Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Project Management Approach to Yearly PCI Compliance Assessment

The Payment Card Industry (PCI) Data Security Standard (DSS) provides a list of over 200 controls that must be inspected yearly by organizations handling credit card data. As several organizations have learned, contracting a QSA to perform a PCI DSS yearly validation is simply not enough to ensure success. A comprehensive, repeatable approach is required to perform the yearly inspection in a uniform and credible manner. This paper provides guidance to prepare for and conduct the PCI yearly validation using project mana...

Copyright SANS Institute

Author Retains Full Rights

AD

PM for PCI

Project Management approach to yearly

PCI Validation

GIAC (GCPM) Gold Certification

Author: Michael Hoehl, mmhoehl@gmail.com
Advisor: Rob VandenBrink

Accepted: October 22, 2012

Abstract

The Payment Card Industry (PCI) Data Security Standard (DSS) provides a list of over 200 controls that must be inspected yearly by organizations handling credit card data. As several organizations have learned, contracting a QSA to perform a PCI DSS yearly validation is simply not enough to ensure success. A comprehensive, repeatable approach is required to perform the yearly inspection in a uniform and credible manner. This paper provides guidance to prepare for and conduct the PCI yearly validation using project management methodology. Several lessons learned are included so the PCI validation project ends with a success story—-not a post-mortem.

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

1. Introduction

Payment Card Industry Data Security Standard (PCI DSS) has been developed by a collaboration of the credit card companies including VISA, American Express, Mastercard, and JCB. The purpose of the standard is to advance cardholder data security globally. This comprehensive standard is intended to reduce the risk of data breaches by guiding merchants with specific requirements to protect customer account data. The program is administered by the PCI Security Standards Council. Requirements are defined for security management, policies, procedures, network architecture, software design and other critical protective measures. PCI DSS is comprised of 6 Categories (Goals) including 12 Requirements.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Just 12 simple requirements equals…

200+ individual security controls that must be inspected
72 pages of requirements and security assessment procedures
Policies for Business and Technology staff
Security Awareness Training
Compliance Attestation, Evidence Collection, and Disclosure
Quarterly vulnerability scans of PCI systems and infrastructure
Yearly penetration testing of PCI systems and infrastructure
Formal yearly validation by Qualified Security Assessor (QSA) or Internal Security Assessor (ISA)

PCI DSS is a contractual obligation for merchants accepting credit cards for

© 2012 The SANS Institute Author retains full rights.

payment. Non-compliance impacts fees charged to the merchant with every credit card transaction. Several U.S. state breach notification laws (e.g., Nevada, California, etc.) now include in scope credit card data. New U.S. state personal information protection laws (e.g., Massachusetts 201 CMR 17.00) and European Union Directives include requirements to safeguard credit card data. PCI DSS represents credible, commercially reasonable safeguards for customer data. Merchants are to assess compliance and report yearly to their acquiring bank.

If data leakage occurs while out of compliance, the merchant might have to bear the entire financial liability of the security incident. This liability is in addition to the organization reputational damage. Expenses including cardholder notification, legal Counsel, public relations consulting, forensic analysis, business continuity expenses, and re-assessment of compliance might be so great that company profitability and solvency are impacted. Further, merchants might find that their financial risk cannot be assigned using general liability and "cyber" insurance. If the leakage is not a result of malicious intent, but because of unintentional loss of confidentiality, the merchant might be required to underwrite the entire expense. Lastly, without evidence of sustained security control due care, banks and credit card companies will not allow a merchant to accept credit cards for payment.

There are 5 major phases for organizations intending to achieve PCI DSS compliance for the first time. Gap Analysis is performed initially when an organization makes the business decision to store, transmit, or process credit card information. A few examples of this condition include customer credit card payment processing, employee travel reservations systems accepting credit cards, loyalty programs that retain credit card data, or major credit card payment processing system changes. If deficiencies are found as a result of the Gap Analysis, the organization must remediate or implement compensating controls. Once the organization has completed the Gap Analysis and Remediate phases, a formal assessment of controls is conducted. Smaller organizations are permitted to self-inspect controls while larger organizations are required to have a certified individual (Qualified Security Assessor or Internal Security Assessor) perform the inspection of the controls. Guidance with determining who can perform the

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

assessment to validate compliance is available on the PCI Security Standards Council website (www.pcisecuritystandards.com) or directly from the merchant acquiring bank.

Once the Assess phase is complete, the organization must prepare to sustain the required controls. The Sustain phase is often skipped when organizations fail to understand that PCI is not a once and done event. Credit card companies and banks expect organizations to demonstrate the credit card information is safeguarded continuously. Collection and presentation of evidence that controls are properly sustained is done annually during the Validate phase. Though all five phases (Gap Analysis, Remediate, Assess, Sustain, and Validate) are necessary for PCI compliance, the Validate phase is the phase this paper primarily focuses on.

IMPORTANT: This document does not provide legal advice. This document provides a comprehensive, repeatable approach to perform yearly validation of PCI controls using project management methodology. A general project management framework is assumed to be in place for implementation of any new controls including people, process, and technology. This existing project management framework would be triggered for elimination of any material risks discovered--not just for PCI validation related discoveries. Do not rely exclusively on this document for guidance about your organization's regulatory requirements. Consult PCI Security Standards Council, legal counsel, certified PCI assessor, credit card companies, and acquiring bank for questions regarding PCI compliance obligations for your organization.

2. What are the benefits of a Project Management approach for yearly PCI compliance validation?

2.1. Increase Credibility

Using established project management methodologies increases credibility when executing yearly PCI validation. Scope and objectives are clearly established in the beginning. Timelines and deliverables are communicated using familiar project management tools (e.g., Project Charter, Work Breakdown Structure, etc). Key resources are identified. Planned and actual resource utilization are monitored. Leaders and functional managers are routinely informed of their duties and progress. Risks to the

© 2012 SANS Institute, Author retains full rights.

project are tracked and reported to stakeholders. Collectively, these project management methodologies demonstrate a mature approach to manage the validation of control compliance.

Discovery of PCI security compliance deficiencies is not a poor reflection on the project manager--however the project manager is accountable for deficiencies associated with project execution. This distinction is very important to establish during the project kick-off meeting. In many cases, the approach used to inspect the controls will be considered as much as the testing results. Project Managers can articulate this using project management plans and reports. This planning as well as compliance status will lend credibility to the merchant when negotiating payment transaction fees with the bank.

The output of the PCI validation project is vital not only for demonstration of sustained compliance, but also when a breach is suspected. Project deliverables will be used by security assessors, risk analysts, forensic analysts, bank inspectors, fraud investigators, and incident handlers. If there is suspicion of PCI data leakage or system compromise, the validation documentation will be one of the first sources of information requested for review. Presumably, the time of the last validation is the most credible moment in time in which all controls were operating properly. The "Book of Evidence" created as a result of the yearly validation is a vital tool for rapid forensic response. The Book of Evidence contains the tangible deliverables of the validation including firewall rules, data flow mapping, as-built configuration documentation, incident handling procedures, and drawings. Promptly providing a comprehensive Book of Evidence is critical for scoping a suspected breach and will increase credibility with the forensic analysts and fraud investigators when determining how much culpability the organization has for the suspected breach. A list of documents intended for the Book of Evidence is provided in Appendix G.

