IT AUDIT CHECKLIST SERIES

ComplianceINSIGHT

☑

Payment Card Industry (PCI)

Practical guidance on how to prepare for successful audits

www.ITCinstitute.com

ITCi
IT Compliance Institute™

Research Sponsor

Configuresoft

ComplianceINSIGHT

IT AUDIT CHECKLIST SERIES

Payment Card Industry (PCI) ☑

About the IT Compliance Institute

The IT Compliance Institute (ITCi) strives to be a global authority on the role of technology in business governance and regulatory compliance. Through comprehensive education, research, and analysis related to emerging government statutes and affected business and technology practices, we help organizations overcome the challenges posed by today's regulatory environment and find new ways to turn compliance efforts into capital opportunities.

ITCi's primary goal is to be a useful and trusted resource for IT professionals seeking to help businesses meet privacy, security, financial accountability, and other regulatory requirements. Targeted at CIOs, CTOs, compliance managers, and information technology professionals, ITCi focuses on regional- and vertical-specific information that promotes awareness and propagates best practices within the IT community.

For more information, please visit: www.itcinstitute.com

Comments and suggestions to improve the IT Audit Checklists are always encouraged. Please send your recommendations to editor@itcinstitute.com.

Limit of Liability/Disclaimer of Warranty: While the copyright holders, publishers, and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of its contents and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be usable for your situation. You should consult with a professional where appropriate. Neither the publishers nor authors shall be liable for any loss of profit or any other commercial damages, including, but not limited to, special, incidental, consequential, or other damages.

Table of Contents

Executive Overview

What Is the IT Audit Checklist Series?

ITCi IT Audit Checklists are a series of topical papers that provide practical guidance for IT, compliance, and business managers on preparing for successful internal audits of various aspects of their operations. In addition to helping managers understand what auditors look for and why, the IT Audit Checklists can help managers proactively complete self-assessments of their operations, thereby identifying opportunities for system and process improvements that can be performed in advance of actual audit.

What Is This Paper About?

This paper, "IT Audit Checklist: PCI," supports an internal audit of a merchant's technical security controls for payment card data. The paper includes advice on assessing the robustness of PCI controls, recommendations for avoiding common PCI compliance failures, guidance on fulfilling management responsibility in relation to audits, and information on ensuring continual improvement of IT security efforts. The paper is intended to help IT, compliance, audit, and business managers prepare for a PCI audit and to provide concrete tools managers can use to ensure that the audit experience and results are as beneficial as possible to both IT leaders and the company as a whole.

Paper Contents

- This paper supports an internal audit of merchant controls for payment card data protection. The paper includes advice on assessing the robustness of PCI controls, recommendations for avoiding common PCI compliance failures, guidance on fulfilling management responsibility in relation to audits, and information on ensuring continual improvement of IT security efforts.
- Penalties for noncompliance include higher transaction processing fees, fines, and, in extreme cases, denial of credit card processing capabilities. Violators also face legal fees, civil lawsuits, customer rejection and related revenue loss, and other costs and losses.
- Understanding the PCI authority structure is key to maintaining control over PCI strategy and audits. A merchant mantra for compliance should be, "Ask your acquirer."
- For your reference, three key resources are attached to this document: The PCI Data Security Standard (DSS), the PCI Security Audit Procedures (SAP), and the PCI DSS Payment Card Industry Self-Assessment Questionnaire (SAQ).
- The essence of PCI compliance is largely good, old-fashioned IT hygiene and information security best practices. But there is quite a bit of devil in the details of the PCI requirements. The SAP contains more than 250 detailed testing procedures.
- There is merchant confusion about all of the PCI DSS's six main themes: Building and maintaining a secure network, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, monitoring and testing networks, and maintaining an information security policy.
- In-scope environment is the most important thing a PCI project manager should keep in mind. Every effort should be made to minimize the in-scope environment.
- As a robust security standard, PCI has potential benefits beyond its immediate requirements. A generic application of its principles can fulfill other regulatory requirements for information security and privacy.

Introduction to PCI

"PCI" generically refers to a set of information security requirements issued by the Payment Card Industry Security Standards Council (SSC). It is the payment card industry's effort at self regulation.

More specifically, PCI is a joint effort by payment card brands—including Visa International, MasterCard Worldwide, American Express, Discover Financial Services, and JCB to force merchants[1], service providers, and acquirers[2] to reduce the risk of payment card fraud by protecting the global information infrastructure that "stores, processes, or transmits cardholder data."[3] Within the context of PCI, these governing companies are referred to as the "brands."

For many companies, the processes surrounding PCI appear at once well ordered and chaotic. This is fitting, considering that it was the rise of payment card systems that gave birth to the term *chaordic*. The word, coined by Visa founder Dee Hock, describes systems that are both chaotic and ordered; where, among other things, "competition and cooperation…have to be seamlessly blended."[4]

It is exactly this blending of stakeholder interests, both competitive and common, that accounts for many of the subtleties and peculiarities of PCI. Notably, from a reporting and enforcement standpoint, much of what appears to be "passing the buck" in regard to accountability and authority is actually influenced by industry structure and the contractual relationships along the payment-systems value chain.

The good news—for the IT professional attempting to prepare an organization to pass its PCI audit—is that the compliance process doesn't have to be insurmountably confusing. For all the corporate confusion and press hype, the essence of PCI compliance is largely good, old-fashioned IT hygiene and security best practices. Beyond this, PCI specifies three special control objectives that are unique to the payment card industry:

- Point of sales (POS) software used in physical retail locations must not store full magnetic-stripe (magstrip) data
- E-commerce and call-center functions must not retain CVV2 data[5]
- Personal account numbers (PANs) must be encrypted while at rest and masked while being displayed, under most circumstances, if the merchant or acquirer chooses to store full PANs

Of course, there is quite a bit of devil in the details of PCI requirements. The PCI DSS Security Audit Procedures (SAP) document[6] contains more than 230 detailed testing requirements. But, while these audit procedures and even the security standard itself might seem dense (or even cryptic), merchants should remember they are not alone in either the responsibility or accountability for PCI compliance. The merchant mantra should be, "Ask your acquirer." You will hear this phrase again and again, and it does bear repeating.

[1] Throughout this paper, the term *merchants* is often generically used to denote both merchants and service providers subject to PCI compliance. The two types of companies share most control requirements. Where control objectives differ, these variances are specified by the PCI DSS and PCI DSS Security Audit Procedures, attached to this document.

[2] An acquirer is a "Bankcard association member that initiates and maintains relationships with merchants that accept payment cards," according to the PCI SSC, an independent group founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International to develop, manage, and support PCI. From the Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms, https://www.pcisecuritystandards.org/tech/glossary.htm.

[3] Visa USA. What to Do if Compromised: Fraud Investigations and Incident Management Procedures. (2006) http://www.usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf

[4] Hock, Dee. *Birth of the Chaordic Age*. San Francisco: Berrett-Koehler Publishers, 1999.

[5] The CVV2 or Card Validation Value is a three- or four-digit number intended to be a security control for credit card transactions processed via telephone or the Internet. On most cards, the CVV2 is a three-digit number printed on the signature line on the back of cards. American Express prints CVV2s above account numbers on the front of cards.

[6] PCI Security Standards Council. PCI DSS Security Audit Procedures. Delaware: PCI Security Standards Council, 2006. Available at https://www.pcisecuritystandards.org/tech/supporting_documents.htm

What Are the Benefits of PCI Compliance?

As with many compliance efforts, the most obvious benefit of PCI compliance is avoiding the penalties of noncompliance. Because PCI is an industry standard and governed by contract, rather than public law, the exact penalty structure and severity for noncompliance are not well known or standardized. Penalties vary by credit card brand and contract, but generally include higher credit-card processing fees, fines of up to $500,000 per instance of noncompliance, and, in extreme cases, denial of credit card processing capabilities. Visa alone has reported levying $4.6 million in fines in 2006, up from $3.4 million in 2005.[7] Since the payment card brands cannot directly fine merchants, these penalties go to acquirers, who generally pass them on under contractual obligation to offending merchants.

In addition to enforcer penalties, violators also face legal fees, civil lawsuits, customer rejection and related revenue loss, and other pains concrete and intangible that should only haunt most merchants' imaginations. Banks can also attempt to contractually recoup collateral damages from a merchant compromise, billing merchants for costs related to replacing customer credit cards, for example, or passing on fines from the brands for merchant noncompliance. These fines can be substantial. Under Visa's PCI Compliance Acceleration Program (PCI CAP), announced December 2006:

> Acquirers will be fined between $5,000 and $25,000 a month for each of its Level 1 and 2 merchants who have not validated by September 30, 2007 and December 31, 2007 respectively. For prohibited data storage, acquirers failing to provide confirmation that their Level 1 and 2 merchants are not storing full track data, CVV2 or PIN data by March 31, 2007 will be eligible for fines up to $10,000 a month per merchant, subject to escalation in the event material progress toward compliance is not made in a timely manner.[8]

PCI isn't all fear, uncertainty, and doubt, however. PCI CAP also includes financial incentives for compliance. Larger merchants that validate compliance by August 31, 2007, are eligible for a one-time bonus payment. In addition, Visa is offering lower interchange rates to acquirers who can prove compliance among their merchant groups. Although there is no compulsion for acquirers to share their interchange savings with merchants, Visa has "encouraged" acquirers to use the PCI CAP benefits to help merchants meet security goals.

More broadly, as a robust security standard, PCI has potential benefits beyond its immediate requirements. A generic application of its principles can fulfill other regulatory requirements for information security and privacy. As a baseline, PCI compliance can help companies meet security requirements for laws from Sarbanes-Oxley to Gramm-Leach-Bliley, HIPAA, global privacy laws, US federal security standards, and others.

