KADIR HAS UNIVERSITY
GRADUATE SCHOOL OF SCIENCE AND ENGINEERING

IMPLEMENTATION OF PCI-DSS V3.0 INFORMATION SECURITY STANDARDS

GRADUATE THESIS

ÖZGÜR TAŞDEMİR

2015

ÖZGÜR TAŞDEMİR

M.S. Thesis

2015

IMPLEMENTATION OF PCI-DSS V3.0 INFORMATION SECURITY STANDARDS

ÖZGÜR TAŞDEMİR

Submitted to the Graduate School of Science and Engineering

in partial fulfillment of the requirements for the degree of

Master of Science

in

Computer Engineering

KADIR HAS UNIVERSITY

2015

KADİR HAS UNIVERSITY GRADUATE SCHOOL
OF SCIENCE AND ENGINEERING

IMPLEMENTING PCI DSS V3.0 INFORMATION SECURITY STANDARDS

ÖZGÜR TAŞDEMİR

APPROVED BY:

Asst. Prof. Dr. Taner Arsan ____________

Assoc. Prof. Dr. Zeki Bozkuş ____________

Assoc. Prof. Dr. Osman Kaan Erol ____________

"I, Özgür Taşdemir, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis."

Özgür Taşdemir

____

Abstract

IMPLEMENTATION OF PCI DSS V3.0
INFORMATION SECURITY STANDARDS

Özgür Taşdemir

Master of Science in Computer Engineering
Advisor: Asst. Prof. Dr. Taner Arsan
2015

Way of doing business has changed with rapid spread of the internet and mobile devices, and payment systems must keep up with that. Most of the monetary transactions are done electronically and percentage of internet trade is growing rapidly. Information is being more important for companies and individuals when it comes to payment systems.

Fraudulent transaction rates have been increased significantly with the positioning of payment systems in public networks such as the internet and Wi-Fi which brings along security breaches. Information security requirements and raise of online payment card transactions together with payment card industry demands triggered the founding of PCI DSS information security standards.

This thesis describes PCI DSS, their requirements for compliancy and implementation of the standards to a company which have more than 2000 employee and stores, processes and transmits payment card information.

Keywords: PCI DSS, Information Security, PCI SSC, Payment Systems, Risk Management, Project Management

Özet

PCI DSS V3.0 BİLGİ GÜVENLİĞİ STANDARTLARININ
UYGULANMASI
Özgür Taşdemir
Bilgisayar Mühendisliği Yüksek Lisans
Danışman: Yrd. Doç. Dr. Taner Arsan
2015

İnternet ve mobil cihazların hızlı bir şekilde yaygınlaşması ile Dünya üzerinde iş yapış şekilleri değişmiş, ödeme sistemlerinin teknolojinin hızına ayak uydurması zorunlu hale gelmiştir. Günümüzde para hareketlerin büyük bir çoğunluğu artık elektronik ortamda gerçekleşmekte ve internet üzerinden yapılan alışverişler ile parasal işlemlerin oranı hızla artmaktadır. Ödeme sistemleri söz konusu olduğunda kişiler ve kurumlar için bilgi daha da değerli hale gelmektedir.

Özellikle internet ve kablosuz ağlar gibi kapalı devre olmayan ödeme sistemlerinin yaygınlaşması parasal işlemlerdeki sahtecilik oranlarını da hızlı bir şekilde arttırmış, güvenlik açıklarını ve endişeleri beraberinde getirmiştir. Bilgi güvenliği gereksinimleri ve çevrimiçi para hareketlerinin fazlalığı bankacılık ve ödeme sistemleri endüstrisinin ihtiyaçları ile birleşince PCI DSS güvenlik standartları ortaya çıkarmıştır.

Bu tezde çevrimiçi PCI DSS standartlarının içeriği ve uygunluk gereksinimleri ve çevrimiçi ödeme sistemlerinin kullanıldığı bir firmanın teknoloji altyapısının PCI DSS standartlarına uygun hale getirilmesi için yürütülen çalışmalar anlatılmıştır.

Anahtar Kelimeler: PCI DSS, Bilgi Güvenliği, PCI SSC, Ödeme Sistemleri, Risk Yönetimi, Proje Yönetimi

Acknowledgements

I want to thank my advisor Assistant Prof. Dr. Taner Arsan for his support and advice and my family for their patience.

Table of Contents

List of Tables

List of Figures

Chapter 1 Introduction

Information had become one of the most important assets for all commercial organizations. Protection of the information against unauthorized access and use is becoming more important.

With the emergence of smartphones, tablets and other mobile devices in our lives privacy and information security threats have been significantly increased. Since payment cards being a huge part of economy, identity theft meant monetary loss.

More than 867 million of personal information records have been breached in 4200 incidents that made public since 2005 [1]. One of the biggest retailers in the USA, The Home Depot confirmed in 2014 that their payment systems were hacked, and the attackers exposed more than 56 million payment card numbers as a result [2]. A similar breach happened in 2013, attackers obtained 40 million payment card numbers from Target Corporation. Stolen information included names, card numbers, expiration date & security code [3]. Also in 2013, more than 1400 serious data breach incidents has been made public, and this is just the tip of iceberg [4].

Results of these threats are often costly depending on importance of the information. shows the number of security incidents became public since 2005.

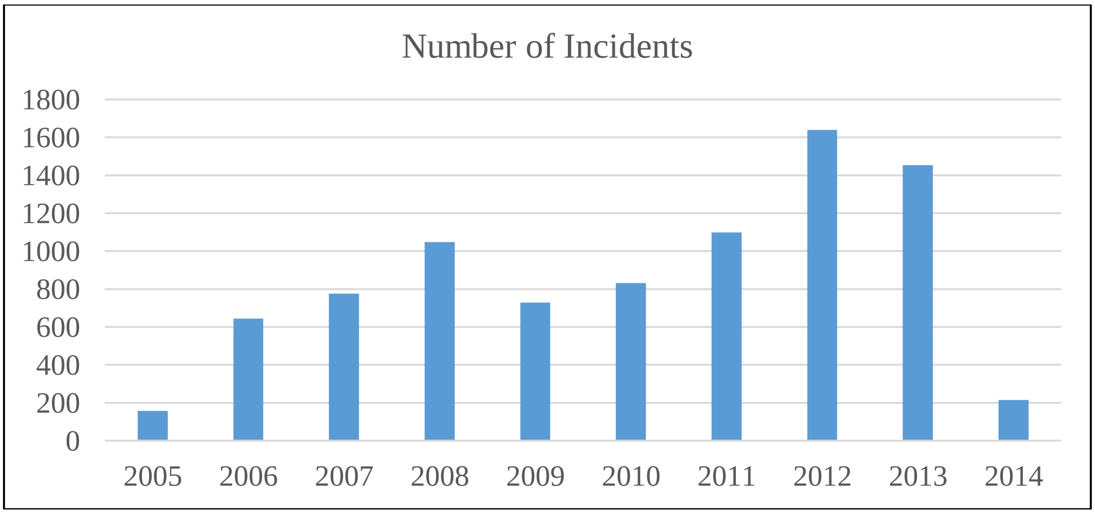

Figure 1.1 Security Incidents over Time

Definition of standards, creation of security procedures and technological research are essential to prevent payment card fraud and data theft. These works should involve merchants, hardware manufacturers, software developers and everyone who has a role in the payment card transactions.

Turkey first introduced with credit cards with Diners Club in 1968. Diners Club Cards given only to the rich as a prestige element, the holder required to pay the entire balance on the final payment date and it did not have a credit feature. Only a few merchants accepted Diners Club Cards, many retailers lacked the equipment needed to process transactions. Hence, usage of Diners Club Cards was very limited in Turkey.

With the increasing tourism, American Express Cards, Eurocard, Mastercard and Access Cards entered Turkish credit card market in 1970s. The credit card network continued to develop with the entrance of Visa, the establishment of bonus-point reward systems, the installation of the first POS (point of sale) terminal, and the founding of Bankalararası Kart Merkezi (BKM). shows the increase of payment card numbers in Turkey.

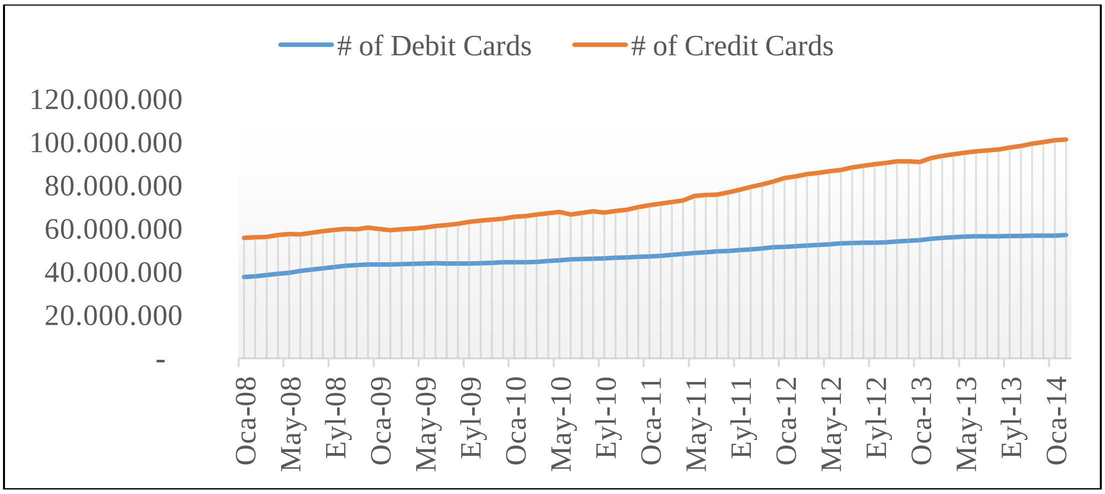

Figure 1.2 Number of Payment Cards in Turkey

In 2013, more than 2.7 billion credit card transactions processed with a total volume of 427 billion Turkish Liras. With 56 million credit cards, the number of credit cards almost tripled in last ten years in Turkey. [5] Figure 1.2 shows the number of credit card transactions in Turkey since 2008.