2.2. Reduce Risk

The Project Management Institute proposes 9 Knowledge Areas for project management processes. One of the key knowledge areas is Risk Management. Project Management processes associated with Risk Management include: Risk Management Planning; Risk Identification; Quantitative and Qualitative Risk Analysis; Risk Response

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Plan; Risk Monitoring and Control. During the PCI validation, there are going to be risks to the project. By following a project management framework, these risks can be better anticipated, avoided, and addressed.

Project Managers are familiar with the "triple constraint" of Time, Cost, and Scope. The concept behind the triple constraint is scope, time, and cost are all closely related. When a change occurs to one of these constraints (e.g., budget reduced, staff resources reduced, time extended, etc.), a project manager determines the associated impact to the other parts of the triple constraint. This constraint occurs whether the organization recognizes it or not. The project manager communicates the results as well as impact to quality, risk, and customer satisfaction. During PCI validation, project changes might be proposed. This might be a result of new discoveries, new business processes, technology improvements, or PCI DSS requirements changing. Effectively managing this triple constraint helps organizations reduce the risk of mismanaging unexpected or undesirable validation events.

2.3. Save Time and Money

In many cases, the key staff resources necessary for demonstrating PCI compliance are otherwise engaged with running the business. This includes IT, HR, Legal, Finance, Corporate Communications, Retail Operations, Service Providers, and Contractors. With so many resources necessary for evaluation of PCI controls, the Security or Audit team must schedule and coordinate effectively. Project Managers can use familiar techniques like activity sequencing, critical path analysis (e.g., Critical Chain Method), float (also known as "slack") calculation, and resource leveling to ensure key resources are used effectively and not over allocated to the PCI validation project. The initial investment of time in authoring a project plan provides a payback in the form of efficient use of limited staff resource time during execution. Coordinated planning of scarce resources will ultimately ensure minimum activity effort and duration to achieve the desired project objectives. This way organization staff can return to their primary objective of running the business and contractor expenses are prudently managed. This saves time and money.

As with all projects, there is the risk of scope creep. Without a project manager

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

keeping an eye on the objectives, changes in scope can result in lost time and money. Change requests are common with projects, and they can take on many characteristics (e.g., addition expenses, addition resource requirements, additional duration, etc). A project manager ensures changes are only requests until authorized. This keeps the validation effort on-track, on-time, and within budget.

2.4. Increase Accountability

When there is a concern about compliance and audit, executives will want to know who, what, why, and how? One of the top concerns for business executives is institutional compliance. In many organizations, executives may suffer personal risk in the form of litigation and financial liability for institutional non-compliance. If non-compliance with a regulated or contracted obligation is likely, organization leadership will want to know who is ultimately responsible and accountable. The project management tools (e.g., RACI, Project Dashboard, Plan, etc.) proposed in this paper provides the organization a clear understanding of management accountabilities and risks.

3. Who should be involved in the PCI Validation project?

3.1. Stakeholders and Sponsors

The very first step to any project is to identify the stakeholders and sponsors. These are ultimately the customer for the project. Sponsors are the officers that will be expected to sign an attestation of compliance and have authority to make enterprise risk management decisions. These individuals must be identified at the project start as they are the source of assigned authority for the Project Manager. Stakeholders include:

Chief Financial Officer (CFO)
Chief Information Officer (CIO) and Chief Technology Officer (CTO)
Chief Privacy Officer
Chief Information Security Officer (CISO) or Security Manager
Chief Operating Office (COO)
Controller
Internal Audit and Internal Controls
Chief Legal Officer (CLO)
VP Human Resources
Manager/Director of IT - Retail Sales Applications
Manager/Director of IT - Infrastructure

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Corporate Communications Manager
Risk Management Executive or Committee
Call Center Manager
Retail Operations Manager
Vendor Management Executive
Acquiring Bank
PCI Qualified Security Assessor (QSA) or Internal Security Assessor (ISA)
Project Management Office (PMO)

Don't forget influencers and stewards! Though these individuals have no formal authority by title, they might have the trust and assigned authority of a sponsor or stakeholder.

3.2. Identify the entire "Security" team

PCI compliance has many touch points within IT. Payment processing applications are not the only inspection item. The PCI DSS is a multifaceted security standard that includes requirements for security infrastructure, network architecture, software applications, database management, system management, and operating procedures. Therefore, many folks are responsible for proactively protecting customer account data.

Most organizations do not have a dedicated team of professionals with the collective responsibility for the entire security program. In many cases, the security program is effective because of the collaborative efforts of many teams along with Security including PC support, database managers, application developers, operations center staff, system administrators, network engineers, Retail Operations, Human Resources, and Legal. Since these teams are responsible for sustaining the security controls, they are also key resources for conducting the validation.

The organization may have elected to outsource or contract services instead of using internal resources. If this approach is used for any of the services associated with sustaining PCI DSS controls, the respective vendor should be engaged early. Contract review is also recommended to ensure the vendor is not kindly assuming responsibilities (and billing for these services) but has no accountabilities.

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

3.2.1. Obtain Organization Charts

To get started with identifying key resources, obtain organizational charts. One of the most important security controls is organizational structure. Typically, organization charts contain only employees. The employees may not be providing all security services. There might be key resources missing from the organization including outsourcing organizations, managed service providers, and stewards. In some cases, it may be appropriate to meet with staff managers to discover these other key resources and services provided.

When approaching staff management, ask for scorecards, dashboards, and recurring risk reports associated with security. In addition to the obvious metrics this provides, it also helps identify the teams and individuals responsible for creating the metrics. Find the folks that create the metrics and you will most likely find the key resources for providing evidence of sustained compliance.

3.2.2. Create a preliminary RACI Document

Organization charts are a great start—but at times can be too high level and not descriptive enough. Documenting resources, roles, and responsibilities is a critical first step when leading any project. A popular tool to help accomplish this for project managers is the RACI document. Project Managers use this tool frequently when leading a multi-team initiative. RACI is a matrix used to clarify roles and responsibilities for cross-functional/departmental duties. There are a few variations of RACI, but all have in common (R)esponsible, (A)ccountable, (C)onsult, and (I)nform. Please see Appendix C for template based on PCI Requirements.

3.3. Validation Team

Evaluation of PCI compliance requires a formally trained and certified assessor for larger organizations. These individuals are known as Qualified Security Assessors (QSA) and Internal Security Assessors (ISA). Service providers are formally qualified by the PCI Security Standards Council to offer certified individuals (QSA) to assess compliance to the PCI DSS standard. Organizations can verify certification of service provider and service provider employee by going to the PCI SSC website listed below:

https://www.pcisecuritystandards.org/approved_companies_providers/verify_qsa_

© 2012 SANS Institute, Author retains full rights.

employee.php

Please note the following about the QSA program. The QSA evaluates compliance and risk—but does not assume any risk associated with the state of the controls evaluated. The QSA program is not an insurance instrument for organizations to assign risk. Risk remains with the merchant and acquiring bank.

