the flow of a card transaction, thus it was difficult to properly determine which servers were participating on the different types of card transactions or were storing cardholder information. Some activities were
performed to try to find out which servers handled critical information related to cards. For example: They did an application list, containing all those applications used for the business operations, either from outsiders or in-house developed\(^7\). According to the connections made by those applications either to databases or other servers they could determine which servers might contain card data. This application classification was a helpful process to separate the cardholder environment from the rest of the systems\(^8\).

Other activities performed for the process of identification and segmentation of the cardholder environment:

Interviews with databases administrator and the people handling applications that had to do with credit cards to discover each possible server used for card transactions. Observing which of those identified servers had interactions among them (network) or interacted with other unidentified servers.

A script was run on all machines to verify which of them was storing card data. This process lasted several weeks because it was a very exhaustive process about 1500 machines.

However it must been said, that cardholder environment is not completely isolated, and shares many resources with other data. It means that the PCI DSS requirements affect the entire infrastructure. Because it is considered that all of it is part of the cardholder environment.

### 7.2. Firewall Implementation

The first thing we can see in the network diagrams is that everything is mixed together. Users and servers coexisted right next to each other under the same environment.

\(^7\) The list of applications is included on Appendix B.

\(^8\) Not a complete separation but at least identification of the vast majority of servers containing Cardholder Data or participate in card transactions
They were segmented in different subnets but there were not other control or restriction mechanisms to separate them. This created a huge security flaw that could allow the success of an attack with no need of a big effort. Since the very beginning a firewall should have been implemented to protect server from internal access. Also those servers should have been separated among them to prevent any unnecessary and unauthorized access from one server to another.

The firewall configuration was poorly implemented. It had a DMZ protecting the database segment from public access but the web servers were not protected because they were reachable without having to go through the firewall. PCI DSS first requirement establishes:

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

1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.

Their proxy server navigated to the outside (internet) going directly from the internal network without having to go pass through the firewalls. This is not compliant with PCI DSS requirement 1.1.3 that establishes the use of a firewall at each Internet Connection (See Appendix A for more Details on PCI DSS requirements).

7.3. **Network and Infrastructure**

One of the content switches had a direct connection to the internal network (check H3 on the Diagram 1). These layer 4-7 communication equipments were used as DNS servers. They were publicly accessible and one of them had a direct connection to the internal network containing servers and users.
The core switch implementation was not homogeneous with the rest of the communication equipments implementation. The management of this core implementation became more and more unfeasible because the local personnel were not properly trained and the administration of those equipments was allegedly difficult. This situation created a dependency of the vendors of those equipments that was creating problems whenever any particular situation appeared and a troubleshooting was required.

The servers network interface cards only supported 10/100 Mbps speed. It worked correctly during many years. However, at some point the business was growing considerably and needs changed. The appearance of new applications, services and users, increased traffic being handled and the demand of resources to function properly also went up. So they thought it was a right move to: 1. Increase the links’ capabilities to 1000Mbps Links and 2. Migrate all NICs on each server to process a higher amount of packets and handle more traffic to take advantage of this higher capacity.

But, were they really conscious on how much they should have increased NICs capabilities or links speed? According to information provided by the personnel working that part, no. Even with applications demanding more and users being added to the company, the network performance did not reach unbearable levels for the business operations. Add to this was the fact that the business did not have a clearly defined network performance goal. There were no metrics on how the performance was on that time or how the network utilization was behaving to support the decision of increasing everything (including costs).

Links capacity was increased, because the network was becoming “slow”. They changed their links capabilities pretty much in an intuitive/perceptive move not supported by the corresponding analysis and metrics captures. At the end it came out to be a good move. Because they did continue growing but also they still face issues
with the performance of the network especially for some specific LAN segments were hundreds of servers are contained.

When changes to the servers and links were implemented, it came up that other equipments in the infrastructure appeared not to be capable of handling 1000Mbps links, and they started saturating the network causing disruptions on the communication of the different parts of the network. Those were the IPSs implementation (Intrusion Prevention Systems). Those IPSs were strategically moved to other segments of the network where they still provided protection without affecting performance (See figure 8).

Unfortunately all this decisions and upgrades because of performance issues were not properly documented and analyzed. There is no information saved from those days that can support the alleged theories of the reason why those changes of speed were made.

7.4. Access Control

The information that is to be accessed by users of the complete company is centralized and located within network segments that also handle critical information such as cardholder data. Which makes access control more critical.

Databases were distributed among multiple servers. Databases serving distinct applications were stored in different locations. Even if those databases had common elements. This caused unnecessary information duplicity. Furthermore, those servers lacked of redundancy in the case of a failure. There were several databases storing cardholder data spread along the network.

The encryption equipments (encryption key holders) were accessible from anywhere in the network. Later on with the latest firewall implementation and due to their criticality, they were segmented on an interface of the firewalls dedicated only to them,
which was a great step for PCI DSS that has requirements for Key Management, even though this part is not being considered on this case study (PCI DSS Requirement 3.5).

In the following lines there will be a discussion of the analysis made of the implementations, considering the standard requirements. The application requirements will be also discussed, because even though they are not part of the networking and infrastructure they are a very important topic on the standard.

**Requirement 6: Developing and Maintaining Secure Applications and Systems**

PCI DSS has requirements for securing payment card applications and systems. A walk through each of the requirements evaluating them against the current situation will clarify the position of the institution towards the standard compliance.