Often, security controls for the various regulations are siloed, inconsistent, even conflicting. Since the PCI Data Security Standard is actually stricter in some regards than HIPAA—and certainly SOX—it offers an opportunity to align disparate control regimes without sacrificing security. For example:

- Establishing an enterprise-wide encryption key management strategy
- Reconciling inconsistent data encryption (and/or hashing and/or masking) protocols
- Standardizing log management and audit trail documentation
- Developing a breach response policy applicable to all systems

[7] Press, David H. Card Association rules and regs 2007: Get ready for scrutiny. The Green Sheet. http://www.greensheet.com/PriorIssues-/070101-/16.htm

[8] "Visa USA Pledges $20 Million in Incentives to Protect Cardholder Data." December 12, 2006. Visa International. http://usa.visa.com/about_visa/press_resources/news/press_releases/nr367.html

The Auditor's Perspective on PCI

Why Audit?

As a robust standard for information security, PCI also offers the risk management benefits of any effective data protection program. All companies possess information that is critical or sensitive, ranging from personal data to financial and product information and customer, brand, and intellectual property information. An information security management program is necessary because threats to the availability, integrity, and confidentiality of the organization's information are great and, apparently, ever increasing.

The benefits of an effective PCI data security program include:

1. The ability to systematically and proactively protect the company from the liabilities and potential costs of credit card data misuse, customer identity theft, and cybercrime

2. Management and control of costs related to information security

3. Greater organizational credibility with the payment card brands, acquirers, staff, and partner organizations

4. Higher customer confidence in the merchant's business systems and practices

5. The ability to make informed, practical decisions about security technologies and solutions and thus increase the return on information security investments

6. Better compliance with other regulatory requirements for security and privacy, such as HIPAA and state and international privacy acts

PCI is chiefly a preventative standard, intended to reduce the risk of payment card-related fraud and information theft. As such, its main benefit can be seen as the reduction of real liabilities related to information breaches. PCI audits provide a level of assurance—and for larger organizations, external validation—that information security controls exist and are effective.

But, while a PCI audit varies little in purpose from most other information security audits, its rationale, scope, participants, and liabilities differ profoundly from those indicated by other laws and standards. Unlike Sarbanes-Oxley and most other regulations, PCI is an industry standard subject to contractual, not public, enforcement. Failure to comply does not result in breach of law, but breach of contract—and customer trust.

The payment card brands can fine only acquirers. They cannot directly fine merchants, software vendors, or (most) service providers. Thus, if a merchant violates PCI rules and incurs a data security breach, the acquirer is initially liable to the brands for any resulting fines. This gives acquirers very strong financial motivation for ensuring merchant compliance with the security standard.

Of course, merchants are not immune to penalty. Acquirers invariably include a clause in merchant contracts that enables them to recoup fines caused by merchant noncompliance. Typically, the acquirer has the ability to unilaterally withdraw funds from the "reserve" they can maintain on a merchant's Demand Deposit Account (DDA). In addition, the merchant risk associated with payment card acceptance is substantially higher than that of the acquirer. Many merchants, including those with physical storefronts, live and die by their ability to accept credit cards. Even a brief ban on credit card processing can have catastrophic consequences for a merchant.

Who Is Responsible for PCI?

The PCI audit responsibility is distributed between merchants, Qualified Security Assessors (QSAs), Approved Scanning Vendors (ASVs), and acquirers. The responsibilities of each party vary by merchant level, as described below. PCI divides the merchant universe into four levels. Audit responsibilities vary by level, which is determined by acquirers based on the volume of transactions processed, the potential risk incumbent in the transactions, and the degree of exposure introduced into the payment system. Merchant levels and requirements, as defined by the brands July 18, 2006, are:

Level 1 merchants that process more than 6,000,000 total transactions per year, any merchant that has suffered a hack or attack that resulted in an account data compromise, and any merchant discretionarily determined by any payment card brand to meet the Level 1 merchant requirements. Level 1 merchants are subject to annual onsite assessments by auditors and must perform quarterly network scans. Audits may be performed by a qualified external auditor or conducted by the internal audit department and certified by a corporate officer. Network scans must be validated by an Approved Scanning Vendor certified by the PCI Security Standards Council (SSC).[9]

Level 2 merchants that process between 1,000,000 and 6,000,000 total transactions per year. Level 2 merchants must complete an annual PCI Self-Assessment Questionnaire, available from the SSC, and perform a quarterly network scan. Questionnaires do not need to be executive certified or validated by an external auditor. Network scans must be validated by an Approved Scanning Vendor certified by the SSC.

Level 3 includes merchants that process between 20,000 and 1 million e-commerce transactions per year. Requirements for Levels 2 and 3 are the same; however, the initial compliance deadlines differ. While the first Level 3 merchant deadlines passed on June 30, 2005, Level 2 merchants have until September 30, 2007, to meet their requirements.

Level 4 includes merchants that process fewer than 20,000 e-commerce transactions per year, and all other merchants that process up to 1 million total transactions per year. Requirements for Level 4 merchants are nominally similar to those for Level 2 and 3 (including a quarterly network scan by an Approved Scanning Vendor); however, validation requirements and deadlines are defined by each merchant's acquirer, as opposed to the SSC or brands.

Irrespective of merchant level, internal information security assurance requires a strong managerial commitment. The board of directors (if one exists), management (of IT, information security, PCI compliance, staff, and business lines), and internal auditors all have significant roles in PCI assurance and the auditing of PCI controls. The big question for many companies is how these stakeholders should work together to ensure that everything that should be done to protect sensitive information is being done—and that cardholder data is protected appropriately.

1. The **board of directors** must provide oversight at a level above other business managers. The directors' role in PCI is to ask managers the right questions and encourage the right results. Directors must set appropriate tone at the top, communicating to executive management the business imperative of effective PCI management. The board also has a role in establishing and overseeing PCI policy and defining the corporate PCI culture—which includes PCI assurance and ethics attitudes.

2. **Executive management** must provide leadership to ensure that PCI efforts are supported and understood across the organization, demonstrating by example the mandate of PCI policies. Executive management must also dedicate sufficient resources to allow controls to be effective.

[9] PCI Security Standards Council (SSC), https://www.pcisecuritystandards.org/

3. **Staff and line-of-business managers** are stakeholders in PCI programs and should understand their responsibilities in regard to compliance, as well as how any changes in network access and system functionality will affect business processes. Managers are accountable for the effectiveness of their own business processes, which often rely on data resources that might incur PCI-related changes.

   Setting a proper "in-scope environment" for your audit can be the most important decision a merchant makes. Start by creating a diagram of how payment card data enters your enterprise, which systems it touches and where the data flows to within your organization. Make an effort to think of the less-than-obvious consumers of this information within your organization. Hidden caches of card numbers in business systems can be a hard-learned lesson, and the biggest repositories of account numbers are often found in databases maintained by the marketing department.

> Setting a proper "in-scope environment" for your audit can be the most important decision a merchant makes. Start by creating a diagram of how payment card data enters your enterprise, which systems it touches, and where the data flows to within your organization.

   Under a separate aspect of management, information security managers should organize and implement the organization's technical information security program, including its monitoring (testing) program.

   IT management must regularly review and monitor PCI controls to ensure they are appropriate, despite ever-changing risks and business requirements. This is, in fact, a form of PCI auditing.

   Although business managers might consider PCI to be a pure-IT function, they can still be affected by technical, procedural, and oversight controls. For example, marketing departments that rely on credit card data for customer analytics are stakeholders in the control process and should be part of the control design and review process. In many cases, the desire to implement compensating controls is driven as much by business needs as by technical feasibility.

4. **Internal auditors** in Level 1 merchants, by mandate, and other merchants at their discretion provide strategic, operational, and tactical support for PCI compliance. For example, internal auditing:

   - Reports to the board and management as to whether key information assets and systems are sufficiently protected, whether business units are adhering to policies, whether programs are in place for continually updating and strengthening safeguards against network assaults, and whether existing security policies are reasonable. In brief, internal audits assess the state of the information control environment and recommend improvements.
   - Independently validates that the organization's PCI efforts are proactive and effective against current and emerging threats. To provide this level of assurance, internal auditors may compare current organizational practices with industry practices and regulatory guidelines.

   To fulfill an audit's potential, internal auditors need to: 1) know what they are doing (have the skills to perform appropriate PCI audits), 2) have a strong understanding of both the technical and the business environment, 3) know what to request, and 4) pursue regular and ongoing training on new guidance and standards of practice. In addition, the auditing function should complement, but never replace or overpower, management's responsibility to ensure its PCI controls are operating properly.

5. **Acquirers** are also responsible for enforcing merchant audits. The brands hold acquirers financially accountable for the effectiveness of merchant information security controls. Acquirers review merchant and vendor audits to ensure control adequacy. Acquirers are "members" of the card association and are bound by the association's operational regulations (*OpRegs* in Visa-speak).

   As an audit authority, each acquirer has some discretion in its interpretation of PCI requirements. This can be both good and bad news for merchants. It means that merchants should make a proactive effort to understand their acquirer's particular interpretation of PCI's audit requirements. Deferring to an acquirer's authority transfers some of the burden (and risk) of interpretation. Since, as a baseline, the goal of PCI compliance is to pass the audit, getting direct advice from your auditor can prevent early guesswork and forestall expensive rework late in PCI projects.

> Merchants should make a proactive effort to understand their acquirer's particular interpretations of PCI's audit requirements.

6. Engagement of **QSAs and ASVs** is required by PCI of some merchants to validate specific aspects of security programs. To support this requirement, the SSC manages certification programs for QSAs and ASVs.

   Level 1 merchants must annually engage a QSA for onsite data security assessments or submit an internal audit assessment signed by a corporate officer. Smaller companies may also opt to engage QSAs to help complete the PCI Self-Assessment Questionnaire (SAQ)[10] that must be submitted to acquirers.

   Engagement of an ASV is required for merchants at all levels. ASVs perform quarterly network vulnerability scans, the results of which are submitted to acquirers along with the QSA audit, certified internal audit, or SAQ.

The size and complexity of various organizations' audit efforts differ, due to PCI's merchant-level requirements, relevant system scope, variations in operating environments, and business and audit objectives. Ensuring appropriate audit focus and scope is another reason management should communicate with auditors, and vice versa, early and often for every audit project.