Larger organizations have available to them a new program from the PCI SSC. The Internal Security Assessor (ISA) program provides an opportunity for eligible employees of qualifying organizations to receive PCI DSS training and certification similar to a QSA. The intention is to improve understanding of PCI DSS so that organizations can perform self-assessment, improve interactions with QSAs, and guide application of PCI DSS controls.

Organizations processing, transporting, or storing credit card information are categorized into specific merchant levels. Each merchant level is a unique category with requirements for compliance validation and documentation. Acquiring Banks determine the organization merchant level. This is typically determined by the number of credit card transactions (not sum total of sales) that the organization processes a year. There are exceptions including a recent security breach event or compliance reporting errors. The merchant level then determines if an organization may self assess (ISA) or engage a third-party (QSA). Project Managers should confirm merchant level with Acquiring Banks early in the project so the correct assessment resources and documentation are identified.

In addition to the QSA and/or ISA, the assessment team typically includes a representative from IT, Internal Audit, and Security. These individuals act as "ambassadors" into the organization. They provide experience based on institutional knowledge, infrastructure design familiarity, and prior control inspection results (e.g., SOX ITGC, HIPAA, etc.). They also serve an important role translating assessment requirements into business terms the organization can understand.

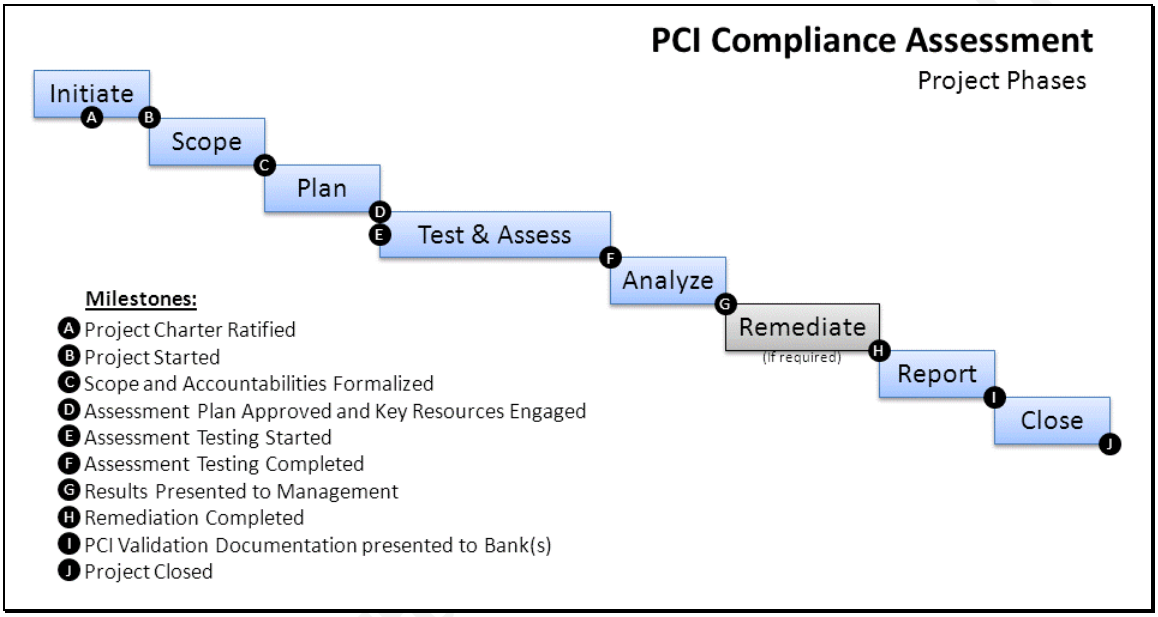
4. How to create a PCI Compliance Validation Project

This paper proposes an 8 phase approach to project managing a PCI Compliance Validation. In phases, work has distinct focus that differs from any other phase, and work

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

in each phase involves different skill sets (PMI, 2008). A waterfall model for phase transition is used. Within each phase, processes are performed iteratively. Progressive elaboration occurs within each phase as processes are initiated, planned, monitored, executed and closed. However, the project cannot advance to the next phase until the milestone is attained. The Gantt chart below provides a high level overview of the phases and associated milestones.



A fully elaborated detailed project plan is included in Appendix A.

4.1. Initiate

4.1.1. Confirm Project Objectives, Scope, and Timing

PCI DSS compliance evaluation is highly technical and detailed. There are over 200 controls to inspect. Start with the fundamentals of project management including defining project objectives, preliminary project scope statement, and timing.

Ensure the objectives are clear from the sponsors. The desired outcome is compliance, but the project objective is to conduct the validation (pass or fail) in a complete and credible manner. Inspection of controls and demonstration that they have been sustained throughout the reporting period are key deliverables. If material deficiencies are identified during the validation, then PCI project scope might expand or additional project(s) created. Be sure to follow project change management procedures formally so that the project does not fail to lose sight of primary objectives (scope creep).

© 2012 The SANS Institute Author retains full rights.

A preliminary project scope statement allows everyone to begin with an end result in mind. The project scope statement defines the project and identifies deliverables. In some cases, multiple validation projects might be appropriate. For example, each region might have a separate project with different scope and milestones. Each region might have a unique Acquiring Bank (financial institution that provides credit card payment processing services for merchant), different change blackout dates, or different fiscal calendar. This is especially true for global organizations. Ensure project scope is very well defined in the project charter.

Establish a time frame for the project as well as deliverables early. This can be driven by multiple conditions including retail busy season freeze, anniversary date from previous PCI attestation of compliance, potential project collisions, and key resource availability. If timelines are externally driven, be sure to understand what penalties will be levied (e.g., fines, increase in transaction fees, etc.) if target is missed. If timelines are internally driven, be sure to identify the stakeholder mandating the deadline and the business requirement for timing.

4.1.2. Author Project Charter

Once project objectives, scope, and timing have been discussed, capture these in a Project Charter. In addition, the Project Charter should include identification of key resources, project management protocol, project approach, milestones, preliminary budget constraints, project risks, assumptions, and deliverables. A brief introduction to PCI is also recommended. Elaborate on the business requirement for the yearly validation. An example of a Project Charter is included in Appendix D.

A signature page for the Project Sponsor and optionally the Project Steering Committee members is recommended. This formally ratifies the project and demonstrates to all project members the importance of PCI validation.

4.1.3. Create Project Management Steering Committee

As mentioned earlier, there are several stakeholders associated with PCI DSS compliance. Requiring all the stakeholders to be members of the project steering committee is not practical for most organizations. A core group of leaders should be

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

identified to serve as the Project Steering Committee. At a minimum, this committee should include the individual(s) that will be signing the PCI Attestation of Compliance (AOC). If members are not employees of the organization (e.g., consultant), ensure there is a non-disclosure agreement in place for confidentiality of communications. Have Legal confirm this agreement is properly executed.

Establish a formal communication protocol for this committee. For situations in which all the stakeholders are not in one geographic location, this is vital. Email is typically too informal. Checkpoint meetings should be established early so that committee members can avoid scheduling conflicts. Examples of meeting collateral and presentation material should be presented to the committee so they have an expectation of how information will be presented.