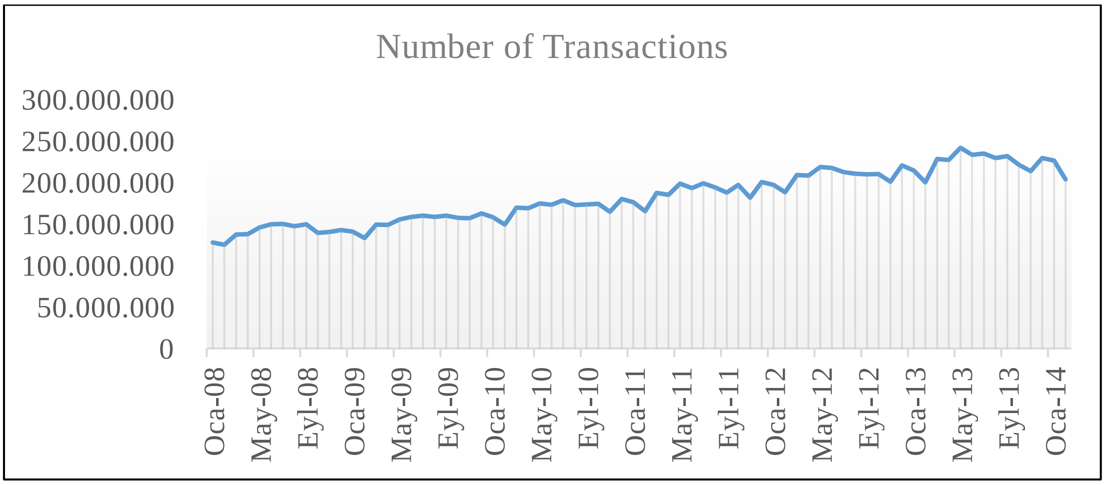

Figure 1.3 Number of Card Payment Transactions in Turkey

In 2013, more than 230 million e-commerce transactions made in Turkey representing 32% growth from 2012. [6] Economic growth, rising IT literacy, improving IT infrastructure and young population are key factors to e-commerce expansion in Turkey. Figure 1.3 shows number of online payment card transactions since 2009.

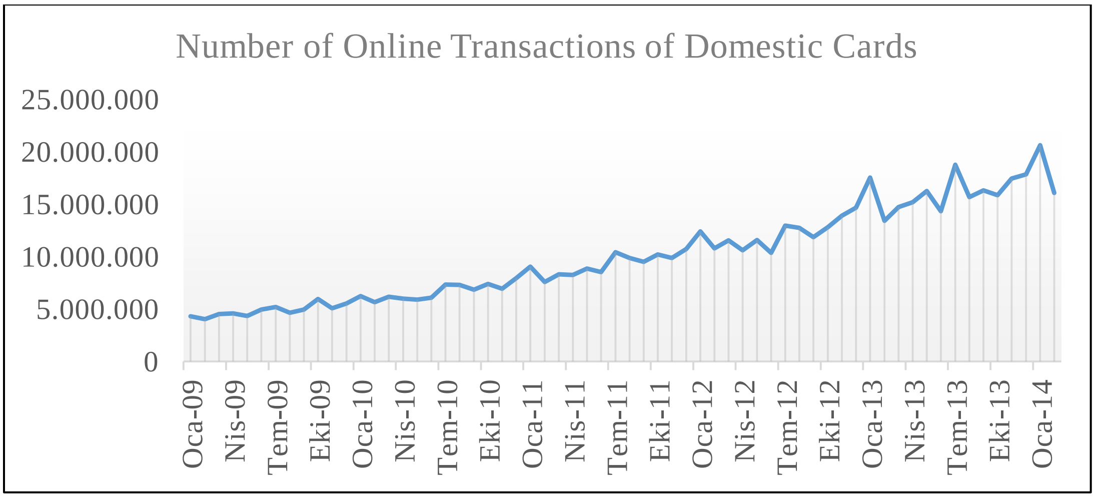

Figure 1.4 Online Usage of Domestic Credit Cards in Turkey

Inter Bank Card Center / Bankalararası Kart Merkezi (BKM): Founded in 1990 with cooperation of 13 public and private banks. Main purpose of BKM is building and operating platforms and systems which realize all kinds of payment or money transfer without carrying cash. BKM’s other purposes include improving procedures applied between banks performing debit and credit card operations, working towards standardization achievement, creating domestic rules for applications in Turkey, carrying out clearing and settlement between banks, building relationships with foreign institutions and commissions and representing its members when needed, executing the operations currently maintained by each bank in a single center which is more secure, faster and less costly to execute. [7]

Chapter 2 PCI Data Security Standards

2.1. Payment Card Industry Security Standards Council (PCI SSC)

All organizations that processing, transmitting or storing the payment card information should apply the PCI security standards. PCI SSC also guides the manufacturers and developers of devices used in payment card transactions. PCI SSC is responsible for managing these security standards.

Payment Card Industry (PCI) Security Standards Council (SSC), a global organization found by all major global payment brands (Visa, MasterCard, American Express, JCB International, Discover) in 2006, for developing, managing and educating the community its own security standards. These standards include the following:

- PCI DSS: PCI Data Security Standards
- PCI PTS: PCI PIN Transaction Security requirements
- PA-DSS: PCI Payment Application Data Security Standard

Each of these five payment brands have incorporated the PCI DSS as the requirements of their data security programs. Every founder also recognized the Approved Scanning Vendors (ASV), Payment Application QSAs (PA-QSA) and Qualified Security Assessors (QSA) recognized by the PCI SSC.

Strategic members and founding partners share equally in governance of the Council and they share responsibility in the organization’s works. Other players in the industry are also encouraged for joining the Council as members and participating organizations to review additions or modifications proposed to the standards. PCI compliance enforced by the PCI SSC member payment card brands (MasterCard, Visa, JCB, American Express, Discover).

PCI SSC offers standards and supporting documents to increase security of the payment card data. Supporting materials include specifications framework, tools, resources and measurements for organizations to reach the goal of safely handling payment card information, and the foundation of this framework is PCI Data Security Standard (PCI DSS). It also provides a framework for creating a strong information security process including detection, prevention and giving effective reaction to security incidents. PCI SSC is responsible for keeping the security standards up to date and includes industry best practices.

PCI DSS compliance enforcement and any non-compliance penalty determinations are handled by the payment brands individually.

This document contains information about the PCI DSS requirements for security consulting companies, vendors, merchants, and the PCI SSC's merchant support and certification services; all created to weaken the effects of the breaches and to prevent payment card fraud.

PCI SSC watches the cases of account data compromise covered all size of merchants and service providers. Security breaches followed by the compromise of cardholder information may have high consequences for affected organizations. Requirement of regulatory notifications, regulatory penalty and fees, litigations, reputation loss and loss of customers are only a few of them.

Compromise review analysis has indicated that the basic weaknesses addressed in PCI DSS were not revealed in the organizations when the most of the breaches occurred. That is why PCI DSS includes detailed requirements, to reduce the chance of compromise and its effects if it occurs. [8]

2.2. PCI Security Standards

PCI DSS is a global standard for information security that applicable to all institutions and systems that handle, transmit or store payment card information.

Figure 2.1 shows data on a payment card:

- (A)Issuer Identification Number (IIN) & Primary Account Number (PAN)
- (B)Expiration date
- (C)Cardholder name
- (D)Chip
- (E) CID (American Express)
- (F) Magnetic stripe (data on tracks 1&2)
- (G)CAV2/CID/CVC2/CVV2 (all other card brands)

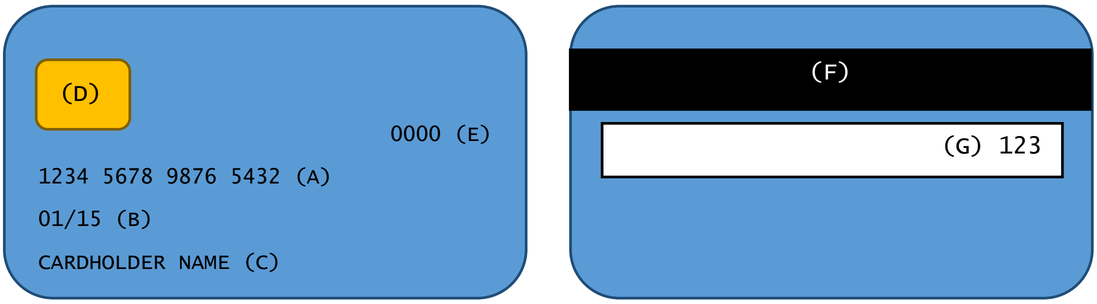

Figure 2.1 Types of Data on a Payment Card

This work includes efforts and methodology in order to make a company PCI DSS compliant which offers subscription based services to customers. PCI DSS consist of three steps:

Assessment: Payment card data identification, inventorying the merchant's information technology assets and methods used in payment card processes and analyzing them for weaknesses that could expose payment card data.

Remediation: Fixing the weaknesses and not storing sensitive data unless merchant needs it.

Reporting: Compiling remediation records if required, submitting compliance reports to the card brands and banks that merchant does business with.

Changes on PCI DSS and PA-DSS follow eight stages in a 3 year lifecycle. This introduces new versions of the standard gradually in order to prevent organizations from becoming noncompliant when the standards are changed. Council evaluate evolving technology and threats during this timeline and make mid-lifecycle changes or provide additional guidance if necessary. [9] shows the cycle of phases according to PCI SSC.

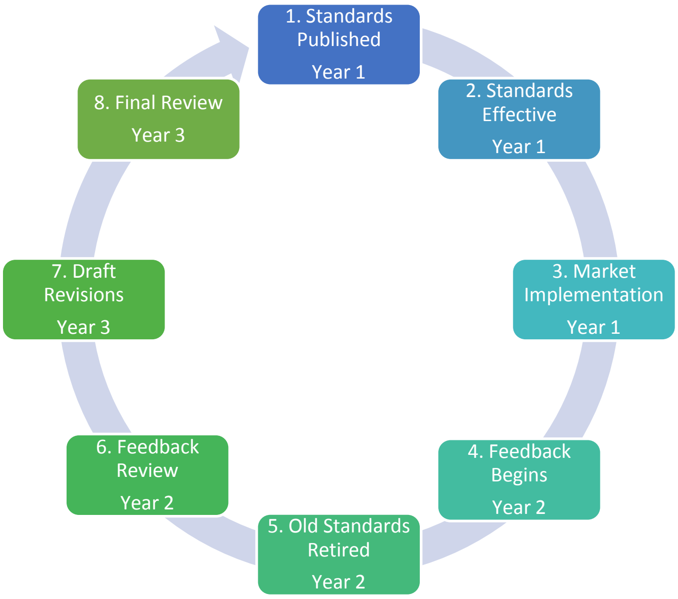

Figure 2.2 Change lifecycle of PCI DSS and PCI PA-DSS

2.2.1 PIN Transaction Security (PCI PTS)

The PCI SSC provides PCI PTS (PIN Transaction Security) requirements for device vendors and manufacturers. These requirements are for the increasing the security of

PIN (personal identification number) operations such as management, processing and transmission of during card transactions at ATMs or POS (point of sale) terminals.

Manufacturers follow these requirements when making their designs, manufacturing devices and transporting it to the organization that implements it. Only PCI SSC approved components or equipment should be used. Approved PIN transaction devices list can be found on PCI SSC website. [10]

2.2.2 Payment Application Data Security Standard (PCI PA-DSS)

PA-DSS consist of 14 requirements which is aimed at helping software vendors or integrators for developing secure payment applications. Card brands support merchants to use PCI SSC approved payment applications. Approved payment applications list can be found on PCI SSC website. [11]

Usage of PA-DSS compliant applications does not make an organization PCI DSS compliant since the environment that payment applications implemented must be PCI DSS compliant [12]. PA-DSS requirements can be found on PCI DSS website [12]

2.2.3 Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is a set of security requirements for all organizations that accepts or processes payment cards. This standard is developed for helping entities protect customer information and includes most of the information security best practices for protecting sensitive data. All merchants who transmit, store or process payment cards must be compliant to PCI DSS. Table shows the PCI DSS version history.

Table 2.1 History of PCI DSS

Date	Version
December ‘04	1.0
September ‘06	1.1
October ‘08	1.2
July ‘09	1.2.1
October ‘10	2.0
November ‘13	3.0
April ‘15	3.1

PCI DSS presents a requirements set for payment card data protection, and can be expanded by extra controls and practices to minimizing the risks or local and sector laws and regulations. Also, regulatory requirements or laws may require specific protection of data elements other than card number (cardholder name, etc.). PCI DSS does not repeal laws, regulations, or other legal requirements.

This study was performed according to the PCI DSS 3.0 standards. PCI SSC has recently released PCI DSS 3.1 including classification of all SSL versions as insecure after the finding of bug [13].

2.2.3.1 Compliance Validation

Organizations processing, transporting, or storing credit card information are categorized into specific merchant levels. Merchant level is a unique category with requirements for compliance validation. This is typically determined by the number of credit card transactions (not sum total of sales) that the organization processes a year. Acquiring Banks determine the organization merchant level. [14]

Table 2.2 Merchant levels and validation requirements

Merchant Level	**Number of Transactions**	**Annual On-Site Audit**	**Quarterly Network Scan**	**Annual SAQ**
1	More than 6.000.000[1]	Required	Required	Not required
2	More than 1.000.000	Not required[2]	Required	Required[3]
3	More than 20.000	Not required	Required	Required
4	Less than 20.000	Not required	Recommended	Required

Payment card brands have their own compliance levels for merchants, requirements and definitions. Even though the PCI SSC developed the standard, compliance actually mandated by the 5 payment card brands individually. Table 2.2 shows the PCI DSS merchant levels based on the number of payment card transactions in one year.

For larger organizations, PCI compliance evaluation requires a certified assessors those are known as QSA (Qualified Security Assessors) and ISA (Internal Security Assessors). An entity may use third-party service providers for store or process payment card information on their behalf, or to manage components like firewall, router, server or databases [15]. Table 2.3 shows the service provider PCI levels.

[1] Merchants that previously hacked or attacked and suffered data compromise considered as level 1

[2] For Turkey, Bankalararasi Kart Merkezi (BKM) requires that level 2 merchants must have annual on-site audits

[3] Since 30.06.2012, internal auditor must obtain the ISA certification for level 2 merchants

Table 2.3 Service provider levels and validation requirements

Service Provider Level	**Number of Transactions**	**Annual On-Site Audit**	**Quarterly Network Scan**	**Annual SAQ**
1	More than 300.000	Required	Required	Not required
2	Less than 300.000	Not required	Required	Required

Service providers are formally qualified by the PCI SSC to offer certified individuals (QSA) to assess compliance to the PCI DSS. Service providers fit to Level 1 required to have annual compliance validation with on-site assessment performed on all system components in the cardholder data environment [14].

2.2.3.2 Qualified Security Assessors (QSA) & Approved Scanning Vendors (ASV)

Council manages QSA and ASV programs to help maintain the PCI DSS compliance assessment. Qualified Security Assessors (QSA) are approved by the Council for PCI DSS compliance assessment. PCI SSC also validate Approved Scanning Vendors (ASV) for PCI DSS requirements compliance validation by performing Internet facing environment scans for service providers and merchants.

2.2.3.3 Self-Assessment Questionnaires (SAQ)

Self-Assessment Questionnaires (SAQ) is a PCI DSS validation tool for service providers and merchants that are not required to go through on-site data security assessments [8]. shows the tools available for PCI DSS compliance and self-assessment.

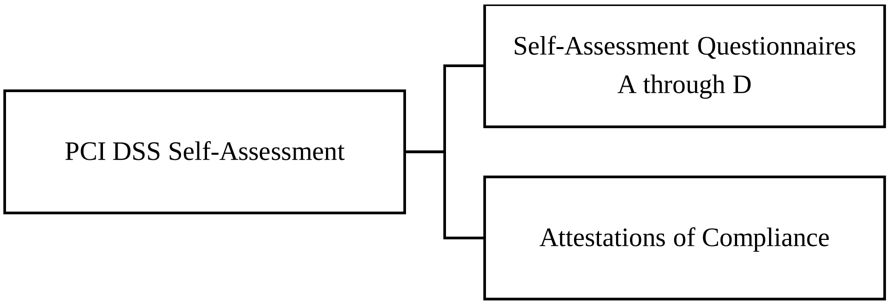
PCI DSS Self-Assessment
Self-Assessment Questionnaires A through D
Attestations of Compliance

Figure 2.3 PCI DSS Requirements and Procedures

Table 2.4 SAQ Types

SAQ	**Description**
A	Card-not-present merchants (mail-order or internet)
B	Imprint-only or standalone, dial-out merchants (no payment card information stored electronically)
C-VT	Merchants that use only virtual web-based terminals (no payment card information stored electronically)
C	Merchants that payment application connected to the Internet (no payment card information stored electronically)
D	Not included in above All service providers eligible to SAQ

SAQ assists organizations evaluating their own compliance, and it may be required to be shared with acquirer or payment brand. Table 2.4 shows the four versions of the questionnaires that meet various business scenarios [8].

2.3. PCI DSS Requirements Overview

“Requirements and Security Assessment Procedures” is the main document that includes twelve requirements and their test procedures as a security assessment tool. It is designed for PCI DSS compliance assessments as part of the validation process of an organization. Full list of requirements can be downloaded from PCI DSS web site [15].

Despite being easy to achieve at first sight, sizes of the companies may cause some problems for PCI-DSS implementations. Information technology based or higher sized companies should have been previously worked on or implemented some of the information security standards like ISO/IEC 27001 or COBIT. PCI-DSS requires comprehensive documentation and procedural workflow in many areas which is mostly provided by implementing other security standards. Also management's information security awareness is highly required for the corrections on possible findings because of the budget allocation.

2.3.1 Build and Maintain a Secure Network and Systems

2.3.1.1 Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

Since firewalls and routers are gates to the outside world securing extranet access mentioned in all information security standards.

PCI DSS requests firewall and router configurations provide the standards that fits most common security best practices. These include formalizing processes of testing, approving and changing router and firewall configurations.

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

Attackers often use default credentials and other default settings to get into the systems. Default security settings, usernames and passwords can be found by even novice users by a couple of search over the internet and are easily determined [15].

2.3.1.3 Requirement 3: Protect stored cardholder data

Company should not store payment card information unless it is a business requirement. If an organization decides to store PAN, it is important not to store it as clear text or a readable format. PAN should be unreadable in anywhere it is stored, and encryption keys should be protected against disclosure and misuse.

Table 2.5 Payment card data elements

	Description	**Can be stored?**	**Encryption / Display**
Data on Card	IIN & PAN	YES	Yes / Unreadable
	Firstname & Lastname	YES	No / Plain text
	Service Code	YES	No / Plain text
	Expiry Date	YES	No / Plain text
Sensitive Data	Full Track Data	NO	N/A
	CVV2/ CVC2/CAV2/CID	NO	N/A
	PIN/PIN Block	NO	N/A

PAN should be masked when displayed; only the first six and last four digits may be displayed. Only for business needs, authorized personnel can see the full PAN. Sensitive authentication data after authorization and magnetic stripe or chip data must never be stored even if they are encrypted [16]. Table shows which data on the payment card can be stored.

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

Transmissions of payment card information may get intercepted over public networks. Encryption can be used to prevent interceptor's ability to view this data. Strong cryptography and security protocols should be used and for making transmitted data unreadable by any unauthorized person. Also PANs should not be sent by insecure end user messaging applications such as e-mails and instant messaging.

2.3.2 Maintain a Vulnerability Management Program

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

Systems should be protected by anti-virus software against malicious software threats, anti-virus applications are kept updated, perform periodic scans and generate logs usable by audit purposes. These systems also must cannot be disabled or altered by users unless a specific management authorization for the case.

Systems not commonly affected by malicious software should be periodically evaluated to confirm whether such systems continue to not require anti-virus software.

2.3.2.2 Requirement 6: Develop and maintain secure systems and applications

A security vulnerability identification process using reputable outside sources should be established as well as risk ranking based on potential impact.

All critical systems must be updated with the most recent patches to minimize security risks. Less-critical systems should be also patched as soon as possible, based on the risks and vulnerability management program.

Both duty and system level separation of test/development environments from production environments required.

Secure coding practices for application development should always be followed. Changes should be made according to change control procedures [16].

2.3.3 Implement Strong Access Control Measures

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

Accessing to system components and cardholder data should be limited with only the individuals required by business. Such access should be enforced by comprehensive access control mechanisms.

2.3.3.2 Requirement 8: Identify and authenticate access to system components

All personnel that have access to critical data and systems should be assigned a unique identifier for authorization tracing. One of the below should be asked to the users to authenticate:

- Passwords / Passphrases (something you know)
- Token devices / Smart cards (something you have)
- Biometrics (something you are)

Generic or shared IDs and accounts should not be used and authentication mechanisms such as and certificates, smart cards and tokens must be assigned to individual accounts. Two-factor authentication should be implemented for all remote network access originates from outside the network. Strong authentication methods should be used and all passwords rendered unreadable during transmission, while stored using strong cryptography.

2.3.3.3 Requirement 9: Restrict physical access to cardholder data

Printed documents such as paper receipts should be secured as well. All media contain card data should be physically secured including back-ups. Physical access to data and systems should be appropriately restricted and monitored.

Access to data or systems must be authorized and based on individual job function. Physical access mechanisms like keys and cards must be returned or disabled when termination and all access terminated individual must be revoked immediately.

2.3.4 Regularly Monitor and Test Networks

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

All access to sensitive information and related systems must be monitored and logged. Logging mechanisms should track activities users for forensics and vulnerability management. Audit trails should be automated and secured against altering. Also all system clocks should be synchronized using time synchronization technologies in order to have meaningful audit trails.

Logs and security events should be reviewed to identify anomalies, critical logs should be reviewed at least daily. Audit trails should be retained for at least a year and last three months should be immediately available for analysis.

2.3.4.2 Requirement 11: Regularly test security systems and processes

As malicious individuals and researchers continuously developing vulnerabilities and new software being introduced to system, system components and processes should be tested frequently. Also any new software deployments or system configuration changes should be tested accordingly.

A process should be implemented for detecting and preventing unauthorized wireless access points. Internal (use of an ASV is not required) and external (should be performed by ASV) scans should be performed in at least every quarter, or after significant changes. These findings should be evaluated as defined in Requirement 6.

Also, an internal and external penetration test methodology that based on generally accepted approaches (NIST SP800-115, etc.) should be implemented. These penetration tests should cover entire cardholder data environment perimeter and performed at least once in a year.

Intrusion detection & prevention should be used and kept updated to detect intrusions into the network. Integrity of critical files such as application and system executables, configuration and parameter files, etc. should be monitored against unauthorized changes.

2.3.5 Maintain an Information Security Policy

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

A security policy should be at least annually reviewed and implemented for all personnel that have access to the cardholder data environment regardless of contract (full time or temporary employees, contractors, etc.). This policy should assign an information security management responsible and refer to other documents such as risk assessment process, acceptable use policies, approved product lists, remote access policies. Compliance status of third parties (service providers, etc.) should be monitored at least annually. An incident response plan should be implemented and tested at least every year. Specific personnel should be dedicated for responding breach alerts. These staff should be trained regularly.

Chapter 3 PCI-DSS Compliance Case Study

3.1. Company Profile

The company is a leading electronic security systems company in Turkey. With hundreds of thousands subscribers across Turkey, they have primarily focused installing and monitoring electronic alarms, as well as integrated electronic security and automation systems. They have operations across Turkey through dealer networks and its own regional direct sales offices. It employs around 2.000 staff.

Company's business model requires subscription based payment system, and most of the consumer products are sold with monthly payment option. In 2012, Company has grown almost %50 and number of credit card transactions have increased significantly.

With the fast growth, the company started to face several requirements that involve major changes in its internal processes and technology. Probably the most challenging requirement was from the authorized card-payment service provider in Turkey – Bankalararası Kart Merkezi (BKM). BKM has required that merchants whose number of payment card transactions is in level 2 according to PCI-DSS must have annual on-site audits.

From an information security perspective, the expected result of the oncoming on-site audit was not encouraging. Company started an initiative to make their IT infrastructure more secure while accomplishing the PCI DSS requirements, and they started to put required efforts to make corrections on possible findings for compliance process.

3.2. Company IT Infrastructure

3.2.1 Core Business

Electronic security systems are based on communication networks. Whether an alarm or communication signal has produced, it is carried by the most common analog and digital telecommunication infrastructures from customer to the data center. Figure 3.1 shows information about how alarm signals transmitted from subscribers.

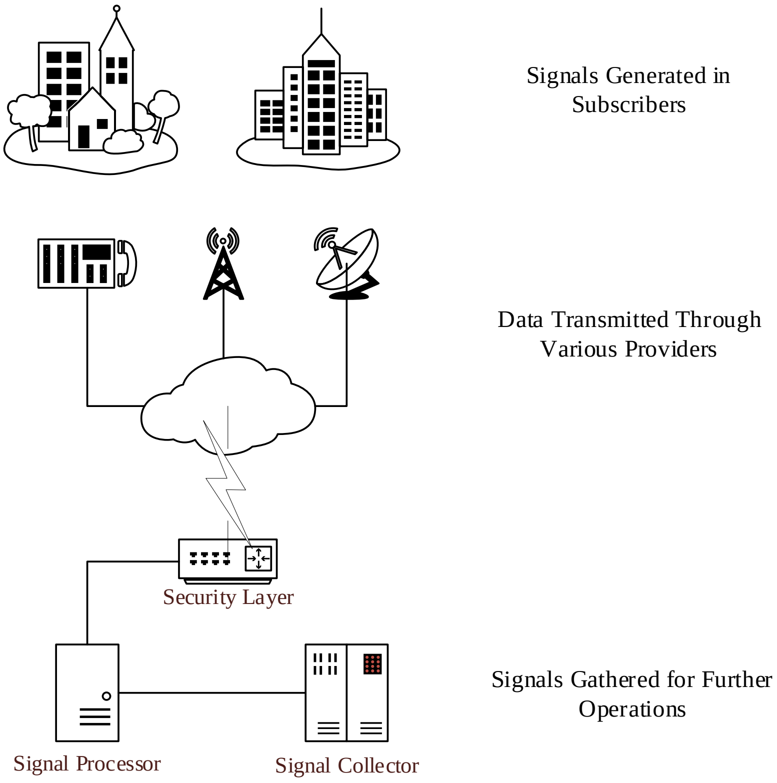
Signals Generated in Subscribers
Data Transmitted Through Various Providers
Security Layer
Signals Gathered for Further Operations
Signal Processor
Signal Collector

Figure 3.1 Alarm Signals

3.2.2 IT Operations

As the information security being one of the most important topics, security vulnerabilities are critical for all organizations. To protect company, detailed technical information about company’s infrastructure and security vulnerabilities not given in this work.

Since it is a technology-based service company, business functions and services offered to customers are highly related to IT processes. Company has their own teams for IT and related support functions:

- System analysis and integration unit
- ERP management unit
- Software development unit
- Server, network, storage administration and security unit
- End user support unit
- Project management unit

3.2.3 Information Security Awareness

In the a rapid growth period of the company some actions like creating procedures or standardizing daily operations disregarded due to high IT workload and also for to take rapid actions for management's requests. Also, for taking actions more quickly every team has ownership and team members almost have full control of their information assets like databases and resources like servers. Information security is a new concept for the Company.

ITIL is not implemented and service quality is often measured by the successful projects and general system uptime. There is a very limited Change Management application was very limited.

3.3. PCI DSS Compliance Project

Company was subject to quarterly vulnerability scan of its Internet facing environments and self-evaluating compliance process (SAQ) before their payment card transactions reach to level 2. Now, they are challenged with annual PCI DSS on-site audit requirement of Bankalararası Kart Merkezi (BKM).

Company Management decided to prioritize PCI DSS compliance since the most services that the company offers are based on subscription with card payment options. Being not compliant with the standard can cause fines and eventually loss of right to do business with card brands. They also decided to take project management approach which is comprehensive for compliance and repeatable for the yearly PCI DSS inspections.

3.3.1 Project Methodology

Waterfall process model decided as the most suitable model for phase transition in this project because:

- Requirements are well understood, no uncertainty in project
- Definition is stable, the risk of change is low

Each phase must be completed fully before the next phase can begin because of the characteristics of the Waterfall Model.   shows the project phases.

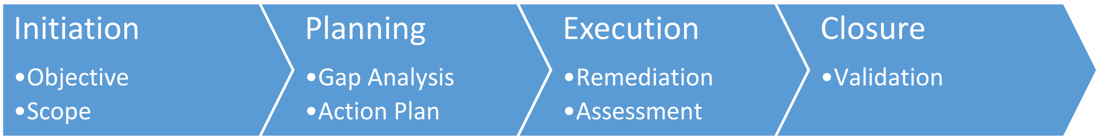

Figure 3.2 PCI DSS Compliance Project phases

3.4. Initiation

The project started with the objective definition, preliminary scope statement budget and timing.

3.4.1 Objective

The desired outcome is to reach compliance within the defined budget and timing. The main goal is not to lose payment card processing rights given by the banks, and not to lose corporate customers which can be caused by possible non-compliancy.

3.4.2 Project Scope

The project scope statement defines the project and identifies deliverables. Project scope statement allows everyone to begin with a target in mind.

Project scope is determined after the preliminary compliance analysis. Some of the requirements were achievable with minor changes in present configuration while others needed major additions in the system or changes in the business processes.

Segmentation of the cardholder data environment (CDE) discovered to be essential since the most items contain strict security measures which impossible to comply for whole network and infrastructure. An environment segmentation is planned as a part of the project. For being able to achieve segmented CDE major changes needed in the network infrastructure.

Project scope consists of PCI DSS compliancy as objective and below major work, allocated budget and workforce for reaching the objective.

- Showing management’s support by publishing information security policies
- Re-arranging permissions according to segregation of duties and least privileges needed
- Reducing the attack surface by segmenting networks and adding additional security layers
- Analyzing the usage of IT functions in business parts, gathering the input and outputs of the processes and creating an information asset database

- Documenting the processes and operations made in daily basis and creating procedures and instructions such as;
    - Documenting the current configurations and tracking configuration changes
    - Revising the processes and establishing approval mechanisms for critical operations

3.5. Planning

Planning stage consists of seeing the company’s position against compliance and building action plans based on the gap analysis findings. PCI DSS Prioritized Approach tool formed a basis for gap analysis and planning. Project has been planned for company reach PCI DSS compliance objective after in one year period. Action plan that built after gap analysis findings have mainly formed the project execution steps timing.

Table 3.1 Expected man/day efforts of teams

Phase	Milestone	Team Efforts (Man/Day)					
		Consul-tancy	IT Mana-gement	Network & System	DBA	ERP	Develop-ment
I	Initiation						
P	Gap Analysis	4	3	2	1	1	1
	Creating Action Plans	2	3	8	2	1	
E	Network Segmentation			30	1	1	1
	Building Inc Mgmt Sys		4	6	1	1	1
	Replacing Log Mgmt Sys		1	8	1	1	1
	Replacing Monitoring Sys		1	3			
	DB Security Imprvmnts			2	2	1	
	App Srvr Security Imprvmnts			1	1	1	1
	Changing the Business		5			2	
	Creating Procs & Policies		4	2	1		
	Assessment	4	3				
C	Validation						
O	Total	10	22	62	10	9	5

Project management is held by IT management and no additional PM teams involved. Table 3.1 shows expected man/day efforts for teams involved.

Phase	Milestone	Weeks																									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
I	Initiation	◊																									
P	Gap Analysis	🟦	🟦	🟦	🟦																						
	Creating Action Plans					🟦	🟦	🟦	🟦																		
E	Network Segmentation									🟦	🟦	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟪	🟪	🟪	🟪	🟩	🟩	🟩	🟩
	Building Incident Mgmt Sys											🟦	🟦	🟧	🟦	🟪	🟪	🟩	🟩	🟩	🟩	🟩	🟩	🟩	▨	▨	▨
	Replacing Log Mgmt Sys											🟦	🟦	🟧	🟦	🟪	🟪	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	▨
	Replacing Monitoring Sys											🟦	🟦	🟧	🟦	🟪	🟪	🟩	🟩	🟩	🟩	🟩	▨	▨	▨	▨	▨
	DB Srvr Security Imprvmnts									🟦	🟦	🟪	🟪	🟩	🟩	🟩	🟩										
	App Srvr Security Imprvmnts									🟦	🟪	🟪	🟩	🟩	🟩												
	Changing the Business									🟦	🟩	🟩	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	🟩	🟩		
	Creating Procs & Policies									🟩	▨	▨	🟩	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	🟩	🟩	🟩	▨
	Assessment																										
C	Validation																										

Figure 3.3 Timeline (Gantt chart) 1st part of the project

Figure 3.3 and Figure 3.4 shows timing of the planned works in the project. A checkpoint added in the middle of the timeline for evaluating the project status and objectives.

Phase	Milestone	Weeks																									
		27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
I	Initiation																										
P	Gap Analysis																										
	Creating Action Plans																										
E	Network Segmentation	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩										
	Building Incident Mgmt Sys	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	🟩	🟩								
	Replacing Log Mgmt Sys	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	🟩	🟩								
	Replacing Monitoring Sys	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	🟩	🟩								
	DB Srvr Security Imprvmnts																										
	App Srvr Security Imprvmnts																										
	Changing the Business																										
	Creating Procs & Policies	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	🟩	🟩						
	Assessment																						◊	🟩	🟩	🟩	
C	Validation																										◊

Figure 3.4 Timeline (Gantt chart) 2nd part of the project

Second half of the project mostly consists of waiting for the completion of network segmentation and adaptation of newly built systems into new network infrastructure.

3.5.1 Gap Analysis

Gap analysis needed to determine the Company’s position for PCI DSS compliancy and what actions needed to be taken in order to be PCI DSS compliant. Straight forward nature of the standard makes the gap analysis easier since PCI SSC defines the scope, controls and expected results for controls clearly in the standard itself.

PCI DSS provides the requirements, testing procedures and guidance to achieving compliance for that particular requirement.

3.5.2 Findings

Gap analysis revealed that the findings were mostly related with the common Information Security principles. Company’s information policies needed to be revised as they were lacking the documentation and need to create new policies and/or procedures as well as improving workflows for some of the business processes.

For business requirements some areas of the company IT environment are more relaxed in terms of security. Before the segmentation of cardholder data environment, these less secure areas possessed an issue for the compliance. According to gap analysis segmentation may instantly remove some items from the compliancy scope like external networks and systems and applications developed by in-house software development teams (considering that they do not process cardholder data). 3.2 shows the percentage of compliance before and after the cardholder data segmentation.

3.5.3 Action Plan

Results of the Gap Analysis have formed the basis of the action plan which has been created to fill gaps between actual and ideal situations. Business impact and budget allocation considerations have also shaped the action plan.

First of all, how the information is used and stored by the people and systems should be defined. Without the segregation of duties in such diverse IT organization, information security cannot be ensured. These two are most important elements to build the foundations of a secure and orderly IT infrastructure.

Technical requirements are relatively easy to apply since most of them consist of configuration changes or upgrades. The important thing is management support for modifying business processes, publishing updated security policies which are compliant and to allocate budget for foreseen costs. Action plan consists below work categories:

- Segmentation of cardholder data environment and network hardening
- Building a comprehensive monitoring and incident tracking system
- Securing cardholder data stored in systems
- Changing the business processes for not to use non-compliant cardholder data
- Updating IT processes for being compatible with the change management
- Updating information security policies and procedures

3.5.3.1 Prioritization

Action plan is affected by the business constraints such as 7/24 continuity as well as budget limits and project delivery time.

The prioritized approach helps the organization prioritize the risk while providing a measurable progress indicator. The Prioritized Approach provides milestones that is useful for protecting the merchants incrementally against the highest risks and escalating threats for PCI DSS compliance.

Council provides the “PCI DSS Prioritized Approach for PCI DSS” document and calculation tool which is downloadable from PCI DSS web site [17]. This document summarizes the goals for all six milestones and includes the mapping of them to all PCI DSS requirements and their sub-requirements. These milestones are intended to provide: [17]

- Establishes a usable roadmap for addressing and prioritizing risks
- Gains quick wins to organization by revealing high priority but relatively easy requirements
- Supports planning
- Gives measurable indicators for progress and make objectives clear
- Issues consistency between assessors

Company decided to follow PCI DSS Prioritized Approach as the action plan with small modifications such as accomplishing the compliancy on technical requirements on all stages except stage 6.

3.5.3.2 Procurements and Budget

Most organizations chose VLANs for CDE segmentation because they are easy to implement and may not require additional hardware purchase. In this case, VLANs are considered not enough to ensure CDE segmentation alone.

3.5.3.3 Scope Limiting and Network Segmentation

While the network segmentation of the cardholder data environment from the other parts of the network is not being a PCI DSS requirement, it is a strongly recommended method that generally reduces PCI DSS scope, cost, risk, and implementation and maintenance difficulties. Table shows comparison of compliance status before and after cardholder data environment segmentation (CDES). Percentage of compliance in some areas significantly increased with the segmentation of cardholder data environment.

Table 3.2 Comparison of compliance status

Milestone	**Goals**	**Compliance**	
		Before CDES	**After CDES**
1	“Remove sensitive authentication data and limit data retention”	70,0%	70,0%
2	“Protect systems and networks, and be prepared to respond to a system breach”	56,9%	76,9%
3	“Secure payment card applications”	31,4%	85,7%
4	“Monitor and control access to your systems”	45,9%	49,2%
5	“Protect stored cardholder data”	63,0%	63,0%
6	“Finalize remaining compliance efforts, and ensure all controls are in place“	74,2%	74,2%
Overall		**53,7%**	**68,6%**

3.5.3.4 Securing Stored Cardholder Data

The cardholder data environment is the sum of people, processes and technologies used to process payment card information or sensitive data used for authentication of IT infrastructure devices such as servers, network devices computing devices, and applications.

Cardholder data environment that appeared after the network segmentation planning, was consist of servers with obsolete operating systems, weak anti-virus protection and a couple of shortcomings about middleware and database security. The separation of role groups needed to be applied according to segregation of duties principle.

While the PCI DSS compliance seems to be straight-forward to accomplish, budget and business constraints made the compliance almost impossible with the current Cardholder Data Environment scope. As a result, cardholder data environment which is subject to PCI DSS controls needed to be reduced from all network to only the devices which store and process sensitive data.

3.6. Project Execution

3.6.1 Stage 1: Remove Sensitive Authentication Data and Limit Data Retention

Some business parts should change their way of handling payment card processes by modifying them for not storing unnecessary cardholder information. Table 2.5 shows which cardholder information allowed to be kept securely for PCI DSS.

Requirement 3 needs entities to keep cardholder data as less as possible, and securely delete those not needed anymore. Retention periods for cardholder data storage has been set.

Requirement 3.2: Agreements made with the issuer banks to be able to use payment cards without CVC or PIN for drawing. That was a crucial requirement since most of the transactions were subscription payments which needs to be drawn automatically with no user interaction.

Company also started an effort for searching cardholder information in every possible storage and deleting from non-compliant data sources or outside the secure cardholder data environment boundaries. A cardholder data discovery tool bought and all PCs, servers and storages inside the company network have been scanned cardholder information. The information found on PCs were mostly consisted of workers own payment card numbers. Some business-related cardholder information found in spreadsheets. This information has been deleted and business parts that noticed about the way of cardholder information handling have changed. Also the cardholder data printed on paper and stored in non-secure media destroyed and such use is prohibited. (Requirement 9.8.1, 9.8.2)

3.6.2 Stage 2: Protect systems and networks, and be prepared to respond to a system breach

Segmentation of cardholder data environment and network hardening is planned as a part of the requirements in Stage 2.

3.6.2.1 CDE Segmentation

Wherever cardholder data is used, it is in the PCI DSS scope and strict security features of the standard are must be applied. Usage and transfer of non-confidential information can be handled in a more relaxed environment in terms of security. Network segmentation can be implemented via various physical or logical ways such as:

- Policies and internal network firewalls
- Access control lists and routers
- Network access control technologies

Company planned to narrow the scope of compliance by separating cardholder data environment using VLANs. They started with updating present network diagrams and identifying required changes to achieve a segmented environment.

By putting the non-sensitive devices onto their own VLANs, they can be cut out of the audit by using the VLAN function of the switch. However, the switch itself still remains in scope. [18] Because of that, an additional VLAN for infrastructure management (switches, routers, etc.) must be defined.

VLAN controls work at Layer 2 can be easily bypassed by the techniques like ARP poisoning and tools like Ettercap [19]. Segmentation based only on Virtual LAN (VLAN) is not enough alone. Having cardholder data environment and wireless network (WLAN) on different VLANs does not take WLAN out of the scope and sufficiently segment from CDE. [20]

Layer 2 VLANs were mostly designed for efficient management of the large networks and should not be used as an instrument of security. An attacker can bounce between VLANs using several techniques if sufficient access controls are defined.

Unnecessary protocols or traffic should be blocked to cardholder data environment. This will reduce the attack risk by reducing the surface, make easier to monitor since CDE will generate less traffic.

Wireless technology can be used for cardholder data transmission such as point-of-sale transactions. PCI DSS has two approach to wireless networks related to the CDE:

In scope WLANs: These requirements are for organizations that transmit cardholder data wirelessly, or having wireless networks are part of the cardholder data environment. If wireless networks is connected to the cardholder data environment, the PCI DSS requirements apply and must be performed. [15] For this use case, wireless clients must be protected from each other.

Generally applicable WLANs: These requirements are essential for organizations to protect their networks against attacks from wireless access points and clients. They apply to all organizations using wireless networks even not in the cardholder data environment. Standard requires that WLANs not used in cardholder data environment must be isolated using a stateful inspection firewall, all traffic should be monitored and logged in accordance with requirement 10.

Virtual LAN (VLAN) based segmentation alone is not sufficient for the standard even if the adequate access controls between are in place. Firewalls must be installed between all WLANs and the cardholder data environment according to PCI DSS requirement 1.2.3. [15]

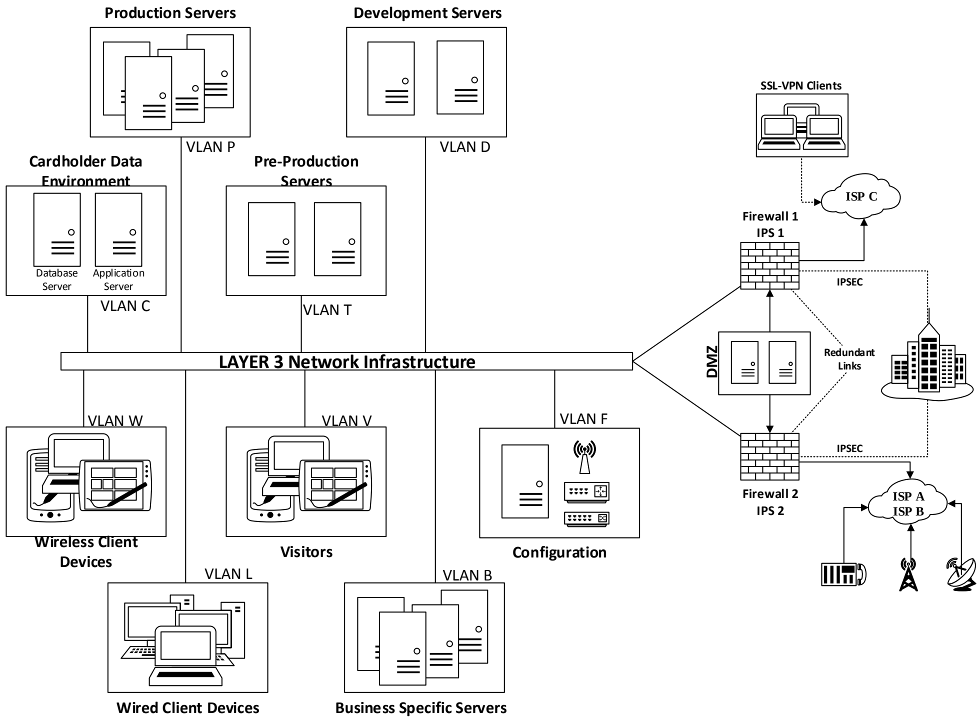

Figure 3.5 Network segmentation plan

shows planned network segmentation. The new network infrastructure requires replacement of new devices for incompatible or obsolete devices and addition of new systems for new functionality requirements. Procurement process should also be planned carefully since the hardware shipments normally take a couple of months.

For considering a system to be out of scope, a proper isolation from the cardholder data environment required. If an out of scope system gets even compromised it must not impact to cardholder data environment security. [15]

3.6.2.2 Ensuring the New Systems are PCI DSS Compliant

PCI DSS standards have requirements and controls for ensuring that new systems built securely and do not possess a risk for CDE by containing known vulnerabilities. Requirement 2 is completely focused on the breaches caused by easily compromised system elements coming from improper security configurations done at the installation of systems with default passwords, default security configurations or unnecessary services on network.

Requirement 2.1: All default configurations have been changed and less secure or not necessary system services (like older versions of SNMP) disabled. All network devices tested against having vendor supplied credentials or weak SNMP community strings. All devices which use SNMP are configured to have connection filters or access lists and using SNMP v3. Even the wireless access point and routers not being a part of the CDE, same security defaults have also applied to them.

Requirement 2.2: Configuration standards must be developed for systems which preventive measures applied against latest known security vulnerabilities. This includes building and updating master operating system images for servers, standard network device configurations and other system components. Systems built or installed recently also checked and moved to the same security level with these master image and standards. Also, all servers required to have only one primary function (Requirements 2.2.1, 2.2.2 and 2.2.5) and additional security features implemented for required insecure services and protocols such as SSH, S-FTP, TLS or IPSEC (Requirement 2.2.3). For being compliant with these requirements all unnecessary roles and services that require different security levels from co-existing on the same server has been removed in the servers in CDE scope.

Requirement 2.3: This requirement demands that administrative remote accesses to all systems should be encrypted by strong cryptography. It is easy for an eavesdropper to intercept sensitive data like logon details since clear-text protocols do not encrypt traffic. Physical and virtual servers, routers and switches in the scope secured with technologies like SSH and TLS.

Requirement 4.1: This requirement is not applicable since cardholder data is not transmitted over the public networks such as the internet or Wi-Fi.

Requirement 8.3: A two factor authentication method implemented into the remote connections. Remote users have started to be asked for OTP (one time password) which is sent on their mobile devices.

3.6.3 Stage 3: Secure payment card applications

Requirement 6 is focused on systems and applications developing and maintaining security. Since development team are not developing applications that store or process cardholder information, company concentrated on separation of platforms used in development and tests as well as development team role and duties.

Requirement 6.1: This requirement asks for establishing a process for security vulnerability identification using reputable sources. Main purpose of this requirement is to increase the company awareness for security threats. A process has been created for following security bulletins published by reputable companies and identifying and ranking the risks of vulnerabilities.

Requirement 6.2: All systems needed to be protected by installing the patches supplied by vendor and critical security patches installed in a month. This requirement was very challenging since the main database server that contains cardholder data was mission critical and not redundant. Installing the security patches on this server was requiring huge effort and business coordination. With the redundancy of this server, this server another servers added for high availability and all patching operations continued without interrupting the business. Also, hot backup web application servers were added for the same purpose and maintenance tasks started to run as scheduled.

Requirement 6.3: This requirement was not applicable since the no in-house application developed and such developments not planned in near future.

Requirement 6.4: The change control processes should be created, test and development environments needed to be completely isolated from production and development, test and production duties separated while the test environments do not contain sensitive data. An ITIL compliant change control process has been implemented and all changes have been challenged for documentation of possible impacts, approvals, completed tests with test patterns and roll-back procedures (Requirements 6.4.5.1, 6.4.5.2, 6.4.5.3, 6.4.5.4). shows the workflow that created for handling all changes including infrastructure and development teams.

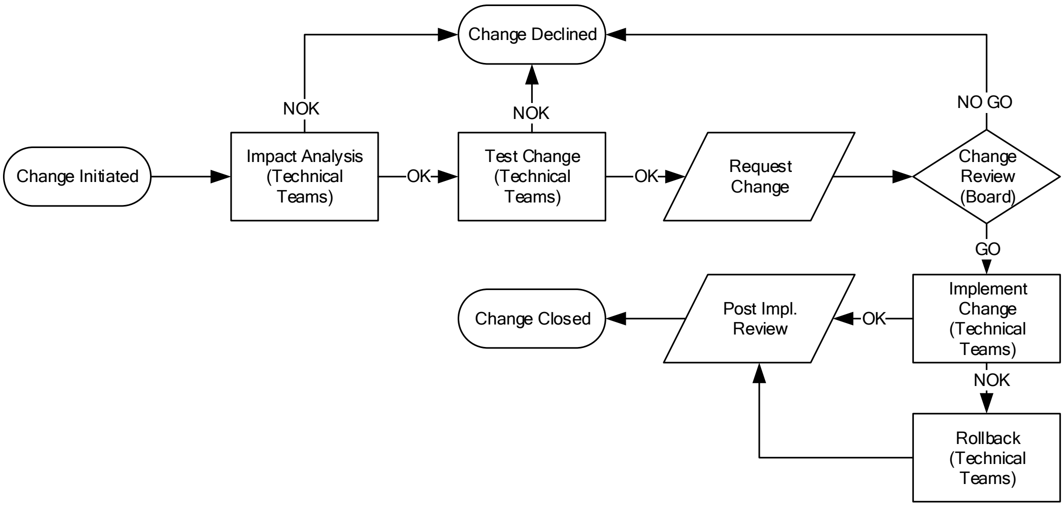
Change Declined
NOK
NOK
NO GO
Change Initiated
Impact Analysis (Technical Teams)
OK
Test Change (Technical Teams)
OK
Request Change
Change Review (Board)
GO
Change Closed
Post Impl. Review
OK
Implement Change (Technical Teams)
NOK
Rollback (Technical Teams)

Figure 3.6 Change control workflow

An isolated test environment needed to be created for being able to test changes and security configurations before they applied for the infrastructure teams in addition to development team test environment. A network an infrastructure test environment has been built for network team and development and test (UAT) environments have been created for application development team. (Requirement 6.4.1)

A separation of duties policy has been applied and personnel with developer or tester role are separated from those assigned to the production environment. (Requirement 6.4.2)

Old test and development environments destroyed due to configurations with insufficient security and being non-compliant to PCI DSS standard. Database tables in test and development servers that contain sensitive or cardholder information changed with non-live (sample) data. (Requirements 6.4.3, 6.4.4)

Requirements 6.5 and 6.6 were not applicable since there is no development done by in-house teams on the local or web facing servers in the cardholder data environment.

3.6.4 Stage 4: Monitor and control access to your systems

A secure and comprehensive logging system and important events monitoring for and audit trails planned in accordance compliance with PCI DSS. Old logging and monitoring systems were mostly failing to provide PCI DSS compliance.

Requirement 10 states that logging mechanisms should have ability to track user activities. [15] Logs needed in all environments to allow tracking, analysis and correlation when a security incident happens. Company decided to revise their central logging system which was not working properly and already obsolete. Replacement of the log system carefully planned to avoid under-logging. The new system should comply with all of the areas highlighted under Requirement 10.

Requirement 10.1: Access to system components and logon events needs to be logged by the operating system for the servers in scope. Operating system auditing levels have been made compliant with this requirement by completing some of the missing event sources.

Requirement 10.2: Critical events and cardholder data access must be logged. This has been done by implementing auditing feature of the database management system in use. The database tables that contain cardholder data started to be audited as well as users with administrative privileges. (Requirements 10.2.1, 10.2.2)

To ensure the integrity of audit trails, these logs are automatically imported into enterprise log and security event database at the time of generation, and access to these trails also logged. Both cardholder database server and this central log repository also monitored against change or changing or stopping of auditing services and sensors. All system level operations (creation or deletion of tables, stored procedures etc.), user operations (user creation or deletion, elevation of privileges etc.), invalid logical access attempts have been logged. (Requirements 10.2.3, 10.2.4, 10.2.5, 10.2.6) Table shows how audit policies configured for servers with Microsoft Windows operating system.

Table 3.3 PCI DSS compliant audit policies for Microsoft® Windows®

Category	**Events**	**PCI Requirement**	**Applicable to**
Account Logon Events	Success and Failure	10.2.4, 10.2.5	Member Servers
Account Management Events	Success and Failure	10.2.2	Member Servers
Directory Service Access Events[4]	Success and Failure	10.2.2	Domain Controller
Logon Events	Success and Failure	10.2.4	Member Servers
Object Accesses[5]	Success and Failure	10.2.1, 10.2.2, 10.2.3, 10.2.6, 10.2.7	Member Servers, File Server
Policy Change Events	Success and Failure	10.2.2	Member Servers
Privilege Use Events	Success and Failure	10.2.2, 10.2.5	Member Servers
Process Tracking[6]	Success and Failure	10.2.2	Member Servers
System Events	Success and Failure	10.2.2, 10.2.7	Member Server

Requirement 10.3: Audit records should contain at least user information, event type, timestamp, success or failure indication, origin and affected resource data which are already provided by the operating system by design.

Requirement 10.4: Usage of a time synchronization technology in servers in the scope is required. All servers in the network were previously synchronized by the designated time server which uses a trusted online time source. Change of the time settings disabled on the servers. (Requirements 10.4.1, 10.4.2, 10.4.3)

Requirement 10.5: Central log repository must be capable to prevent log alteration. With the log alteration the proofs of accesses and activities may be lost forever. Also, change in the audit criteria means that any malicious individual who has stolen the cardholder data can avoid being noticed. New central log repository chosen from one

[4] Directory Service Access Events available on a Domain Controller only

[5] Used in conjunction with Folder and File Auditing. Setting this policy also needs to specify which objects to audit. This policy configured for critical objects like log files, certificates, etc.

[6] Process Tracking not implemented to all servers as it generates too many events

of the many PCI DSS compliant Security Information and Event Management (SIEM) systems on the industry for being compliant with the PCI DSS Requirement 10.5.

Requirement 10.6: Logs must be controlled periodically against anomaly or suspicious activities. Central log repository is also used for that purpose, some types of audit logs are set to generate alarms at creation of their first instance while some log types are set to trigger alarms when the same log type repeated for a specific amount.

For proper and effective event monitoring required by PCI DSS compliance log management system should include not only gather all the relevant log data, but also analyze and remediate the results. Log monitoring system integrated with the incident management for being able to report and record any security incidents may happen to prevent overlook, and remediate them as soon as possible while keeping the track of what actions are taken to fix the issue.

Requirement 10.7: After the application installation, all data stored in previous log system are backed up with the old server binaries for future reference. They needed to keep be kept for at least a year. New logs also configured to be kept for at least a year.

Requirement 11.5: Change detection mechanisms needed to alert unauthorized modifications of defined objects. This has been accomplished by defining operating system audit policies for file system object access and anti-virus system integrity monitoring functionality.

3.6.5 Stage 5: Protect stored cardholder data

Requirement 3.3: PAN should be masked when displayed. Minor changes required in company ERP software to satisfy this requirement. ERP vendor has applied a patch which masks full credit card number and makes only first six and last four digits readable by the operator.

Requirement 3.4: Payment card number should be unreadable in all locations it is stored. This requirement includes database, application or database transaction logs, files and backup media. As the backups were already encrypted since the beginning, company has focused on database and logs. All log files that generated by application has been checked for all logging levels (including debug level) and parts containing clear text payment card information has been excluded from logs.

Database management system supports Transparent Data Encryption (TDE) with cell-level encryption. This encryption method has been used to secure cardholder data. Which data on a payment card can be stored is listed on Table with the information of how to store them.

Requirement 3.5: Applications needed to have at two set of encryption keys:

- Data-Encrypting Keys (DEK)
- Key-Encrypting Keys (KEK)

Requirement also states that both DEKs and KEKs should be encrypted and separately stored. Separation of the storage means that both keys cannot be present at the same configuration file, etc. Hardcoded encryption keys also removed from applications because it gives developers to ability to read payment card information stored encrypted in production database.

Requirement 3.6: A key management process should be implemented. A process created and documented with such including as generated keys should be strong according to “strong cryptography” section of the standard and keys should be retired and destroyed when a key is suspected to be compromised.

3.6.6 Stage 6: Finalize remaining compliance efforts, and ensure all controls are in place

Standard requires from entity to ensure below for all of the requirements. [16]

- Complete documentation of related procedures and policies
- Procedures actively used in operations
- Policy and procedures known by the parties

Requirement 12 also concentrated on creation, usage and review of the information security policies, usage policies and clearly defining information security responsibilities. A group of network and server team personnel from has been assigned to have information security management responsibilities at the beginning of the project. These responsibilities include creation and distribution of policy and procedures, monitoring and responding the security alerts. This team also established a security incident response team and created according procedures.

Requirement 12.2: Information security management team also took its part in the risk assessment process. Risk assessment has been done for all IT organization of the company instead of focusing only PCI DSS and incorporated the following core activities:

- Identification of critical information assets and threats for company and the to assets
- Identification of organizational and technological vulnerabilities that possesses risk to the organization
- Creating a risk strategies and mitigation plans

Table 3.4 Documentation requirements

Documentation	Status
Information security policy	Updated
Data classification policy	Created
Physical security policy	Updated
Access control policy	Updated
Network access and connection policy	Updated
Application and system development policy	Updated
Remote access policy	Updated
Operations security policy	Created
Media & equipment disposal policy	Created
Change control procedure	Updated
Encryption key management procedure	Created
Network device review procedure	Created
System and network device configuration standards	Created
Vulnerability review and testing procedure	Created
Security incident response plan	Created

Information security policy has updated to include change control process, principles, segregation of duties. Most of the policy and procedures modified in accordance to the standard. Table shows the list of required documentation by PCI DSS.

3.7. Proposed Changes for Increasing PCI DSS Compliancy

3.7.1 Preventing Cardholder Data Leakage

Data Leakage Prevention / Data Loss Prevention systems deny end users to send or carry sensitive information outside the company network. While no regulation explicitly requires the deployment of a DLP system, having a DLP in corporate network can significantly increase the PCI DSS compliancy. DLPs can also be used in compensating control role.

DLP is useful especially in the areas that fall into PCI DSS scope and cannot be changed because of technical or business reasons. DLP can restrict intended or unintended misuse of cardholder data by scanning traffic across systems and blocking the data that matches specific patterns.

In this case, business processes needed some users to have access to customer payment card data. DLP can scan the external communication such as e-mail and messaging platforms.

Requirement 4.1: DLP Systems help to keep sensitive data safe by recognizing and blocking the payment card data to be sent unencrypted over public networks.

Requirement 4.2: Protective DLP policies should be applied on the firewalls and messaging systems in order to prevent users sending unprotected PANs by applications classified as insecure.

Requirement 7.1: The sub requirements state that access to system components and cardholder data should be limited to only the individuals need to access cardholder data by their job descriptions. With the proper business processes, having a DLP supports compliancy to these requirements.

Requirement 11: DLP can also help all of these sub requirements by regularly generating reports on system and processes.

3.7.1.1 Detecting Payment Card Information

Payment card numbers are allocated in accordance with ISO/IEC 7812 [21]:

- First six digits on the payment card identify the card issuer (IIN or BIN): First digit as Major Industry Identifier (MII) and following 5 digits as Issuer Identification Number (IIN)

- Remaining numbers up to 12 digits represent the Primary Account Number (PAN)
- One check digit calculated using Luhn algorithm.

Typical payment card numbers are sequences of 13 to 16 numbers which start with each Issuer's corresponding numbers.

DLP systems scan credit card information in transmitted data. Since payment card issuers have different numbering patterns, different mechanisms needed in the detection process. Regular Expression (RegEx or RegExp) is the best option for matching payment card number patterns in the data transmitted over network.

Table 3.5 Credit card number patterns

Issuer Company	**Nb of digits**	**Starting with**	**Regular Expression**
Visa	13 16	4 4	?:(?4[0-9]{12}(?:[0-9]{3})?)
MasterCard	16	51 to 55	5[1-5][0-9]{14}
Discover	16	6011 or 65	6(?:011|5[0-9]{2})[0-9]{12}
American Express	15	34 or 37	?3[47][0-9]{13}
Diners Club	14	300 to 305 or 36 or 38	3(?:0[0-5]||[68][0-9])?[0-9]{11}
JCB	15 16	2131 or 1800 35	(?:2131|1800|35[0-9]{3})[0-9]{11}

Searching a pattern in a text block increases CPU traffic on the DLP system. For prevent adverse effects caused by high CPU utilization like slowness in response and transmission, preliminary rules can be added to the DLP system in order to detect and block outgoing payment card data.

A preliminary rule can detect numbers with 13 to 16 digits. A non-separated card number can be identified by this rule:

[0-9]{13,16}

Card numbers usually written as blocks separated by space or hyphen:

Visa / MasterCard Style: [0-9]{4}(-|)[0-9]{4}(-|)[0-9]{4}(-|)[0-9]{4}

American Express Style: [0-9]{4}(-|)[0-9]{6}(-|)[0-9]{5}

Checking more data like security codes and expiry dates can add extra precision.

Luhn algorithm is a checksum formula to validate ID, account or credit card numbers. [22] It is designed for preventing accidental errors using an integrity check, while providing no cryptographic security. It is now in the public domain and mostly used by credit card issuers and identification card providers as a simple number validation method.

Algorithm verifies account number against check digit, which is the last digit on the card. Verification consist of three steps:

- Double the value of every second digit and move left, starting from the last digit
- Sum all the digits
- If modulo 10 is equal to 0 the number is valid.

An example Luhn verification is shown in Table .

Table 3.6 Card number verification using Luhn algorithm

1. Numbers on Card	**4**	5	**0**	9	**4**	2	**6**	7	**5**	4	**3**	8	**7**	5	**4**	1
2. Double every second	**8**	5	**0**	9	**8**	2	**12**	7	**10**	4	**6**	8	**14**	5	**8**	1
3. Sum all digits	**8**	5	**0**	9	**8**	2	**3**	7	**1**	4	**6**	8	**5**	5	**8**	1
Result	Sum of all in step 3 is 80, card number is valid.															

Network traffic scanners or messaging servers can be modified to check transmitted data using Luhn algorithm in order to add confidence to the payment card number detection. Considering that payment card numbers are quite long (13 to 16 digits) best way to handle them will be converting into array.

Chapter 4 Conclusion

Considering the payment card fraud incidence is being almost 0.1% of all transactions; resultant financial loss is huge since the fraudulent transactions mostly have large values. PCI DSS requirements created to weaken the effects of the data breaches and prevent card data fraud.

PCI DSS compliance can cost great deal of money and a lot of effort, but benefits to the company is not just being able to continue payment card transactions but also having a more secure and organized infrastructure. Being compliant is not just replacing security related insecure or end-of-life hardware and software, it requires establishing a comprehensive information security management system which should increase information security awareness in the management level. Human factors always have high impact in Information Security.

Establishing the Information Security Management System and implementing the common information security practices have significantly improved the compliancy rate in this case:

- 10% in Milestone 1
- 5% in Milestone 2
- 6% in Milestone 3
- 25% in Milestone 4
- 27% in Milestone 5
- 10% in overall

Implementing the ITIL is also a big value for companies for PCI DSS compliance since it requires most of the processes defined in Incident Management, Configuration Management, Problem Management, and Change Management. In this case, ITIL was partly implemented with only Incident Management before the project and implementation of Change Management with other ITIL processes has reflected increase in the compliancy as below:

- 9% in Milestone 3
- 20% in Milestone 6
- 5% in overall

Although having a DLP solution is not mandatory, it supports compilation on milestones 3, 4, 7 and 11 for all cases, sometimes DLP can be only way to achieve in the cases that CDE cannot be segmented

This work showed that compliancy with other information security standards can significantly reduce the effort required by PCI DSS according to PCI DSS Prioritized Approach.

Yearly validation is another requirement, thus making the compliancy a continuous effort for the organization. Policies, procedures and forms needed to be established, up to date, easy to reach, staff using them should be well trained and most importantly they needed to be followed. Management support is needed in order to establish sufficient enforcement mechanisms. Planning can be easier for the organizations to achieve yearly validation since project management methodology brings a repeatable approach. Without proper planning and lack of management support, yearly validation efforts can be very expensive for the entities.

References

[1] Privacy Rights Clearinghouse, 2014, Chronology of Data Breaches, https://www.privacyrights.org/data-breach

[2] Home Depot, 2014, Home Depot, https://corporate.homedepot.com/MediaCenter/Documents/FAQs.pdf

[3] The Wall Street Journal, 2013, Target Faces Backlash After 20-Day Security Breach, http://www.wsj.com/news/articles/SB10001424052702304367204579267992268980478

[4] Open Security Foundation, 2014, DataLossDB, http://www.datalossdb.org/statistics

[5] BKM, 2014, BKM - Bankalararası Kart Merkezi, http://www.bkm.com.tr/istatistik/kredikarti_toplam_issuer_islemleri2.asp

[6] BKM, 2014, BKM - Bankalararası Kart Merkezi, http://www.bkm.com.tr/istatistik/sanal_pos_ile_yapilan_eticaret_islemleri.asp

[7] BKM, 2014, Tarihçe, http://www.bkm.com.tr/tarihce.bkm

[8] PCI SSC, 2010, PCI DSS, https://www.pcisecuritystandards.org/documents/pci_dss_saq_instr_guide_v2.0.pdf

[9] PCI SSC, 2010, PCI DSS, https://www.pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_dss_and_padss.pdf

[10] PCI SSC, 2014, Approved PIN Transaction Security (PTS) Devices, https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

[11] PCI SSC, 2014, Validated Payment Applications, https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

[12] PCI SSC, 2013, PCI PA-DSS, https://www.pcisecuritystandards.org/documents/PA-DSS_v3.pdf

[13] PCI SSC, 2015, PCI DSS, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

[14] Michael Hoehl, 2012, SANS Institute InfoSec Reading Room, http://www.sans.org/reading-room/whitepapers/compliance/project-management-approach-yearly-pci-compliance-assessment-34117

[15] PCI SSC, 2013, PCI DSS, https://www.pcisecuritystandards.org/documents/PCI-DSS_v3.pdf

[16] PCI SSC, 2014, PCI DSS, https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

[17] PCI SSC, 2011, The Prioritized Approach to Pursue PCI DSS Compliance, https://www.pcisecuritystandards.org/documents/Prioritized_Approach_V2.0.pdf

[18] Cisco Systems, 2012, Cisco, http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Compliance/Compliance_DIG/Compliance_DIG.pdf

[19] Alberto Ornagh and Marco Valleri, 2015, Ettercap Home Page, https://ettercap.github.io/ettercap/

[20] PCI SSC, 2009, PCI DSS. https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

[21] ISO/IEC, 2015, ISO/IEC, http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66011

[22] USPTO, 2015, United States Patent and Trademark Office, http://pdfpiw.uspto.gov/.piw?Docid=2950048&idkey=NONE&homeurl=http%3A%252F%252Fpatft.uspto.gov%252Fnetahtml%252FPTO%252Fpatimg.htm

[23] TCMB, *Türkiye'de Kredi Kartı Piyasası*. Ankara, 2011,

[24] Christopher Schoell, "Turkey's Credit Card Industry: Swipe Wisely," *Perspectives on Business and Economics*, 2011,

[25] TÜBİTAK BİLGEM, 2012, Ulusal Bilgi Güvenliği Kapısı, https://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/pci-kapsaminda-pin-ve-key-guvenligi.html

[26] PCI SSC, 2012, PCI DSS, https://www.pcisecuritystandards.org/documents/PCI_DSS_Risk_Assmt_Guidelines_v1.pdf

[27] Visa, 2014, http://usa.visa.com/merchants/protect-your-business/cisp/merchant-pci-dss-compliance.jsp#anchor_4

[28] MasterCard, 2014, http://www.mastercard.com/us/company/en/whatwedo/determine_merchant.html

[29] American Express, 2014, https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=US&tabbed=merchantLevel

[30] Discover, 2014, http://www.discovernetwork.com/merchants/data-security/identifying-organizations.html

[31] JCB, 2014, http://partner.jcbcard.com/security/jcbprogram/

[32] Wikipedia, 2014, http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

[33] BKM, 2014, BKM - Bankalararası Kart Merkezi, http://www.bkm.com.tr/istatistik/pos_atm_kart_sayisi.asp

[34] Techtarget, 2014, The history of the PCI DSS standard: A visual timeline, http://searchsecurity.techtarget.com/feature/The-history-of-the-PCI-DSS-standard-A-visual-timeline

[35] BKM, 2014, BKM - Bankalararası Kart Merkezi, http://www.bkm.com.tr/istatistik/kredikarti_toplam_issuer_islemleri.asp

[36] BKM, 2014, BKM - Bankalararası Kart Merkezi, http://www.bkm.com.tr/uyeisyerikilavuzu.pdf

[37] Ken Beames, 2012, McAfee, http://www.mcafee.com/de/resources/white-papers/foundstone/wp-pci-guidance-windows-logging.pdf

[38] Biznet, 2014, BiznetPCI, https://www.pcibiz.net/BiznetPCI/loginPCIdetay.seam;jsessionid=D5BDE76F238860CF2403B4C3C944A07A