Understanding the PCI authority structure is key to maintaining control over PCI strategy and audits. To encourage successful audits, merchants should communicate with auditors early and often and request written clarification on acquirer expectations. As a best-practice approach:

1. Develop PCI objectives, stratgies, and implementation plans

2. Communicate your plans with audit staff at your acquirer

3. Ask the acquirer to reply with an accept/decline response

These steps should be performed before you initiate major PCI projects or purchase expensive equipment. By formally accepting your proposed controls, the acquirer accepts any residual risk. This is important in the event your organization ever finds itself in "Safe Harbor" discussions following a security breach.

[10] PCI Security Standards Council. PCI DSS Self-Assessment Questionnaire. Delaware: PCI Security Standards Council, 2006. Available at https://www.pcisecuritystandards.org/tech/supporting_documents.htm

Management's Role in the Audit Process

Where a corporate internal auditing function exists, it may be involved in PCI audits to a greater or lesser degree, according to the requirements associated with its merchant level and the company's capabilities. In larger companies—particularly where PCI is integrated into a broader information protection practice—internal auditors should follow established best practices for audit structure, process, and scope

An internal audit engagement or security self assessment typically has three phases: planning, testing, and reporting. Management has an important role in each phase:

□ **During planning**, management should first focus on the audit plan (the auditor's "road map") and ensure that managers understand and are in general agreement with the audit purpose, focus, and approach. An open, positive discussion with the audit team regarding these defining factors helps management and the audit team communicate expectations up front. Audit planning should focus on critical or sensitive risks, but all risks should be considered. To this end, active involvement by management in audit planning is vital to the overall success of an internal audit.

Management should also discuss the evaluation criteria auditors will use in assessing the risk management program. Finally, managers and auditors should broadly discuss planned audit testing, although auditors must have the authority and discretion to select tests they deem appropriate.

□ **During testing**, management facilitates the auditors' access to appropriate people and systems. Management confirms the audit results, not re-performing the actual tests, but verifying processes and data in order to gain confidence in the audit findings. The audit team leader and senior executives of the areas being audited should communicate regularly throughout the audit process to discuss audit progress, identified issues, and potential actions.

Open, transparent dialogue between management and the audit/assessment team can do much to avert misunderstandings or resolve disputed findings before the audit team issues its draft report. The audit team should communicate critical findings to management as early as possible, even outside of the established meeting schedule. These findings may also be reviewed during regular meetings, but prompt notice is necessary and usually appreciated.

□ **During reporting**, management receives and reviews the auditor findings, plans and develops corrective actions, and implements change

What Auditors Want to See

PCI audits exist to assess how well an information security program meets card data protection requirements. In terms of auditor expectations, PCI is much more explicitly defined than most government regulations. The PCI SAP and self-assessment guide produced by the SSC document a detailed, intrinsically checkbox approach to assessing narrowly defined information security controls that meet (generally) explicit control objectives. From a certain perspective, understanding what PCI auditors—including SVAs and acquirers—want to see is simply a matter of reading the manual.

Even detailed requirements, however, generate some questions of interpretation. The issues documented in the Audit Checklist section of this paper testify to a large body of questions about, and even contention over, PCI requirements. When companies consider integrating PCI requirements into enterprise information security practices, the questions grow.

As noted throughout this paper introduction, PCI managers can seek guidance from acquirers, assessment and testing vendors, and brands, as to what's expected from audit reports. Internal auditors and security assessors should also consider how well PCI efforts support organizational performance goals, as dictated by the CEO, COO, board, and investors.

In general, the managerial goal in the audit process is not simply to make auditors—external and internal—happy, but to demonstrate how well operations, controls, and results meet the needs of the business. During audit planning, managers help internal auditors design an audit process that truly reflects business processes, strategies, and goals. Thus, the managerial response to auditors throughout the process is for the benefit of the business and compliance program, not the benefit of auditors.

Internal auditors exist to provide the board, senior management, and internal and external auditors with an objective, independent assessment of the security program—including what they see as key opportunities for improvement. To prepare their opinions and conclusions, auditors must review and assess evidence of the PCI program and its performance. Under PCI, this assessment is generally in accordance with the SAP and SAQ. If auditors are able to demonstrate control existence and effectiveness and show that accountability is established and enforced, they should produce a positive audit report.

Accordingly, auditors and managers should work toward common goals—auditors striving to earnestly, honestly, and completely assess program effectiveness, and management working to help auditors make valid assessments. In that vein, there are some typical compliance characteristics and managerial processes that auditors do and don't like to see. In all aspects of audit and risk management programs, auditor likes and dislikes vary by company; however, the following list itemizes typical indicators of good and bad audits.

Auditors Like...

□ Good management practices: planning, direction, monitoring, reporting, etc.

□ Proactive management, including required operational monitoring

□ Supervisory review of key performance reports

□ Supervisory review of operating results (especially exception reports and analyses)

□ Well-documented policies and procedures

□ Organized, clear, and up-to-date documentation

□ Managerial actions based on facts, not habits

□ A documented chain of command, roles, accountability, and responsibilities (e.g., organization charts, job descriptions, separation of duties)

□ Adherence to policy and procedures, from senior management through frontline staff

□ Good staff management, including workforce development (bench strength and cross training), assurance that absences do not compromise controls, and policies for secure staff turnover

□ A balance between short- and long-term focus, for both objectives and results

□ Managerial willingness to embrace new ideas

Auditors Don't Like...

□ Interviewing defensive or uninformed managers and executives

□ Wading through piles of disorganized analyses

□ Managers who can't or won't comprehend the level of risk they are incurring

□ The opposite of the "like" items listed above

How Companies (Inadvertently or Intentionally) Help or Hinder Auditors

□ (Not) having requested documentation available at the prearranged time

□ (Not) meeting deadlines and responding to requests

□ (Not) communicating at an appropriate managerial level

□ (Not) ensuring key staff are available to auditors, especially at critical milestones

□ (Not) informing relevant staff about the audit and its goals, impacting the time and effort auditors must spend to explain the audit to affected personnel

□ (Not) having administrative support where needed

□ (Not) providing accurate documentation

Who Should Talk to the Auditors?

An efficient audit process depends on effective communication between auditors, managers, and workers. Management and auditors should strive to balance efficiency (having a minimal number of staff dealing directly with the auditors) with the need for "open access" to management and staff by the audit team (when needed).[11] Obviously, it is impractical and unproductive for both teams to put too many staff in front of auditors. Instead, management should:

□ Provide knowledge of operations through several informed "point" people to interact with auditors. A shortlist of interviewees within the program area being audited can more quickly answer auditor queries and provide better continuity of audit support.

□ Allow ready access to all management and staff, if required by the audit team to gain a clearer picture of overall operations

□ Work with the audit team to draw up a staff interview schedule as part of the planning effort. Update the schedule as necessary during the audit fieldwork phase, if circumstances change.

In many situations, a single internal point of contact for each audited program will provide the vast majority of documentation to the auditors. The role of that individual—and, indeed, for all auditor contacts—is to ensure that the audit team receives accurate and adequate information for the task. Auditors will still use their professional judgment to determine if and when additional sources of information (other staff interviews) are required. The audit team will also conduct a variety of audit tests, if necessary, to confirm their audit analysis.

[11] The audit team is always expected to ensure all their interactions (with all staff) are professional and result in a minimal disruption.

PCI Audit Checklist

A PCI audit should determine that key information security risks are being controlled, that required controls exist and are operating effectively and consistently, and that management and staff have the ability to recognize and respond to new threats and risks as they arise.

If a company processes more than 1 million transactions per year and is a forward-looking organization, it should base its PCI compliance and remediation on the DSS SAP, available from the PCI SSC. Smaller companies may refer to the DSS, but are more likely to focus on the SAQ.

Currently, most brands require a full “Report on Compliance” based on the SAP only from merchants that process more than 6 million transactions annually. However, some brands and acquirers are increasingly training their sights on Level 2 merchants, as well. For example, the Visa CAP program also involves Level 2 merchants. CAP includes extra incentives and penalties for Level 1 and 2 merchants that process more than 1 million transactions per year.

The PCI SAP contains more than 230 specific testing procedures for validating PCI compliance of an organization. These testing procedures are directly related to the 12 requirements and 6 security themes outlined on the DSS.

For most Level 1 and 2 merchants, many of the controls outlined in the SAP are fairly comprehensible. For example, the deployment and use of antivirus protection is straightforward. The most important thing the PCI project manager should keep in mind is the “in-scope environment” to which the control must be applied. Under PCI, the typical merchant needs only ensure antivirus protection is deployed to in-store systems, e-commerce hosts, and the few back-end systems that are 1) on the protected network segment; or 2) reach into the protected network from less-trusted networks, typically via a virtual private network (VPN). There is no need for a merchant to validate antivirus protection for all desktops within the corporate network.[12]

The PCI SSC publishes several free resources to help merchants and auditors meet assessment requirements. For your reference, three key resources are attached to this document:

- The PCI Data Security Standard (DSS)
- The PCI DSS Security Audit Procedures (SAP)
- The PCI DSS Payment Card Industry Self-Assessment Questionnaire (SAQ)

Each of these documents can serve (and in the case of the SAQ is designed) as a PCI checklist. To supplement these lists, the remainder of this section highlights the most common technical-control challenges encountered by PCI stakeholders.

[12] For general information security protection, the merchant should ensure antivirus protection for all systems and machines, but for the sake of passing a PCI audit, merchants can limit focus to only the “in-scope” environment.

Theme 1: Building and Maintaining a Secure Network

Requirements:

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

Number of related testing procedures in SAP: 38

Technologies: Firewall, VPN, routers, configuration management software, network nodes, and computing devices

Most common issue: Egress filtering

Acing an audit for PCI network security requirements is all about segmentation: defining what is in scope and out of scope for each requirement.

Merchants should make every effort to minimize the footprint of the in-scope environment. Typically, a quick win can be found by studying the network path that cardholder data travels during normal day-to-day store transactions. For example, many retailers user a hub-and-spoke strategy for card processing: the transaction starts with a card swipe at the store and travels over a "private network"—a secure socket layer (SSL), standard VPN, or Multiprotocol Label Switching (MPLS) VPN, frame relay virtual circuit, or dial-up line. At the merchant headquarters the connection hits a router and is forwarded to the internal private IP address of a second router, provided by the card processor.