The Project Steering Committee provides guidance in areas of project risk, resource, financial, and decision management. The primary intent of the Project Steering Committee is to assign authority to the project team to achieve the deliverables proposed. Project Managers must be conscious of how this authority is conveyed. The tone of the Project Manager and Auditor must not be threatening. Life continues after the project ends, so maintenance of relationships is very important during this sometimes stressful event.

Please note that the Project Steering Committee is not intended to serve in the role of Enterprise Risk Management (ERM) Committee. The Enterprise Risk Management Committee is a recipient of the project outputs (e.g., assessment findings, risk treatment plan, etc.). Though some individuals might be on both committees (e.g., CFO)—the committee missions are different. The Project Steering Committee mission is to guide and advance the project management aspects of the PCI compliance validation only.

4.1.4. Conduct Project Kick-off Meeting

Assemble the key individuals and project steering committee to announce the project. If possible, have the project sponsor or senior member of the project steering committee call the meeting. A brief opening statement by this individual at the project kick-off meeting is ideal. A short Microsoft PowerPoint presentation can also be helpful. An example is provided in Appendix B. This approach of leading with the sponsor helps

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

sets the proper expectation of project priority.

The agenda should be short and meeting should be brief (lasting no more than 1 hour). Creation of the entire validation plan and assignment of work are not to be performed at this time. Review of the project charter is a great start. Be sure to cover objectives, scope, timing, role of project manager, role of auditor, and role of attendees. At a high level review the validation approach. Finally, review how progress will be communicated to the Project Steering Committee. An example presentation for this project kick-off meeting is provided in Appendix B.

Expectations should be set that follow-up breakout sessions will occur. Confirm all test results will be shared and reviewed prior to formal disclosure. The most important outcome of this meeting is commitment by resource managers to support the project. Again, ensure the tone of the meeting is positive and not threatening. The purpose of the validation is not to identify problems, but to confirm controls have been sustained. Essentially, this project will document the good work being done by the organization to continuously safeguard customer data.

4.2. Scope

4.2.1. Establish Cardholder Data Environment Scope

This is typically one of the most controversial parts of the project. There will be many opinions as to the exact scope of Cardholder Data Environment (CDE). The cardholder data environment is comprised of people, processes and technology that handle cardholder data or sensitive authentication data. If cardholder data is being processed, transported, or scored, then consider this item in scope for inspection and validation.

To minimize debate, identify the authoritative compliance decision-maker in the beginning. This is most likely a Qualified Security Assessor (QSA), Merchant Internal Security Assessor (ISA), or compliance representative from Acquiring Bank. This individual is responsible for clarifying and qualifying compliance. They also determine the applicability of compensating controls. Please note that project managers, functional managers, and architects are not appropriate roles for determining PCI scope and compliance condition. Their input is valuable in contributing to a determination,

© 2012 SANS Institute, Author retains full rights.

however only a certified assessor or the acquiring bank are authoritative source for final determination of control compliance.

4.2.2. Author/Update RACI

The RACI was discussed earlier as a helpful tool to identify the entire "security team". The RACI is used in 3 different phases of the PCI validation project lifecycle. During initial project formation, the RACI establishes collective understanding of who is ultimately accountable for each security control and who is performing the daily duties to ensure the appropriate state of the security control. Advisors, auditors, vendors, and secondary support staff roles are also identified as part of drafting a RACI.

There are over 200 controls that must be inspected for PCI DSS compliance. The RACI matrix conveniently organizes the relationship between PCI requirements and people. The RACI matrix can be authored using simple tools like Excel. Once completed, pivot tables and filters can used to identify resources (e.g., people, vendors, etc.) with the most PCI requirement assignments, PCI requirements with no resource assignments, and organizational single points of failure for sustaining the PCI requirements.

The second phase where the RACI is valuable is to determine the specific individuals or service providers that are the source of compliance attestation and evidence data. The RACI offers great guidance for resource planning and scheduling. The RACI can be used to help organize requests for resources and information. Project resource leveling efforts are made easier with the RACI on-hand.

Advancing thru all the 12 PCI requirement details in order may not be the most effective use of resources. Expecting all individuals to know all PCI controls might be unrealistic. With the RACI, Project Managers can target specific PCI requirements that must be spoken to during interviews with various groups. Individuals accountable or responsible for controls can see their own reflection in the 200+ controls. With this understanding, they will be able to focus better on demonstration of relevant controls for evaluation.

For the last phase (project close and resource recognition), the RACI is used to

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

help with recognizing and rewarding the folks that are accountable and responsible for sustaining the security controls (and ultimately a passing assessment). It provides a convenient way to put names to roles so that "job well done" messages can be personalized.

4.3. Plan

4.3.1. Develop Project and Validation Plans

This phase begins with developing fully elaborated plans for the project and validation. Please note these are separate plans. The project plan focuses on management of scope, resources, and timing of tasks necessary to accomplish a business objective (i.e., conducting the PCI Compliance Validation). Phases of the project are established to complete deliverables, associated activities are defined, and dependencies are identified. Prominent de facto standards and organizations in this space include the Project Management Body of Knowledge (PMBOK®) Guide from Project Management Institute (PMI), Projects in a Controlled Environment (PRINCE2), and International Project Management Association (IPMA).

The validation plan provides prescriptive details as to what is being inspected, how, when, and where as part of the compliance assessment. Additional aspects of the validation include assessment methodology (e.g., interview, examine, test, etc.), assessment depth (e.g., basic, focused, comprehensive, etc.), high-level calendar of events, security incident handling protocol during assessment, communication requirements in advance of testing, authorization to perform testing, removal of tools and data after validation, permitted transmission of assessment data through trusted and untrusted environments, safeguarding of test results, confidentiality of disclosure and distribution of findings. Prominent de facto standards and organizations in this space include SANS and NIST.

4.3.2. Identify and Engage Validation Team

Now that the Validation Plan has been ratified, the resources necessary to perform the validation can be engaged. As mentioned earlier, the validation team (in collaboration with the Acquiring Bank) determines if a PCI security control is in/out of compliance. A QSA or ISA is required for larger organizations. When contracting a QSA, the

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

aforementioned Validation Plan can be used as part of the Request for Quote (RFQ) and Statement of Work (SOW). This resource can be one of the most expensive parts of the project. Project Managers find that effective coordination of this resource has one of the biggest impacts to the project budget. Pre-work and disclosure prior to assessor arrival is vital to successful management of this key resource.

4.3.3. Document Handling Requirements

Project Management Information System and Project Progress Dashboards are selected at this time. An example of a Project Dashboard for PCI is provided in Appendix F. Access controls into these systems should be carefully considered. In addition, Project Managers must be conscientious of confidentiality requirements associated with project artifacts. Document management and security are critical. Project documents are great reconnaissance information for hackers, and might be evidence for litigation after a breach.

As mentioned earlier, the "Book of Evidence" created as a result of the yearly validation is a key output of the project. The Book of Evidence contains the tangible deliverables of the validation including firewall rules, data flow mapping, as-built configuration documentation, incident handling procedures, policies, and drawings. The Book of Evidence can be in electronic form, however at least one copy of the Book of Evidence should be printed and secured. The purpose of this printed version is for document integrity verification as well as rapid response. Examples of documents found in a Book of Evidence is provided in Appendix G.