Requirement 6.1 is about updates and latest patch. In this company there is a policy that establishes the implementation of updates and patches but it is limited only to a certain platform. Thus the updates and patches policy is not applicable to another software and applications. Although the firewall policy, for example, establishes that they must updated to the latest software version and have the latest updates and/or corrections released by the vendors. However, there is not a general updates and patches application policy establishing, among other things, a timeframe required for this updating activity. According to PCI DSS most recent patches and updates must be applied not later than 30 days after its release. Also, there is not a process to identify newly discovered security vulnerabilities affecting applications different from web applications specific vulnerabilities.

Requirement 6.3: Developing software application in accordance to PCI DSS and based on industry best practices. For software development, there is an established process that includes points like validation of data inputs, error handling (for example
errors referring to login methods (Requirement 6.3.1.2) do not provide an explicit explanation of the failure cause, generic error messages for any application errors, etc.). However, in this process there is not a validation for the use of secure communications methods requirement (Requirement 6.3.1.4), for example. There is not an auditing of the coding for applications developed in-house or used from externals; activities contemplated on the development established process are not evaluated for applications bought from outside.

The test, production and development environments are separated and partially controlled (Requirement 6.3.2). There is not a duty separation between tests, development and production environments (Requirement 6.3.3), developers do have access to production environment. Connections are kept from development to production, and from test to production and test to development. Having those connections is necessary because otherwise the development and test activities could be completely stopped since there are functionalities existent only on production and any new development for those cases implies using the production environment. This also happens for several applications that do not have a dedicated test environment. Correcting this implies the creation of the three separated environments for each and every single application and/or system, which can provide an enhancement on security, but it might also cost a considerable amount of money.

Primary Account Numbers in production are still used for test and development for some applications (Requirement 6.3.4). This is a consequence of the lack of separation on the different environments (Production, Test and Development).

Requirements 6.3.5 and 6.3.6 for removing data before a system is released to production is not established as a requirement. It is done in some cases but not because is an obligation.
There is not a coding revision since there are not personnel responsible for this. Developers freely create applications following the best practices, but nobody certifies this.

There are changes control procedures (Requirement 6.4) documented both through automated applications and manually created, however there is not an exhaustive documentation of changes impact (Requirement 6.4.1) because is not required thus is obviated in documentation of changes control. There is a provision to have appropriate management sign-off (Requirement 6.4.2), testing (Requirement 6.4.3) and back-out procedures (Requirement 6.4.4) with the use of written documents to implement changes.

All web applications are tested (Requirement 6.5 and 6.6) by the testing personnel and controlled by integrity personnel. There are dedicated teams for those tasks. Each application is also tested with different automated tools to validate the security against Cross-Site Scripting (XSS), SQL Injection, Xpath Injection, Malicious File Execution, etc. However the process is informal, does not have a written procedure or policy requesting so. There is not a specific requirement of using a web-application firewall (Requirement 6.6) for publicly accessible web applications but host IPS installed on web servers fulfill this requirement.

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

Access restriction to cardholder data cannot be checked as performed completely successfully because cardholder data resides not only on specific servers and databases; it is also contained in file texts, physical paper/documents, e-mails and so on.

The control implemented in computing systems is the creation of profiles with explicit access limitations based on the type of work performed by an individual (Requirement
7.1.2\(^9\) and 7.2.2). There is no written requirement on a form to configure an access, or to elevate the privileges of a user, but the compensation measures is the requirement of an email from the superior authorizing the access (Requirement 7.1.3).

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

Since each username in the network is created for a specific user it is possible to link all access to an individual user (Requirement 10.2). The mechanism to control that each user is unique is through the use of both personal IDs and employee number assigned at the moment of hiring someone.

There are applications for log consolidation. There are logs activated on every database to keep track of any changes performed on the systems (Requirement 10.2): individual accesses, invalid access attempts, initialization of the audit logs, among other activities. They use 3 applications to satisfy this particular point of the standard. Those tools were approved to be PCI Compliant, however, the personnel handling those tools must be highly trained in the use, because they not only do track and monitoring as require by PCI in part 10, but also can impact the performance of the systems being monitored.

The time synchronization still lacks of a dedicated server for these purposes. This is critical because in the occurrence of an event it will not be possible to correlate logging and audit trails to perform an investigation.

There is a log server dedicated only for this purposes it is controlled through the firewall. But backups of this server do not have any special security requirement (Requirement 10.5.3). Those automated tools control logs Integrity. Alerts are generated whenever data is altered.

\(^9\) Numbers with this nomenclature refer to standard requirements subsections and can be checked on Appendix A.
There is not a policy establishing the timeframe for storing logs (Requirement 10.7), and the required availability of those logs.

**Requirement 11: Regularly test security systems and processes**

Wireless Access Points are non-existent within this enterprise, but there is not a formal requirement and/or procedure for periodically testing the presence of wireless access points (Requirement 11.1). It is known that an illegitimate access point can be introduced either by an internal employee or by a customer taking advantage of lack of security at a certain point.

There is not a formal procedure establishing the frequency of network vulnerability scans. It is not required to do vulnerability assessment after major changes on the network. However the personnel responsible of the network security perform this task at least twice a month being this is a particular initiative. It should be established as a formal procedure for security reasons and to comply with Requirement 11.2 of the standard.