To reduce compliance and audit complexity in this scenario, a merchant could reconfigure the incoming router so that cardholder information is sent only to a protected "PCI in-scope network" interface—a physical or virtual local area network (VLAN). In this way, the remainder of the entire corporate network can be eliminated from the PCI audit scope.

Trouble Points

□ Egress Filtering (DSS sections 1.4.2, 1.3.5, 1.3.7)

A high percentage of retailers incur an adverse audit finding because of poor egress filtering. Most IT organizations focus on implementing ingress filtering (limiting network access from the outside), but the PCI DSS is also very specific about the need for outbound filtering (limiting the traffic that leaves a network). Auditors will look for documented policies, standards, and testing evidence to verify egress filtering.

□ Databases in the DeMilitarized Zone (DSS section 1.3.4)

This failure applies only to applications that are Internet facing, such as e-commerce Web applications, not applications that are used exclusively internally. PCI says the database used by the Internet-facing application cannot also be in the DeMilitarized Zone (DMZ). This is typically accomplished by placing the database on a separate physical server, placed in a different "security zone" than the DMZ.

□ Wireless networks and WiFi encryption (Multiple DSS sections)

Wireless security is addressed throughout the DSS. In general, management should treat wireless networks the same way they treat the Internet—as an untrusted network. Companies should always put a firewall between the WiFi network and the protected network. This is mostly an issue at retail locations that use wireless scanners. Firewalls should be configured for maximum restriction, allowing access only to specific IP/port numbers to which the card scanner needs to communicate. If you are using scanners for inventory control purposes only and no cardholder data traverses them, you may consider the WiFi network to be "out of scope" for the PCI audit. If handheld scanners are used to process transactions (for "line busting," for example), the WiFi network is "in-scope" and you must make sure all security controls are in place, including WiFi encryption.

☐ Segregation of servers (DSS Section 2.2.1)

Section 2.2.1 states: "Implement only one primary function per server (for example, Web servers, database servers, and DNS should be implemented on separate servers)." This requirement generates much confusion and frustration, especially at in-store locations, where retailers want to reduce the number of computing devices they need to support. Management should strive to prevent auditors from interpreting the requirement too literally. The requirement is primarily for infrastructure-type servers. While it is advisable from a security perspective to have multiple servers for sensitive functions, your acquirer may accept an in-store point of sale (POS) server that also supports some other non-POS applications that, for example, may be used by a store manager. In such a case, however, the acquirer might request that the merchant implement compensating controls, such as running the non-POS applications in a separate virtual machine.

Theme 2: Protecting Cardholder Data

Requirements:

3: Protect stored cardholder data

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

Number of related testing procedures in SAP: 34

Technologies: Cryptography; key management

Most common issue: Key management

Many people consider cardholder data protection requirements to be the heart of the DSS. The DSS specifies key information assets that must be protected. Similarly, it lists information that must never be stored after authorization: full magnetic stripe (magstrip) data, CVV2s (card security codes), and personal identification numbers (PINs). Finally, the standard details control objectives that must be implemented if a company stores personal account numbers (PANs).

The first step in audit preparation is to confirm that you are not storing PCI-prohibited data. You can do this manually by reviewing the data flow within your POS application to find the file where the results of a card swipe are written. PCI compliance staff should view relevant data files and verify they are not storing full track data. For example, in SAP's Triversity POS solution, card data is stored in the ld.txn file. The file can be read with any hex viewer.

Be sure to check any debugging logs, transaction logs, and trace files. Restricted data often is written to these outputs in non-compliant systems.

A more exhaustive method of assurance involves using a tool to parse through an entire drive looking for regular expressions that are characteristic of payment card magnetic stripe data. Vendor software like the opensource tool Autopsy Forensic Browser or EnCase Enterprise analyze an entire disk image (including the slack space) for magstrip data. This level of forensic analysis is not specified by the SAP, but is often requested by the brands in cases of data compromise.

Trouble Points

□ Encryption and key management (DSS section 3.34-3.6)

As an indication of just how contentious and problematic encryption is for the average merchant, the PCI council breaks with its common practice and outlines in an official document, specifying compensating controls by which merchants can avoid deploying encryption in some cases.

But the brands are expected to become stricter about encryption. Visa's CAP program is an example of the brands' effort to eliminate the "low-hanging fruit" causes of the worst cases of fraud. CAP targets full track data, CVV2, and PIN-related data. Next, Visa is expected to turn its attention to the "second-worse" cause of fraud: PANS that are not rendered "unreadable wherever [they're] stored."

Implementing encryption, per se, is becoming less technically demanding. Certified AES or 3DES crypto libraries are widely available. The most difficult issue typically is adapting legacy AS/400 applications that were originally written in a fragile manner.

These days, the most persistent difficulty with encryption is not encryption itself, but rather symmetric key management. About 80 percent of the 22 SAP testing procedures related to encryption are about key management, and the PCI SAP is very specific about control objectives for key management (see Testing Procedure 3.4.a, Bullet 4). According to the SAP, proper key management is critical to the acceptability of a solution that "renders PAN unreadable."

Fortunately, the rise of Enterprise Key Management Infratructure (EKMI) represents an approaching watershed for companies struggling with this aspect of PCI compliance. EKMI is an open source effort[13] to reconcile fractious approaches to key management through standardized protocols, implementation guidelines, and controls. Increasingly stringent enforcement of PCI over time will be a major driver of EKMI development and adoption.

EKMI promises an economical way to centrally manage symmetric encryption keys across many different computing devices. Symmetric keys are used by symmetric encryption standards such as AES and 3DES, which are considered "strong encryption" by the PCI DSS.

EKMI should particularly benefit retailers with physical locations. It offers companies an enterprise approach to managing ecryption for hundreds or thousands of geographically dispersed POS devices, in addition to various backend systems that store or process PANs—marketing analytics systems, fraud detection systems, transaction consolidation, and settlement systems. EKMI will even encompass other uses of encryption, such as endpoint security for laptops.

The evolution of symmetric key management issues is similar to that of domain name resolution. Before the development of the Domain Name System (DNS), resolving the IP address of a human readable "host name" was handled via a "host table" file managed manually and individually on each node on the network. As the boundary of managed systems grew to include more hosts, this "provincial" approach to domain name management proved unscalable. Thus, the DNS was adopted as a standardized way to abstract an important, but "ancillary," service from applications and consolidate it on a "centralized" server on the network. In a similar vein, the goal of EKMI is an abstraction of key management capabilities from applications into a scalable enterprise solution.

EKMI standardization is currently managed by the Organization for the Advancement of Structured Information Standards (OASIS), a not-for-profit international consortium that drives the development, convergence, and adoption of e-business standards. Visa International co-chairs the EKMI Technical Committee.

[13] EKMI open source development is managed by the Organization for the Advancement of Structured Information Standards (OASIS) and sponsored in part by the Defense Information Systems Agency of the US Department of Defense (DoD). http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ekmi

However, while EKMI may smooth some of the technical path to encryption, process and people hurdles may prove more persistent. Trying to convince C-level business executives to support encryption by quoting DSS subrequirements such as "Split knowledge and establishment of dual control of keys" or debating the definition of "secure key distribution" is likely to draw limited success. A stronger case can be made by explaining the business value of EKMI from the mundane perspective of key rotation (testing procedure 3.6.4 and 3.6.8). Your PCI auditor is likely to ask for evidence that you have rotated encryption keys at least annually. Furthermore, the standard requires managers to be able to quickly change "known or suspected compromised keys" enterprise-wide. The labor cost of annually and manually replacing keys throughout a distributed POS quickly adds up to more than the cost of deploying an EKMI solution, such as the open source StrongKey.

The labor cost of annually and manually replacing keys throughout a distributed POS quickly adds up to more than the cost of deploying an EKMI solution.

Management should be aware, however, that commercial off-the-shelf POS software is not likely to be plug-and-play when it comes to EKMI. Bought applications must be modified by their vendors to integrate the key-management system's API and accommodate encrypted data and a Global Key-ID(GKID). According to EKMI co-chair Arshad Noor:

> How does one use the SKMS [symmetric key management system] if a specific COTS [commercial off-the-shelf software] at a site does not support it? Currently we are at a stage of the SKMS' evolution, just as DNS and RDBMS [relational database management systems] were at their inception. Before the creation of these "abstraction" technologies, applications had to resolve hostname-IP addresses and perform data management on their own. As DNS and RDBMS protocols and APIs became standards, application developers abandoned their proprietary implementations to adopt industry standards–the monetary benefits were too good to ignore. It is anticipated that SKSML [Symmetric Key Services Markup Language] will be adopted faster than DNS and the RDBMS, because of the same benefits that would accrue to independent software vendors, and also due to the regulatory and TCO [total cost of ownership] pressures on IT organizations.[14]

Another obstacle that arises in EKMI implementation is protecting digital certificates at client machines (POS registers and in-store servers). Typically this process involves using a hardware security model (HSM), which is expensive, or a USB dongle,[15] which can be inconvenient. Over the long term, this issue will go away, as hardware that POS software runs on is refreshed and the new hardware is shipped with a trusted platform module (TPM) chip on the motherboard. It is expected that the widespread proliferation of TPM chips over the next five years will be a crucial and potent enabler of the uptake of EKMI in POS environments.

[14] Noor, Arshad. Symmetric Key Management Systems. http://www.oasis-open.org/committees/download.php/22096/Noor_Symmetric%20Key%20Management%20Systems-1.pdf ISSA Journal. Feb 2007

[15] http://en.wikipedia.org/wiki/Dongle

In the short term, best practices for advancing EKMI (and thereby promoting an easier tomorrow) include:

- If you use a vendor-developed POS system, start urging the vendor to investigate the EKMI standardization project at OASIS.
- If you participate in an "enterprisewide encryption project committee," or other encryption management effort, champion an enterprisewide key-management project that can accommodate multiple encryption engines suited to various applications deployed throughout the enterprise.
- Urge internal development groups to integrate the royalty-free SKCL (Symmetric Key Call Library) with internal applications. Programs written in C/C++ can use a Java Native Interface (JNI). AS/400 must be integrated to an RPG Native Interface (RPGNI).[16]

□ PAN storage (DSS section 3.1)

The requirement to render stored PANs unreadable has probably generated more strategy meetings than any other requirement. This is because concealing PANs involves encryption, a process that can disquiet even experienced IT managers. Not only does encryption involve cryptography (read: math), but it also has significant implications for existing IT systems. As a specific challenge, cryptographic key management is a wholly new field for most IT managers, and even PCI compliance managers.