4.3.4. Map RACI to PCI DSS Requirements and Testing Procedures

The PCI Security Standards Council has published requirements and compliance procedures on their website. This document should be shared with those accountable or responsible for sustaining PCI compliance. It conveniently identifies the specific artifacts and testing actions that the assessor will require. As mentioned earlier, mapping this information to the aforementioned RACI document can be very useful. This allows the project members to focus in on deliverables that will be required of them individually as part of the PCI Compliance Validation. This mapping can also be a useful tool for identifying critical validation participants and resource planning.

© 2012 SANS Institute, Author retains full rights.

4.3.5. Pre-work Artifacts for Validation Team

As with most security assessments and audits, the assessor(s) typically request documentation to review prior to arrival. This helps prepare the assessor to understand the environment being evaluated. In addition, testing approaches can be discussed and planned better. Documentation commonly requested includes:

Cardholder Data Matrix
Cardholder Data Flow Maps
Network Topology Drawings
Security Policies and Procedures
Prior PCI Compliance Assessment Reports
Recent Vulnerability Scanning Results
Recent Penetration Testing Results
Organization Charts

The Cardholder Data Matrix is used to document all applications and associated systems that store, process, or transmit cardholder data. It is essentially a simple asset inventory for the assessor. In some cases, the organization's CMDB is used to provide this information. An example of fields in a Cardholder Data Matrix is provided in Appendix D. Cardholder Data Flow Maps are very helpful because they visually represent how cardholder data moves throughout the organization. Both assessors and forensic investigators typically request these documents prior to arrival.

4.4. Test and Assess

This phase of the project is when assessor(s) are fully engaged. Controls are inspected and tested at this time to validate compliance. It should be noted that for an organization to be PCI DSS compliant, evidence must be provided that demonstrates the controls were sustained during the entire year—not just during the assessor engagement.

4.4.1. Validation Kick-off Meeting

The Validation Kick-off Meeting (also known as Entrance Conference) is an important event and should not be skipped. This meeting is separate and distinct from the Project Kick-off Meeting, however a successful Project Kick-off Meeting can set the right tone for this meeting. Ideally, the project sponsor (individual who will sign the Attestation of Compliance) should be present to kindly remind the project team and

© 2012 SANS Institute, Author retains full rights.

contributors of the validation priority. The QSA or ISA meets with all the project team at this time. By now attendees should have a good insight into their role with PCI compliance, so this meeting is a great opportunity for the assessor to get to know everyone and their role (i.e., put a face to the control function). This meeting should ideally be brief (less than 1 hour). Remember, the assessor might be new to the organization. Do not overwhelm the assessor with introductions and information day one. To help relate, consider what it was like for the project manager during the first day on the project.

The validation plan should be reviewed during this meeting. This provides a kindly reminder and ensures everyone is on the same page. Timelines for the validation as well as response expectations should also be spoken to. If the assessor is only on-site a few weeks, turnaround time for evidence requests and test samples will be important. The project manager should consider drafting a high level calendar of events for the attendees to review and share.

The project team might have technical questions for the assessor. This may not be the best forum for technical questions and answers. Some of the attendees might not find the questions relevant. The only exception to this recommendation is discussion around the Cardholder Data Environment (CDE) scope. This has a direct impact on the validation and effort. Project Managers should foster conversation with the assessor as the ultimate authority for determining the CDE. If the conversation appears to be lengthy, a follow-up meeting may be in order. Again, this meeting is the first of many and is intended to be brief.

4.4.2. Establish Testing Rules of Engagement and Assessment Logistics

All testing has inherent risk. Some of the testing performed to validate PCI compliance is intentionally intrusive (e.g., Penetration Testing). Therefore, Rules of Engagement are required so that the business can continue to run with minimum interruption. The Rules of Engagement discussions should include key function contacts, communication protocol, schedule for testing (and schedule for when testing is not permitted), testing targets and boundaries, test locations, test quality control, and incident

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

handling protocol. Rules of Engagement should also give guidance to the assessor to determine when defined activities can be advanced without the need for additional permissions and when additional permission is required. The assessor should present an overview of testing tools and techniques that will be used. Logistics including who, what, where, and when should be discussed. During the control evaluation, operational procedures should advance as normal. Threat response is part of the scope of any assessment. However, Operations team management must have available a clear communication channel to the assessment team to distinguish real threats from control evaluation during the validation. If any testing is done unattended, the assessor must have a plan for delegating termination actions or remote access to stop testing upon request.

4.4.3. Test and Confirm proper CDE Scope

The assessor will ask probing questions to understand the Cardholder Data Environment (CDE) scope. In addition, testing may occur to confirm the scope. PAN Scanners (systems used to broadly inspect data stores for credit card data) are occasionally used by assessors. PAN Scanner targets may include Point-of-Sale PCs, File Servers, Payment Gateways, IT staff computers with access to Cardholder Data Environment, Database Servers, Web Application Servers, removable media, and Tape Backup Systems.

4.4.4. Conduct Testing

Now that the scope of the Cardholder Data Environment has been confirmed, testing procedures begin. Typically, the assessor conducts interviews with the individuals/teams accountable for each control. This is a significant amount of document collection during this activity. In some cases the test simply requires an interview or examination of documents (e.g., Acceptable Use Policy and employee sign-off compliance report). In other cases, testing of the control is required. Project Managers and Assessors should frequently refer to the Rule of Engagement prior to performing testing. In preparation for testing, samples will be identified. Sample size will vary depending on design uniformity and configuration standards.

4.4.5. Perform Initial Compliance Assessment

An initial compliance assessment will be done after performing interviews,

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

examination, and testing. Assessors will use this opportunity to organize their findings and assign a risk rating. Identifying a risk does not necessarily imply non-compliance. Assessors will also evaluate compensating controls and mitigating circumstances (e.g., time based security controls). The first draft of the assessment is authored by the assessor. This draft is intended for the functional managers to analyze and verify findings. It would be premature to present this draft to the Enterprise Risk Management committee to take action.

4.5. Analyze

The purpose of this phase is to review assessment findings (good and bad) and confirm validation accuracy. Gap Analysis is performed if deficiencies are discovered.

4.5.1. Perform Assessment Quality Control

The purpose of this activity is to ensure that the findings are accurate and the manner in which the testing performed is appropriate. In some cases, the assessor might make a mistake in interpreting test results. In other cases, the organization might provide the wrong evidence in error. In either case, the assessor focuses on the quality of the assessment so the findings are credible and risk assessment correct. The assessor will also revisit earlier scope statements and control states to ensure they match with what was observed.

Evidence (test samples, technical documents, meeting notes, policies, etc.) is organized and mapped to each control inspected. The Book of Evidence is in semi-final draft at this point. Project Managers and Assessors must confirm document handling requirements are being followed.

4.5.2. Author Gap Analysis and Confirm Control Effectiveness

If the assessor discovers a deficiency, a Gap Analysis is prepared. This document might initially take the form of a punch list. It is still informal at this point and does not include recommendations for remediation. Findings are presented to the accountable managers for review and verification. Some assessors may also use this opportunity to discuss the compensating controls considered. If compensating controls are not accepted, deficiencies will be discussed. The assessor will attempt to get consensus with the

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

accountable managers on control effectiveness. This is when the Project Manager will have an important contributing role coordinating meetings and taking meeting minutes.

