PCI-DSS Compliance Integration

Phillip N. Borne

A Prospectus Presented to the Information Technology College Faculty
of Western Governors University
in Partial Fulfillment of the Requirements for the Degree
Master of Science in Information Security and Assurance
November 24, 2014

Abstract

Currently the credit card industry utilizes PCI-DSS compliance as their set of security standards aimed at protecting credit card data. Once compliance is achieved the organization has to continue with due diligence to ensure a high level of security and audit requirements are maintained. The average technology team with minimal knowledge in PCI-DSS compliance will encounter many challenges while achieving this goal. The most common problem faced by many organizations is the ability to interpret the standards putting the organization at great risk. The strategy for this project is to discuss the different areas of compliance recommended by PCI Security Standards Council along with information and data from credit card service providers in order to provide a better understanding of the process. The process of conducting research will be sourced by the PCI Security Standards Council, Credit card service providers and challenges organizations have encountered. Implementation of process will be structured with the goal of compliance but also creating a format that is customizable for the any organization's individual needs. The anticipated outcome of this project will be to provide an implementation strategy that can be integrated into daily operations which will greatly increase the organization's ability to not only achieve but also maintain compliance.

Table of Contents

Introduction

During the past few years credit card use is continuously on the rise because of its convenience and flexibility. The modern consumer often prefers credit and debit cards as a method of payment for everything from groceries to goods available on the Internet. As with many luxuries certain risks are unavoidable especially when there are opportunities for someone to exploit systems. The problems this project will address are the challenges organizations encounter when trying obtaining and/or maintaining PCI-DSS compliance. The importance of this solution is not only to perform due diligence to ensure confidential remains safe but also raise organizational security awareness. In some cases organization may be subjects to other regulatory or standards. The framework for PCI overlaps or has many similarities with other types of regulations the organization may be subjected. (PCI Security Standards Council, 2006) Organizations that are unfamiliar or less experienced with this audit process encounter the same common challenges such as knowledge, misinterpretation of requirements, available resources able to perform compliance tasks, funding, etc.

Project scope

The scope of this project will be based on the current requirements and security assessment procedures set by the PCI-DSS Security Standards Council. PCI-DSS-DSS compliance involves specific processes, procedures and management of all devices that hold or transport card holder data along with general best practices used within the industry regarding information security. The items included in scope of the project are described in the following:

- Change control process and procedures
- Implementation of all hardware and software within the scope of PCI-DSS-DSS compliance

- Management of security monitoring components (anti-virus, firewalls, IDS, syslog messages, etc.)
- Auditing (user accounts, syslog messages, unauthorized configuration changes, change control tracking, account creation, account removals, etc.)
- Penetration testing
- Annual updates of processes and procedures to align with current PCI-DSS-DSS requirements.
- Physical security operations (physical access, background checks, employee training, separation of duties, etc.)
- Encryption (implementation, monitoring, handling of cryptographic keys, etc.

Items that will not be included in the scope of the project are the following:

- Work applied to other regulatory items such SOX, HIPPA, etc.
- Custom security measures and controls outside the scope of PCI-DSS compliance but is deemed necessary to the organization to mitigate business related risk.
- Other technology infrastructure the business requires which are outside the scope of PCI.

Defense of the Solution

Since the amount of business processing credit cards continue to increase, the amount of those failing PCI auditing will continue at the same rate. In regards to this project the failure group will mostly be in the small-to medium size business. Organizations in this category often lack the experience, human and technical resources to be fully complete compliance requirements. Defense of the proposed implementation strategy is explained in the following:

- Decreased risk of failing compliance objectives- Using a formal strategy to perform all necessary requirements will decrease the risk of failing compliance objectives. When all twelve requirements are broken into the smaller modular components an organization will be able to better maintain better control and management of individual items. The phased implementation used in the project will enable the business to integrate the compliance requirements into their daily business routine which over a short time will be an everyday habit which will not only fulfill the compliance requirements but also increase the use of security best practices.
- Increased business efficiency- Implementation of compliance requirements into the daily routine of the business increases the efficiency of the technology team by streamlining processes such as configuration security settings as desktops are being setup for deployment or configuring security settings and performing change control as network devices are being deployed into production.
- Increased security posture- The requirements for PCI-DSS-DSS compliance are synonymous with industry security best practices. Implementing the security standards as recommended by other security groups and regulatory requirements will increase the security posture of the organization. These days it's commonly assumed that attacks are originated from outside the network whereas in reality studies have proven that most are originated from the inside. Implementing the best practices in the industry would protect the organization from all angles.
- Reduced risk of liability- Performing the due diligence of implementing the necessary security standards will reduce the organizations risk damaged

reputation and liabilities producing legal litigation. Any organization would be able to perform the items in the phased approach then complete then document their actions to prove they are performing due diligence

Methodology Justification

The project goal of obtaining and maintaining PCI-DSS compliance will be performed in a five phase approach. The five phase approach strategy was created to ensure all similar tasks are grouped together for simplify the complexity of the all tasks leading up to the auditing process. The approach also integrated a verification phase which provides a system of checks to ensure all compliance requirements are met and not overlooked. This particular strategy is preferred over methods since it serves as a system of checks and balances, along with ease of task management and other moving parts of the project. The phases of initiation, implementation, verification, auditing and monitoring and maintenance will ensure that all sub-sections within the twelve requirements are handled properly with the end goal of obtaining compliance. This process can be used not only for the first time of becoming compliant but also the recurring auditing process year after year by repeating the cycle.

Organization of the Capstone Report

This project was created for use by personnel not experienced in PCI or similar regulatory standards. The remainder of the report will explain both the technical and non-technical requirements covered in PCI standards. Once the reader goes through the entire document they will be have a better understanding on how to manage the many different sections of PCI compliance auditing. The reader will also be able to use the same layout and processes to assist with other types of regulatory requirements and similar technical projects. All templates provided will be easy to use and customizable to the organization’s needs.

Systems and Process Audit

Audit Details

During the scope of an audit it was determined that a groups of organizations especially those which were new to PCI compliance often failed their compliance audits. This was mainly due to not being able to interpret the standards information, technical skill gaps and failure to create a systematic approach leading up to the audit. This problem is mostly noticed in small to midsize companies. The problem is less relevant to large organizations which are subjected to other regulatory efforts or have experienced personnel onsite which can lead the compliance projects. The problem can be minimized with general guidance and understanding of security requirements based upon the type of organization is being subjected to PCI compliance.

Problem Statement

Since credit card use is on the rise along with theft of credit information credit card information security has become a high priority with credit card processors. The problem at hand is more businesses are accepting credit cards as a convenient method of payment which subjects their organization to the requirements of PCI-DSS compliance. The problem comes into play when either a new or midsize to small organization need to fulfill requirements without any formal guidance or prior experience. An organization in this state has a high probability of not being able to obtain compliance and produce substantial impact upon the organization due to lower security posture, inability to process credit cards and fines.

Problem Causes

The cause for noncompliance generally falls into a general set of challenges. The following items are directly related to the cause of non-compliance or failure to maintain compliance:

- Knowledge- This topic covers both technical and auditing knowledge. The lack of technical knowledge may be challenging on how to successfully implement the action items needed. (Mills, 2010) In this case training or specific guidance is needed to overcome this challenge. In regards to auditing knowledge personnel may not have the knowledge or guidance to correctly perform and document the auditing items. In some cases an organization can become non-compliant not by incompletion of the requirements but failure to document action items correctly.
- Business priorities- In some cases upper management may see other business needs as a higher priority over compliance requirements. In this scenario staff members are directed to take care of these needs first and dedicate limited amount of time to compliance action items necessary compliance action items are at risk of not being completed. In the case of failure to manage time accordingly, staff members are often rushes to complete work that is considered necessary as that of compliance near the end date. This increases the probability of mistakes and minimal time allowed to make any corrections if needed.
- Incorrect security practices- Incorrect security practices are normally the cause or incorrect guidance regarding security implementations. An example of this item would be entering rule rules in an incorrect manner. Firewall rules are helpful in restricting specific types of traffic but if implemented incorrectly then the person entering the configuration may allow other unsafe protocols or other harmful traffic through the firewall.
- Discipline to follow requirements- Lack of discipline towards completing the necessary requirements is another reason for failure to obtain or maintain

compliance. Some action items either being daily or follow other schedules require consistency in order to be complete. The organization needs to realize this is necessary not only for the purpose of taking credit card payments but also increase the security posture of the organization in order to protect other types of confidential information. The requirements are put in place for a specific reason to not intend to be disregarded if needed.

- Incorrect implementation of technologies and applications- New technologies such as the latest generations of firewalls up to the newest application that will greatly promote the business can be troublesome when not installed or implemented correctly. Some small to mid-size organizations will perform self-installation of hardware and software to reduce overall project expenses. The problem with this topic is if the staff is not fully qualified or experienced enough to perform the task and make it fully secured it could open new vulnerabilities to exploit. Some of the greatest security breaches begin with something minor that was overlooked or the cause of misconfiguration.

Business Impacts

Failure to gain or maintain compliance can lead to significant business impacts upon the organization. The main three problems for an organization not being PCI-DSS compliant is loss of revenue, fines against the organization and inability to process credit cards. An organization would be subjected to significant revenue loss if the company is not able to process credit card payments. This would greatly affect the organization's customer base especially when they are not able to purchase the required goods and services as needed. The inability to take credit cards may convince some customers to go elsewhere for their purchases. Another impact upon the

business is large fines imposed by the credit card processor. The fines can vary depending on type of offense and the card processor. An example of the fines listed for 2014 range from $5,000 to $500,000 for the organization. (MiJireh Checkout, 2014) Fines and other financial related issues may capture the attention of investors or stockholders where applicable. Even though failure to be compliant can indirectly lead to quite a few other impacts upon the organization the three listed above are the most significant.

Cost Analysis

The cost factors relating to the project are commonly known and can vary according to the organizational size, current security posture, current hardware/software in production, etc. Additional expenses regarding PCI are common to additional hardware/software, training, and consultant services. An example of cost and other expenses related to PCI-DSS compliance in a medium size business environment will be the following:

Expense Description	Quantity	Cost Per Unit	Total Cost for Expense
Anti-virus software	200	$25.00 per license	$5000
Juniper NS 320 Firewall (2 devices to implement a failover pair)	2	$4,000.00/per pair	$8000
Syslog software	2	$800.00/per server	$1600
Juniper IPS (2 devices to implement a failover pair)	1	$6,000.00/per pair	$6000
Computer deployment console software	2	$10,000.00	$20,000.00

Contractor services (assistance with configuration and implementation	1	$15,000.00	$15,000.00
			Total
			$55,600.00

Risk Analysis

When integrating PCI-DSS requirements into an organization there are certain risks involved with the compliance effort. The risks that are common to PCI-DSS compliance such are the following:

- Organizational buy-in- When implementing an organization wide effort which requires the cooperation of all personnel organizational buy-in is necessary for the success of the initiative. If the implementer is not able to get the full support of all participants the initiative has an increased probability of failure.
- Management sign off- Another risks factor is management sign-off. When certain initiatives have support from senior management this displays to the employees the high level of importance. Also the compliance effort would require an executive sponsor to provide items such as support, guidance, funding, etc.
- Lack of effort- Some participants may see the required action items as not important, relevant or a waste of time. The reason for integrating the process should be fully explained to all employees along with the effects of failure upon the organization. All stakeholders need to understand how this will affect themselves, their coworkers and the organization.

- Consistency of effort- Compliance is not a onetime effort and needs to be constantly monitored and maintained. The way to counter this type of behavior is assigning a person whose secondary duties are to oversee the compliance items. Management will need to provide oversight on this work to ensure the work is being performed and is also consistent. This way any variation in the process can be quickly corrected. This will ensure all compliance action items are performed since a single source is responsible to maintaining compliance.

Detailed and Functional Requirements

The project will need to meet specific requirements in order to be successful in not only completing the compliance audit but also raise security awareness throughout the organization. This section of the document discusses all the necessary requirements of everyone from the technical staff to other personnel within the organization required to participate in the efforts.