Before you rush headlong into an encryption and key management, first investigate whether it would be possible to eliminate PAN repositories within your company. In most cases, the business value of keeping PANs is less than the cost of precautions necessary to secure them.

In many cases, marketing departments provide the strongest objections to eliminating PANS. Marketing departments use PANs as unique identifiers that link customer buying patterns, and in marketing-driven companies this can be particularly hard dependency to break. One solution is hashing card numbers to create a different unique identifier that marketing can use. Or the merchant can keep multiple databases—one with complete PANs on a secure server and another production database with hashed numbers. When a new PAN enters the system, two copies of the information are made: one is hashed and entered into the production database; the other is copied into the secure "archive" which is itself protected with whole-disk encryption. The archive's purpose is protective and preventative, in case a valid business reason arises for accessing PANs.

Masking the stored PANs (replacing some numbers with a "mask" value, such as "x"), is also an option, but is impractical for most merchants. Note that masking stored PANs is different than the masking requirement listed in DSS section 3.3, which refers to conditionally masking on the fly, when the PAN is displayed.

[16] Noor, Ashad. Enterprise Key Management Infrastructure (EKMI) (2006). http://www.oasis-open.org/events/adoptionforum2006/slides/noor.pdf

Theme 3: Maintaining a Vulnerability Management Program

Requirements

5: Use and regularly update anti-virus software

6: Develop and maintain secure systems and applications

Related testing procedures in SAP: 33

Technologies: Anti-virus, patch management; Web application firewall; change management system

Most common issue: Web application firewalls

The DSS requires several development controls, per sections 6.3.2, 6.3.3, 6.3.7.b. These include separation of development, testing, and production environments; segregation of duties between development, test, and production environments; and verification of reviews of new code and code changes.

This requirement applies to code reviews for custom software development, as part of the System Development Life Cycle (SDLC). In June 2008, Web-facing applications will also become subject to some specialized control requirements.

Code reviews may currently be conducted by internal personnel for all merchant levels. This situation will also change in 2008, however, as Level 1 merchants become (generally) required to get control validation from external security auditors.

Trouble Point

□ Web application controls (DSS section 6.6)

In 2006, a hype bubble formed around the rumor of a new requirement for the deployment of Web application firewalls (WAFs). Since this was a new concept to many PCI managers, it seemed as if PCI was single-handedly creating a new industry. In fact, the PCI DSS has always required managerial review of new and changed code, per section 6.3.7 in DSS version 1. With version 1.1, however, the standard explicitly divided the review requirement in two categories: custom code that is Web facing and custom code that is not Web facing.

All custom code must still be reviewed by someone other than its author. Version 1.1 says that non-Web-facing code may be reviewed by internal personal; however Web-facing code must be reviewed by an external organization that specializes in application security. This third-party review requirement will go into effect June 30, 2008. Since the requirement is potentially costly and onerous, particularly for smaller merchants, PCI allows a WAF as a compensating control that replaces the third-party review.

PCI's definition of WAF is a bit vague, and many vendors are rushing in to promote the definition that mostly closely resembles their product. Even when WAFs become a "requirement," however, PCI will not "recommend" or "validate" any particular solution. You may also propose other compensating controls that fulfill on the control objective; for example, products like Fortify Software's Defender protect Web-facing networks, but are not marketed as WAFs.

Theme 4: Implementing Strong Access Control Measures

Requirements

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

Number of related testing procedures in SAP: 50

Technologies: ID management systems; directory services; two-factor authentication; physical access control devices (video monitoring, badges); media control systems

Most common issue: Two-factor authentication

Assigning unique IDs can be difficult at the POS level, where retailers may need to design a control workaround or compensating control. An overly rigid or strict interpretation of the requirement on the part of auditors can be costly, so management should make a (diplomatic) effort to control the audit discussion.

Trouble points:

☐ Group accounts (8.1, 8.2)

Requirement 8 is all about passwords. As much as possible, merchants should avoid group or "generic" accounts, in order to be able to tie potentially malicious actions to individuals. Strict enforcement of an individual-account policy is a good place to start. Most sub-requirements of the section can be fulfilled by using MS Active Directory or another modern identity management system, but compliance can get more difficult in POS applications. Merchants should ask their POS system vendors how other customers are ensuring compliance or implementing compensating controls, and how the vendor supports compliance solutions.

☐ Two-factor authentication (8.3)

The DSS requirement 8.3 requires merchants to "Implement two-factor authentication for remote access to the network by employees, administrators, and third parties." The success and cost of meeting this control objective is heavily influenced by the network scope to which the objective applies.

To reduce audit (and security) liabilities, merchants should pursue a scope reduction strategy. The DSS does not require two-factor authentication for all user accounts. It applies only to users who access the in-scope network that "stores, processes, or transmits cardholder data." In a highly segmented approach, two-factor authentication[17] is required of only a handful of people, mostly system administrators.

One goal of an aggressive scope reduction strategy is to put users who have only occasional need for in-scope access outside of the in-scope network. Such users can be on the general corporate network without dragging the entire corporate network into the scope.

Excluding occasional users can be accomplished by using a VPN server and two-factor authentication on the perimeter of the "in-scope" network (not the entire network). Another approach is to configure your perimeter VPN box and internal routers so that only users belonging to a specific group policy (Active Directory group, in Microsoft environments) are allowed access to the in-scope network, after two-factor authentication.

This use of an internal VPN to control access to the in-scope network is heavily promoted by the brands during their training of Qualified Security Assessors (QSAs), vendors certified to perform third-party assessments of PCI-compliant processes.

[17] Two-factor authentication is most often implemented with a one-time password key fob.

□ Access authentication (8.5)

A frequently misunderstood specification is DSS requirement 8.5.16, which requires merchants to "Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users." To confirm this requirement, PCI SAP instructs auditors to: [18]

- (8.5.16.a) Review database configuration settings for a sample of databases to verify that access is authenticated, including for individual users, applications, and administrators
- (8.5.16.b) Review database configuration settings and database accounts to verify that direct SQL queries to the database are prohibited (there should be very few individual database login accounts. Direct SQL queries should be limited to database administrators)

This requirement has generated such controversy that Visa has issued clarification on access logging requirements.[19] The bulletin essentially says that users who access data through a secure application do not need to be authenticated on each access.

□ Video monitoring (9.1)

Requirement 9.1.1 directs companies to "Use cameras to monitor sensitive areas." In recent years, video monitoring technology has become increasingly affordable and easy to implement. Small companies, however, may still struggle to justify the cost and hassle of installing, managing, and storing video logs. As with other requirements, the key to meeting the requirement affordably is limiting the scope of relevance. Since only in-scope machines must to be monitored, meeting the requirement can be as simple as training a camera on the door to one server closet.

Theme 5: Regularly Monitoring and Testing Networks

Requirements:

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

11: Regularly test security systems and processes

Number of related testing procedures in SAP: 39

Technologies: Log management system, network time protocol (NTP)

Most common issue: Log management

Along with vulnerability scanning, log management is an achievable "low-hanging fruit" for compliance that can be quickly and (relatively) inexpensively implemented without incurring much risk.

The key challenge for merchants is to secure audit trails so they cannot be altered. Log management systems (LMSs) can help. An LMS has two main roles: 1) as a forensic tool, and 2) as a monitoring tool. While the DSS[20] refers to both roles, having the raw data as a forensic asset is the brands' primary concern.

In addition to satisfying PCI auditors, proper log management can generate goodwill with the brands in a post-compromise incident response. One of the first questions forensic investigators ask is, "Where are the logs?" Visa CISP in particular has long stressed log maintenance in post-compromise situations.

Trouble spots

□ Log retention and security (10.2-10.5, 10.7)

DSS requirement 10.7 states merchants should "retain audit trail history for at least one year, with a minimum of three months available online."

[18] PCI Data Security Standard Security Audit Procedures Version 1.1. (September 2006) Page 32

[19] Visa. CISP Bulletin: Clarifications to PCI Requirements 3.4 and 10.2-10.3 (July 28, 2006) http://www.usa.visa.com/download/merchants/pci_clarification_assessors.pdf

[20] "The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs." Payment Card Industry Data Security Standard, Version 1.1 (2006). Page 11.

Deploying a log management system (LMS) is the most common way to meet this requirement.

Log management can be as simple as configuring devices to send event logs to the syslog port of a home-made file server, although several vendors offer turnkey appliance solutions. For a home-built LMS, new-generation network-based WORM ("write once, read many") drives offer an affordable way to secure audit trails. In all cases, log collection should reference an NTP server to ensure consistent and accurate time notations.

If removable storage media is used for log retention, the log should be frequently written to the media, in order to achieve an acceptable level of compliance with Requirement 10.5 to "secure audit trails so they cannot be altered."

□ Vulnerability scanning (11.2)

Sections 11.2a and 11.2b are the only DSS subrequirements that address vulnerability scanning. Despite this small footprint—less than 1 percent of the testing procedures required to pass an audit—vulnerability scanning vendors certified under the SSC's ASV program have been some of the primary and most notable beneficiaries of the push for PCI compliance.

Explaining this phenomenon is the fact that engaging an ASV is a relatively low-cost, easily achieved effort for most merchants. It is not an "in-line" activity such as resegmenting a network.

□ File integrity monitoring software (11.5)

A literal reading of Requirement 11.5, which requires the use of file integrity monitoring (FIM) software, might suggest that the software must be deployed on every device that handles cardholder data, as well as other critical file locations—such as log files, to ensure they don't decrease in size. In reality, however, few merchants have FIM deployed extensively. Many merchants request an FIM waiver from their acquirer on the basis of compensating controls that meet the same control objective.

Theme 6: Maintaining an Information Security Policy

Requirements

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

Number of related testing procedures in SAP: 39

Technologies: Hosted vulnerability scanning services from an AVS, penetration and internal testing solutions, intrusion detection system (IDS), FIM software

Most common issue: Policy enforcement

DSS section 12 has extensive requirements for policy management, including employee training. In fact, however, many merchants lack comprehensive information security policies. They struggle to draft policies and, more importantly, implement them once they exist.

Trouble spot

□ Policy enforcement (12.1-12.4)

Merchants often contract a QSA to provide, for a price, boilerplate policies that can be tailored to specific environments. Whether you generate policies from scratch or a template; however, bear in mind two stress-saving measures:

- You can implement a "lightweight" set of policies
- For the purposes of PCI, policies need apply only to the in-scope network

Audit Reporting

During the reporting phase, management and the board of directors receive formal feedback from the audit team (or vendor). This knowledge transfer should be an open and transparent process. PCI supplies auditors and vendors with free tools to facilitate the assessment process. The SAP and SAQ (attached) can help focus both audit testing efforts and reporting discussions.

Almost every audit identifies opportunities for improvement. The primary goal of management and auditors should be to address critical issues first, followed by important issues. Both management and auditors should work to ensure that, whatever action plans they agree to, the goals are achievable and beneficial to the organization.

During the reporting phase, management must determine which corrective actions it will implement, based on audit findings. Managers will provide oversight and support to ensure the timely resolution of found issues. Although the audit team may make recommendations based on its assessments of risks and consequences, it cannot make or dictate managerial decisions.

The following are typical steps an audit team takes to confirm and release the audit results.

□ Auditors debrief management, formally discussing significant audit findings and conclusions before they issue the final audit report

□ Managers receive a written draft report from auditors

    __ The report communicates audit results clearly and precisely

    __ Results are presented in an unbiased tone, noting where management has taken actions to correct deficiencies and acknowledging good performance

□ Management and auditors discuss the draft report

□ Management provides feedback on the draft report

□ Auditors review managerial comments and action plan(s)

□ Auditors finalize and distribute the final audit report

□ Auditors close out the internal audit project and plan any necessary follow-up efforts regarding management's action plans

Auditors might also choose to communicate some audit findings that might be useful for PCI efficiency and effectiveness, but do not warrant inclusion in the formal report. This type of communication should be documented, if only as a note in audit findings that the issue has been verbally discussed.

Preparing for an Audit

A well-managed business unit or governance program includes robust plans, procedures, goals, objectives, trained staff, performance reporting, and ongoing improvement efforts. When an internal auditing team is involved, it looks for evidence that the PCI program is well organized and well managed. The program must also specifically and evidently mitigate security risks related to cardholder data. Managerial preparation should mainly be routine, day-to-day practices.

Management's ultimate goal in the audit process is not to make auditors happy, but rather to demonstrate that PCI efforts meet the demands of the CEO and other executives, payment card brands, and acquirers. Likewise, auditor requests should be aligned with these overarching needs; that is, to support responsible program performance within a sound, ethical business environment.

Prior to the audit, managers should collect the information and documentation necessary to demonstrate how well they manage their operations in concert with the overall organizational business objectives. They should be prepared to provide auditors with evidence of well-managed PCI efforts and results. This might include documentation of information security plans, supporting budgets, policy and procedure manuals, organizational charts, logs and trending information, and finally, any other relevant evidence that demonstrates a well-run, compliant program.

In selecting documentation, management should not try to overload the audit team with information, but to provide genuine insight into how the information PCI program is run and how well it is doing. The PCI SAP is fairly specific about what sort of evidence auditors require and should be a primary resource for audit preparation.

Other steps management should take to prior to the audit or assessment:

□ Learn early and contribute often to the internal audit goals, approach, and testing procedures. In particular, setting an appropriate purpose and the audit approach are the two most important elements of every successful audit.

□ Discuss with audit management the evaluation criteria and standards and how the audit will actually be conducted, in order to ensure that you'll receive a "quality" audit.

□ Know who is on the audit team and their qualifications, talents, and motivations. The audit team exists to help make your operations more efficient and effective, but they are also individuals with strengths and weaknesses common to many employees. It pays to know the experience of your auditors, whether they're rookies or veterans (and perhaps to push for the latter). Showing an interest in their work can also influence and increase the benefits from the audit—within reason. At the end of the day, auditors still need to be independent and objective.

Throughout any discussion with an internal audit team prior to the audit, management should try to strike a balance between influence and deference. Managers should neither yield entirely to the audit team nor micro-manage its efforts.

Communicating with Auditors

Like any interaction between people, but particularly in the work environment, a professional and trusting relationship is a strong precursor to successful collaboration.

When managers interact with the auditors in a professional manner, they tell the audit team its function is respected and supported. Likewise, lackadaisical efforts by managers and staff reflect poorly on the business unit or process, its capabilities, and its performance. Managers should also expect professional interaction from the audit team and push back whenever they see an exception to this practice.

To contribute to a successful and accurate audit report, managers should be receptive to auditor observations and the audit team's recommendations. Managers should also be firm when discussing anything they see as incorrect, in order to ensure there are no misunderstandings.

Finally, always remember: managers, not auditors, are responsible for defining and implementing solutions to issues found in the audit. Thus, it is in everyone's best interest to have a cooperative, collaborative audit process that respects the independence and discretion of all participants. Auditors should listen to management. And for its part, management should encourage staff to be open and honest with auditors.

Research Sponsor

Security, Compliance and Control for the Virtualized World.

Configuresoft

Configuresoft is an innovator in systems management technology, delivering the enterprise Configuration Intelligence™ to effectively and efficiently manage today's heterogeneous computing infrastructures. Spanning both security and operations, the Company's configuration management, compliance and remediation products are used by 12 of the world's 25 largest companies to keep their critical systems properly configured, while ensuring compliance with regulatory requirements such as Sarbanes-Oxley, FISMA, GLBA, Basel II, HIPAA and DISA, and industry standards such as ISO 27001, PCI DSS and Microsoft Security Hardening Guides.

To contact Configuresoft, please call (888) U-CONFIG or visit www.configuresoft.com.

ABOUT THE AUTHORS

Ken Adler, PCI-QDSP, CISA, CISSP, CPMP

Ken Adler is a Visa-certified PCI-QDSP, Certified Information Security Auditor (CISA), Certified Information System Security Professional (CISSP), and a Certified Project Management Professional (PMP) with ITIL certifications. Adler has more than 20 years of experience in the enterprise computing and Internet industries. A Pioneer Member of the Internet Society and early participant in APCCIRN, APNG, and APRICOT, he is a veteran of numerous start-ups, including NetSpeed, acquired by Cisco Systems in 1997. Since 2000, he has focused on information security consulting. His contracts have included Visa USA's Cardholder Information Security Program (CISP), Level 1-4 merchants, service providers, auditing firms, and financial institutions. Adler is a member of the Enterprise Key Management Infrastructure technical committee at OASIS, a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. Adler graduated magna cum laude, Phi Beta Kappa from the Syracuse University Honors Program (1984) with dual degrees in telecommunications management and Russian studies. Adler is co-founder of pciFile, the payment card industry's first grassroots effort to improve the PCI compliance-reporting process. The pciFile discussion group, pciFile.ORG, is the Internet's most active forum for discussing PCI topics. A related site, pciFile.COM, is an open platform for PCI compliance operations.

Dan Swanson, CMA, CIA, CISA, CISSP, CAP

Dan Swanson is a 24-year internal audit veteran who was most recently director of professional practices at the Institute of Internal Auditors. Prior to his work with the IIA, Swanson was an independent management consultant for over 10 years. Swanson has completed internal audit projects for more than 30 different organizations, spending almost 10 years in government auditing at the federal, provincial, and municipal levels, and the rest in the private sector, mainly in the financial services, transportation, and health sectors. The author of more than 75 articles on internal auditing and other management topics, Swanson is currently a freelance writer and independent management consultant. Swanson recently led the writing of the OCEG internal audit guide for use in audits of compliance and ethics programs (www.oceg.org) and participated in the COSO small business task force efforts to provide guidance for smaller public companies regarding internal control over financial reporting (www.coso.org). Swanson is a regular columnist for Compliance Week and also writes the ITCi "Auditor Answers" column.

If you have ideas for improving ITCi's IT Audit Checklists, please write editor@itcinstitute.com.

Legal Notice

When assessing any legal matter, do not rely solely on materials published by third parties, including the content in this paper, without additionally seeking legal counsel familiar with your situation and requirements. The information contained in this IT Audit Checklist is provided for informational and educational purposes and does not constitute legal or other professional advice. Furthermore, any applicability of any legal principles discussed in this paper will depend on factors specific to your company, situation, and location. Consult your corporate legal staff or other appropriate professionals for specific questions or concerns related to your corporate governance and compliance obligations.

ITCi makes every effort to ensure the correctness of the information we provide, to continually update our publications, and to emend errors and outdated facts as they come to our attention. We cannot, however, guarantee the accuracy of the content in this site paper, since laws change rapidly and applicability varies by reader.

The information in this publication is provided on an "as is" basis without warranties of any kind, either expressed or implied. The IT Compliance Institute disclaims any and all liability that could arise directly or indirectly from the reference, use, or application of information contained in this publication. ITCi disclaims any liability, whether based in contract, tort, strict liability, or otherwise, for any direct, indirect, incidental, consequential, punitive or special damages arising out of or in any way connected with access to or use of the information in this paper.

ITCi does not undertake continuous reviews of the Web sites and other resources referenced in this paper. We are not responsible for the content published by other organizations. Such references are for your convenience only.

Glossary of Terminology and Abbreviations

The following list explains abbreviations used throughout this paper. Where a single abbreviation has both a strict expansion (the actual words used to form the abbreviation) and *common* usage that is broader than the *strict* expansion, the different uses are noted.