In some cases, the organization might have a disagreement with the assessor regarding deficiencies or plan of action to remediate. The ultimate arbitrator is the Acquiring Bank (not the organization's Enterprise Risk Committee or Security Team). The Acquiring Bank has the ability to accept risk on behalf of the merchant.

4.6. Remediate

This phase of the project is the most elastic and hardest to forecast because the deficiencies are not known early in the project planning. Some progressive elaboration can take place, however project managers cannot quantify the complexity and duration of this phase until the prior Gap Analysis is presented. A general project management framework is assumed to be in place for implementation of any new controls including people, process, and technology. This existing project management framework would be triggered for elimination of any material risks discovered--not just for PCI validation related discoveries.

The primary purpose of this paper is to present an approach using project management methodology to conduct yearly validations to demonstrate PCI compliance. Though all five phases proposed by the PCI Security Standards Council (Gap Analysis, Remediate, Assess, Sustain, and Validate) are necessary for PCI compliance, the Validate phase is the area of focus for this paper. For purposes of project continuity, this phase is expected to contain the following activities if material deficiencies are discovered:

Create and Present Risk Treatment Plan to Management
Develop Prioritized Plan of Action
Conduct Risk Review with Acquiring Bank
Initiate Remediation Actions
Test and Assess Remediation
Present Remediation Results to Management and Acquiring Bank

4.7. Report

At this phase in the project, the validation is complete. Validation documentation must be prepared, approved, and submitted to the Acquiring Bank.

© 2012 SANS Institute, Author retains full rights.

4.7.1. Inventory Book of Evidence

Project managers should spend time with the assessor to take inventory of the Book of Evidence. This should be done for multiple reasons. Contents in The Book of Evidence might be requested by the Acquiring Bank before accepting the Attestation of Compliance. As mentioned earlier, the Book of Evidence will be requested by the forensic investigators if there is a suspicion of breach. Lastly, this collection of documents will be used when the next validation occurs. Several of the documents will remain relevant for the successive validations. Conveniently, the table of contents can be used in preparation for the next validation, to guide accountable managers with the specific deliverables they will be required to produce.

4.7.2. Author SAQ or Obtain ROC

Larger organizations are required to submit an Attestation of Compliance (AOC) to the Acquiring Bank. In addition, a Self-Assessment Questionnaire (SAQ) from the ISA or Report on Compliance (ROC) from the QSA is required. The SAQ and ROC are comprehensive documents and require a considerable amount of time to complete. Documentation describing compensating controls is required as part of the documentation submitted to the Acquiring Bank.

4.7.3. Present Final PCI Assessment to Management and Obtain Formal Approval

An Exit Conference is typically scheduled at the end of the assessment. At this point the presentation is a formality—the control effectiveness has been confirmed with the accountable managers. There should be no surprises with the findings at this phase of the project. The primary objectives of this meeting are to provide a business level overview of the assessment results, present the validation documentation, and obtain formal approval to release this documentation to the Acquiring Bank. Compensating controls and potential risks are also briefly spoken to so that the organization can have a credible conversation with compliance officers of the Acquiring Bank.

4.7.4. Submit Compliance Documents to Acquiring Bank

The project manager should conduct a meeting between the Assessment team and Acquiring Bank. Depending on the findings and compensating controls, the organization

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

may want to include the QSA\ISA for clarification. All PCI DSS compliance validation documents should be sent using a traceable method (e.g., certified mail, email receipt acknowledgement, web portal screen print, etc.). The Acquiring Bank will then represent the merchant compliance status to all the credit card brands.

4.8. Close

This part of the project is familiar to project managers. Though the Assessment is complete, additional project management administration activities must be completed formally.

4.8.1. Advance Data Retention and Destruction Procedures

The project manager must ensure all documentation is properly labeled, retained securely, or destroyed properly. As mentioned earlier, this documentation will be very helpful for the next validation of PCI compliance.

4.8.2. Conduct Project Quality Control Review

A Lessons Learned Meeting is optional, but highly recommended. In addition, an on-line survey (such as www.surveymonkey.com) is a fast and convenient way to solicit the project team for their opinion of project approach and progress. The purpose of this quality control review is continuous process improvement of project management practice. Please note that this solicitation of opinion is not intended to provide a forum for disagreement with assessment findings. This effort is intended to improve the manner and methods by which the project was managed.

4.8.3. Review Project Performance and Outcome with Management

Completed project artifacts including dashboards, plan, budget, and quality control feedback are presented to the project sponsor at this point for sign-off. Use the RACI to call out top performers. Feedback from Lessons Learned Meeting should be shared with management at this time. The Project Management Office (PMO) might choose to audit the project at this time, too.

4.8.4. Release Resources and Close Project

All project documentation is completed at this time. Time reporting systems are

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

updated so that effort can no longer be reported against project activities. Project financial instruments are updated (e.g., expense reports all submitted, purchase orders and invoices reconciled, general ledger updated reflecting project close, etc.). Project Management Information System is updated and project closed. Resources including people and technology are all formally released. PMO is notified of project conclusion.

5. Project Lessons Learned

This section provides additional insight based on experiences (good and bad) conducting a PCI Compliance Assessment project.

5.1. Distinguish PCI Project and Assessment Risk Management

One of the most common risks to the quality of a PCI Assessment is to confuse project risk management with the security risk management done as part of the PCI compliance assessment. There are several risks to a project including key resource availability, budget constraints, scope creep, and project collisions. These risks are true for any project—not just a PCI compliance assessment. A project manager is familiar with these risks and is experienced with managing them.

The individual assessing PCI compliance might be exceptional at security control evaluation. However, this same individual might be a poor communicator, resource coordinator, planner, or project manager. Without mature project management practices during the PCI compliance assessment, problems can manifest that undermine the credibility and success of the PCI compliance assessment itself. Project Manager(s) and Assessor(s) must collaborate during the validation. In some cases, this might be the same individual wearing two hats. The Project Management function is accountable for ensuring project risks are clearly communicated routinely. The PCI Assessor function is ultimately responsible for clearly communicating PCI compliance risk.

5.2. Obtain Executive commitment and assigned authority from the start

Do not wait until there is a project risk to engage executives for the first time. As mentioned earlier, obtain executive commitment during the initiate phase of the project.

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

When executive leaders are unaware of the project or not engaged, the organization may misinterpret the project as a low priority. If the tone at the top is this compliance validation is important to the business, then the organization will respond.

5.3. Communicate secondary benefits of PCI compliance (e.g., state law, quality improvement, operational excellence)

Be sure communications are not too negative when promoting the project and assessment. Focusing on failure to comply is not much of a team motivator. The PCI DSS Requirements include several best practices that organizations may already be considering for improving service quality and achieving operational excellence. Include these benefits during discussions with leadership, management, and staff. The PCI DSS compliance initiatives might provide the needed authority to implement planned improvements. In this case, the organization enjoys multiple benefits from this single initiative. Example secondary benefits include:

Faster incident response for operations events
Reduced system configuration variance during initial build
Increased confidence in design based on recognized benchmarks
Better insight into intended and unintended changes
Increased customer and business partner trust
Greater awareness of risks and better understanding of appropriate risk response.