Penetration Tests both internal and external are established as a policy (Requirement 11.3). However there is not a procedure to implement corrections to vulnerabilities found on those penetration tests. This should be done according to PCI DSS requirements.

IPSs (Intrusion Prevention Systems) are implemented to monitor traffic coming in going out of the network. These systems are configured to emit alerts low, medium or high. Those alerts are sent to a 24x7x365 monitoring team. IPSs are configured with a policy containing a number of signatures to detect different type of possible attacks. The policy is continuously tuned to include the largest amount of firms to detect several different attacks. This IPSs use different methods to detect and prevent intrusion such as port assignment, heuristics, port following, protocol tunneling,
protocol analysis, RFC compliance, TCP Reassembly, Flow Reassembly, and Statistical Analysis and pattern Matching (Rouland, 2004). Those devices are constantly updated but there is not a formal requirement for this. There are network IPS and host based IPS to monitor the traffic over servers considered critical, sensitive and containers of cardholder data (Requirement 11.5).

File integrity monitoring is inspected by two software applications but it was not possible to get details on this point.

7.5. Costs

The whole implementation of micro and macro projects for PCI DSS compliance purposes ascended to almost a million dollars for this company. Remember this is a level one company transacting with more than six millions credit cards annually and total benefits over 16 million dollars\textsuperscript{10}. This might sound as a high cost for a “security project” but it is worth the value if the repercussions of having fines and eventually losing the right to negotiate with card brands are considered. Card transactions are part of the most profitable activities for a company like this one of the type being used in this case study.

<table>
<thead>
<tr>
<th>Solution</th>
<th>Requirement</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus</td>
<td></td>
<td>US$90,000.00</td>
</tr>
<tr>
<td>Logging and events correlation tools</td>
<td></td>
<td>US $100,000.00</td>
</tr>
<tr>
<td>Two Factor Authentication Solution (Tokens)</td>
<td>8.2 - 8.3</td>
<td>US $30,000.00</td>
</tr>
<tr>
<td>Database Security Auditing Software (Active Blocking)</td>
<td>10.2 Y 10.3</td>
<td>US $200,000.00</td>
</tr>
<tr>
<td>Web Applications Security Assessment tools</td>
<td>6.3</td>
<td>US $32,000.00</td>
</tr>
<tr>
<td>External Assessors: Gap Analysis, Internal and External Penetration Tests.</td>
<td></td>
<td>US $100,000.00</td>
</tr>
<tr>
<td>Data Loss Prevention Solution</td>
<td></td>
<td>US$70,000.00</td>
</tr>
<tr>
<td>External assessors for correcting internal</td>
<td></td>
<td>US $50,000.00</td>
</tr>
</tbody>
</table>

\textsuperscript{10} This are general gains, no statistics about gains only because of card transactions could be gathered
Is important considering that this is an initial investment, this might make it seem extremely high, but after this, there should be less costs for keeping the compliance status.
8. Findings and Results

In general security has three important stages:

- Policy creation: to regulate the correct use of resources
- Infrastructure implementation: to ensure the policies are being followed
- Alertness: to evaluate how effective the implementation. Also, to consider whether new changes are necessary to improve security.

It can be affirmed that PCI DSS also considers those stages. The standard is not only about implementing solutions for security, data loss prevention antivirus or encryption, just to name a few. It is also about documenting those implementations as well as creating policies and making users aware or them.

This particular company has made a big effort about policy creation. They currently have policies for password management, firewall installation, information classification, antivirus software, access control, and secure application designing and information security in general.

For example the configuration norm for firewalls being used include requirements for:

- Changing the default usernames and passwords, with a password that complies with the robustness required by the password policy.
- Configuring the equipments to synchronize with a central NTP Server (Network Time Protocol). This is important in case of an event occurrence logs and data to be analyzed and correlated properly in the considered timeframe for auditing.
- Stateful Inspection of packets and connections and anti-spoofing mechanisms to be enabled. This provides the possibility of reducing the risk of attacks
through illegitimate connections and false traffic sources impersonating legal ones.

- Key exchange encryption, data integrity and data encryption for VPN (Virtual Private Network Settings) to be made implementing protocols and algorithms such as IPSec, IKE, AES128 and AES256.
- Configurations requirements for blocking all traffic (deny all) by default.
- Disabling of routing services on the firewalls
- Proper configurations for SNMP (Simple Network Management Protocol) including proper community settings and specified host from whom SNMP requests can be accepted.
- Requirements of justifications to enable rules allowing services and protocols not commonly known.
- Restrictions of ICMP traffic.
- Configurations of banners displaying messages alerting the access to secure and restricted equipment which use is auditable and intended to be accessed only by authorized personnel.
- Restriction of accesses to the equipment from anywhere in the network by default. Only authorized personnel can have the access and only through a secure protocol such as SSL.
- Only SFTP should be allowed. In case of inevitable requirement of FTP configuration allowance this connections must be restricted to specific servers from specific machines.
- Configuration of NAT rule to protect disclosure of internal network IP addresses.
- All servers accessible from the outside should be placed on a DMZ.
- Any access to the exterior will be restricted by default.
- Logging requirement for any connection except those of SNMP protocol generating trivial and excessive amount of traffic.
• Restrictions of certain services and ports\textsuperscript{11} unless they are strictly required by business activities.
• Analysis of SMTP traffic.
• Enabling of TCPSYN defenses.

However they do not have a configuration norm for routers and communication equipments. This point is being currently worked out.

There is a firewall implementation on each Internet connection and between the DMZ and the internal network. This firewall implementation is on a high availability configuration to ensure business continuity. But in the firewall configuration norm there is not an explicit requirement for this type of configuration, which is required by the standard.

They also have a formal process for approving and testing connections through the firewall (Requirement 1.1.1\textsuperscript{12}). This formal process includes the completion of a form with the source and destination IP addresses, the protocol and service, justification and systems being affected by the required access. The correspondent administrative personnel in the security department evaluate this form and approve or disapprove it.

A current network diagram is kept for the general infrastructure. This diagram is updated every time a change in the network is performed. However they do not have a detailed connection diagram representing connections to the cardholder environment (Requirement 1.1.2). They do not have a diagram describing the flow of card connections whenever a transaction is performed. This flow is not completely identified for some activities (for some other it is).

\textsuperscript{11} Explicit Description of the services and ports has been omitted for privacy

\textsuperscript{12} See Appendix A for details on the requirements
In the configuration policy there is a description of groups and roles for the management of the firewalls. In there it is clearly explained who is responsible for what, creating an adequate limitation/restriction of authorized people that can make changes on the firewalls (this is not applicable to all network components as required in 1.1.4).

Within the firewall configuration norm there is a description of specific ports and services allowed for the business operations but this list is not exhaustive. It needs to be completed and more detailed. There are common ports and services such as (HTTP, HTTPS or SSH) and some others not that common that are part of business specific applications (this part is still incomplete). There is a requirement of documenting which of those protocols and services is insecure and that is also incomplete. It requires an analysis for identified protocols and services that has not been made yet. (Requirement 1.1.5).

Requirement 1.1.6 establishes a review of firewall and routers rules at least every six months. This is not established on any of the policies or configuration norms and there is not a defined formal process to complete this activity.

Connection to critical servers containing cardholder data is restricted. Inbound and outbound traffic to those servers network segment is strictly controlled with the requirement of proper justification. However cardholder data environment is not restricted only to those servers. Any intermediate host that this data goes through is part of the cardholder data environment and some of those hosts probably cannot be restricted as much as those servers. So there is an issue in here about the “restriction to what is necessary for the cardholder environment” point established on Requirement 1.2.1.

The personnel in charge of handling it back up router configuration files periodically. Configuration files are also collected daily with the use of the monitoring tool. But there is not a secure repository specifically destined to store all this backups in a
secure manner. They are not properly synchronized either, it means that the configuration running on equipment is not verified against the backed up configuration after a reboot for example. (Requirement 1.2.2)

Requirement 1.2.3. Wireless traffic to the cardholder environment is controlled and restricted to the specified servers identified to be handling cardholder data, and also to databases containing cardholder data as well. But it is not possible saying that wireless access is completely controlled to the cardholder environment, because of what was previously explained of this environment scope. It is important to note that this company only has wireless links to support transmissions of high amounts of data among its different branches. They do not have wireless Acces Points.

Direct access to the Internet is prohibited (Requirement 1.3) There is a DMZ created for any of those services accessible by the public and controlled by the firewall (Requirement 1.3.1), any access from the internet only goes to servers contained within that DMZ. Accesses from internal IP addresses coming from the Internet (1.3.4) are prohibited through specific rules configuration in the external firewalls (this is established on the configuration norm of the firewalls).

No direct routes (1.3.3) are configured between the Internet and the servers and databases containing cardholder data. Actually there is a firewall protecting those servers and databases. Any connection to those segments is highly restricted by that firewall implementation.

Cardholder data container servers and databases do not pass traffic directly to the Internet. Any data going out to the Internet first goes to a protected segment. These servers can only access IP addresses within that segment (Requirement 1.3.5). However some of those servers still access Internet addresses because of business necessities. The compensation control for this is that the access is restricted to a specific IP address through a specific port.
Stateful inspection is implemented for all connections through the network (Requirement 1.3.6). Databases to be accessed for services published for outsiders are on a segment separated from the DMZ and separated from the internal network as well. (Requirement 1.3.7). NAT (Network Addressing Translation) is used for Internal IP addresses going to the Internet or to any third party.

Installation of personal firewall on any laptop is established as a policy but some personnel using laptops can disable the firewall and this is not controlled by a policy. Disk Encryption is being implemented as part of an end point security solution also required for laptops.
9. Recommendations

They should create a configuration norm for routers and communication equipments configuration norm. Methods of enforcing the application of the norm should be created.

There should be a correction on the updates and patches policy:

- To make it extensive to the whole system components
- To establish the minimum timeframe in which the updates must be applied.
- To include a structured procedure to audit the updates activities.

Personnel in charge of reviewing code on used applications should be hired (There is neither a person nor a department responsible of this activity).

Production, Test and Development environments should be isolated. This might have a high cost depending on the system or application being separated. But an insecure test and/or development environments can give access to an intruder to production systems causing a data breach. There should be an evaluation on how much you can invest on securing and separating those environments and find ways to handle that security the most cost efficient possible and without interrupting business operations.

They should create a policy for separating duties between production, test and development personnel, and educate the personnel to not incurring in activities that they are not authorized to do even if they have enough power to do it (because in some cases there is not possible to restrict users for operations’ sake).

Primary Account Number in production could be scrambled or use an algorithm method to convert PAN data into fictitious values to be used in test and development.
There should be a consideration of changing these values on any test/development system/application where they appeared.

There should be a paragraph on the policy for production date requiring the elimination of test data. Another paragraph should be added for changes control requiring a measure of impact the changes can have over the entire infrastructure.

Procedures to perform web-applications assessment should be formally instituted. Requiring the use of both automated tools and manual verification.

Centralized Log Server should be backed up in another server controlled by the firewall and in tapes stored in a physically controlled location and backups should be created daily, weekly and monthly.

Creation of a log and log backup policy, specifying the period of time that logs must be available for immediate use (3 months minimum according to the standard), and the total period for keeping system logs (at least one year to comply with the standards).

Implementation of wireless analyzers to detect illegitimate access points should be considered and a formal process to perform this activity. Also keep a log providing constancy of when it is done.

Whenever a Penetration Test is performed there must be a requirement to implement corrections in a minimum timeframe. In case the correction involves long-term activities this should be planned, projected and start to be executed in the minor time possible. Especially for high or medium vulnerabilities.
10. Conclusions

PCI DSS Compliance is not a project, is a transformation process. Your first link on that process is the user (as in almost every system). They have to be actively participants on the security schema. They have to know policies. And you should encourage and motivate them to work under those policies as well as make the security team aware of any particular situation that they considered is violating PCI DSS mandates.

You can have all policies and procedures well designed, established and easily accessible but if there are not enforcement mechanisms it is possible that the vast majority will not follow those guides. It is not that you will turn your organization into a military base, but you must find a way to make users follow policies. Or even better keep them motivated to do it.

You should never use a technology if do not have the expertise on your personnel to manage and troubleshoot this technology. If despite of not having the required knowledge on the personnel you are still willing to use the technology, considering an outsourcing option. Make sure this outsourcing is a 100% available depending on how critical the implementation is, and the impact it can have on your business if it fails.

If you get the compliance you should work actively on maintain it. It is not enough to have deployed a well-designed network and security infrastructure that probably cost you a lot of money. You should constantly keep track on what is happening on that infrastructure and how are changes being handled and documented. This might be overwhelming if you infrastructure is big enough, but you should find the most adequate methods to do this. Either by using automated tools of by having personnel dedicated only to this purposes. This might be costly but it would be more costly losing
the compliance status or even worst having your business involved in a case of data breach.

Achieving PCI DSS can be very expensive depending on which point the company is. But it can be more expensive to face a security breach case for not being compliant. However this compliant status does not ensure that you have a secure infrastructure but at least means that you are following well-known security best practices for specific sensitive data as cardholder data is.

Being compliant gives you a wildcard in case you have a data breach case. Also the brands have economical incentives for that who are compliant, and even more attractive is the fact that the company can be listed as PCI compliant, which will be known by all the people that do business with the company. This is a good boost for in terms of reputation.

By October 2010 the PCI Security Standards Council will release a new version of the standard. New technological advances offer the possibility of enhancing security in any sector, but also posse a higher risk of having data compromised, this will be considered for the modifications that will be introduced to the standard. For example, chip and pin technologies, end-to-end encryption and tokenization(Westervelt, 2010) are part of the technologies that might be considered for the new version of the standard.

Cloud (Westervelt, 2010) computing and virtualization are relatively new fields that still have several security issues to be solved but are being widely implemented.
11. Glossary

PCI DSS: Payment Card Industry Data Security Standard.

Phishing: a social engineering method where the attacker makes a victim believe that is the legitimate person/business and ask for confidential information either electronically or by phone).

PAN: Principal Account Number
PIN: Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message
NAT: Network Addressing Translation
NTP: Network Time Protocol
12. Bibliography


Appendix A

PCI DSS Requirement: Regular Letters
Testing Procedures to ensure compliance with the requirement: Italic Letters

1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.

1.1.1 Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.

1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks.

1.1.2.a Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.

1.1.2.b Verify that the diagram is kept current.

1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.

1.1.3 Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. Verify that the current network diagram is consistent with the firewall configuration standards.

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.

1.1.5.a Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.

1.1.5.b Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.

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 Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.

1.2.1.a Verify that inbound and outbound traffic is limited to that which is necessary for
1.2.1.b Verify that all other inbound and outbound traffic is specifically denied, for example by using explicit “deny all” or an implicit deny after allow statement.

1.2.2 Secure and synchronize router configuration files.

1.2.2 Verify that router configuration files are secure and synchronized—for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations.

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.

1.2.3 Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

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

1.3 Examine firewall and router configurations, as detailed below, to determine that there is no direct access between the Internet and system components, including the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment.

1.3.1 Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.

1.3.1 Verify that a DMZ is implemented to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.

1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.

1.3.2 Verify that inbound Internet traffic is limited to IP addresses within the DMZ.

1.3.3 Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.

1.3.3 Verify there is no direct route inbound or outbound for traffic between the Internet and the cardholder data environment.

1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.

1.3.4 Verify that internal addresses cannot pass from the Internet into the DMZ.

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.
1.3.5 Verify that outbound traffic from the cardholder data environment to the Internet can only access IP addresses within the DMZ.

1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)

1.3.6 Verify that the firewall performs stateful inspection (dynamic packet filtering). [Only established connections should be allowed in, and only if they are associated with a previously established session (run a port scanner on all TCP ports with "syn reset" or "syn ack" bits set—a response means packets are allowed through even if they are not part of a previously established session).]

1.3.7 Place the database in an internal network zone, segregated from the DMZ.

1.3.7 Verify that the database is on an internal network zone, segregated from the DMZ.

1.3.8 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).

1.3.8 For the sample of firewall and router components, verify that NAT or other technology using RFC 1918 address space is used to restrict broadcast of IP addresses from the internal network to the Internet (IP masquerading).

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.

1.4.a Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization’s network, have personal firewall software installed and active.

1.4.b Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by mobile computer users.

6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.

6.1.a For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.

6.1.b Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.

6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.
**6.2.a** Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities.

**6.2.b** Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information and updating the system configuration standards reviewed in Requirement 2.2 as new vulnerability issues are found.

**6.3** Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle.

**6.3.a** Obtain and examine written software development processes to verify that the processes are based on industry standards, security is included throughout the life cycle, and software applications are developed in accordance with PCI DSS.

**6.3.b** From an examination of written software development processes, interviews of software developers, and examination of relevant data (network configuration documentation, production and test data, etc.

**6.3.1** Testing of all security patches, and system and software configuration changes before deployment.

**6.3.1.1 Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)

**6.3.1.2 Validation of proper error handling

**6.3.1.3 Validation of secure cryptographic storage

**6.3.1.4 Validation of secure communications

**6.3.1.5 Validation of proper role-based access control (RBAC)

**6.3.2** Separate development/test and production environments

**6.3.2 The development/test environments are separate from the production environment, with access control in place to enforce the separation.

**6.3.3** Separation of duties between development/test and production environments

**6.3.3 There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.

**6.3.4** Production data (live PANs) are not used for testing or development

**6.3.4 Production data (live PANs) are not used for testing and development, or are sanitized before use.

**6.3.5** Removal of test data and accounts before production systems become active

**6.3.5 Test data and accounts are removed before a production system becomes active.

**6.3.6** Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers
6.3.6 Custom application accounts, user IDs and/or passwords are removed before system goes into production or is released to customers.

6.3.7 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 cycle required by PCI DSS Requirement 6.3. 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.

6.3.7.a Obtain and review policies to confirm all custom application code changes for internal applications must be reviewed (either using manual or automated processes), as follows:

- Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices.
- Appropriate corrections are implemented prior to release.
- Code review results are reviewed and approved by management prior to release.

6.3.7.b Obtain and review policies to confirm that all custom application code changes for web applications must be reviewed (using either manual or automated processes) as follows:

- Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices.
- Code reviews ensure code is developed according to secure coding guidelines such as the Open Web Security Project Guide (see PCI DSS Requirement 6.5).
- Appropriate corrections are implemented prior to release.
- Code review results are reviewed and approved by management prior to release.

6.3.7.c Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.7a and 6.3.7b above.

6.4 Follow change control procedures for all changes to system components.

6.4.a Obtain and examine company change-control procedures related to implementing security patches and software modifications, and verify that the procedures require items 6.4.1 – 6.4.4 below.

6.4.b For a sample of system components and recent changes/security patches, trace those changes back to related change control documentation.

6.4.1 Documentation of impact

6.4.1 Verify that documentation of customer impact is included in the change control documentation for each sampled change.

6.4.2 Management sign-off by appropriate parties
6.4.2 Verify that management sign-off by appropriate parties is present for each sampled change.

6.4.3 Testing of operational functionality

6.4.3 Verify that operational functionality testing is performed for each sampled change.

6.4.4 Back-out procedures

6.4.4 Verify that back-out procedures are prepared for each sampled change

6.5 Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes, to include the following: Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.

6.5.a Obtain and review software development processes for any web-based applications. Verify that processes require training in secure coding techniques for developers, and are based on guidance such as the OWASP guide (http://www.owasp.org).

6.5.b Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques.

6.5.c Verify that processes are in place to ensure that web applications are not vulnerable to the following:

6.5.1 Cross-site scripting (XSS)

6.5.1 Cross-site scripting (XSS) (Validate all parameters before inclusion.)

6.5.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.

6.5.2 Injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries.)

6.5.3 Malicious file execution

6.5.3 Malicious file execution (Validate input to verify application does not accept filenames or files from users.)

6.5.4 Insecure direct object references

6.5.4 Insecure direct object references (Do not expose internal object references to users.)

6.5.5 Cross-site request forgery (CSRF)

6.5.5 Cross-site request forgery (CSRF) (Do not reply on authorization credentials and tokens automatically submitted by browsers.)

6.5.6 Information leakage and improper error handling
6.5.6 Information leakage and improper error handling. (Do not leak information via error messages or other means.)

6.5.7 Broken authentication and session management

6.5.7 Broken authentication and session management (Properly authenticate users and protect account credentials and session tokens.)

6.5.8 Insecure cryptographic storage

6.5.8 Insecure cryptographic storage (Prevent cryptographic flaws.)

6.5.9 Insecure communications

6.5.9 Insecure communications (Properly encrypt all authenticated and sensitive communications.)

6.5.10 Failure to restrict URL access

6.5.10 Failure to restrict URL access (Consistently enforce access control in presentation layer and business logic for all URLs.)

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

6.6 For public-facing web applications, ensure that either one of the following methods are in place as follows:

- Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows:
  - At least annually
  - After any changes
  - By an organization that specializes in application security
  - That all vulnerabilities are corrected
  - That the application is re-evaluated after the corrections

- Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks. Note: “An organization that specializes in application security” can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.

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

7.1 Obtain and examine written policy for data control, and verify that the policy.

7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities
7.1.1 Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.

7.1.2 Assignment of privileges is based on individual personnel's job classification and function

7.1.2 Confirm that privileges are assigned to individuals based on job classification and function (also called “role-based access control” or RBAC).

7.1.3 Requirement for an authorization form signed by management that specifies required privileges

7.1.3 Confirm that an authorization form is required for all access, that it must specify required privileges, and that it must be signed by management.

7.1.4 Implementation of an automated access control system

7.1.4 Confirm that access controls are implemented via an automated access control system.

7.2.1 Coverage of all system components

7.2.1 Confirm that access control systems are in place on all system components.

7.2.2 Assignment of privileges to individuals based on job classification and function

7.2.2 Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.

7.2.3 Default “deny-all” setting

7.2.3 Confirm that the access control systems has a 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.

10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.

10.1 Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.

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

10.2.1 All individual accesses to cardholder data

10.2.1 Verify all individual access to cardholder data is logged.

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

10.2.2 Verify actions taken by any individual with root or administrative privileges is logged.

10.2.3 Access to all audit trails

10.2.3 Verify access to all audit trails is logged.

10.2.4 Invalid logical access attempts
10.2.4 Verify invalid logical access attempts are logged.

10.2.5 Use of identification and authentication mechanisms

10.2.5 Verify use of identification and authentication mechanisms is logged.

10.2.6 Initialization of the audit logs

10.2.6 Verify initialization of audit logs is logged.

10.2.7 Creation and deletion of system-level objects

10.2.7 Verify creation and deletion of system level objects are logged.

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

10.3.1 User identification

10.3.1 Verify user identification is included in log entries.

10.3.2 Type of event

10.3.2 Verify type of event is included in log entries.

10.3.3 Date and time

10.3.3 Verify date and time stamp is included in log entries.

10.3.4 Success or failure indication

10.3.4 Verify success or failure indication is included in log entries.

10.3.5 Origination of event

10.3.5 Verify origination of event is included in log entries.

10.3.6 Identity or name of affected data, system component, or resource

10.3.6 Verify identity or name of affected data, system component, or resources is included in log entries.

10.4 Synchronize all critical system clocks and times.

10.4 Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components.

10.4.a Verify that a known, stable version of NTP (Network Time Protocol) or similar technology, kept current per PCI DSS Requirements 6.1 and 6.2, is used for time synchronization.

10.4.b Verify that internal servers are not all receiving time signals from external sources. (Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.)
10.4.c Verify that specific external hosts are designated from which the timeservers will accept NTP time updates (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). See www.ntp.org for more information.

10.5 Secure audit trails so they cannot be altered.

10.5.1 Limit viewing of audit trails to those with a job-related need.

10.5.1 Verify that only individuals who have a job-related need can view audit trail files.

10.5.2 Protect audit trail files from unauthorized modifications.

10.5.2 Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.

10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

10.5.3 Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.

10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.

10.5.4 Verify that logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media.

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).

10.5.5 Verify the use of file-integrity monitoring or change-detection software for logs by examining system settings and monitored files and results from monitoring activities.

10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.

10.6.a Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required.

10.6.b Through observation and interviews, verify that regular log reviews are performed for all system components.

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).

10.7.a Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year.
10.7.b Verify that audit logs are available for at least one year and processes are in place to restore at least the last three months’ logs for immediate analysis.

11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.

11.1.a Verify that a wireless analyzer is used at least quarterly, or that a wireless IDS/IPS is implemented and configured to identify all wireless devices.

11.1.b If a wireless IDS/IPS is implemented, verify the configuration will generate alerts to personnel.

11.1.c Verify the organization’s Incident Response Plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are 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). Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.

11.2.a Inspect output from the most recent four quarters of internal network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder data environment occurs. Verify that the scan process includes rescans until passing results are obtained. Note: External scans conducted after network changes, and internal scans, may be performed by the company’s qualified internal personnel or third parties.

11.2.b Verify that external scanning is occurring on a quarterly basis in accordance with the PCI Security Scanning Procedures, by inspecting output from the four most recent quarters of external vulnerability scans to verify that:

- Four quarterly scans occurred in the most recent 12-month period;
- The results of each scan satisfy the PCI Security Scanning Procedures (for example, no urgent, critical, or high vulnerabilities);
- The scans were completed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. 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.c Verify that internal and/or external scanning is performed after any significant change in the network, by inspecting scan results for the last year. Verify that the scan process includes rescans until passing results are obtained.

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 subnetwork added to the environment, or a web server added to the environment).

11.3.a Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment. Verify that noted vulnerabilities were corrected and testing repeated.
11.3.b Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).

11.3.1 Network-layer penetration tests

11.3.1 Verify that the penetration test includes network layer penetration tests. These tests should include components that support network functions as well as operating systems.

11.3.2 Application-layer penetration tests

11.3.2 Verify that the penetration test includes application-layer penetration tests. For web applications, the tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.