Functional (end-user) Requirements

During the compliance process all employees are considered critical to the project. Even though most personnel are not responsible for performing technical tasks directly related to PCI-DSS compliance they are still responsible for handling and protecting confidential data. In addition to the traditional task to gain PCI-DSS compliance additional features must be available to the end users to ensure success. These features are listed as the following:

- General explanation of compliance efforts- In order for all employees to participate in the program explanation of the project's purpose and reason for application. Most times a small percentage of employees will not buy-in to the program based on not understanding the importance of the initiative. People in this group must also understand the impact upon the organization if they are at

fault for not cooperating with the requirements. Being that all employees are stakeholders in the organization they must be part of the efforts to increase its success. Everyone involved in the compliance efforts must clearly understand how their participation is critical regardless of their role within the organization.

- Training- Training must be provided not only in regards to annual security training but also what is required while performing their daily work functions. Some personnel may not be as technical as others which would require additional training for items such as encrypting sensitive data on email, protecting sensitive data within the workplace, etc. With this project training for the technical and project staff may be applicable if needed. Some personnel that are relatively new to PCI compliance may need supplemental training to assist in the efforts of the project. (Mills, 2010)
- Support- End users will feel more accepting of new practices when support is provided. If they feel alone and on their own to figure out problems users will quickly become frustrated making the end user resent the technology or processes in place to enhance information security. In order to make the users feel comfortable assigning a person they can contact when needed can alleviate end user stress.
- Structured process- Structured processes must be provided for the end users in order for the effort to be successful. The organization must inform the users with clear documented instructions rather than word of mouth or emails. When daily processes are verbally explained or distributed via email the main information which is soon lost, forgotten or misinterpreted. Structured processes that are

readily available when needed by the users in a centralized storage location will ensure that all users are performing the same functions as a unified effort. Creating a webpage containing only information compliance and organizational security would give the staff a centralized location for information they need. These processes for information distribution are applicable not only to the end-users but also to the technical staff performing the compliance work.

- Ease of functionality and usage- Ease of functionality and use for users is critical. When users have to perform additional work that appears to make their job more complex or confusing the success rate of performing the required task is greatly reduced. When purchases of hardware/software or changes in processes are done without consideration of the users it could cause problems. When users feel that certain changes are hindering them from performing their jobs duties it can inversely affect all operations within the organization. In cases such as this the technical leaders need to consult with business leaders and users if necessary to ensure the correct technology or processes being imposed will not only fit the needs of compliance but also not hinder business operations.

Detailed Requirements

The main condition that must be met in order to make this project successful is the assignment of proper personnel. If all personnel (management, technical, etc.) required for the project are not available when required the project will not be completed within the allocated timeframe or those working on the project will be rushed making mistakes or possible information misinterpretation. As with all organizations today especially with technology teams they are all understaffed and overworked with other business priorities. The organization will

have to set compliance efforts as a business priority in order for the project to obtain the appropriate personnel and funding. If the organization has specific skill gaps especially in regards to technical skills third-party or contractors can be used for temporary augmentation of staff. This will be an additional expense towards the organization but it will ensure that compliance requirements are met in the timeframe which they are required.

Existing Gaps

Based on my observation the common gaps that exist with completing PCI compliance tasks are based on organizing compliance requirements and management of all tasks involved. I have seen some organizations wait until the last minute to perform PCI related tasks and when rushed personnel will sometime perform the tasks incorrectly or misunderstand the requirements. I have also observed the method of just assigning all tasks out to personnel and hope it gets completed or find out once completed the work or remediation efforts is wrong. Another common problem is the organization not performing periodic task and continuous monitoring required by PCI compliance. The monitoring and maintenance portion of PCI is just as important as performing the actual audit. This portion of the process also requires accurate documentation of actions performed. If documentation is not maintained or loosely written it may not be acceptable to the auditors. This project will cover all the common pitfalls with PCI compliance such as implementing a methodical approach, timely phased approach with verification time to ensure all items are accurate along with a maintenance listing of when certain task need to be performed and documented.

Project Design

Creation of a project plan was carefully considered in determining how to address the problems of PCI compliance within an organization. The main goal of the project was to create a

phased approach which could be used by either technical and non-technical personnel to increase their success rate of completing all compliance requirements.

Scope

The scope of this project will be based on the current requirements and security assessment procedures produced by the PCI Security Standards Council. PCI-DSS compliance involves specific processes and procedures, management of all devices that hold or transport card holder data along with general best practices pertaining to information security. The items included in scope of the project are described in the following:

- Change control process and procedures
- Implementation of all hardware and software within the scope of PCI-DSS compliance
- Proper operations of security monitoring components (anti-virus, firewalls, IDS, syslog messages, etc.)
- Auditing (user accounts, syslog messages, unauthorized configuration changes, change control tracking, account creation, account removals, etc.)
- Penetration testing
- Annual updates of processes and procedures to align with current PCI-DSS requirements.
- Physical security operations (physical access, background checks, employee training, separation of duties, etc.)
- Encryption (implementation, monitoring, handling of cryptographic keys, etc.

Items that will not be included in the scope of the project are the following:

- Work applied to other regulatory items such SOX, HIPPA, etc.

- Custom security measures and controls outside the scope of PCI-DSS compliance but is deemed necessary to the organization to mitigate business related risk.

Assumptions

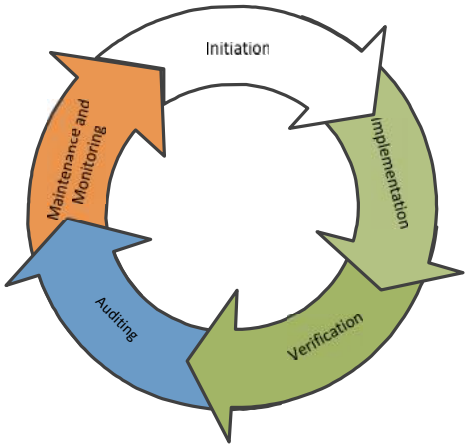
When implementing a strategy towards PCI-DSS compliance certain assumptions can be made against the type of organization which the solution would be applicable. Discussing the necessary assumption will enable a person to better identify any challenges while defining the solution. Some of the assumptions are the following:

- General knowledge about PCI-DSS- Regardless if the staff in the organization is knowledgeable about the compliance requirements; if a person is technically proficient the requirements can be understood with minimal effort. Non-technical personnel would find the information to be complex and not able to interpret the requirements.
- Organizational security practices- Even if compliance wasn't a requirement of the business if the average person can assume the organization has implemented some security measures such as anti-virus, firewalls, user authentication system, etc. If a company is performing the bare necessities of security the main action items for compliance may require some work along with fine tuning of settings and services.
- Budget- Another assumption is the organization will have the necessary budget to support any purchases regarding the effort. Depending on the security posture of the organization additional hardware, software or third party support may be required. Funding would need to be available for purchases to obtain hardware, software, and other resources or maintain compliance.

- Support of senior management- Senior management support is necessary for the initiative to be successful. The assumption can be made since credit card payments are crucial means of revenue for an organization senior management would be fully supporting of the items required.
- Support of personnel- When all employees understand the importance and repercussions of this type of compliance the success rate can be increased and the risk of information mishandling will be reduced. When employees understand how crucial it is to obtain compliance and the affects upon the organization which employs them it can be assumed that employees will participate since they are stakeholders in the organization.
- Resources- It is assumed the organization has the necessary human resources to complete the action items necessary for compliance. This topic is even more challenging for departments that are encountering PCI-DSS for the first time. This normally will require starting at the ground level to cover all twelve documented levels of requirements.
- Adequate time to complete compliance action items- It is assumed that adequate time is available to perform all the necessary action items to obtain and maintain compliance. In situations where organizations are rushed to complete all the task required information can easily be misinterpreted, work is performed incorrectly, documented is incorrect along with other mistakes In regards to efforts such as this a certain amount of time is required dependent upon the organizations current security posture.

Project Phases

Completing the necessary requirements for PCI-DSS compliance will be performed in five phases consisting of Initiation, Implementation, Verification, Auditing and Monitoring and Maintenance. This method of approach was chosen for its simplistic use of a repetitive cycle that can adjusted to meet the needs of the organization and any changes within PCI-DSS compliance requirements.



A brief description of the five phases is listed in the following:

1) Initiation- This is the first phase which is used primarily to establish a security baseline, begin creating the framework and provides the information necessary to progress into the next phase. In this phase tasks will include defining current security posture, establishing budgets, assign task owners and understand any critical gaps in security that need to immediately resolve.
2) Implementation- The second phase is implementation. In this phase the most work will occur such as policy and procedure creation, technical remediation, implementation of new hardware where needed, implementation of change

control process, planning of security training for personnel, etc. The information provided from the initiation phase is used to plan and complete this phase.

3) Verification- The verification phase is as the name states, where it's used to verify the work conducted in the implementation phase. In this phase the requirements for compliance are verified as complete or implemented such as change control, policies, ensuring all vulnerabilities are remediated and conducting security training for employees. One of the last tasks for this phase is discussion with approved auditor to proceed with the fourth and final phase.
4) Auditing- The auditing phase is the fourth and final step of the process. This phase mainly concerned with working with the auditor and verifying all requirements for PCI-DSS compliance is completed. If any item was possibly overlooked or newly discovered, this phase will also be used to complete and verify with the auditor. Once auditing is complete all documentation will be stored in a secured location for future reference. The last task of this phase is to document any process correction or changes that would need to be implemented on the following year's audit.
5) Maintenance and Monitoring- The maintenance and monitoring phase is the longest phase of all five which is used to performing monitoring of all alarms, logging information, etc. This phase is also used to perform the required vulnerability scans and testing. Once all scans and testing procedures are performed remediation of any high-risk items will require immediate action. This phase is the one which requires the most and accurate documentation of action

items. Performing the scheduled items require documentation as proof of completion and being performed correctly.

Timelines

The auditing process will take place once the organization is required to become compliant by senior management and annually afterwards to ensure the requirements continue to be completed. The general time requirements of the five phases are the following:

1) Initiation- This phase will require 4-6 weeks to complete depending on the size, requirements and current state of the infrastructure.
2) Implementation- This phase will require 8-12 weeks to complete depending on the size of the organization, requirements and the current state of the infrastructure.
3) Verification- This phase will require 2-3 weeks to complete depending on the size of the organization, requirements and the current state of the infrastructure.
4) Auditing- This phase will require 4-6 weeks to complete depending on the size of the organization, requirements and the current state of the infrastructure.
5) Monitoring and Maintenance- There is no set timeline for this phase. This phase will consume the time between the completion of the auditing phases and the start of the initiation phase of the cycle.

Dependencies

The five phases described earlier in this document have a strong dependency upon the actions performed in the previous phase. The systematic approach to the phases is considered ineffective if any critical steps are missed or a phase is bypassed. Some components in the twelve PCI-DSS requirements are considered critical to compliance and/or may take a great deal

of effort. Missing any of the tasks assigned to each phase may risk obtaining compliance or cause serious delays to the project. Each of the five phases was carefully created to cover all the necessary requirements for PCI-DSS compliance which eases complexity and ensures all areas are properly covered.

Resource Requirements

In order for this project to be successful certain resources are required. Resources in regards to this project can be internal personnel directly from the organization, third-party personnel assisting in the compliance efforts, technical hardware and software. The resources needed throughout the duration of the project are described in the following:

- Project coordinator- This person is needed as the focal point of the project for progression tracking and completion of the many individual requirements for each phase. This person can be in management or equivalent stakeholder that is responsible for the overall success of the project. A person in this role will be required from the initial start of the project until the very end once the project is complete. Upon the following annual audits this person or others that can fulfill this role is needed to monitor the compliance efforts. A person in this role will be required throughout the project.
- Technical management-A technical manager will be the person that supports the project coordinator and ensures the technical aspects of the project are being completed in the most efficient manner. This person also serves in different roles such as a liaison for the technical staff in scheduling tasks with the project coordinator, ensuring technical requirements are sounds and can be completed as designed and identification of risks that can create additional delay and prevent

the project from meeting critical deadlines. A person in the technical management role will be required throughout the project.