5.4. Recognize the Importance of Influencers (not on Org chart)

Project managers should partner with the business stewards and influencers, too. The stewards are the advocate of the business and serve as proxy for "beneficiaries" of security controls. They are in touch with the current business priorities, current initiatives, risk appetite, and financial status. They also have a trusted relationship with the business leadership and may have assigned authority from their business executive. Though indirect, this can be successful alternative to obtain commitment and assigned authority to advance the project.

5.5. Over communicate near horizon goals and activities

There are many moving parts to a PCI compliance validation. Many of the resources that contribute to PCI Compliance Validation have operations responsibilities, too. Unplanned work can result from daily operations events. This must be balanced

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

with the planned work associated with the project. Successful project managers kindly remind project contributors of their duties and project progress routinely. In addition to tracking work completed, the project manager should regularly walk-thru the planned approach to achieve future deliverables.

Weekly meetings are highly recommended. This helps clearly establish where the team is and where they are going. This will help reveal unanticipated project conflicts and resource constraints before they become impactful to the project timeline. Project managers should not stop business, however they are accountable for keeping planned activities in focus.

6. Conclusion

Achieving PCI compliance is a major milestone for many organizations. However, PCI compliance is not a once and done endeavor. All organizations processing, transporting, or storing credit card information are required to sustain safeguards to protect confidentiality and validate their effectiveness yearly. Without proper planning, this recurring commitment can be expensive and consume critical resources.

The project management methodology proposed by this paper provides an organization a repeatable and credible approach to conducting this yearly validation. Whether a project manager and assessor collaborate or a single security professional is wearing multiple hats, the tools and guidance provided are helpful for advancing the security control assessment. Ultimately, this makes inspecting what is expected easier for organizations.

7. References

Bernstein, M. (n.d.). *Managing Information Security Assessment Projects for Success*. Retrieved September 2012 from http://techrepublic.com.com/5208-1035-0.html?forumID=102&threadID=329814

Chuvakin A., Williams, B. (2009, December 1). *PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance.* Syngress.

Davis, C., Schiller, M. & Wheeler, K. (2011, January 5). *IT Auditing, Using Controls to*

© 2012 SANS Institute, Author retains full rights.

Protect Information Assets. McGraw-Hill Osborne Media.

Hoelzer, D. (2010). *Auditing Networks, Perimeters, and Systems – Auditing Principles and Concepts (507.1).* The SANS Institute.

Moeller, Robert. (2010, November). *IT Audit, Control, and Security.* John Wiley & Sons, Inc.

Mulcahy, R. (2009). *PMP Exam Prep, Sixth Edition*. RMC Publications, Inc.

PCI Security Standards Council. (2010). *Navigating PCI DSS – Understanding the Intent of the Requirements.* Retrieved July 8, 2012 from https://www.pcisecuritystandards.org/security_standards/documents.php

PCI Security Standards Council. (2010). *Requirements and Security Assessment Procedures Version 2.0 October 2010*. Retrieved July 8, 2012 from https://www.pcisecuritystandards.org/security_standards/documents.php

PCI Security Standards Council. (2010). *Why Comply with PCI Security Standards?* Retrieved July 8, 2012 from https://www.pcisecuritystandards.org/security_standards/why_comply.php

PCI Security Standards Council. (2010). *PCI Quick Reference Guide*. Retrieved July 8, 2012 from https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

Project Management Institute. (2008). *A Guide to the Project Management Body of Knowledge (PMBOK Guide) – Fourth Edition*. Pennsylvania, USA.

Ross, R., Johnson, A., Katzke, S., Toth, P., Stoneburner, G., & Rogers, G. U.S. Department of Commerce, National Institute of Standards & Technology. (2008). *Guide for Assessing The Security Controls in Federal Information Systems – Building Effective Security Assessment Plans* (Special Publication 800-53A). Gaithersburg, MD

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. U.S. Department of Commerce, National Institute of Standards & Technology. (2008). *Technical Guide to Information Security Testing and Assessment* (Special Publication 800-115). Gaithersburg, MD

Snedaker, S., & Rogers, R. (2006, August 31). *IT Security Project Management Handbook.* Syngress.

© 2012 SANS Institute, Author retains full rights.

Wright, C., Brian Freedman, B., Liu, D. (2008). *The IT Regulatory and Standards Compliance Handbook.* Syngress.

© 2012 SANS Institute, Author retains full rights.

Appendix A: Project Phases and Associated Activities

1.0	**Initiate**
1.1	Develop Preliminary Project Scope Statement
1.2	Establish Timeframe for PCI Assessment
1.3	Author Project Charter
1.4	Obtain formal Project Authorization
A	***MILESTONE - PCI Assessment Project Charter Ratified***
1.5	Announce PCI DSS Assessment
1.6	Create Project Steering Committee
1.7	Author Executive Presentation
1.8	Conduct Project Kick-off Meeting
B	***MILESTONE - PCI Assessment Project Started***
2.0	**Scope**
2.1	Establish Cardholder Data Environment (CDE) Scope
2.2	Identify key resources (staff, Service Providers, etc.) that maintain CDE controls
2.3	Author/Update RACI
2.4	Review PCI DSS Requirements with resources identified in RACI
C	***MILESTONE - PCI Assessment Scope and Accountabilities Formalized***
3.0	**Plan**
3.1	Develop Assessment Plan
3.2	Identify and Engage Assessment Team (Security/ISA/QSA)
3.3	Establish Document Handling requirements and Book of Evidence
3.4	Schedule initial Interviews with individuals accountable for CDE controls
3.5	Review PCI SSC Testing Procedures and Evidence Gathering Requirements
3.6	Gather Pre-work Artifacts for Security Assessor (QSA/ISA)
D	***MILESTONE - PCI Assessment Plan Approved and Key Resources Engaged***
4	**Test and Assess**
E	***MILESTONE - PCI Assessment Testing Started***
4.1	Conduct Testing and Assessment Kick-Off Meeting
4.2	Establish Testing Rules of Engagement and Assessment Logistics
4.3	Test and Confirm proper CDE Scope
4.4	Conduct Interviews with individuals accountable for CDE controls
4.5	Perform Control Testing and Evidence Gathering
4.6	Perform initial Compliance Assessment
F	***MILESTONE - PCI Assessment Testing Completed***
5	**Analyze**
5.1	Confirm Assessment Accuracy
5.2	Perform Assessment Quality Control
5.3	Prepare Gap Analysis (if deficiencies identified)
5.4	Confirm Control Effectiveness with Accountable Managers
G	***MILESTONE - PCI Assessment Results Presented to Management***
6	**Remediate (If Required)**
6.1	Create and Present Risk Treatment Plan to Management
6.2	Develop Prioritized Plan of Action
6.3	Conduct Risk Review with Acquiring Bank
6.4	Initiate Remediation Actions
6.5	Test and Assess Remediation
6.6	Present Remediation Results to Management and Acquiring Bank
H	***MILESTONE - PCI Remediation Completed***
7	**Report**
7.1	Inventory Book of Evidence
7.2	Author SAQ or Obtain ROC

© 2012 The SANS Institute Author retains full rights.