11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.

11.4.a Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic in the cardholder data environment is monitored.

11.4.b Confirm IDS and/or IPS are configured to alert personnel of suspected compromises.

11.4.c Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.

11.5 Deploy file-integrity monitoring software 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. Note: For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).

11.5 Verify the use of file-integrity monitoring products within the cardholder data environment by observing system settings and monitored files, as well as review in results from monitoring activities. Examples of files that should be monitored:

- System executables
- Application executables
- Configuration and parameter files
- Centrally stored, historical or archived, log and audit files
## Appendix B

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Application Type</th>
<th>Criticality</th>
<th>Comments</th>
<th>Card Related</th>
</tr>
</thead>
<tbody>
<tr>
<td>APP01</td>
<td>CMR</td>
<td>Extremely critical</td>
<td>Complete, integrated solution for CRM (Managing Customer Relations), optimization and business intelligence. It is a powerful Internet-based solution for companies that aim to increase sales, improve customer relationships, generate higher incomes and greater retention. Using personalized portals and roles-based, provides easy scalability and high performance.</td>
<td>X</td>
</tr>
<tr>
<td>APP02</td>
<td>GPN</td>
<td></td>
<td>Solution Business Process Management (NSG) which includes the management, monitoring, control and analysis procedures. We currently have automated processes and approvals for credit applications, application flow and administrative payments</td>
<td>X</td>
</tr>
<tr>
<td>APP03</td>
<td>IVR, CTI and Smart Dialer</td>
<td>Extremely critical</td>
<td>Contact Center Management</td>
<td>X</td>
</tr>
<tr>
<td>APP05</td>
<td></td>
<td>Extremely critical</td>
<td>Financial System that manages, processes, authorizing transactions with Prepaid Cards</td>
<td>X</td>
</tr>
<tr>
<td>APP06</td>
<td></td>
<td>Extremely critical</td>
<td>Solution packages that cover all business areas of financial sector in a comprehensive way</td>
<td>X</td>
</tr>
<tr>
<td>APP07</td>
<td>Mail, Calendar</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>APP08</td>
<td></td>
<td>Extremely critical</td>
<td>Wrapped management system and validation of information security Credit Card</td>
<td>X</td>
</tr>
<tr>
<td>APP09</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP10</td>
<td></td>
<td></td>
<td>Management System for Loyalty Programs</td>
<td>X</td>
</tr>
<tr>
<td>APP11</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>APP12</td>
<td></td>
<td></td>
<td>Corporate solution for electronic document management, such as document management,</td>
<td></td>
</tr>
<tr>
<td>APP13</td>
<td>Integrated Application System for the Administration Online Accounting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP14</td>
<td>Web publishing</td>
<td>Extremely critical</td>
<td>A system that allows customers to connect to the Bank for financial services without the need to visit any of our branches</td>
<td>X</td>
</tr>
<tr>
<td>APP15</td>
<td>Web publishing</td>
<td></td>
<td>Internet banking manager</td>
<td></td>
</tr>
<tr>
<td>APP16</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>APP17</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>(APP18</td>
<td>Management system that allows electronic transfer of Interbank</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP19</td>
<td>Corporate finance, banking, managed funds and risk management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP20</td>
<td>Management system and sending customizable by an end user or departmental</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP21</td>
<td>System for Human Resource Management, Payroll and Staff Training</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP22</td>
<td></td>
<td>Extremely critical</td>
<td>Is a fully comprehensive EFT switching system for banks and retailers to manage their self-service systems with a united delivery channel. Its layered and extensible architecture enables the future development of the bank's business. By setting up a united system interface for various service delivery channels, can be integrated seamlessly with various systems such as core banking systems, card management systems and third-party switching systems.</td>
<td>X</td>
</tr>
<tr>
<td>APP23</td>
<td></td>
<td></td>
<td>Manage automatically monitoring the compliance requirements related to the requirements of the departments of the Bank, established by laws, regulations, administrative provisions, state regulatory agencies</td>
<td></td>
</tr>
<tr>
<td>APP24</td>
<td>Web publishing</td>
<td></td>
<td>Internal communication to keep employees informed about news of interest</td>
<td></td>
</tr>
<tr>
<td>APP25</td>
<td>Extremely critical</td>
<td></td>
<td>Financial System that manages, processes, transactions Authorizes Credit Card Collection and Management</td>
<td>X</td>
</tr>
<tr>
<td>APP26</td>
<td>System for managing the operations of the Stock Exchange</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP27</td>
<td>Recording System Customer Surveys to measure satisfaction with products and services we have in the bank</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP28</td>
<td>Based system that serves as Business Development program that allows to monitor and assess the growth and performance of business executives, as well as showcase the achievements of the goals set for each</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP29</td>
<td>A system that aims to present the results of the efforts made by business executives, in addition to displaying performance statistics, trends, and it supports decision-making in the organization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP30</td>
<td>System monitoring and preventing fraud through electronic transactions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP31</td>
<td>System used for the operation of ATMs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP32</td>
<td>A system that lets you create, publish and collect the results of an online survey</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP33</td>
<td>Delivery system of accounts and credit cards by email</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP34</td>
<td>E-mail marketing software for managing your mailing list</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APP35</td>
<td>Backup</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Processes Card Information but does not stores it. Just processes the Backup data.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>