- Technical personnel- This group of personnel is responsible for fulfilling the technical skills needed to complete the compliance task. This group can be either internal personnel or subcontractors maintaining a wide array of information technology skills from computer configuration to servers and network engineering. Personnel in this group will be needed until the project is complete and once again for fulfilling annual audit needs to complete any remediation items relating to discovered security discrepancies. Technical personnel will be required throughout the duration of the project to ensure all technical needed are met.
- Required hardware- Depending upon the current technological state of the information systems and network, specific hardware such as routers, firewalls, servers, etc. will be required to impose the necessary security enhancements for compliance. A survey will first be required to determine the components needed for the project. From time to time as technology changes along with new threats or PCI-DSS compliance requirement updates new hardware may be required in the future. New technology will be required prior to the implementation phase of the project.
- Senior management sponsor- A person in this role is crucial to the project from start to finish. A person in the project sponsor role will be important to perform tasks such as obtaining funds, executive representation of the project, leadership decision making and approval for any organizational policy or procedure changes.

The person fulfilling this role will be required throughout the project until the end to ensure project completeness.

- Third party personnel- Third party personnel may be required to fulfill certain technical or non-technical aspects of the project. An initial analysis of current team will need to be performed and documented to ensure that any gaps in skills or other human resources are fulfilled by third party vendors or subcontractors. If the particular skill set is constantly required to handle any new security tasks an internal position may need to be considered to handle not only compliance items but also new threats as they arise. Depending upon skill gaps personnel in this group may be required for specific phases or the entire project if the missing skillset is required for the duration of the project.

Risk Factors

When an organization is working towards PCI-DSS compliance there are a few critical factors that can put the project at risk. Some of the risks that need to be carefully monitored are:

- Technical skills- If the organization doesn't have the personnel with specific skill sets. Personnel training may need to take place or supplementing with third-party personnel may be required. If the organization is missing a specific skillset to complete the compliance tasks the organization will risk obtaining compliance.
- Timelines- Timelines are very important to ensure all compliance items are completed and verified. Depending upon the card processor fines and other measures may be taken against the organization that fails to become compliant within the required timeframe.

- Organization of information- Information needs to be completed, organized and securely stored for future use. Throughout the year when certain tasks are completed such as wireless scanning, syslog message monitoring, firewall rule auditing, etc. will need to be documented as being performed. This will be useful to the auditor to ensure the work is being performed as required.
- Implementation- Implementation and continuation of processes and procedures are very important to compliance and regulatory efforts. Some organizations may assume that continuing processes such as change control for example are only done during certain times of the year. The processes and procedures as defined in the twelve requirements are required to be performed all throughout the year and not done during the auditing timeframe.
- Planning for funding- Depending on changes in technology or compliance requirements purchasing of additional hardware and/or services may be necessary. In cases where projects are not properly identified, planned or simply funding isn't available will put compliance efforts at risk of being incomplete. In the initiation phase of the project all necessary purchases of hardware or services will need to be properly identified and ensure funds are available to proceed with the project.

Important Milestones

Since the project will have many moving parts and assigned task each phase of the project will have specific milestones to achieve before moving forward onto the next phase. Once all milestones are completed in the fourth phase the project of obtaining compliance will be

complete. The milestones to verify completion of the five phases is fairly straight forward and simple as described in the following:

- Initiation- Security assessment is completed, budgets are drafted, and responsibilities are assigned.
- Implementation- All policies/procedures are created, change control implemented and all technical remediation is completed.
- Verification- All work performed in the implementation phase is verified as complete, accurate and fulfills all of the requirements.
- Auditing- Compliance efforts are approved by the qualified auditor and compliance is obtained, all documents are stored and required process corrections are documented.
- Maintenance and Monitoring- The milestones in this phase will be the completion of all required scanning and testing as required by compliance.

Deliverables

The deliverables for this project will be a collection of documents which are utilized throughout the different phases of project implementation. The documents created for this project cover a wide range of uses from initial technology analysis to a maintenance schedule of continuing tasks.

Methodology

The methodology, approach and strategy for the different phases of the project were based upon the experiences I have encountered with PCI compliance over the years. The problems that both I and others in my field have encountered are rooted in failure to implement a systematic approach to compliance efforts from start to finish.

Approach Explanation

The approach to the project was to create a strategy that would be simple to use and reduce the risk of failing compliance due to not properly assigning responsibilities, missing critical task, failing to verify completeness of work performed, etc. Its common when an organization is not experienced in performing compliance activities is at risks of failure due to not implementing a strategy to address all the necessary requirements.

The most common approach to completing all the tasks is to compile a list of the items to remediate then proceed with the auditing process. The problem with this particular method of approach it increases complexity of tracking all of the tasks along with manage the project as a whole. Normally what occurs in this method is timelines are missed and remediation efforts are miscommunicated. When one or both of these problems occur all personnel involved are under a high level of stress to ensure the problems are corrected as quickly as possible. Due to past experience errors and/or problems will cause the team to work afterhours in order to not jeopardize the project timelines. The phased approach to reaching the required level of compliance is better suited utilizing the phased approach as a method of checks and balances along with ensuring that adequate time is allocated for the project.

Approach Defense

The defense of this project can be easily proven by the increased success rate of obtaining PCI-DSS compliance. A systematic approach was created as a simple way of handling the many moving parts will greatly assist ether the typical organization that is new to PCI-DSS compliance and/or the organization not in able to handle complex compliance or other regulatory efforts. When an organization doesn’t have any method or procedure to obtain compliance the risk or

delay of obtaining compliance is greatly increased. The complexity in regards to PCI-DSS is it contains many individual tasks which some are technical or others non-technical. These different tasks are required during specific times and/or during the different phases of the gaining of compliance and then afterwards during the annual audits. If certain tasks are not performed in the sequential manner required or during certain phase the project as a whole can be severe delays or impact other compliance work or processes. The systematic approach when used as a method of progression management and tracking will greatly reduce the complexity of work involved throughout the project and increase the success rate of obtaining compliance. An organization that is experienced with PCI-DSS may not have a need for all of the guidance provided in this document but may be used to identify gaps in their processes and procedures which may reduce complexity, time, cost or a combination of all three.

Project Development

This section of the document covers the technical and other necessary resources required for the success of the project. Discussion will also include hardware, software, tech stack, and architecture details used in regards to obtaining PCI compliance.

Hardware

The following hardware devices/systems will be used in order to monitor the security requirements of PCI-DSS compliance:

- Current network infrastructure- The current infrastructure will remain in use and will be adjusted for the necessary security configurations as required my compliance requirements.
- Firewalls- Firewalls will be required to provide a boundary of protection on the outer edge of the network that separates the internal and external networks. The

type of firewall is based on the size and needs of the organization. For the project a Juniper based project was used based on the priced and assumption of network size.

- IPS units- IPS (Intrusion Prevention System) will be used to detect intrusion on the network along with monitoring of other modern threats.

Software

The following software systems will be used in order to monitor the security requirements of PCI-DSS compliance:

- Syslog server software- Syslog server will be used to collect and manage syslog messages from all devices on the network.
- Authentication software/systems- Authentication systems are necessary to manage access to all network resources. It is normally assumed that Microsoft Active Directory authentication is used but additional systems may be required to provide services such as TACACs or RADIUS for specific services.
- Anti-virus- Anti-virus is a necessary item for PCI-DSS compliance to monitor and protect the end-point devices. The application of anti-virus software will be necessary on all computers, laptops and servers.
- Computer management console- Computer management software will be used to manage all software including system patches. This system provides a manageable method of software control throughout the organization. These systems depending on type can also generate reports to supplement auditing along with information for technology management.

- Software for documentation of PCI related work such as audit t racking, vulnerability remediation, monitoring efforts, etc. Software may be necessary ranging from SharePoint or equivalent applications to Microsoft office to generate simple spreadsheets.

Tech Stack

Throughout the duration of this project different levels of technical services will be involved. These technical services required can be anything from management to complex technical engineering and architectural skills. Detailed explanation about the required technical services will be provided in this section.

Architecture Details

The configuration of hardware on the network will be performed to fit the purposes of business usability, security requirements of compliance and other security requirements not required by compliance. These three are more described in the following:

- Business usability- There is isolated scenarios when older systems or services are required by the organization to function. These older systems or services may need to be secured through other means or allowed as an exception. The reason for questioning these systems is due to using unsecured protocols such as telnet. Stopping the services would impair the business operations. Other methods to secure this use may be access list on routers or firewalls.
- Compliance security requirements- All hardware and network devices will be configured to the standard requirements of PCI-DSS compliance. Some of these required settings are user authentication, sending all syslog messages to the centralize server, removal of all default settings such as passwords, etc. All

firewalls will be configured to allow only required services across the different network segments. No rules will be used allowing “any” statements or other ways of allowing all network segments or protocols.

- Other security requirements- All network devices will have additional security configurations that may be required beyond the need of PCI-DSS compliance. These requirements may be for the purpose of protecting other confidential data such as proprietary data which is only accessed by specific personnel such as HR documents, organization strategy, competitor information, etc. Another need for additional security configurations is to comply with other regulatory requirements the organization may be subjected to such as HIPPA, SOX, etc.

Resources Used

Throughout the project a number of resources will be required to complete all task for PCI-DSS compliance. The required resources are described in the following:

- Funding- Funding will be budgeted and approved in the initiation phase of the project. This will ensure funding is readily available for the implementation phase when the hardware and/or software are needed.
- Adequate technical staff- Adequate technical staff is required to fulfill both the man power and specific technical skills needed to complete all of the required tasks for compliance.
- Assigned management- Management in this project is a key element to monitor all of the moving parts of the project. Assigned management personnel will be required throughout all five phases of the project to ensure all tasks and personnel remain on track to meet deadlines.

- Additional hardware/software- Depending on the current state of the infrastructure and services additional hardware and/or software may be required to fulfill compliance requirements.
- Executive sponsor- The person fulfilling the executive sponsor role will be required especially from the beginning of the project in the initiation phase to ensure the project starts properly in regards to executive support, leadership, making critical decisions, providing funding, etc.

Final Output

The final result of the project ultimately will be to complete the annual PCI audit. Once all PCI compliance requirements are completed and the approved auditor verifies all the conditions are met the project is considered to be successful. Even through monitoring and remediation efforts will continue after the completion of the audit the project goal has been reached based upon its intended purpose.

Quality Assurance

The quality assurance portion of this project is conducted in the verification phase of the project. This set period of time was specifically created as a method of checks and balances for all work and other efforts performed for PCI compliance. During this phase all documentation and technical work performed will be verified to ensure accuracy before the audit is conducted. Based on past experiences when a system of task verification isn't in place the risk of audit failure is increased due to task being missed or performed incorrectly.

Quality Assurance Approach

The verification phases of the project will be used to check all work performed and documents produced for the project. Way too often PCI and other types of regulatory tasks are

not verified as complete or accurate which causing problems for the organization which is in a rush to remediate. During this phase the following will occur:

- Verify all policies are created as described in the compliance requirements.
- Verify all processes are created as described in the compliance requirements.
- Verify all vulnerabilities from pervious internal and external network scans are completed.
- Verify that all personnel completed annual security training and is properly documented.
- Verify that change control process is implemented and operating as designed.
- Generate all necessary reports for auditing (clean internal and external network scans, etc.)
- Produce all other documents (firewall reviews, patching, updates, etc.)

Solution Testing

These details of this project were not officially tested but successful results were produced when implementing a similar program created a few years ago and continuously used for annual audits. During my experience with PCI auditing similar templates and documents were created but were not as detailed as those delivered in this project and were able to satisfy PCI requirements. I have also passed the same documents and templates I had created to other departments which simplified their auditing approach and documentation efforts.

Implementation Plan

This section of the document contains information relating to the implementation of PCI compliance efforts. The implementation strategy for this project was carefully considered to ensure that any organization using this strategy would have an increased level of success when

working through compliance or other similar regulatory compliance standards. This discussion will also include the resources, training and documentation required to completing the audit process.

Strategy for the Implementation

The phased approach produced for this project is deemed the best strategy for PCI implementation due to its modular grouping of similar functions. The reason being all similar functions are performed in the same phase which eliminates confusion and mistakes from performing dissimilar functions. This also allows the project coordinator to manage the project as a whole easier by having a tighter focus on a smaller set of ongoing tasks. Each phase also has a small set of simple milestone which allows the team to progress to the next phase once all are completed. Once the team enters into the fifth phase this means the auditing process for the organization is complete and returns to normal operations but continue with scheduled PCI tasks.

Phases of the Rollout

The organization will first go through the initiation phase which the team will begin the process with the ultimate goal of completing the annual audit. This phase is used to prepare and plan before moving into the implementation phase. The implementation phase is the one which takes the most effort with the creation of documentation, performing all technical work to ensure all security requirements are met. The third phase is for verification which is basically used to verify the all work efforts performed to ensure accuracy of information. This phase was created to test the correctness of all compliance requirements and was intended as a first line defense to make any corrections or changes before the auditing proceeds. In the verification phase all policies, procedures, technical work performed, etc. will be checked against the requirements in use. Once the project coordinator feels confident about the status of the project they can make

the judgment call to move forward into the auditing phase. During the auditing phase the team will work with the auditors to ensure all documentation and other information is surrendered to complete the audit. During the auditing process the auditor may find some minor discrepancies which the organization would have a brief timeframe to make any adjustments or corrections. The audit phase will be complete once the auditor determines the organization's efforts and documentation satisfies the requirements of PCI compliance and gives formal approval. When the auditing phase is complete the organization will return to normal business operations with the exception of performing routing task such as monitoring and security remediation. Monitoring and security remediation is required to be performed through the remainder of the year until the repeat of the cycle in the following annual audit.

Details of the Go-Live

The project will be fully implemented once the fourth phase or auditing is complete. The end of the auditing phase means the organization has met all of the PCI compliance requirements. During this time the approved auditor will provide the organization with formal approval of the auditing process. The project lists the fifth phase which is used to conduct periodic tasks and other actions that are integrated into daily business operations. By the completion of the fourth phase the main purpose of the project has been fulfilled and the team will return to normal business operations. Once the fifth phase ends and it's time for annual auditing the cycle will repeat itself annually.

Dependencies

The strategy of this project is based upon a phased implementation plan which takes all participants through a series of defined steps which have to occur in a pre-set order. Due to this method of approach each of the phases will have to occur in exact sequential order. Neglecting to

take action upon individual tasks or bypassing one of the phases entirely will greatly increase the risk of obtaining PCI-DSS compliance or incur a great time delay in completion of the auditing process. This is especially the cases for specific action items that are time consuming such as technology documentation, policy creation, etc.

Deliverables

The main form of deliverables is the documents created for this project. The documents can serve as basic guidance and can be adjusted to meet the needs of the organization and compliance requirements as they are adjusted from time to time. Adjustment of the documents provided is also critical since the standards will continuously change over time as new threats emerge. In regards to PCI efforts documentation is crucial not only to ensure the work performed is correctly but also to ensure the work is actually being performed and produces a paper trail of what was done.

Training Plan for Users

Users will be trained annually in regards to general technology security during the first quarter of the calendar year. The training will be conducted by someone from the technology team or technology management. The person that is assigned this task will coordinate and schedule with the business department to ensure all personnel are available. Topics to be covered during the training are general security items, new trends in threats for users to be made aware. Any changes in technology policies will also be discussed during this time. Documentation of security task such as protecting confidential information, password security, and defense from social engineering will be provided to support the training along with current technology policies which can be accessed on demand. Additional training must also be provided new business impacting threats and to support newly implemented technologies. An example of this is

employees encrypting emails with confidential data. If the organization expects all users to perform the requirement along with ensuring it's performed when needed and correctly training must be provided.

Depending if the organization sees fit they may provide training for the staff spearheading the project to ensure they are aware of the process from start to completion. This would be especially helpful for teams who are new to PCI compliance and needs additional assurance all requirements, processes and action items are understood. Training of this nature can be provided by an approved auditor or organization that specializes in this type of training.

Risk Assessment

As with all projects and business related initiative proper planning requires a risk assessment which involves an analysis of all risk the organization will encounter. During this project some specific risk were recognized and a brief summary explaining the risk along with risk mitigation techniques will be provided.

Quantitative and Qualitative Risks

There are a few risks related to obtaining PCI-DSS compliance. Listed below are the critical risks with a brief description of each:

- Misinterpretations of requirements- The organization can be put at great risk if the information listed within the twelve requirements are misinterpreted. This type of action would cause the incorrect actions to take place and prevent compliance depending on time and size of tasks.
- Device misconfiguration- If any device is misconfigured and recognized during the auditing process, this pay put the project at risks of not being complete.

- Obtaining appropriate hardware- Obtaining the proper hardware to enforce security and compliance can produce a large delay in the project completion. If this occurs obtaining the proper devices may take weeks or months depending on availability.
- Availability of third party personnel- The availability of third party personnel could create time delays and put the project at risk of timely completion. Since third party personnel rely on assisting other customers the risks of being available when needed is high if not properly planned.
- Missing compliance deadline- The main reason for missing compliance project deadlines would be related to mismanagement of personnel or tasks completion. This sometimes will occur when other business priorities are pushed ahead of the needs of compliance.
- Inability to become compliant- Not being able to become compliant especially when the organization is in great need to process credit cards can greatly impact not only the businesses revenues but also customer confidence. If the organization was previously compliance but are currently missing requirements the credit card processor can impose fines against the organization dependent upon the severity of the situation. If the organization is not compliant this will also affect the investors and shareholders if the organization is publicly traded.
- Lower security levels and awareness- If the organization is not able to conform to the compliance requirements they increase the risk of being exposed to many security threats. Organizations that don’t apply many of the common best practices leave themselves exposed to loss of confidential information, security

breaches and other malicious activities. The organization will not only be affected by the action itself but also held responsible for any items that could have been prevented.

Cost/Benefit Analysis

The implementation of this project will incur some cost throughout the five phases depending on the organizations ability to perform the audit, technical requirements, third-party intervention, etc. The total cost will be dependent upon mainly the size of the organization and the project related resources that are available within the organization. These and other related factors are described in detail below:

- Supplemental technical personnel- Supplemental technical personnel will be required to assist and provide technical guidance in areas where current staff is not skilled. This will be an additional expense to the project but if technical contractors or vendors in this area can assist the current staff can reuse the work learned to continue the same process when needed again without the additional expense. Not using additional technical personnel could risk PCI compliance due to failing compliance and not being able to process credit cards or be subjected to fines from the card processor.
- Additional auditing guidance- Additional auditing guidance may be required especially when the organization will perform this project for the first time. The organization can take the new information from this experience and reuse during the next following auditing cycles. The risk of not obtaining this resource will put the company at risk of not performing the required task correctly or not fulfilling all of the requirements directly related to the organization.

- Failure to purchases required hardware/software- In some cases the requirements for compliance will demand additional hardware and software. In these instances the new resources will be able to satisfy the requirements along with increasing the security posture of the organization. The cost associated with this would be greatly dependent upon the current state of the organization's infrastructure. If the organization has kept up with current technology the expense will be minimal whereas the organization that has slow to update technology hardware and software this expense will be greatly increased. Not performing the necessary upgrades will risk the organization from being compliance along with exposure to possible security breaches. The estimates for this cost would range from $10,000.00 to $200,000.00 depending upon current state of infrastructure.
- Reduced security procedures- An organization that doesn't follow through on implementing the actions required by PCI compliance risk operating at lower security standards. The best practices recommended by the PCI standards are general practices in the industry and if not implemented an organization is at higher risk of data breaches and information loss/theft. The effects on the organization can range from financial losses in fines, liabilities, etc. to damages in reputation and customer confidence. (PCI Security Standards Council, 2006) Depending on the type of security incident which can occur within an organization the business can be affected for years.
- Failure to gain PCI compliance- If the organization being subjected to compliance is not fully compliant there are some financial and operational impacts to consider. Depending on the credit card processor requirements and current

contracts the organization may be subjected to fines based upon the facts revolving around failing compliance. The fines for failure to meet compliance ranges from $5,000.00-$500,000.00 monthly until the requirements are completed. (MiJireh Checkout, 2014) Depending on the critical nature and/or contract requirements the organizations ability to process credit cards may be terminated. There are other repercussions for not being compliant such as risk of lawsuits, government fines, and loss of customer confidence. Customer confidence is critical in this case and longer lasting since if another organization is able to process their purchases. The customer may prefer not to do business with an organization due to its inability to safely process their credit card payments. The ability not to process credit cards would impact the organization if they are not able to process credit cards. This problem would be more impacting upon organizations that rely heavily on this method for customer payments such as an online retailer.

Risk Mitigation

During the creation of this project there were a few risk items that would create completion delays or the risk the organization being able to process credit cards within the timeframe required. Listed below are the risk mitigation techniques that will be discussed and implemented:

- Misinterpretations of requirements- This risk will be mitigated by hiring a third party consultant to review the requirement to ensure the interpretation is accurate and the organization isn't misled and put a great deal of effort into performing incorrect actions. This can produce additional delay into the project plan. It may

be safe to approach a third party or a consultant to review the requirements to ensure any minor misinterpretations are prevented.

- Device misconfiguration- Device configuration risk will be prevented by holding peer-views before submitting the configuration changes to the change control team. When the configuration change is submitted the team manager will also review the changes also. This will enable to the configuration to be double checked to ensure accuracy. The problem can be easily resolved with minutes or can be severely impacting depending on the amount of wrong configurations and the number of devices that require correcting.
- Obtaining appropriate hardware- Obtaining the wrong hardware causes great time loss and other indirect problems. Depending upon the availability of the required hardware the project can be delayed one to eight weeks to receive necessary hardware. When vendor recommends hardware the internal team will perform research and verify hardware data sheets to ensure correct hardware is being ordered. If team needs additional verification a consultant can be used to verify the hardware against the needs of the organization.
- Availability of third party personnel- Sometimes compliance problems arise when current personnel are missing specific skills, mostly technical to support compliance efforts. Third party personnel can be used to augment current staff temporarily in order to complete compliance tasks and maintain timelines. If compliance efforts are taking place in a large organization partnering with multiple third-party vendors may ensure that experienced personnel are available to assist if needed immediately.

- Missing compliance deadline- Timeliness completion of task will put compliance and other project at risk of being completed on time. If project timelines are missed, depending upon the situation the organization may be delayed in processing credit cards or possibly required to pay large fines. To mitigate this risk the project coordinator will need to place the appropriate time to perform task with buffer time between tasks. The buffer time will be used to compensate for any delays outside control of the team (sick personnel, business emergencies, resource delays, etc.).
- Inability to become compliant- The inability to become compliant is a great risk that can become costly to the organization. This can be mitigated by accurate time and resource management. This would affect organization revenue if not able to process credit card customers and also affect expense accounts by payments in fines to the credit card processor. The project coordinator will need to ensure that all time and tasks are being tracked as accurate as possible. During the project rollout senior management needs to be kept current on status. Also this is important when project delays are inevitable and crashing the project time with additional resources may be required for timely completion.
- Other business needs- Its common today in busy business operations urgent needs arise quickly and without warning. If this occurs during the PCI process management will be required to determine the priority and to ensure resources are being allocated with the most critical projects. In cases where resources are pulled off the PCI efforts the project coordinator must be immediately aware in order to adjust the schedule or get additional personnel from a third party or other sources.

Post Implementation Support and Issues

The following section will discuss the post-implementation support required for the success completion of the project. This area will also provide detailed information in regards to post-support for PCI compliance tasks which continuous during a predetermined schedule outside of the annual audit cycle. After the audit cycle the organization will continue to monitoring systems, performing other scheduled checks and performing remediation efforts towards new threats.

Post Implementation Support

Once PCI-DSS compliance is obtained the auditing process will be required annually. Someone within the organization would be assigned the responsibility of spearheading the annual auditing process. This is normally assigned to someone in management of the technology team or auditing/compliance team. The person assigned to this role would be responsible for tracking all required tasks throughout the year such as monitoring, documentation, etc. This person would also be responsible for the collection of all necessary documentation for future use or auditing purposes. Along with the person to continuously monitor the compliance tasks technical staff will also be needed to continue the complete periodic tasks and continuing monitoring of systems.

Post Implementation Support Resources

After completion of the project there are some last items to complete. The completion of these items will ensure the information from current audit is stored, lessons learned or process corrections for the following annual audit are properly documented. Once all of the information is collected and stored in a secured location this post implementation requirement is completed. The project coordinator will ensure the information gathering is complete after the auditing

process. Another crucial part of compliance is continuing the monitoring and maintenance tasks required for compliance such as firewall rule reviewing, syslog message monitoring, security training, etc. A person will need to be assigned to ensure these continuing tasks are taking place and being documented. The person responsible for the continuing monitoring and maintenance tasks preferably would need to be in IT management to ensure the correct tasks are being completed as required.

Maintenance Plan

A long term maintenance plan will be required throughout the year to ensure all compliance tasks are being performed as needed and on time. When the tasks described in this section are complete the action item must be documented along with date of completion for future auditing purposes. The basic maintenance schedule is shown below:

Task Description	Date Required	Notes/Instructions
Firewall rule review	Bi-annually	All firewall rules will need to be reviewed to ensure they are required by the business to operate. Any rules not required will need to be removed during an approved maintenance window.
Syslog message review	Daily	All syslog messages must be reviewed daily to ensure if any security breaches or other security related issues are recognized and resolved immediately.

Rogue access point scanning	Quarterly	All locations within the organization will be scanned to ensure any rogue (unauthorized) access points are not on the network. If any are found they will need to be removed immediately.
Process correction	Bi-annually	Any corrections to processes due to organization, technical or compliance requirement changes must be documented at this time to ensure problems are created on the following audit.
Change control procedures	Daily	Change control procedures will continue to be used on a daily basis. All changes will need to be documented and retained for future use when needed by auditors.
Compliance requirement review	Prior to audit	Prior to the upcoming all compliance requirements must be reviewed to ensure no changes or process adjustments have been made since the previous audit. The standard documentation for PCI-DSS will need to be reviewed.
Anti-virus definition updates	Daily	Anti-virus definitions must be updated daily to ensure immediate protection against new threats. This will have to be set up on both

		maintenance server, other servers and user computers
Internal network scanning	Monthly	Internal scanning of all network devices and components (computers, printers, etc.) will need to be conducted once a quarter to ensure that all new threats are recognized and reviewed.
External network scanning (penetration testing)	Monthly	External scanning of all external (public) ip addresses will need to be conducted once a quarter to ensure that all new threats are recognized and reviewed.
Urgent remediation efforts	As soon as required	Urgent remediation efforts will need to take place when high priority vulnerabilities are detected. A plan of remediation will need to be created, reviewed and documented into the change control process to move forward. Once the remediation effort is complete the device will be re-scanned to ensure the vulnerability has been resolved. If the vulnerability is still present after re-scanning further review will need to take place along with another attempt at remediation to correct the problem.

Conclusion, Outcomes, and Reflection

The following section provides summary information about the project. In this area we will also cover the solution provides in the project, any short comings of the solution and common pitfalls an organization working through PCI compliance task will encounter.

Project Summary

The project was conducted to provide guidance along processes and other resources to assist any organization being held to PCI compliance. The problems noticed by some organizations especially those which are new to the compliance requirements fail to process all of the information correctly. Another reason for failure is not creating a systematic approach to performing work and managing all tasks. This document provides a systematic approach which groups all similar functions accordingly along with a phase for verification of work and requirements before the auditing process is started. Once the auditing is completed the organization is also provided guidance on the task that still depends on periodic attention and documentation until the next annual audit begins repeating the process.

Deliverables

The project produced the documentation that will guide the organization through their PCI-DSS compliance efforts. The documents created are intended for general instruction but can be easily customized to meet the needs of the organization. The deliverables are described in further detail below:

- Explanation of the five phase approach (Appendix-A)
- Project Personnel Assignment (Appendix-B)
- Budget Draft (Appendix-B)
- Preliminary Technology Assessment (Appendix-B)

- Documentation of Known Security Concerns (Appendix-B)
- Change Control Integration (Appendix-C)
- Change Control Submission Form (Appendix-C)
- Compliance Documentation (Appendix-C)
- Summary of PCI-DSS Requirements (Appendix-C)
- Annual Employee Security Training Topics (Appendix-C)
- Technical Recommendations (Appendix-C)
- Job Roles Description- Example (Appendix-C)
- Firewall Rule Review Document-Example (Appendix-C)
- Verification (Appendix-D)
- Maintenance Schedule (Appendix-E)

Outcomes

The idea of this project was based against the problems I personally encountered with past PCI compliance audits. The implementation of a phased approach was similar to a process I had created for the team I managed and have achieved successful results. Similar methods used in this document enabled me to complete tasks ahead of schedule and complete tasks and remediation efforts the first time. In this project I took some of the procedures I had created in the past, expanded to other areas besides network devices and provided additional information intended for organizations obtaining PCI-DSS compliance from the start.

During past audits using a similar processes have produced surprising results with auditors. Normally when other managers have to go through their first annual review which normally takes an hour, the review of my area would take only 15 minutes due to the organization of completed tasks and constant requirement maintenance. I have received positive

feedback from the auditors such as “Your area is the easiest to audit due it being simple and organized”.

In regards to the overall project there are some shortcomings mainly based on personnel assignments and focus. If the business doesn’t assign or acquire the appropriate resources to ensure all task are performed and managed the risk rate for compliance failure is high. This is especially the case for the project coordinator, if this person is not assigned or designates a high level of focus on the efforts toward becoming compliant. If this occurs the project will fall apart and the organization will be fines or risk not being able to process credit cards to conduct daily business transactions.

Overall I feel comfortable about the information produced in the project. I am confident that anyone who is new to PCI compliance would be able utilize the information as a guide for the implementation team and help identify common compliance problems. During my past experience with PCI compliance I was subjected to only the network components. After the completion of this project I feel well rounded and able to provide compliance guidance not only on the network devices but also computer, device, software, access control management, etc. Another learning curve was also becoming familiar with the version 3.0 compliance requirements. Prior to the project I had always worked with previous versions and did not have the opportunity to review the latest version of the document.

Reflection

Even though I have had a few years of experience with PCI-DSS compliance I have still learned quite a great deal while compiling the information for this project. Some of the items learned are:

- Better understanding of previous compliance requirements- Regardless of previous experience in regards to PCI-DSS this project has increased my knowledge. This is mainly due to only being responsible for fulfilling network requirements. Now I have a better understanding of computer, server and other requirements that I was never exposed to in the past.
- New requirements learned with update of version 3.0- Since the implementation of PCI-DSS version 3.0 there have been some changes which some were minor and others where quite major. Since reviewing the twelve requirements of the version 3.0 standard I know have a better understanding where I had gaps in different areas of this version.
- Reducing complexity of auditing procedures- Creating a systematic approach to completing large complex compliance or regulatory projects. I have learned that when the system as a whole is broke down into modular components it is not only easier to track but also to manage and control. In the past I have experienced when projects or problems of this scale are not managed correctly the risk of failure is greatly increased.
- New technical security measures- Due to the tight focus on technical security while performing research for this project I learned about new security measures such as adding firewalls to protect critical resources and/or provide additional filtering. Also learned about a couple new scanning tools that are approved by the PCI council which will come in useful as I start working more in this field.
- Better methods of problem solving- Working on a project such as this enabled me to think deeper about the problem at hand. Researching a problem thoroughly

rather than examining only the top layer helps to not only propose a standard solution but also aids in preventing possible problems indirectly due to the changes made.

References

Why Comply with PCI Security Standards? (2006, January 1). Retrieved September 15, 2014, from https://www.pcisecuritystandards.org/security_standards/why_comply.php

What you need to know about PCI Compliance. (2014, January 1). Retrieved September 15, 2014, from http://www.mijireh.com/docs/what-you-need-to-know-about-pci-compliance/

Mills, E. (2010, February 8). PCI compliance: What it is and why it matters (Q&A). Retrieved September 18, 2014, from http://www.cnet.com/news/pci-compliance-what-it-is-and-why-it-matters-q-a/

Appendix A- Supporting Documents for Five Phase Approach:

Five Phases for PCI Implementation:

Phase-1 (Initiation)	
Phase Details	This phase is the first step into the compliance process which the organization has the opportunity to focus on compliance requirements and starts the planning of the project. Components of this phase are the following: ▪ Perform initial assessment ▪ Draft any budgetary requirements and expedite approval if necessary ▪ Assign responsibilities to team members ▪ Assign management personnel to oversee the efforts ▪ Initial review of PCI standards and any possible changes in revisions from previous year ▪ Gather input from all team members about project planning and coordination ▪ Determine weak points **All items within scope of PCI compliance are considered any network device or application which transmits or transports for credit card information is within scope. If not certain if this rule is applicable to specific devices or systems either consult with an auditor or assume that it is within scope. ** All relevant information regarding full details about the twelve requirements can be obtained from the following Internet site: https://www.pcisecuritystandards.org/

Phase-2 (Implementation)	
Phase Details	The next phase of the project is implementation which starts the main efforts of PCI compliance. This is the time where policies are created, technical work is performed and other requirements are performed and documented. Components of this phase are the following: ▪ Create policies and procedures ▪ Manage integration of procedures into business operations ▪ Create standard templates to ensure information presentation is consistent year after year

	▪ Implement technical requirements (configurations, etc.) ▪ Implement new hardware and software where needed ▪ Implement change control procedures ▪ Perform any internal or external scanning (if needed at the time) ▪ Perform internal or external penetration testing (if need at this time) ▪ Verify all applications meet the needs of compliance ▪ Ensure all restricted areas are protected against unauthorized access ▪ Plan security training for employees **This phase will require the standards be performed within the specifications based upon the instructions that can be found at the PCI security standards organization link provided in the verbiage in the prior phase.

Phase-3 (Verification)	
Phase Details	The third phase of the project of verification and was created to verify all of the work performed in the second phase and to prepare for the auditing phase. This time is used to check all work performed up to this point against the PCI requirements. Components of this phase are the following: ▪ Check completion of all requirements ▪ Ensure all business procedures (change control, hardware implementation, etc.) are in place ▪ Set up preliminary discussions with approved assessor ▪ Generate necessary reports of current vulnerabilities ▪ Perform security training for employees ▪ Contact qualified auditor to schedule and prepare for audit ▪ Start internal preparation for audit process **This phase demands the highest level of scrutiny due to ensure accuracy and success of audit as a whole.

Phase-4 (Auditing)	
Phase Details	The fourth phase of the project is auditing which involves all personnel involved in the project along with the services of a qualified auditing vendor. During this phase all work performed in the prior phases will be verified along with all documentation of required policies and procedures. Components of this phase are the following: ▪ Have assessor ensure all the requirements are complete ▪ Generate any reports required for audit ▪ Remediation any requirements that are not met ▪ Deliver all documentation to auditor (policies, procedures, etc.) ▪ Make any corrections based on auditors findings **This phase requires all auditing document including that received from the auditor be categorized and secured in a centralized location for future retrieval if needed.

Phase-5 (Maintenance and Monitoring)	
Phase Details	This final phase is maintenance and monitoring and is used for performing maintenance and continuous monitoring of systems. Components of this phase are the following: ▪ Document any continuing efforts for improvement ▪ Implement and corrections or lessons learned during the audit ▪ Save all auditing information for immediate retrieval if needed and as reference for next year's audit ▪ Perform all internal and external network and devices during time frames as required ▪ Perform all internal and external penetration testing during the time frames required ▪ Continuous monitoring of syslog messages and device alarms ▪ Auditing of firewall rules during time frame as required by compliance ▪ Perform all wireless scan at all locations quarterly

	▪ Creating documentation of all work and related task performed during the year ▪ Checking all manufacturers for patches and updates for all organization owned hardware and software monthly ▪ Immediate remediation of vulnerabilities categorized as high priority **This phase requires that all work performed during this phase is documented in the highest level of detail to ensure the auditor can confirm the work was performed to the required level of standards required by compliance.

Appendix B- Supporting Documents for Initiation Phase:

Project Personnel Assignment:

Role	Person Assigned	Role Requirements
Senior Management Sponsor		Senior management liaison to support budgetary needs, decision making support, etc.
Technical Management		Provides leadership of technical personnel, assignment of resources and a point of escalation when needed.
Technical Lead		Technical point of contact to verify technical information.
Technical Personnel (Computers)		Point of contact to carry out work and remediation efforts in regards to computers, laptops, printers and other user devices.
Technical Personnel (Servers)		Point of contact to carry out work and remediation efforts on servers, storage and other related devices.
Technical Personnel-(Network)		Point of contact to carry out work and remediation efforts on routers, switches, firewalls, wireless and other related devices.
Project-Audit Coordinator		This person is the focal point for the entire audit. This person will provide the oversight for all technical and business efforts along with working with the senior management sponsor on reporting and other related tasks.
Insert additional personnel role name here		Additional personnel assigned depending upon size of organization, specialized needs, third party, etc.
Insert additional personnel role name here		Additional personnel assigned depending upon size of organization, specialized needs, third party, etc.
Insert additional personnel role name here		Additional personnel assigned depending upon size of organization, specialized needs, third party, etc.
Insert additional personnel role name here		Additional personnel assigned depending upon size of organization, specialized needs, third party, etc.

Budget Draft:

Hardware/Software Required	Business Justification	Vendor	Quantity	Unit Price	Total Price
Example: Cisco 5505 ASA Firewall	*Required to protect the outer perimeter of the network, enforce network security policies and required for PCI-DSS compliance.*	*CDW*	*2*	*$3,500.00*	*$7,000.00*

Total

Preliminary Technology Assessment:

Requirement	Status	Need for action	Notes
Are outer perimeter firewalls present and in full operation?			
Do all computers, laptops and applicable mobile devices have anti-virus software installed, configured and updated daily?			
Do all servers have anti-virus software installed, configured and updated daily?			
Do all network devices and servers have syslog services configured and directed to a centralized repository?			
Do all network devices and servers utilize external authentication that will lock out the account after multiple attempts?			
Is the organization currently using wireless for an alternative means of access?			
If wireless is used are internal and external users separated along with access rules in place?			
Is there a change control program in place to support, review and approve all technology changes?			
Is there currently a separate of duties and job rotation policy or procedure in place?			
Are all computers, network devices and other critical resources synchronized with a centralized time server?			
Are all network and other critical device configurations backed up to a secure centralized location?			

Are all laptops and other devices currently utilizing hard drive encryption?			
Does the organization use any type of remote connectivity utilizing public transport services such as VPN, RAS, etc.?			
Does the organization have any network LAN connections that are in an unsecured or public area?			
Does the organization use group policy or other technical restrictions limiting users from manipulating computer settings?			
Does the organization have any current technology policies such as computer use, protections of confidential information, media destruction, etc.?			
Does organization have processes or procedures to add or remove employee accounts?			
Does the organization have a current information technology inventory along with documentation of all network devices in production?			
Does organization have protected areas within the facility which are controlled from unauthorized access?			
Does organization send or transport confidential information offsite? If so how is this handled?			
Is there any type of file integrity software or other means in place to detect any file tampering?			
Is there a system or process in place to detect rogue access points within the facilities?			
Is internal or external scanning take place currently?			

Is any type of intrusion detection software or systems currently in use?			
Have any risk assessments been performed in the past year?			
Are areas that contain network devices, servers and other critical technology devices secured with restricted access?			
Does organization have any DMZ segments or networks that allow inbound connections from the Internet? Examples would be customer access, vendor access, etc.			
Do the users within the organization currently conduct annual security training?			
Do all users have unique login ID's?			
Is there currently an incident response plan in place?			
Has the organization had any security incidents within the past year? If so please provide documentation.			
Does the organization use applications or other services that require the use of unsecure protocols such as telnet, ftp, etc.?			
Does the organization have a policy or process to patch all devices, servers, applications, etc.?			
Does the organization have a password policy to ensure the information is kept safe along with timely rotation?			
Does the organization have a process of reviewing new technology for implementation and/or addressing security concerns?			

Documentation of Known Security Concerns:

Item of concern	Notes
Example: Organization has problems with employees becoming victim of phishing emails	*Method to overcome this problem would be adding phishing attempt methods and prevention to annual security training. Explore the option of using technology (hardware or software) as prevention techniques.*

Appendix C- Supporting Documents for Implementation Phase:

Change Control Integration:

Change Control Requirement (in order)	Status	Notes
Ability to develop applications or test changes in an environment that is separate from production applications and/or systems		
Change process for implementing security patches or other required code		
Process for documenting all requirements and business justification for changes		
Created scheduling requirements based on type of critical nature of change		
Ability to document impact of changes upon organization		
Ability to document impact of changes upon the organization if not performed		
Method of discussing via committee or other meeting type to discuss change information with peers or impacted personnel		
Ability to produce formal authorization of changes by management personnel		
Process for pretesting and post-testing to ensure systems are operations both before and after changes occur		
Rollback procedures for changes to ensure systems can be restored to the pre-change state of operations		
Process for communicating changes to appropriate personnel of approvals or rejections of changes		
Process for closing all documentation for completed changed and saving documentation in a centralized location.		
Primary person responsible for leading and controlling change control efforts		
Assembled change control board to review, approve and control other process initiatives		

Change Control Submission Form

Submission Information	
Submitted by	
Date of Submission	
Date and time of changes to be performed	
Change number (Assigned Identifier)	

Change Information	
Change to be performed	
Systems to be affected	
Personnel affected by change	
Personnel requiring communications about the change	
Business justification for changes	
Impact of not performing changes	

Change Action Items	
Steps to perform pre-testing	
List of steps to perform changes	
Steps to perform post-testing	
List for steps for rollback procedures (if needed)	

Change Approvals	
Was change details discussed with change committee?	Yes or No
Committee approval	Yes or No
Name of committee representative approver	
First line management or department lead approval	Yes or No
Name of first line manager or department lead approver	

Post Change Summary	
Was change performed successful	Yes or No
Was all pretesting and post testing performed?	Yes or No
If not successful provide a brief summary	

If change was successful provide additional information if necessary	
Was change committee informed about the status of the change	Yes or No

Compliance Documentation:

Required Action Item	Status	Notes
Creation of firewall and router rule review policy		
Creation of change control process to review and approve all technical changes		
Procedure to protect encryption keys		
Security policies for protecting card holder data		
Policy for installation and maintenance of anti-virus software on applicable devices		
Policy for identification to identify security vulnerabilities and categorize threats		
Procedures for the application of security patches and software modification		
Policy to define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components		
Policy for password use, protections and rotation		
Policy for securing, destroying and transporting media		
Policy for syslog and other log message reviewing		
Process to test for presence of unauthorized access points		
Incident response procedure		
Organizational security policy		
Employee acceptable computer use policy		
Procedure to implement security awareness program		
Policy to manage service providers		
Process for engaging service providers		
Implement a response plan		
Document all network devices and connections		
Diagrams that shows all card data flow through the network		
Document of groups, roles and responsibilities		

Documentation and business justification for use of all protocols and services allowed including insecure protocols		
Document configuration standards		
Document inventory of all components within PCI-DSS scope		
Procedure for configuring/settings of computers, laptop and/or mobile devices for use as assigned by job role		
Procedures for testing or development of applications		
Policy for using two-factor authentication		
Policy for authentication and resetting user passwords		
Policy for authenticating and resetting customer passwords (if applicable)		
Process for user account auditing		
Policy for physical access to public and restricted areas including visitors, vendors, etc.		
Procedure for inspection of all technology devices to prevent threats from tampering		
Document retention policy- log files, syslog messages, audit, change control, etc.		
Documentation explaining use of file integrity software		
Procedure for conducting periodic risk assessments		
Procedure for responding to monitor and analyze security alerts		
Additional customized compliance items		

Summary of PCI Requirements:

Network Devices and Systems:

- Create router and firewall configuration standards
- Apply change control for approving and testing configuration changes
- Maintain up to date network diagrams of all devices
- Maintain diagrams illustrating card holder data flow
- Defined requirements for firewalls with public connections
- Document explaining groups, roles and responsibilities of access to network components
- Document providing business justification for all protocols and services (including both secured and unsecure protocols)
- Firewall and router rule review process conducted every six months
- Allow card holder traffic to only required users and network segments, all others are restricted
- Synchronization of router configuration files
- Implement firewalls between wireless segments and network segments in scope of compliance
- Prevent access from Internet to cardholder network segments
- Implement DMZ segments to protect card holder environment from Internet access
- Configure anti-spoofing on all routers and firewalls
- Restrict outbound Internet access from card holder segment
- Ensure all firewalls utilize stateful packet inspection
- Ensure all card holder systems are placed on internal networks and not DMZ or other external segments.
- Do not disclose private, public or other confidential network information unless there is business justification
- Install firewall software or all mobile devices that have Internet or other than internal network access.
- Ensure security policies and procedures for managing network devices including firewalls are in use.
- Change all vendor default configuration setting on all network devices, wireless and systems
- Develop configuration standards for network devices and systems

- Implement server per service to ensure differences in security settings are enabled
- Disable all unnecessary services and functionality on network devices and systems which may have been enabled by default
- Implement security measures for unsecure protocols
- Encrypt all non-console administrative access
- Maintain inventory of all devices and system within PCI-DSS scope
- Maintain policies and procedures for managing vendor default settings
- Ensure third-party providers are protecting organizations internal network segments

Protecting Card Holder Data:

- Store minimal card holder data as required
- Do not store sensitive data authentication information
- Do not store magnetic data or card chip information, verification codes or PIN numbers
- Mask PAN when displayed
- Render the number unreadable in the event of unauthorized access
- Use disk encryption where applicable on systems
- Document procedures to protect encryption keys and restrict information to only those required
- Procedures for storing private and private encryption keys
- Procedures for generating strong encryption keys
- Ensure secure encryption key distribution and storage
- Process for handling used encryption keys
- Destruction of used or compromised keys
- Use of split knowledge or dual controls for clear-text encryption keys
- Procedure to protect against and prevent substitution of cryptographic keys
- Process for authorized encryption key custodian
- Use strong encryption and security protocols to transmit data
- Ensure wireless segments to transmit card holder data is encrypted
- Process to prohibit transmission of unprotected PAN information
- Ensure all security policies and procedures are in use to protect hard holder data

Maintain Vulnerability Management Program:

- Deploy and configure daily updates on anti-virus software on all computers, servers and other applicable systems
- Periodic review of devices not commonly affected by malware

- Ensure all anti-virus programs generates audit logs and settings cannot be altered by users
- Ensure security policies and procedures are in use to protect against malware
- Implement process to identify security vulnerabilities along with risk ranking
- Process to review and implement vendor applicable patches within one month of release
- Process for developing secure internal and external software
- Ensure removal of test or other unnecessary accounts from production systems.
- Process to review of custom code prior to activation in production environment
- Implement change control process to review, test and approval configuration changes of network devices and other systems
- Implement change control process for security patch and other software modifications
- Process to address common coding vulnerabilities
- Ensure policies and procedures are in use to maintain secure systems and applications are in use

Implementing Strong Access Control Measures:

- Limit access to systems and card holder data only to those required
- Document need for access to systems depending on role
- Restrict access to system to privileged users necessary to perform job functions
- Assign access based on job function
- Process for approving system access by authorized personnel
- Establish access controls to systems that restricts access to only authorized personnel
- Ensure that all policies and procedures for restricting access to card holder data are in use
- Establish policies and procedures to ensure user identification for system components
- Process for additions, deletion of modification of credentials
- Process to invoke access due to termination
- Process for reviewing and removal of accounts every 90 days
- Process to manage vendor accounts
- Implement account disabling after more than six failed access attempts
- Set account locks to thirty minutes or when an administrator enables the account
- Procedure for users to re-authenticate after fifteen minutes of inactivity
- Implement use of dual-factor authentication to systems
- Ensure that all authentication protocols utilize strong encryption to protect information during transmission
- Process to verify users identity prior to modifying credentials

- Implement organizational password policy to use PCI criteria
- Implement password rotation procedures
- Procedure to prevent re-use of passwords until after a set amount of passwords have been used
- Procedure to allow password reset after first time of use
- Implement dual-factor authentication for remote access from external network segments
- Document and communicate authentication procedures and policies
- Polices to prevent use of common or generic usernames and passwords
- All vendors must have unique credentials to access internal systems
- Ensure unauthorized access to databases are prohibited
- Ensure all security policies and procedures are in use for identification and authentication
- Limit physical access to card holder environment systems
- Use of cameras and access controls to monitor physical access to restricted areas
- Implement physical access controls or restrict access to publically accessible network jacks
- Restrict physical access to all network devices, systems and mobile devices
- Implement procedures to distinguish onsite personnel, vendors and visitors
- Control access to sensitive areas based on job function
- Implement procedures to identify and authorize visitors
- Process to authorize and escort vendors prior to entry into sensitive areas
- Visitors and vendors are required to present and surrender a type of identification
- All vendors and visitors must sign into a log book during entry and out during exiting
- Procedure to secure and store all media
- Process to classify media due to sensitivity
- Procedure to transport media by secured courier
- Ensure media requires management approval prior to removal from secured area
- Maintain strict control over storage and accessibility of media with log books and media inventory
- Process to destroy media when it’s no longer needed.
- Procedure to protect devices that capture card holder information
- Maintaining a current list of devices including location, make and model
- Periodic inspect all devices for tampering or modifications
- Train all users to detect any tampering and modifications to devices
- Ensure security policies and procedures for restricting physical access to card holder data are in use

Maintaining Information Security Policies:

- Establish and maintain an organizational security policy
- Process to review the organizational policy annually
- Implement a risk assessment process defined in the PCI requirements
- Implement computer usage policies for users to define appropriate use of all technical devices
- Process to accurately determine device owner
- Maintain a list of company approved devices
- Procedure to terminate sessions for remote access during a specified period of inactivity
- Process to activate remote access for vendors and other third part users with immediate deactivation after use
- Ensure all security policies and procedures are clearly defines information security to all personnel
- Assignment of PCI specified responsibly to individual or team
- Process to train new hire and current personnel at least annually regarding information safeguarding and security
- All personnel must acknowledge required training by the organization
- Implement process to screen personnel prior to hiring
- Polices and process to manage service providers as listed in PCI standards
- Implement an incident response plan for vendors or third-party groups
- Process to test the incident response plan annually
- Process to provide training to staff in regarding security breeches
- Process to review and process alerts and alarms
- Implement process to modify and update incident response plan

Annual Employee Security Training Topics:

Subject	Annual, other training or urgent	Reason	Has subject been approved for addition to training plan
Phishing techniques and prevention	Annual	Current threat	yes
Social engineering	Annual	Current threat	yes
Malware	Annual	Current threat	yes
Add additional subjects			
Add additional subjects			
Add additional subjects			
Add additional subjects			
Add additional subjects			
Add additional subjects			
Add additional subjects			

Technical Recommendations:

Computers and Servers	
Computers-Group and user policies	Ensure the groups and user policies are configured on all computers and laptops. Ensure that any user is not able to install, remove or manipulate software or settings.
Servers- Groups and user policies	Ensure that all users of the server are able to access only approved resources and services. Administration will also need to be isolated to authorized personnel for administration of the server.
Anti-Virus (computers and servers)	All computers and servers will require anti-virus software which will automatically update the latest signatures. The software will need to be configured to not be altered by the users of the device.
Encryption- Laptops	Apply drive encryption to laptops since they are mobile and can be easily removed from the work environment.
Host Intrusion Detection (Recommended)	Install HIDS (Host Intrusion Detection Systems) to detect if a system has been compromised or has any traffic with abnormal patterns
Laptop Firewalls	Ensure that all laptops have firewall software and automatically enabled when not on the internal network.
Computer and server patching	Ensure that all computers and servers are being patched periodically according to the operating system vendor.
Software/Application patching	Ensure that all computers and servers software/applications are being patched periodically according to the operating system vendor.
Logging of security and software problems	Ensure that all security and software is creating security logs which report to a centralized location and is not able to manipulate by the user.
Time synchronization	Ensure that all network devices have time synchronization configured to a centralized device. Once configured ensure that all devices have the same time and date being used.
User accounts	Ensure that all users will log in with individual accounts which have the authorized rights and restrictions configured.

Networking Devices (Routers, Switches and Wireless)	
Router and Switch authentication	Ensure that all routers and switches have external authentication (TACACS, RADIUS, etc.) to authenticate against users with individual accounts. Back accounts can be configured in the event of external authentication failure. The backup account information will be secured until needed. The account passwords will be rotated every 30 days for added security.
SNMP settings	All devices will have SNMP configured and will be utilizing SNMP version 3 for the highest level of security.
Remote Access	All routers and switches will be configured to use SSH version 2 or higher. No telnet or other unsecure protocols will be allowed to perform administration functions.
Unnecessary services	If routers or switches have unnecessary services which are not required for business use or administration it will be disabled. Allowing unnecessary function to remain on when not in use may present additional security vulnerabilities.
Allowed subnets for administration	If possible configure access list for administration to only be allowed from approved subnets. This will prevent someone on the network the ability to access device's management.
Access List	If access list are configured on routers ensure that all rules are configured for exact source and destination ip addresses or subnets along with the service protocol. No "any" statements are allowed regarding protocols, source and destination ip addresses or subnets. All rules must have a specific business justification to be implemented.
Device security	Ensure that all network devices are not installed in public areas. These devices will be installed in areas which are locked and prevents access to unauthorized personnel
Port security (Recommended)	Enable port security on switches where possible to ensure users or unauthorized personnel cannot move or access network resources without authorization.

Public accessible LAN ports	If the organization has any network ports accessible to the public business justification must be documented and port security must be enabled. If possible the Mac-address of the public device (IP phone or computer) to ensure if removed another device cannot connect to the network.
Wireless	Ensure that all wireless networks have to access internal network resources through a firewall. If a system is not implemented to monitor Rogue or unauthorized access points ensure that all areas or locations are scanned quarterly with the necessary detection software.
Device updates and patches	Ensure that all routers and switches are being updated as recommended by the manufacture to resolve any security vulnerabilities.
Device configuration backup and storage	Ensure that all device configurations are collected periodically and stored in a secure location.
Syslog messages	Ensure that all syslog messages are being generated and transmitted to a centralized location for secure storage.
Time synchronization	Ensure that all network devices have time synchronization configured to a centralized device. Once configured ensure that all devices have the same time and date being used.
Network device inventory	Ensure the team maintains an accurate inventory of all network devices.

Networking Devices (Firewalls)	
Router and Switch authentication	Ensure that all routers and switches have external authentication (TACACS, RADIUS, etc.) to authenticate against users with individual accounts. Back accounts can be configured in the event of external authentication failure. The backup account information will be secured until needed. The account passwords will be rotated every 30 days for added security.
SNMP settings	All devices will have SNMP configured and will be utilizing SNMP version 3 for the highest level of security.

Remote Access	All routers and switches will be configured to use SSH version 2 or higher. No telnet or other unsecure protocols will be allowed to perform administration functions.
Unnecessary services	If routers or switches have unnecessary services which are not required for business use or administration it will be disabled. Allowing unnecessary function to remain on when not in use may present additional security vulnerabilities.
Allowed subnets for administration	If possible configure access list for administration to only be allowed from approved subnets. This will prevent someone on the network the ability to access device's management.
Access List	If access list are configured on routers ensure that all rules are configured for exact source and destination ip addresses or subnets along with the service protocol. No "any" statements are allowed regarding protocols, source and destination ip addresses or subnets. All rules must have a specific business justification to be implemented.
Encryption	If encryption is being used for VPN or other services ensure the keys are rotated periodically. Ensure that all keys are secured whether if in use or previously used.
VPN access	If VPN is in use ensure that all VPN access is utilizing dual-authentication for access.
Device updates and patches	Ensure that all routers and switches are being updated as recommended by the manufacture to resolve any security vulnerabilities.
Device configuration backup and storage	Ensure that all device configurations are collected periodically and stored in a secure location.
Syslog messages	Ensure that all syslog messages are being generated and transmitted to a centralized location for secure storage.
Time synchronization	Ensure that all network devices have time synchronization configured to a centralized device. Once configured ensure that all devices have the same time and date being used.
Firewall Implementation	Firewalls for use in a DMZ environment can be used as a single pair for redundancy if properly configured. Additional security can

	be provided with a secondary pair of firewalls behind the first (outer) pair. This will allow the organization to implement an additional filtering mechanism to reach the internal network. Another measure that can be used in a dual-pair firewall environment is utilized different firewall vendors per pair. This prevents software vulnerabilities of one manufacturer to affect the other set of firewalls.
Intrusion Prevention Systems Implementation	IPS units are highly recommended to monitor all access into a DMZ environment. These devices are used to monitor the active traffic activity traversing the patch between the firewalls and servers.
Firewall inventory	Ensure the team maintains an accurate inventory of all firewall devices.

PCI Documentation: Team Roles and Responsibilities (Example)

Summary:

Listed below are the names and description of team members which are responsible for the administration of devices within PCI scope.

Information Listing:

Person's Name	Job Title	Job Description	Other Applicable Information

PCI Documentation: Firewall Rule Review (Example)

Summary:

Listed below are the rules and justification to satisfy the rule review requirements which are to occur every six months.

Information Listing:

Device Name:

Rule Number	Rule	Reason for business operations justification or required removal
	Insert firewall rule	*Insert justification or if not required label field as "remove"*

Device Name:

Rule Number	Rule	Reason for business operations justification or required removal
	Insert firewall rule	*Insert justification or if not required label field as "remove"*

Appendix D: Supporting Documents for Verification Phase

Verification Checklist

Action	Verified as Complete	Notes
Establish configuration standards for all network devices including firewalls and routers (document)		
Create a formal process for approving and testing all network connections and changes (document)		
Create network diagram identifying all connections between card holder environment and other networks including wireless (document)		
Create diagram displaying card information flow through network (document)		
Implementation of firewall at each Internet connection and between DMZ /internal network (document and action item)		
Description of groups, roles and responsibilities of network components (document)		
Create document of business justification for all services, protocols and ports including all unsecured protocols (document)		
Create a firewall rule review scheduled every six months (process)		
Standard for firewall and router configurations that restrict connections between untrusted networks and network segments in card holder environment (document and action item)		
Create and implement standards to restrict traffic to only what's necessary into the card holder environment and specifically deny all other traffic (document and action item)		
Synchronization of router and firewall configuration files (document and action item)		

Install perimeter firewalls between internal network and wireless segments with restrictions to the card holder environment (document and process)		
Prohibit direct public access into card holder environment (document and action item)		
Implement DMZ to limit inbound traffic to only system components allowed (document and action item)		
Limit inbound Internet traffic to IP addresses within the DMZ (document and action item)		
Prevent direction connections inbound into the card holder environment (document and action item)		
Configure anti-spoofing measures and block forged IP addresses from entering network (document and action item)		
Do not allow outbound Internet access from card holder environment (document and action item)		
Configure stateful inspection on firewalls (document and action item)		
Place systems that store card holder information in the internal network, segregated from the DMZ and other untrusted networks (document and action item)		
Prevent disclosure of public IP information (document)		
Install firewall software on any mobile devices and laptops (document and action item)		
Ensure security policies and operational procedures are in place for managing firewalls and routers (documentation)		
Change all vendor supplied default configurations of all network devices including wireless (document and action item)		

Implement one function/service per server that required different security levels (document and action item)		
Enable only necessary services on networks and systems, ensure all unused services are disabled (document and action item)		
Implement additional security features for unsecure protocols (document and action item)		
Configure system security parameters to prevent misuse (document and action item)		
Remove all unnecessary functionality such as scripts, drivers and unused features (document and action item)		
Encrypt all non-console admin access using protocols such as SSH, VPN or SSL (document and action item)		
Current inventory of all system components in PCI scope (document)		
Ensure all security policies and operational procedures for management vendor defaults are in use (document)		
Shared hosting providers must protect entity's host environment and card holder data (document and action item)		
Store minimal card holder information by implementing data retention and disposal policies, procedures and processes (document)		
Prevent storage of sensitive authentication data after authorization (document and action item)		
Prohibit the storage of card components (magnetic stripe, card PINS, code, chip or other physical information (document and action item)		
Render PAN information unreadable (document and action item)		

Use disks encryption for all servers and computers (document and action item)		
Process to protect encryption keys used to store secure data in card holder environment (document)		
Document and implement procedures to protect keys to secure stored cardholder data against disclosure and misuse (document)		
Restrict access to cryptographic keys to the fewest number of custodians (document)		
Store secret and private keys to encrypt/decryption cardholder data (document)		
Store cryptographic keys in the fewest possible location (document)		
Document and implement all key management process and procedures for cryptographic keys used for encryption for card holder data (document and action item)		
Process for generating strong cryptographic keys (document)		
Process for cryptographic key distribution (document)		
Process for secure cryptographic key storage (document)		
Process for cryptographic key life cycle, retirement, replacement and disposal (document)		
Use split knowledge when clear-text cryptographic keys are used (document)		
Process for prevention of unauthorized or substitute cryptographic key use (document)		
Process for cryptographic key custodian to formally acknowledge responsibilities (document)		

Ensure all policies and procedures for protecting card holder information is in use (document)		
Use strong cryptographic and security protocols to safeguard information (document and action item)		
Ensure use of strong encryption to transmit card holder information on wireless networks (document and action item)		
Prevention of transmitting PAN by end-user messaging technologies (document and action item)		
Ensure that all security policies and procedures for encrypting card holder data are in use (document)		
Process for implementing anti-virus software on computers and servers which cannot be changed by user, automatic update of signatures removed malicious items (document and action item)		
Create processes to identify security vulnerabilities by categories (document)		
Process to update and patch all vendor supplied software within one month (document and action item)		
Process to remove all test or developmental accounts from production systems (document and action item)		
Process to review code prior to release to production environment (document)		
Implementation of change control process (document and action item)		
Process to segment test/development environment from production environment (document and action item)		
Process for separation of duties between development/test and production environments (document)		

Process to ensure production data is not used for testing or development (document)		
Process to address common vulnerabilities in software development (document)		
Process to verify broken authentication and session management (document)		
Ensure all security policies and procedures for development and maintaining systems and applications are in use (document)		
Process to limit access to system components and card holder data to job function which requires access (document and action item)		
Define need for access as defined by role (document and action item)		
Restrict access to privileged user IDs to least privilege in order to perform job role or function. (document and action item)		
Process for documented approval of additional rights or privileges (document)		
Process to allow authorized access to system and implements deny all unless specifically allowed. (document and action item)		
Ensure all security policies and procedures for restricting access to card holder environment are in use (document)		
Implement policies and procedures to ensure proper identification management for non-consumer users and administration on all system components by assigning unique IDs, control of changes, revoking of access, etc. (document)		
Process to remove any inactive accounts in 90 days (document)		
Process to manage all vendor IDs for system access (document)		

Process to lock out account with multiple login attempts (document and action item)		
Process to set lock out duration to a minimum of 30 minutes (document and action action)		
Process to force re-authentication after 15 minutes of idle time (document and action item)		
Process to use strong cryptography to render all authentication information unreadable during transmission (document and action item)		
Process to verify user identify prior to any account changes (document)		
Policy for password requirements (document)		
Policy for password rotation every 90 days (document)		
Policy to prevent re-use of prior four passwords (document)		
Process to create a unique password for new account access for each user (document)		
Process to implement 2-factor authentication for remote network access (document and action item)		
Document and communicate authentication procedures and policies (document)		
Process to prevent use of shared or generic user accounts and/or passwords (document and action item)		
Process to provide service providers with remote access to network (document and action item)		
Policy for access to databases containing card holder data (document and action item)		
Ensure policy and procedures for identification and authentication are in use (document)		

Process to use appropriate facility controls to limit access to restricted areas (document and action item)		
Use of video cameras to monitoring access to restricted areas (document and action item)		
Process for physical or logical controls for pubic accessible network jacks (document and action item)		
Process to restrict physical access to all networking devices (document and action item)		
Develop procedures to easily identify internal personnel and visitors (document and action item)		
Process to restrict unauthorized internal personnel to restricted areas (document and action item)		
Create process to authorize visitors and other personnel (document)		
Create process to for visitors to have identification, surrender identification prior to leaving, and maintain a visitor log (document)		
Create a process to secure all physical media (document)		
Create a procedure that ensures all backup media is stored in a secure location (document)		
Create a process to categorize all media (document)		
Create a process for transferring media offsite either by internal personnel or courier (document and action item)		
Process to handling media by inventory, storage and destruction (documentation)		
Process on method of destruction for media (document)		
Process to create and maintain an inventory of all devices (document)		

Process to detect devices for tampering (document)		
Process to train personnel to detect device tampering (document)		
Ensure all policies and procedures to restrict physical access is in use (document)		
Process to implement audit trails to link all actions to a unique individual (document)		
Process to implement audit trails for all system components to reconstruct a security event (document and action item)		
Process to record the following audit trail entries such as user identification, event type, data-time, origin of the event, synchronized time and name of affected component (document)		
Process to ensure that audit trails are secured and not able to be manipulated (document and action item)		
Process to limit viewing of audit trails, protect from unauthorized modifications, trail information is sent to centralized location and use of file-integrity monitoring to ensure existing logs are not altered (document)		
Process to review logs and security events for all system components (document and action item)		
Process to review all logs and alerts daily (document and action item)		
Process to follow up on exceptions and anomalies during log and alert review (document)		
Process to retain audit trail information for a minimum of one year (document and action item)		
Ensure all policies and procedures for monitoring all resources are in use (document)		
Create process to detect and incident response to remove rogue or unauthorized access points (document)		

Process to maintain inventory of wireless access points (document and action item)		
Process to perform internal and external vulnerability scans on networks at the minimum every three months (document and action item)		
Process to remediate high priority items immediately once a scan is complete (document)		
Process to perform external and internal penetration testing with qualified ASV at the minimum of annually (document)		
Implement a methodology for penetration testing (document and action item)		
Process to exploit vulnerabilities found during penetration testing (document and action item)		
Process to utilize IDS or IPS to detection any intrusions in the network (document and action item)		
Process to implement file integrity software for monitoring unauthorized changes to files (document and action item)		
Process to respond to alerts generated by change detection system (document)		
Ensure all security policies and procedures for monitoring and testing are in use (document)		
Establish and disseminate an organizational security policy (document and action item)		
Process to review the security policy annual and perform updates if needed (document)		
Process to perform risk assessments in the organization (document)		
Develop user polices to describe appropriate use of organization's technical resources (document and action item)		

Create a process to accurately determine owner and related information and purpose devices (document)		
Process to produce an inventory list of assets (document and action item		
Ensure that all security policies and procedures can clearly defined information security responsibly (document)		
Assign responsibilities to team or individual for all security management responsibilities (document)		
Process to create a formal security awareness program a9document)		
Process that requires personnel to acknowledge assigned responsibilities annually (document and action item)		
Process to screen candidates prior to hiring (document)		
Create policies and procedures to manage service providers (document)		
Process to maintain a list of service providers (document)		
Process to maintain a written agreement that includes an acknowledge that service providers are responsible for card holder data (document)		
Establish process to engage service providers including proper due diligence (document)		
Create a program to monitor service providers (document)		
Produce documentation showing service providers acknowledging they are responsible for card holder data (document)		
Create an incident response in the event of a systems breach (document and action item)		

Process to test the incident response plan annually (document and action item)		
Process to designate personnel to be available 24/7 to respond to alerts (document and action item)		
Provide training for staff with security breach response and responsibilities (document and action item)		
Process to modify and evolve the incident response plan according to lessons learned and industry developments (document and action items)		

Appendix E: Supporting Documents for Monitoring and Maintenance Phase

Maintenance Schedule

Task Description	Date Required	Notes/Instructions
Firewall rule review	Every 6-months	All firewall rules will need to be reviewed to ensure they are required by the business to operate. All rules required must have business justification to valid its use. Any rules not required will need to be removed during an approved maintenance window.
Syslog message review	Daily	All syslog messages must be reviewed daily to ensure if any security breaches or other security related issues are recognized and resolved immediately. If any abnormal items are detected they must be analyzed to ensure it's not a threat.
Rogue access point scanning	Quarterly	All locations within the organization will be scanned to ensure any rogue (unauthorized) access points are not on the network. If any are found they will need to be removed immediately. When scans are performed proper document must be filed to ensure the process has been performed.

Process correction	Bi-annually	Any corrections to processes due to organization, technical or compliance requirement changes must be documented at this time to ensure problems are created on the following audit. All changes must be approved by management to ensure all changes are applicable to the organization.
Change control procedures	Daily	Change control procedures will continue to be used on a daily basis. All changes once completed will need to be documented and retained for future use when required by auditors.
Compliance requirement review	Prior to audit	Prior to the upcoming all compliance requirements must be reviewed to ensure no changes or process adjustments have been made since the previous audit. The standard documentation for PCI-DSS currently in use will need to be reviewed. This will ensure the organization is auditing against the most accurate information and lower the risk of failing audits due to using wrong information.

Anti-virus definition updates	Daily	Anti-virus definitions must be updated daily to ensure immediate protection against new threats. This will have to be set up on both maintenance server, other servers and user computers
Internal and external network scanning	Monthly	Internal scanning of all network devices and components (computers, printers, etc.) will need to be conducted once a quarter to ensure that all new threats are recognized and reviewed. Scanning will be performed by an external vendor or someone internal who understands the process and procedures.
External network scanning (penetration testing)	Every 6-months	External scanning of all external (public) ip addresses will need to be conducted once a quarter to ensure that all new threats are recognized and reviewed.
Urgent remediation efforts	As soon as required	Urgent remediation efforts will need to take place when high priority vulnerabilities are detected. A plan of remediation will need to be created, reviewed and documented into the change control process to move forward. Once the remediation effort is complete the device will be re-scanned to ensure the

		vulnerability has been resolved. If the vulnerability is still present after re-scanning further review will need to take place along with another attempt at remediation to correct the problem. Once all remediation efforts is complete the prior actions will be documented to verify the scan was performed and all vulnerabilities have been remediated.
Inactive account review	Every 90 days	Review must be conducted to ensure all inactive accounts which will remain unused are removed. Once the accounts are removed document all actions to validate review is being conducted.
Perform risk assessment	annually	Perform risk assessment annually to ensure organization is not exposed to new threats. Once risk assessment is complete store all documentation to validate procedure was completed.
Vender patching and updates	Monthly	Patching and other software updates provided by manufactures both for hardware and software will need to be completed within one month of the software being

		released. Organization will test new updates prior to full deployment.
New computer deployment	As needed	When configuring a new computer ensure that it has all software required to perform job function, all necessary security policies, default configurations changed, auditing configured and all unnecessary services removed.
New server deployment	As needed	When configuring a new server ensure that it has all software required, all necessary security policies, default configurations changed, auditing configured and all unnecessary services removed.
User account modifications	As needed	Any account can be performed on an as needed basis. The requirement for this is to ensure that all modification obtains the appropriate approvals and all changes are documented through the change control process to create an audit trail.
Application code review	As-needed	When need applications are created or purchased for the needs of the organization. The applications processes and code must be reviewed to ensure new security threats are

		not being introduced into the technical environment.