7.3	Present Final PCI Assessment to Management
7.4	Obtain Formal Management Approval of PCI Validation Document Drafts
7.5	Submit Compliance Documents to Acquiring Bank(s)
I	***MILESTONE - PCI Validation Documentation presented to Bank(s)***
8	**Close**
8.1	Advance Data Retention and Destruction procedures
8.2	Conduct Project Lessons Learned
8.3	Review Project Performance and Outcome with Management
8.4	Formally Release Resources
8.5	Close Project
J	***MILESTONE - PCI Assessment Project Closed***

© 2012 SANS Institute, Author retains full rights.

Appendix B: Project Kick-off Meeting Presentation

This appendix provides an example presentation material for the PCI DSS Compliance kick-off meeting.

2012 PCI DSS 2.0 Compliance Assessment

Project Kick-off Meeting

June 1, 2013
B. Gold, PMP

© 2012 SANS Institute, Author retains full rights.

Appendix C: PCI Compliance Assessment RACI example

This appendix provides an example RACI document based on Payment Card Industry (PCI) Data Security Standard 2.0. The RACI is versatile and can be used to map roles and responsibilities for any security program.

PCI Data Security Standard Requirements

Requirements	Priority	Larry Lead	Steve Smart	Michale Manager	Adam Act	Greg Guru	Harry Helpful	Network	Systems	Security
Requirement 1: Install and maintain a firewall configuration		MANAGERS			STAFF			OFFICERS		
1.1 Establish firewall and router configuration standards that include the following:	6	A	I		R			I		I
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	6	A	I		R			I		I
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	1	A	I		R			I		I
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	2	A	I		R			I		I
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	6	A	I		R			I		I
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure	2	A	I	I	R	C		I		I
1.1.6 Requirement to review firewall and router rule sets at least every six months	6	A	I		R	C	R	I		I
1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	2	A	I		R	C	R	I		I
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	2	A	I		R		R	I		I
1.2.2 Secure and synchronize router configuration files.	2	A	I		R		R	I		I

The RACI document is a matrix used to clarifying roles and responsibilities for cross-functional/departmental security duties. It is a very valuable tool to document this understanding as well as identify gaps in duty assignments. Project Managers use this tool frequently when leading a multi-team initiative.

There are a few variations of RACI, but all have in common (R)esponsible, (A)ccountable, (C)onsult, and (I)nform. Definitions are provided below:

Responsible – Individual(s) performing the work
Accountable - Individual who are obligated and ultimately manage correct and

© 2012 The SANS Institute Author retains full rights.

thorough completion. This individual manages Responsible, ensuring work is done and compliance is sustained. Common practice is to ensure only one Accountable individual is specified for each duty or deliverable.

Consult – Individual(s) providing expert or management guidance, but not specific duties or recurring tasks.

Inform – Individual(s) kept up-to-date on progress and compliance. Often this is a stakeholder or sponsor. Typically this is a one-way communication.

© 2012 SANS Institute, Author retains full rights.

Appendix D: Project Charter example

Attached is an example merchant PCI Compliance Assessment Project Charter for reference.

PCI DSS Compliance Assessment
Project Charter

B Gold, PMP
PMO
June 1, 2013

© 2012 The SANS Institute Author retains full rights.

Appendix E: Cardholder Data Matrix

The following fields are proposed for a Cardholder Data Matrix. The associated data can be tracked using Microsoft Excel, Microsoft Access, or a CMDB.

Application Name
Application Vendor
Application Version
Application Description
Application Purpose
PABP/PA-DSS Compliance Status
PABP/PA-QSA Name
User Department/Function
Database Name
Database Vendor
Database Version
Table\File name
Cardholder Data Type(s)
Cardholder Data Protection
Operating System Name
Operating System Vendor
Operating System Version
Hardware Platform
Virus Prevention
File Integrity Monitoring
Log Management
Vulnerability Management
Sample/Total Size
Compensating Controls
Accountable Manager
Operations Team(s)
Vendor Contracts

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Appendix F: Project Dashboard example

Below is an example project dashboard for reference.

PCI DSS 2.0 Compliance Assessment

Project Dashboard for October 2013

Project Status: RED

Confidential – Internal Use Only!

Compliance Status Summary

- Draft compliance reports (SAQ, ROC, etc.) prepared for Project Steering Committee review
- Capital spend for PCI projects closed for 2013. Completed under budget.
- Asia and Western United States Book of Evidence completed. Review by QSA has started.

Issues Requiring Management Attention

- As-built documentation for firewalls overdue.
- Review of Master Services Agreements has revealed Field Repair Services contractor does not include terms for safeguarding PCI data.
- EVA for PCI Project is showing actual completion date running 2 weeks late from plan for Requirement 12.

Requirement Compliance Status		Target Date
1 – Firewalls	Y	November
2 – Configuration Standards	R	November
3 – Protect Cardholder Data	Y	October
4 – Encrypt Transmission of Cardholder Data	C	Compliant
5 – Use Anti-Virus	C	Compliant
6 – Patch Systems	G	October
7 – Restrict Access to Cardholder Data	C	Compliant
8 – Assign Unique IDs for Network Admins	G	October
9 – Restrict Physical Access to Cardholder Data	C	Compliant
10 – Track and Monitor Access to Network Resources	G	October
11 – Regularly Test Security Systems	C	Compliant
12 – Develop Standard Operating Procedures	Y	November

Key In-Progress Project Activities	#	P	Lead	Director	
Revise network diagrams reflecting new CDE segment	1.1.2	1	J Smith	B Gold	Y
Example 2					
Example 3					
Example 4					
Example 5					
Example 6					

Legend

- Not Started
- G – Advancing as planned
- Y – Advancing, but requires Management attention
- R – Not Advancing as planned, Management engaged
- C – Completed

© 2012 SANS Institute, Author retains full rights.

Appendix G: PCI Book of Evidence

Below is an example list of items found in a Book of Evidence.

Cardholder Data Matrix
Cardholder Data Flow Maps
Network Topology Drawings
Security Policies and Procedures
Prior PCI Compliance Assessment Reports
Recent Vulnerability Scanning Results
Recent Penetration Testing Results
Organization Charts
RACI
Firewall Configurations
Security Patch Reports
Web Application Security Testing
System Build Guides
Screen Print of POS PC showing PAN masking
Screen Print of Anti-Virus Settings
Screen Print of Encryption Settings
Screen Print of FIM settings
PKI Policy and Design
PAN Scanner Results
Service Provider PCI Certification
Payment Application PCI Certification
Payment Application Security Configuration Guides
Logical Access Control settings
Logical Access Control procedures
Security Incident Handling Plan
Standard Operating Procedures (SOP)
Data Center Building Card Access List
Audit Settings for Security Event Logging
Receipts
Evidence of New Employee Background Checks
Compensating Control Description
Evidence of firewall review
Evidence of entitlement review
Microsoft GPOs

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Last Updated: August 30th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Milan 2015	Milan, IT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
FOR578 Cyber Threat Intelligence	OnlineVAUS	Aug 31, 2015 - Sep 04, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced