LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Evaluating and designing a network and information security solution for a company in accordance with PCI DSS

Porter, Jere

2017 Leppävaara

Laurea University of Applied Sciences
Leppävaara

Evaluating and designing network and information security solution for company in accordance to PCI DSS

Jere Porter
Degree Programme in Business information technology
Bachelor's Thesis
December, 2017

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology
Bachelor's Thesis

Jere Porter

Evaluating and designing network and information security solution for company in accordance to PCI DSS

Year 2017 Pages 38

The payment industry is slowly shifting away from cash purchases to payment card solutions. Crimes related to stealing funds are often due to thieves obtaining card information. The objective of this thesis was to understand a target company's environment and define what actions are required to be taken to improve payment card security.

The standard Payment Card Industry Data Security Standard (PCI-DSS) used worldwide the theoretical base and methodology of the thesis project. PCI clearly defines the requirements that must be fulfilled to guarantee that no outside parties can gain access to customer card data. The standard also offers self-assessment-questionnaires for companies to understand what exactly is required from their business. Different business solutions have different requirements, and therefore must adapt accordingly.

During the thesis project, the company environment was assessed in accordance with PCI guidelines. With the scope established, it was possible to determine the points of improvement. The result of the thesis is an analysis and proposal to the target company to use for improving security. The report allows the company to understand how a single security breach can have enormous consequences on business continuity and what repercussions may follow. To avoid such an event, the company should fix the problems explained.

Keywords: PCI DSS, payment card, security, network

Table of contents

1 Introduction

This project is done in collaboration with a client company to address their network and information security issues using PCI DSS as the framework

The client company shall remain anonymous due to the request of the management to avoid publishing possibly sensitive information contained within the report. Any references of the client are omitted or generalized to prevent malicious outside parties from potentially tracing the client.

The company has suffered from undocumented network implementations and thus has occasionally encountered issues that could escalate and induce loss of revenue. This also poses security problems for the company and its clients, as the network configurations and physical security provide an opportunity to outside parties to spy the network and payment devices.

1.1 Project background

The company has a need of improving their network, both physically and logically. As new additions were implemented throughout the years, coherency within the environment was not applied and common practices were ignored. Thus, problems have occurred during everyday use within the company's campus, including latency, downtime, possibilities of loops and undocumented network data flow.

During the assessment, it became evident that the company is lacking in information security safeguards as well, mainly regarding payment devices. The project shifted towards addressing the issues using PCI DSS as the framework for designing the network and security policies. Especially with payment by cash has been in decline at a rate of 5-6 percent per year (Nordea 2016) and per an interview conducted with the Bank of Finland, cash payments may disappear completely as early as 2030 (Niemitalo, 2016). Card payment security becomes more relevant as payment with cards becomes more prominent and thus should be addressed.

In addition, as compliance with the PCI DSS is a requirement on pain of fine, the company's readiness for compliance will be evaluated. The company sells its products and services with the possibility of card payment, stores the receipts of card payments for accounting and bookkeeping purposes and therefore is compelled to comply.

1.2 Project objectives

The objectives of the project are:

A PCI compliant Security plan

- Physical security policies must be determined
- Documentation of the network and its continuous upkeep
- Design a PCI compliant network topology
- The network must be flexible for future implementations
- The network must be capable of sustaining business continuity

The project will not include the implementation of the solutions. The aim is to evaluate the client company's environment and assess what requirements must be met in order to achieve compliance. The project references the PCI DSS 2016 version 3.2 for this project.

2 PCI Theory Background

The Payment Card Industry Data Security Standard or PCI DSS is an international information security standard that defines security measures of cardholder data. It is used for this project as the theory background and framework reference.
It is important to realize that PCI DSS does not entirely enhance enterprise security as it was designed to improve payment security.

The standard was created and is governed by VISA, MasterCard American Express, Discover and JCB to standardize card payment security. Banks, merchants, service providers who wish to improve their security measures may undergo the PCI DSS assessment and become compliant. With compliancy, the company improves not only their environments security, but also the confidentiality of the customers' payment card information.

It is also important to note that compliance must be maintained even after the initial assessment. As described by Verizon, probably the most important factor in compliance is to design a plan to maintain security policies to continue remaining compliant, which in turn results in a secure environment.

Compliance is defined as fulfilling each requirement within the scope of the company in question. When compliant, the company has ensured that the card data of the customers is securely protected from unwanted individuals and greatly reduces the likelihood of human error. Per Verizon in their compliance report in 2015, over a 10-year period of investigations of

companies that fell victim to security breaches, none were fully PCI compliant at the time of the attack.

The PCI has defined 12 requirements that define the goals to achieve compliance and firm security practices. The requirements are as follows:

Goals	Requirements
Build and maintain a secure network and systems	1. Install and maintain a firewall configuration to protect card-holder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel

Table 1: PCI DSS requirements and goals (PCI DSS 2016b, 9)

The requirements are briefly described below (see Appendix 1 for more details).

2.1 Network and system security

As technology has evolved and become more dominant for storing data in business operations as opposed to paper documents, network connected computers are used to process and store payment information.

To prevent unwanted access to the systems, strong firewall configurations must be made. Reducing the access into the network also reduces the scope of the PCI assessment. The requirements are summarized as follows:

- Establish and implement a firewall configurations standard that guides how to test the environment, document the network, document the business justifications and document the data flow
- Restrict all unwanted traffic from and to other networks
- Prohibit access to the internet from the card data environment
- Install firewall software to all devices that access the cardholder data environment
- Firewall security policies are to be documented and used (PCI DSS 2016b, 12)

Outside parties may attempt to gain access to the systems by exploiting vendor-supplied default settings such as passwords and software versions. PCI has recognized that many merchants do not change the settings that become liabilities. PCI has established the following requirements:

- Vendor-supplied defaults must be changed before the system is installed into the network
- Configurations standard must be established that addresses known vulnerabilities to all systems. Update as necessary
- All non-console access must be strongly encrypted
- Maintain an inventory of systems
- Ensure that the security policies are documented and known to all relevant parties (PCI DSS 2016b, 13)

2.2 Cardholder data

Cardholder data is payment card information stored, processed, transmitted or printed in any from. Parties accepting card data are expected to ensure that non-authorized access is prevented, regardless whether the data is physical or electronic. Card data should not be stored unless there is a business need. PCI has established the following requirements:

- Card data should only be collected and stored as needed. Unnecessary data should be deleted
- Authentication data should not be stored after authorization
- PAN should be masked when displayed
- PAN should be unreadable when stored
- Document and implement the safeguards for encryption keys
- Make sure all security policies and operational procedure are documented, in use and known to relevant parties. (PCI DSS 2016b, 14-15)

If the data transmission is not encrypted, outside parties may be able to intercept them through open public networks. PCI requires the following:

- Strong cryptography measures should be implemented

- Unprotected PANs should never be sent through emails, SMS etc.
- Related security policies are documented and in use (PCI DSS 2016b, 16)

2.3 Vulnerability management program

Malicious software target system vulnerabilities by entering the network through regular business activities, such as email. Anti-virus software must be installed and kept updated with the following measures:

- Install Anti-virus software on devices commonly affected by malicious software, such as PC's and servers.
- Regularly update the software to tackle against most recent malware
- Ensure that the software keeps running and cannot be disabled by regular users
- Make sure all security policies and operational procedure are documented, in use and known to relevant parties. (PCI DSS 2016b, 16-17)

Systems and devices have vulnerabilities that can be exploited by outside parties. Most of these can be fixed with security patches. It is important to identify which systems require regular updating and generate a process to follow.

- Create a process to identify vulnerabilities
- Ensure that known vulnerabilities are fixed with security patches.
- When developing internal and external software, follow PCI guidelines
- Ensure that new or changed systems cover the PCI DSS requirements
- Make sure all security policies and operational procedure are documented, in use and known to relevant parties. (PCI DSS 2016b, 17-18)

2.4 Access control

Restrict access to cardholder data to ensure that the data is only accessed by people who require it by job responsibility. When granting access, only the minimum amount should be given.

- Limit data to those who require it
- By default, the access should not be available unless permitted
- Make sure all security policies and operational procedure are documented, in use and known to relevant parties. (PCI DSS 2016b, 18-19)

Access to the systems should be secured so that only personnel with access may enter.

- User accounts and passwords must be unique to each use. Avoid using groupwide authentication

- Implement multifactor authentication
- Access to cardholder data must be restricted only to those who require access.
- Policies must be documented (PCI DSS 2016b, 19-20)

The devices that store and handle payment card data must be also physically secured from unwanted access. It is important to allow access only to those who require it and access lists and policies should be maintained.

- Visitors should not be allowed to access unwanted areas.
- Personnel should be identifiable with e.g. ID badges
- Payment devices should be secured so that direct physical interaction, tampering or otherwise can be avoided.
- The devices should also be regularly inspected for possible tampering. (PCI DSS 2016b, 20-21)

2.5 Network monitoring and testing

Whenever something is done in the network devices and systems, an audit trail must remain in order to prevent personnel from exploiting their privilege and possibly stealing information or causing vulnerabilities.

- An audit trail must remain for each user
- The audit trail must log access, action, errors, changes to privileges or authentication methods, deletions, stopping or pausing audit logs.
- The logs must contain details of the user, date and time, type of event, success or failure indication and system in use
- Time should be synchronized between systems
- Audit trails should be secure so that they cannot be altered.
- Logs should be reviewed to detect abnormal activity (PCI DSS 2016b, 21-22)

Network and system devices should be tested regularly to ensure that new software does not contain possible vulnerabilities.

- Wireless access points should be tested for vulnerabilities
- Internal and external network vulnerability scans
- Penetration testing
- Network intrusion detection (PCI DSS 2016b, 23-24)

2.6 Policy management

Security policies should be implemented to ensure that the entire organization follows the company's security guidelines.

- Establish security policy and maintain it
- Implement risk assessment process
- Define how critical technologies should be used by the personnel
- Implement a security awareness program
- Screen potential personnel prior to hire
- Implement an incident response plan. (PCI DSS 2016b, 24-25)

2.7 Consequences of non-compliance

The consequences of non-compliance vary between the card brands and banks. In the event that a merchant is found guilty of non-compliance, the acquiring bank will be held responsible the by card companies and can be fined from $5000 to $100 000 per month. The bank is likely to pass the fines to the non-compliant merchant and possibly terminate the service or increase transaction fees (PCI DSS 2017).

Nordea's Terms and conditions for merchants reports the following: "The Merchant must at all times comply with the common standard PCI … should the Merchant fail to comply with the PCI DSS requirements and the cardholder data goes astray, the Merchant will be financially liable for the investigations, forensic costs and any losses that arise as a result of misused cards. In addition, the Bank may charge the Merchant for the fines that the card companies impose on the Bank as a result of the Merchant's incompliance with the PCI DSS requirements." (Nordea 2013)

As seen above the bank will hold the responsible merchant accountable should the data become compromised. Smaller businesses may go out of business due to unrecoverable financial problems caused by the fines, legal costs, diminished sales and service terminations.

3 PCI Methodology

The methods used in the project are as determined by the PCI guidelines and security standards. The PCI compliance process consists of three distinct phases:

- Assess
- Repair
- Report

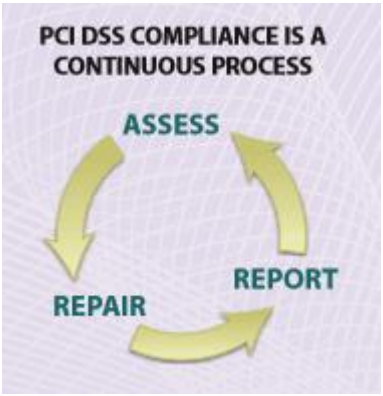


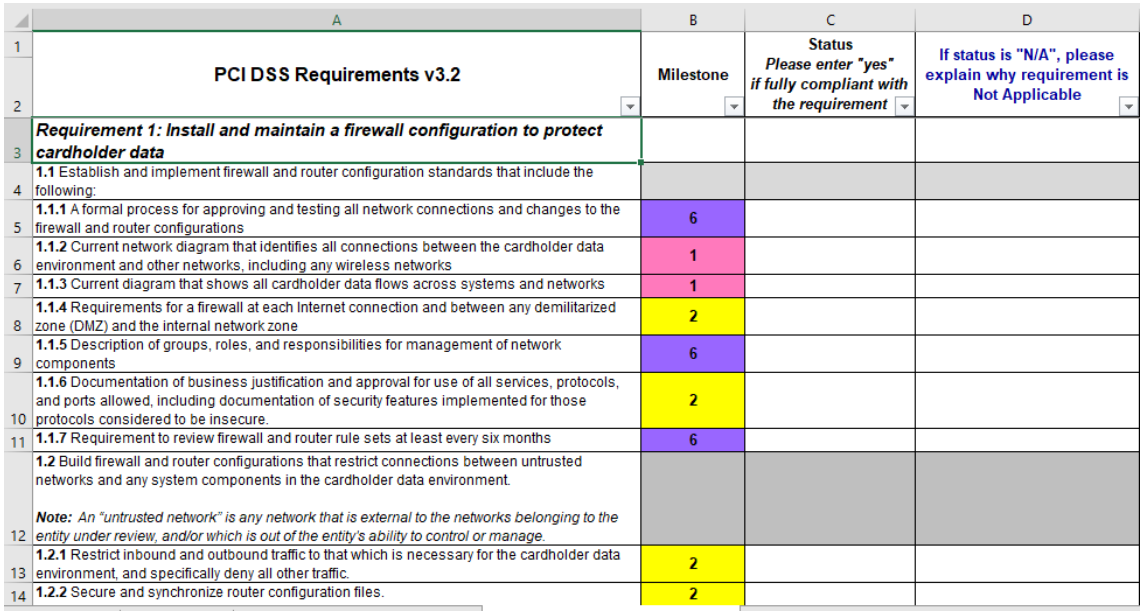
Figure 1: The PCI DSS compliance process (PCI DSS 2016b, 5)

The project focuses on assessing the environment and its vulnerabilities and establishing the recommended actions for the repair phase. The report phase is not included.

3.1 Assess

Companies fill out a Self-Assessment Questionnaire (SAQ) to compare the current environment to the PCI requirements. There are several variations in the scope and requirements, depending on the current implementation and nature of the company in question. In some cases, the SAQ can be used as the validation tool for compliance and thus do not require to submit a PCI DSS Report on Compliance. This differs between acquirers and card brands (PCI DSS 2016b, 3)

PCI offers a set of requirements that must be fulfilled to achieve compliance. The prioritized approach tool lists the requirements in an excel sheet whereupon the company can track their applicability and progress. The requirements are divided into milestones to categorize the goals.



	A	B	C	D
1				
2	**PCI DSS Requirements v3.2**	**Milestone**	**Status** *Please enter "yes" if fully compliant with the requirement*	**If status is "N/A", please explain why requirement is Not Applicable**
3	***Requirement 1: Install and maintain a firewall configuration to protect cardholder data***			
4	**1.1** Establish and implement firewall and router configuration standards that include the following:			
5	**1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations	6		
6	**1.1.2** Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1		
7	**1.1.3** Current diagram that shows all cardholder data flows across systems and networks	1		
8	**1.1.4** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	2		
9	**1.1.5** Description of groups, roles, and responsibilities for management of network components	6		
10	**1.1.6** Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	2		
11	**1.1.7** Requirement to review firewall and router rule sets at least every six months	6		
12	**1.2** Build firewall and router configurations that restrict 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.*			
13	**1.2.1** Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	2		
14	**1.2.2** Secure and synchronize router configuration files.	2		

Figure 2: A section of the official Prioritized approach excel sheet. (PCI DSS 2016e)

Milestone	Goals
1	Remove sensitive authentication data and limit data retention
2	Protect systems and networks and be prepared to respond to a system breach
3	Secure payment card applications
4	Monitor and control access to your systems
5	Protect stored cardholder data
6	Finalize remaining compliance efforts and ensure that all controls are in place

Table 2: Prioritized approach milestones and goals (PCI DSS 2016e)

3.2 Repair

The assessment of the environment will reveal the requirements that are not fully compliant. Each requirement listed in the SAQ must be fulfilled in a satisfactory manner. The requirements specify exactly how to achieve compliance, but the methods may differ on a company to company basis, depending on how the environment is built. During the repair phase, the company will be establishing processes on how to maintain compliance in the future as well.

3.3 Report

Once everything is in order in accordance to the SAQ, the assessment is reported to the acquirer or service providers with the filled out SAQ, or a official PCI DSS Report on Compliance, depending on the acquirer or card brand.

The cycle would continue from this point onwards, with the company reassessing the environment and ensuring that the requirements are still met. As mentioned before, this is an ongoing process to ensure that the company remains compliant.

4 PCI scope and assessment

As the company is scoping the environment, it should be assumed that the entire environment is within the scope until necessary controls are in place.

4.1 Choosing an SAQ

Before assessment, a suitable SAQ needs to be identified to determine the requirements to fulfill. For this case, the objective is to reduce the scope as much as possible in order to use the least work demanding SAQ. In this project, two SAQ's will be considered.

4.2 SAQ P2PE HW

To reduce the risk of exposing the consumers card data to malicious outside parties, encrypting the data flow is a required. The PCI council has established a standard called P2PE (Point to point encryption). Using P2PE certified products allows the payment data to flow through the network in a format that is useless to outside parties and attacks. P2PE certified products encrypt the data flow from the point of payment to the system that approves the payment. The keys used for the encryption are not disclosed to any parties, not even the merchant who has purchased the service. Compared to E2EE (end-to-end encryption), no other systems are present between the two points, thus decreasing the likelihood of outside parties gaining access to the data.

Using a validated P2PE solution also reduces the scope of the PCI assessment, due to isolating the data flow from the rest of the network, thus resulting in the number of requirements to address drop from twelve to four. The sub-requirements drop from over 250 to 26. (PCI DSS 2014)

To use SAQ P2PE, the following requirements must be met:

- The company does not store, process or transmit any cardholder data on any system or electronic media outside the validated P2PE hardware payment terminals.

- The company has confirmed that the implemented P2PE solution is PCI validated
- If cardholder data is stored, it is in physical form only, such as paper
- The company has implemented all security controls as listed in the P2PE instructions manual provided by the solution provider (PCI DSS 2014)

Once the criteria are met, the company can proceed do become compliant with the SAQ P2PE HW requirements.

4.3 SAQ B-IP

If the company is unable or willing to invest to a P2PE or equivalent solution, the remaining alternative is to comply with the requirements of a more demanding SAQ, designed to address merchants who are using PTS payment devices.

The criteria to use this SAQ are:

- The company uses standalone PTS-approved payment devices
- The devices are validated to the PTS POI program
- The devices are not connected to other systems in the network environment
- The devices are the only method of payment card data transmissions
- The devices do not require an external device to be connected to the payment processor
- The company only retains card data in paper
- The company does not store cardholder data in electronic format

Most merchants should be able to achieve the criteria and will most likely use this to validate their scope.

4.4 Non-listed Encryption Solutions Assessment

NESA is a documentation guideline provided by PCI to address non-validated encryption solutions. The purpose is for solution providers to assess how much of the SAQ P2PE can be used without implementing P2PE, but rather a similar method tailored by a service provider.

PCI does not fully endorse the use of solutions E2EE with NESA and instead encourage companies to use of P2PE technology. The widespread use of P2PE has been slow and hasn’t become a common standard in the field.

4.5 Results of the assessment

According to Verifone, the use of P2PE has not become widespread in Finland and thus is unavailable. It is also uncertain if the companies have opted to use NESA documentation to validate their products encryption solution and so it falls to the merchant to use the more wider scope of SAQ B-IP.

The SAQ was filled out through investigating the environment and company practices. The results are summarized as follows:

- Removing sensitive authentication data and limit data retention.
    - The company does not store payment card data in electronic form, only copies of the receipts which mask the numbers appropriately. Unneeded copies are disposed by incineration.
    - A risk-assessment and disposal process is lacking
- Protect systems and networks
    - The devices that handle card data require segmentation from the private company network and public customer network.
    - The devices in the card data network must have default security setting changed
    - Physical locations to network devices and ports must be limited
    - Relevant personnel should receive training to be aware of attempted tampering of replacement of devices
    - Processes and incident response plans should be created
- Secure payment card applications
    - The devices require a process which allows to identify security vulnerabilities and patch them as necessary
- Monitor and control access to your systems
    - Access restrictions to least privileges necessary in accordance to job description must be maintained
- Protect cardholder data
    - Media and devices must be moved and stored in a secure manner
- Finalize remaining compliance efforts
    - Policies regarding security and how to maintain it should be established

The detailed results of the SAQ are listed in Appendix 1.

4.6 Network assessment

Initial assessment of the network revealed that the environment is lacking in documentation and coherency. The following figure represents the current network topology:

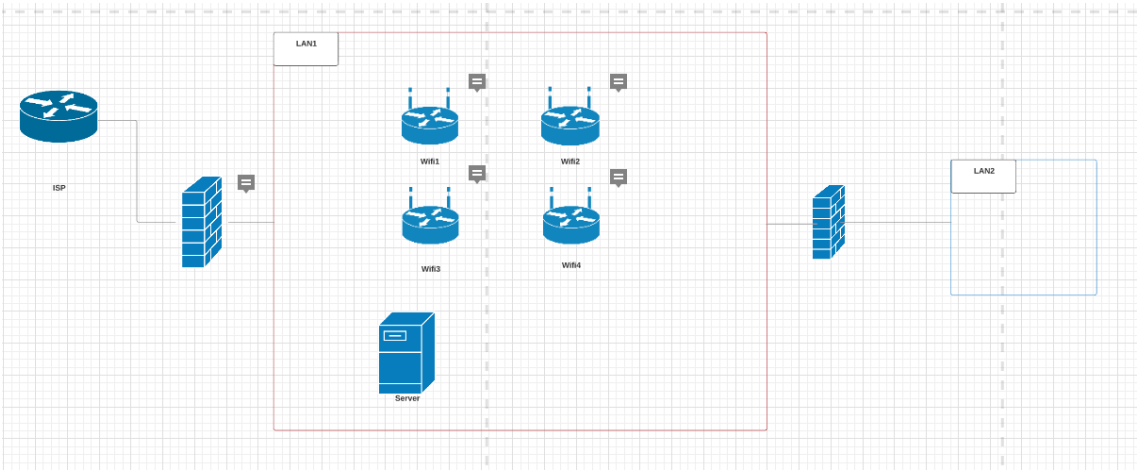


Figure 3: The current network topology

The network holds two separate network segments, with most of traffic travelling within or through LAN1, essentially creating a flat network. All customer and the company office data are mixed together which results in unoptimized network traffic and liability for security breaches. This results in the entire network being susceptible to man-in-the-middle attacks, due to the customer WLAN being connected to rest of the network, allowing malicious parties tapping into the network traffic.

The network traffic flows everywhere, resulting in reduced speed during high traffic hours and in the event of a loop, the entire network will be jammed.

5 Repair

The following chapters will explain what the company should address to achieve compliance and improve overall security.

5.1 Network safe guards and segmentation

Dividing the network into subnets and VLANs reduces the scope and the cost of the PCI DSS assessment. It also reduces the risk of security breaches as dividing information into several appropriate locations diminishes the likelihood of attackers obtaining any valuable information or cause harm to the systems. Creating a logical flow of data and documenting it provides a better understanding of the environment and allows further changes when necessary. (PCI DSS 2016a, 11).

Even though implementing security controls on systems outside the PCI scope, PCI strongly recommends doing so, as it can prevent the environments and devices outside the scope from being potentially used by malicious parties (PCI DSS 2016c 13). Therefore, this project recommends implementing network solutions regardless of the chosen SAQ.

The following recommendation shows a figure of a segmented network:

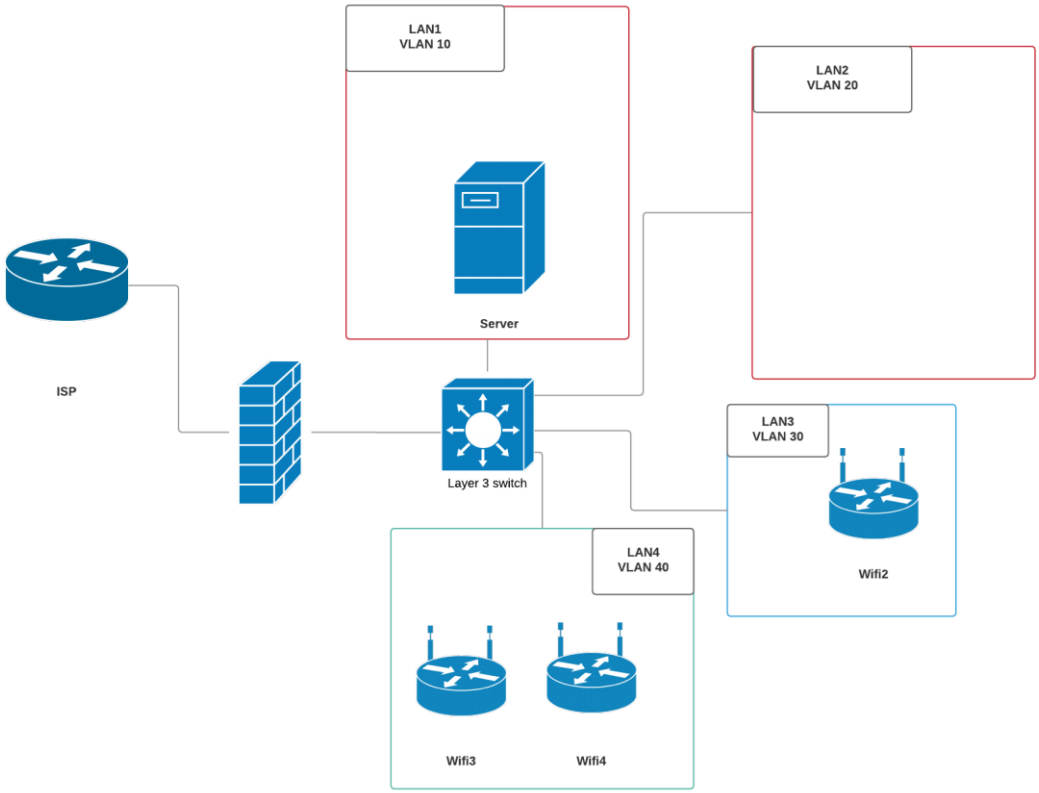


Figure 4: Recommended layer 3 network topology

The network will be divided into 4 distinct VLAN's:

- VLAN 10 for administration devices and servers
- VLAN 20 for payment devices
- VLAN 30 for a staff WLAN
- VLAN 40 for a customer WLAN

The VLAN traffic should be restricted with Access Control Lists to avoid the networks from interacting with the payment data. With the network segmented, the flow of traffic is more direct. In addition, it separates the wireless networks away from the payment environment.

The new network aims to complete the following requirements:

1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).

Table 3: Network requirements (PCI DSS. 2016a)

If the environment stores, processes or transmits payment data through the network, it is included within the scope of PCI (PCI DSS 2016a, 11). The transmitted data requires strong cryptography to prevent outsiders from eavesdropping on the wireless data flow. It also allows stronger authentication to prevent unwanted users from accessing the network and using it to access other data or portions of the network. (PCI DSS 2016a, 48)

PCI recommends using wireless connections for non-sensitive information transmissions as wireless technology is easier to access and intercept than wired ports. (PCI DSS 2016a, 11)

5.2 Critical requirements

To ensure that payment card data is secure, the following requirements should be addressed:

1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)
1.3.5 Permit only “established” connections into the network.
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.
2.3 Encrypt all non-console administrative access using strong cryptography.
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.
7.1.3 Assign access based on individual personnel's job classification and function.
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with

active network jacks.
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.

Table 4: Critical requirements (PCI DSS 2016a)

These requirements require action and will have an immediate effect on security. With these requirements complete, the company will be very secure against possible data leaks or breaches.

5.3 Minor requirements

The following requirements detail what must be achieved in order to make sure that the critical requirements remain complete. In addition, the table includes policy, training and other documentation processes:

1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.
9.6.1 Classify media so the sensitivity of the data can be determined.
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification.

9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.
12.2 Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk.
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
12.8 Maintain and implement policies and procedures to manage service providers, with whom cardholder data is shared, or that could affect the security of cardholder data, as follows
12.8.1 Maintain a list of service providers including a description of the service provided.
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.
12.8.3 Ensure there is an established process for engaging service providers includ-

ing proper due diligence prior to engagement.
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.
12.3 Develop usage policies for critical technologies and define proper use of these technologies.
12.3.1 Explicit approval by authorized parties
12.3.2 Authentication for use of the technology
12.3.5 Acceptable uses of the technology
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
12.5 Assign to an individual or team the following information security management responsibilities:
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.

Table 5: Minor requirements (PCI DSS 2016a)

6 Conclusion

The PCI assessment serves as a base for the company to understand where they stand as a merchant, what vulnerabilities exist and what potential repercussions they may cause. It is up to the company to decide if they wish to strive for compliance, due to the monetary investment required. However, it is recommended to consider fixing partially the critical require-

ments, as having more security is always beneficial. At the very least, the company accepted and implemented the network proposal as recommended.

References

Niemitalo, Mirja. 2016. Käteinen syrjäytyy nopeaa tahtia. Accessed 7.2.2017
http://www.kaleva.fi/uutiset/kotimaa/kateinen-syrjaytyy-nopeaa-tahtia-kolikoiden-kysynta-jo-vahentynyt/721121/

Nordea. 2013. Rules of Card Acquiring Merchant Agreement. Accessed 15.6.2017
https://www.nordea.fi/Images/60-77298/Rules_of_Card_Acquiring_Merchant_Agreement_11_2013.pdf

Nordea. 2016. Käteisen käyttö vähenee. Accessed 7.2.2017
http://www.nordea.com/fi/media/uutiset-ja-lehdistotiedotteet/News-fi/2016/2016-07-22-kateisen-kaytto-vahenee.html

PCI DSS. 2014. Self-Assessment Questionnaire P2PE-HW and Attestation of Compliance

PCI DSS. 2016a. Requirements and security assessment procedures. Accessed 31.5.2016
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

PCI DSS. 2016b. Quick Reference Guide. Accessed 1.6.2016
https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf

PCI DSS. 2016c. Guidance for PCI DSS Scoping and Segmentation
https://www.pcisecuritystandards.org/documents/Guidance-PCI DSS-Scoping-and-Segmentation_v1.pdf

PCI DSS. 2016d. Assessment Guidance for Non-Listed Encryption Solutions
https://www.pcisecuritystandards.org/documents/Assessment_Guidance_Non-Listed_Encryption_Solutions.pdf

PCI DSS. 2016e. Prioritized Approach for PCI DSS. Accessed 1.6.2016

PCI DSS. 2017. Frequently asked questions. Accessed 17.5.2017
https://www.pcicomplianceguide.org/pci-faqs-2/

PCI Security Standards Council. 2014. Best practices for maintaining PCI DSS Compliance. Accessed 7.3.2017
https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf

Verizon. 2015. PCI Compliance report. Accessed 16.2.2017
http://www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf

Figures

Tables

Appendixes

Appendix 1: SAQ results

PCI DSS Requirements v3.2	**Milestone**	**Status**
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	**1**	**Yes**
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**2**	**yes**
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	**2**	**no**
1.2 Build firewall and router configurations that restrict 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*.		**yes**
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	**2**	**Yes**
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	**2**	**Yes**
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.		**no**
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	**2**	**no**
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	**2**	**Yes**
1.3.5 Permit only "established" connections into the network.	**2**	**No**

1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	**2**	**N/A**
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	**2**	**Yes**
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	**2**	**No**
2.3 Encrypt all non-console administrative access using strong cryptography. ***Note**: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*	**2**	**No**
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	**1**	**No**
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: • There is a business justification and • The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	**1**	**Yes**

3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note**: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • *The cardholder's name* • *Primary account number (PAN)* • *Expiration date* • *Service code* *To minimize risk, store only these data elements as needed for business.*	**1**	**Yes**
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.	**1**	**Yes**
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	**1**	**Yes**
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.***Note**: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*	**5**	**Yes**
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. ***Note**: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the*	**5**	**yes**

same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.		
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. ***Note**: This requirement applies in addition to all other PCI DSS encryption and key-management requirements.*	**5**	**n/a**
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	**5**	**No**
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	**2**	**No**
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. ***Note**: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.* *Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or*	**3**	**no**

would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.		
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.	**3**	**no**
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.		**yes**
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	**4**	**no**
7.1.3 Assign access based on individual personnel's job classification and function.	**4**	**no**
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.	**2**	**N/A**
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. ***Note**: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.*		**no**

8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	**4**	**yes**
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.	**2**	**no**
9.5 Physically secure all media.	**5**	**Yes**
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	**5**	**no**
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:		**no**
9.6.1 Classify media so the sensitivity of the data can be determined.	**5**	**no**
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	**5**	**no**
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	**5**	**no**
9.7 Maintain strict control over the storage and accessibility of media.		**no**
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	**5**	**no**
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:		**Yes**
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	**1**	**Yes**
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. ***Note**: These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale.*		**No**

This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.		
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification.	**2**	**No**
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). ***Note**: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.*	**2**	**No**
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	**2**	**No**
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	**5**	**No**

11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. ***Note**: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*	**2**	**no**
12.1 Establish, publish, maintain, and disseminate a security policy.	**6**	**No**
12.1.1 Review the security policy at least annually and update the policy when the environment changes.	**6**	**NO**
12.2 Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk. *Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.*	**1**	**No**
12.3 Develop usage policies for critical technologies and define proper use of these technologies. ***Note**: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.* *Ensure these usage policies require the following:*	**6**	**no**
12.3.1 Explicit approval by authorized parties	**6**	**no**
12.3.2 Authentication for use of the technology	**6**	**no**
12.3.5 Acceptable uses of the technology	**6**	**no**
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	**6**	**no**
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	**6**	**no**

12.4.1 ***Additional requirement for service providers only***: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication to executive management ***Note****: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	**6**	**N/A**
12.5 Assign to an individual or team the following information security management responsibilities:	**6**	**no**
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	**2**	**no**
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.	**6**	**no**
12.8 Maintain and implement policies and procedures to manage service providers, with whom cardholder data is shared, or that could affect the security of cardholder data, as follows	**2**	**no**
12.8.1 Maintain a list of service providers including a description of the service provided.	**2**	**no**
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. ***Note****: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	**2**	**no**
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	**2**	**no**
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	**2**	**no**
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	**2**	**no**

12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.		**no**
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.	**2**	**no**