Acquirer	A financial institution, usually a bank, that processes credit card transactions received through merchants *Also*: Acquiring bank
AES	Advanced Encryption Standard, a cryptographic algorithm published by the US National Institute of Standards and Technology (NIST) and specified in Federal Information Processing Standard (FIPS) 197
ASV	Approved Scanning Vendor, an independent company engaged to perform quarterly network vulnerability scans
Asymmetric encryption	A form of encryption in which different keys must be used for encryption and decryption
Brand	A payment card company, such as Visa or MasterCard, responsible for governing PCI
Cardholder	An individual who owns or uses a payment card
Cardholder data	Payment card and customer data, including, but not limited to, the cardholder name, card expiration date, customer primary account number (PAN), and CVV2
Chaordic	A term coined by Visa founder Dee Hock to describe systems that are both chaotic and ordered
Compensating control	Policies and procedures that meet a stated control objective, but are not consistent with the control requirement of the DSS
Compromise	An information security breach that allows unauthorized access to cardholder data
CVV2	Card Validation Value 2, a three-digit security number, usually printed on the back of physical payment cards *Also*: Security code, CID or Card Identification Number, CAV2 or Card Authentication Value 2, CVC2 or Card Validation Code 2
DMZ	DeMilitarized zone, a network added between a private and a public network to provide an additional layer of security
DNS	Domain name system or domain name server, a system that stores information associated with domain names in a distributed database on networks
DSS	Data Security Standard *Also*: PCI DSS
Egress	Traffic exiting a network
EKMI	Enterprise Key Management Infratructure, an open source effort to reconcile fractious approaches to key management through standardized protocols, implementation guidelines, and controls
Encryption	The process of encoding information so that it that cannot be readily interpreted. The product of encryption is ciphertext.
IDS	Intrusion detection system, a technology used to alert system managers about network events that represent illicit use or access *Also*: Intrusion protection system or IPS
Ingress	Traffic entering a network
Key	An algorithmic value used to encrypt and/or decrypt information

Glossary of Terminology and Abbreviations (cont.)

LAN	Local area network, a highly localized computer network
MagStrip	Magnetic stripe data, cardholder data encoded in the magnetic stripe on the back of credit cards *Also*: Track data, full-track data
Network	Two or more connected computers
NTP	Network Time Protocol, a method for synchronizing the clocks of computer systems over a network
PAN	Primary account number, the unique account number embossed (or printed) on a payment card that identifies the account holder and the payment card brand
Payment card	A credit or debit card
PCI	Payment Card Industry (strict); Payment Card Industry requirements (common); Payment Card Industry Data Security Standard (common)
PIN	Personal identification number, a cardholder-defined security number
Policy	A documented rule designed to support or meet a particular control objective
POS	Point of sale, a merchant environment where a product can be purchased
POS system	Point of sale system, a computer used to process electronic transactions at the point of sale
Procedure	A description of the actions required to implement a policy
QSA	Qualified Security Assessor, an independent vendor certified by PCI SSC to perform onsite security audits
RSA	An encryption algorithm published by RSA Laboratories, a subdivision of EMC
SAQ	Self-Assessment Questionnaire, a tool published by the PCI SSC to help merchants validate the existence and effectiveness of PCI-compliant security controls
SQL	Structured query language, a computer language used to interact with relational database management systems (RDBMSs)
SSC	Security Standards Council (also PCI SSC), an independent association of major payment card companies charged with managing the PCI Data Security Standard and its supporting documents
SSL	Secure socket layer, an encryption standard for Web traffic
Symmetric encryption	A form of encryption in which a single key can be used for both encryption and decryption
Two-factor authentication	An access management controls that requires users to present two verifiable pieces of information (credentials) to enter a system. Each credential is something the user knows (personal data), has (a software or hardware device), or is (a biometric) *Also*: Strong authentication
VPN	Virtual private network, a secure, controlled-access network established over a public network
Vulnerability	A security weakness that can be exploited to gain illicit access to a network, network resources, or data
Vulnerability scan	An automated scan used to identify vulnerabilities on a network
WiFi	Initially a truncation and concatenation of *wireless fidelity*, but now generally referred to independently. A wireless network.

PCI Security Standards Council™

Payment Card Industry (PCI) Data Security Standard

Version 1.1

Release: September, 2006

Build and Maintain a Secure Network

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

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

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

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

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

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

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

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

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Preface

This document describes the 12 Payment Card Industry (PCI) Data Security Standard (DSS) requirements. These PCI DSS requirements are organized in 6 logically related groups, which are “control objectives.”

The following table illustrates commonly used elements of cardholder and sensitive authentication data; whether **storage** of each data element is permitted or prohibited; **and if each data element** must be **protected**. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply.

	Data Element	**Storage Permitted**	**Protection Required**	**PCI DSS Req. 3.4**
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

** These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.*

*** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).*

These security requirements apply to all “system components.” System components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (Internet) applications.

Build and Maintain a Secure Network

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

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

1.1 Establish firewall configuration standards that include the following:

- **1.1.1** A formal process for approving and testing all external network connections and changes to the firewall configuration
- **1.1.2** A current network diagram with all connections to cardholder data, including any wireless networks
- **1.1.3** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
- **1.1.4** Description of groups, roles, and responsibilities for logical management of network components
- **1.1.5** Documented list of services and ports necessary for business
- **1.1.6** Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)
- **1.1.7** Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented
- **1.1.8** Quarterly review of firewall and router rule sets
- **1.1.9** Configuration standards for routers.

1.2 Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.

1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include the following:

- **1.3.1** Restricting inbound Internet traffic to Internet protocol (IP) addresses within the DMZ (ingress filters)
- **1.3.2** Not allowing internal addresses to pass from the Internet into the DMZ
- **1.3.3** Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network)
- **1.3.4** Placing the database in an internal network zone, segregated from the DMZ
- **1.3.5** Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment
- **1.3.6** Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted) should have the same secure configuration

1.3.7 Denying all other inbound and outbound traffic not specifically allowed

1.3.8 Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)

1.3.9 Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.

1.4 Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).

1.4.1 Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic

1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ.

1.5 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).

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

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

2.1 Always change vendor-supplied defaults **before** installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).

2.1.1 **For wireless environments**, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

2.2.1 Implement only one primary function per server (*for example, web servers, database servers, and DNS should be implemented on separate servers)*

2.2.2 Disable all unnecessary and insecure services and protocols *(services and protocols not directly needed to perform the devices' specified function)*

2.2.3 Configure system security parameters to prevent misuse

2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.

2.4 Hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: "PCI DSS Applicability for Hosting Providers."

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.

3.2 Do not store sensitive authentication data subsequent to authorization (even if encrypted).

Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3*:*

3.2.1 Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data

In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements. Note: See "Glossary" for additional information.

3.2.2 Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions

Note: See "Glossary" for additional information.

3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.

3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).

Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point of sale [POS] receipts).

3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:

- Strong one-way hash functions (hashed indexes)
- Truncation
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key management processes and procedures.

The MINIMUM account information that must be rendered unreadable is the PAN.

If for some reason, a company is unable to encrypt cardholder data, refer to Appendix B: "Compensating Controls for Encryption of Stored Data."

3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.

3.5 Protect encryption keys used for encryption of cardholder data against both disclosure and misuse.

3.5.1 Restrict access to keys to the fewest number of custodians necessary

3.5.2 Store keys securely in the fewest possible locations and forms.

3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:

3.6.1 Generation of strong keys

3.6.2 Secure key distribution

3.6.3 Secure key storage

3.6.4 Periodic changing of keys

- As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically
- At least annually.

3.6.5 Destruction of old keys

3.6.6 Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)

3.6.7 Prevention of unauthorized substitution of keys

3.6.8 Replacement of known or suspected compromised keys

3.6.9 Revocation of old or invalid keys

3.6.10 Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities.

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

Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.

4.1 Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).

4.1.1 **For wireless networks transmitting cardholder data**, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:

- Use with a minimum 104-bit encryption key and 24 bit-initialization value
- Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS
- Rotate shared WEP keys quarterly (or automatically if the technology permits)
- Rotate shared WEP keys whenever there are changes in personnel with access to keys
- Restrict access based on media access code (MAC) address.

4.2 Never send unencrypted PANs by e-mail.

Maintain a Vulnerability Management Program

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

Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.

5.1 Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers)

Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.

5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.

5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.

6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.

6.3 Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.

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

6.3.2 Separate development, test, and production environments

6.3.3 Separation of duties between development, test, and production environments

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

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

6.3.6 Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers

6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.

6.4 Follow change control procedures for all system and software configuration changes. The procedures must include the following:

6.4.1 Documentation of impact

6.4.2 Management sign-off by appropriate parties

6.4.3 Testing of operational functionality

6.4.4 Back-out procedures

6.5 Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:

6.5.1 Unvalidated input

6.5.2 Broken access control (for example, malicious use of user IDs)

6.5.3 Broken authentication and session management (use of account credentials and session cookies)

6.5.4 Cross-site scripting (XSS) attacks

6.5.5 Buffer overflows

6.5.6 Injection flaws (for example, structured query language (SQL) injection)

6.5.7 Improper error handling

6.5.8 Insecure storage

6.5.9 Denial of service

6.5.10 Insecure configuration management

6.6 Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:

- Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security
- Installing an application layer firewall in front of web-facing applications.

Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.

Implement Strong Access Control Measures

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

This requirement ensures critical data can only be accessed by authorized personnel.

7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.

7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.

Requirement 8: Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

8.1 Identify all users with a unique user name before allowing them to access system components or cardholder data.

8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users:

- Password
- Token devices (e.g., SecureID, certificates, or public key)
- Biometrics.

8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

8.4 Encrypt all passwords during transmission and storage on all system components.

8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:

8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects

8.5.2 Verify user identity before performing password resets

8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use

8.5.4 Immediately revoke access for any terminated users

8.5.5 Remove inactive user accounts at least every 90 days

8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed

8.5.7 Communicate password procedures and policies to all users who have access to cardholder data

8.5.8 Do not use group, shared, or generic accounts and passwords

8.5.9 Change user passwords at least every 90 days

8.5.10 Require a minimum password length of at least seven characters

8.5.11 Use passwords containing both numeric and alphabetic characters

8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used

8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts

8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID

8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal

8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

9.1 Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.

- **9.1.1** Use cameras to monitor sensitive areas. Audit collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law
- **9.1.2** Restrict physical access to publicly accessible network jacks
- **9.1.3** Restrict physical access to wireless access points, gateways, and handheld devices.

9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible.

"Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.

9.3 Make sure all visitors are handled as follows:

- **9.3.1** Authorized before entering areas where cardholder data is processed or maintained
- **9.3.2** Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees
- **9.3.3** Asked to surrender the physical token before leaving the facility or at the date of expiration.

9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law.

9.5 Store media back-ups in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility.

9.6 Physically secure all paper and electronic media (including computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder data.

9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data including the following:

- **9.7.1** Classify the media so it can be identified as confidential
- **9.7.2** Send the media by secured courier or other delivery method that can be accurately tracked.

9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).

9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.

- **9.9.1** Properly inventory all media and make sure it is securely stored.

9.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:

- **9.10.1** Cross-cut shred, incinerate, or pulp hardcopy materials
- **9.10.2** Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.

Regularly Monitor and Test Networks

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

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

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

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

10.2.1 All individual user accesses to cardholder data

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

10.2.3 Access to all audit trails

10.2.4 Invalid logical access attempts

10.2 5 Use of identification and authentication mechanisms

10.2.6 Initialization of the audit logs

10.2.7 Creation and deletion of system-level objects.

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

10.3.1 User identification

10.3.2 Type of event

10.3.3 Date and time

10.3.4 Success or failure indication

10.3.5 Origination of event

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

10.4 Synchronize all critical system clocks and times.

10.5 Secure audit trails so they cannot be altered.

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

10.5.2 Protect audit trail files from unauthorized modifications

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

10.5.4 Copy logs for wireless networks onto a log server on the internal LAN.

10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.

10.7 Retain audit trail history for at least one year, with a minimum of three months online availability.

Requirement 11: Regularly test security systems and processes

Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.

11.1 Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

Note: Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry. Scans conducted after network changes may be performed by the company's internal staff.

11.3 Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:

11.3.1 Network-layer penetration tests

11.3.2 Application-layer penetration tests.

11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.

11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.

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

Maintain an Information Security Policy

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

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:

- **12.1.1** Addresses all requirements in this specification
- **12.1.2** Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment
- **12.1.3** Includes a review at least once a year and updates when the environment changes.

12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).

12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:

- **12.3.1** Explicit management approval
- **12.3.2** Authentication for use of the technology
- **12.3.3** List of all such devices and personnel with access
- **12.3.4** Labeling of devices with owner, contact information, and purpose
- **12.3.5** Acceptable uses of the technologies
- **12.3.6** Acceptable network locations for the technologies
- **12.3.7** List of company-approved products
- **12.3.8** Automatic disconnect of modem sessions after a specific period of inactivity
- **12.3.9** Activation of modems for vendors only when needed by vendors, with immediate deactivation after use
- **12.3.10** When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access.

12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.

12.5 Assign to an individual or team the following information security management responsibilities:

- **12.5.1** Establish, document, and distribute security policies and procedures
- **12.5.2** Monitor and analyze security alerts and information, and distribute to appropriate personnel
- **12.5.3** Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations
- **12.5.4** Administer user accounts, including additions, deletions, and modifications
- **12.5.5** Monitor and control all access to data.

12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.

- **12.6.1** Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions)

12.6.2 Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures.

12.7 Screen potential employees to minimize the risk of attacks from internal sources.

For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.

12.8 If cardholder data is shared with service providers, then contractually the following is required:

12.8.1 Service providers must adhere to the PCI DSS requirements

12.8.2 Agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses.

12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.

12.9.1 Create the incident response plan to be implemented in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing the Acquirers and credit card associations)

12.9.2 Test the plan at least annually

12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts

12.9.4 Provide appropriate training to staff with security breach response responsibilities

12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems

12.9.6 Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

12.10 All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following:

12.10.1. Maintain a list of connected entities

12.10.2. Ensure proper due diligence is conducted prior to connecting an entity

12.10.3. Ensure the entity is PCI DSS compliant

12.10.4. Connect and disconnect entities by following an established process.

Appendix A: PCI DSS Applicability for Hosting Providers

Requirement A.1: Hosting providers protect cardholder data environment

As referenced in Requirement 12.8, all service providers with access to cardholder data (including hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that hosting providers must protect each entity's hosted environment and data. Therefore, hosting providers must give special consideration to the following:

A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, as in A.1.1 through A.1.4:

- **A.1.1** Ensure that each entity only has access to own cardholder data environment
- **A.1.2** Restrict each entity's access and privileges to own cardholder data environment only
- **A.1.3** Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10
- **A.1.4** Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.

A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. *Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not necessarily guaranteed. Each entity* must *comply with the PCI DSS and validate compliance as applicable.*

Appendix B: Compensating Controls

Compensating Controls – General

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a technical specification of a requirement, but has sufficiently mitigated the associated risk. See the PCI DSS Glossary for the full definition of compensating controls.

The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments. Each compensating control must be thoroughly evaluated after implementation to ensure effectiveness.

The following guidance provides compensating controls when companies are unable to render cardholder data unreadable per requirement 3.4.

Compensating Controls for Requirement 3.4

For companies unable to render cardholder data unreadable (for example, by encryption) due to technical constraints or business limitations, compensating controls may be considered. *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Companies that consider compensating controls for rendering cardholder data unreadable must understand the risk to the data posed by maintaining readable cardholder data. Generally, the controls must provide additional protection to mitigate any additional risk posed by maintaining readable cardholder data. The controls considered must be in addition to controls required in the PCI DSS, and must satisfy the “Compensating Controls” definition in the PCI DSS Glossary. Compensating controls may consist of either a device or combination of devices, applications, and controls that meet **all of the** following conditions:

1. Provide additional segmentation/abstraction (for example, at the network-layer)
2. Provide ability to restrict access to cardholder data or databases based on the following criteria:
   - IP address/Mac address
   - Application/service
   - User accounts/groups
   - Data type (packet filtering)
3. Restrict logical access to the database
   - Control logical access to the database independent of Active Directory or Lightweight Directory Access Protocol (LDAP)
4. Prevent/detect common application or database attacks (for example, SQL injection).

Payment Card Industry (PCI) Data Security Standard

Security Audit Procedures

Version 1.1

Release: September 2006

Table of Contents

Introduction

The PCI Security Audit Procedures are designed for use by assessors conducting onsite reviews for merchants and service providers required to validate compliance with Payment Card Industry (PCI) Data Security Standard (DSS) requirements. The requirements and audit procedures presented in this document are based on the PCI DSS.

This document contains the following:

- **Introduction**
- **PCI DSS Applicability Information**
- **Scope of Assessment for Compliance with PCI DSS Requirements**
- **Instructions and Content for *Report On Compliance***
- **Revalidation of Open Items**
- **Security Audit Procedures**

APPENDICES

- **Appendix A: PCI DSS Applicability for Hosting Providers (with Testing Procedures)**
- **Appendix B: Compensating Controls**
- **Appendix C: Compensating Controls Worksheet/Completed Example**

PCI DSS Applicability Information

The following table illustrates commonly used elements of cardholder and sensitive authentication data; whether **storage** of each data element is permitted or prohibited; **and if each data element** must be **protected**. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

	Data Element	Storage Permitted	Protection Required	PCI DSS REQ. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

Scope of Assessment for Compliance with PCI DSS Requirements

The PCI DSS security requirements apply to all "system components." A system component is defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include, but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (internet) applications.

Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from the rest of the network, may reduce the scope of the cardholder data environment. The assessor must verify that the segmentation is adequate to reduce the scope of the audit.

A service provider or merchant may use a third party provider to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment. The relevant services of the third party provider must be scrutinized either in 1) each of the third party provider's clients' PCI audits; or 2) the third party provider's own PCI audit.

For service providers required to undergo an annual onsite review, compliance validation must be performed on all system components where cardholder data is stored, processed, or transmitted, unless otherwise specified.

For merchants required to undergo an annual onsite review, the scope of compliance validation is focused on any system(s) or system component(s) related to authorization and settlement where cardholder data is stored, processed, or transmitted, including the following:

- All external connections into the merchant network (for example; employee remote access, payment card company, third party access for processing, and maintenance)
- All connections to and from the authorization and settlement environment (for example, connections for employee access or for devices such as firewalls and routers)
- Any data repositories outside of the authorization and settlement environment where more than 500 thousand account numbers are stored. Note: Even if some data repositories or systems are excluded from the audit, the merchant is still responsible for ensuring that all systems that store, process, or transmit cardholder data are compliant with the PCI DSS
- A point-of-sale (POS) environment – the place where a transaction is accepted at a merchant location (that is, retail store, restaurant, hotel property, gas station, supermarket, or other POS location)
- If there is no external access to the merchant location (by Internet, wireless, virtual private network (VPN), dial-in, broadband, or publicly accessible machines such as kiosks), the POS environment may be excluded

Wireless

If wireless technology is used to store, process, or transmit cardholder data (for example, point-of-sale transactions, “line-busting”), or if a wireless local area network (LAN) is connected to or part of the cardholder environment (for example, not clearly separated by a firewall), the Requirements and Testing Procedures for wireless environments apply and must be performed as well. Wireless security is not mature yet, but these requirements specify that basic wireless security features be implemented to provide minimal protection. Since wireless technologies cannot yet be secured well, before wireless technology is put in place, a company should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission or waiting to deploy more secure technology.

Outsourcing

For those entities that outsource storage, processing, or transmission of cardholder data to third party service providers, the *Report on Compliance* must document the role of each service provider. Additionally, the service providers are responsible for validating their own compliance with the PCI DSS requirements, independent of their customers’ audits. Additionally, merchants and service providers must contractually require all associated third parties with access to cardholder data to adhere to the PCI DSS. *Refer to Requirement 12.8 in this document for details.*

Sampling

The assessor may select a representative sample of system components to test. The sample must be a representative selection of all of the types of system components, and include a variety of operating systems, functions, and applications that are applicable to the area being reviewed. For example, the reviewer could choose Sun servers running Apache WWW, NT servers running Oracle, mainframe systems running legacy card processing applications, data transfer servers running HP-UX, and Linux Servers running MYSQL. If all applications run from a single OS (for example, NT, Sun), then the sample should still include a variety of applications (for example, database servers, web servers, data transfer servers).

When selecting samples of merchants’ stores or for franchised merchants, assessors should consider the following:

- If there are standard, required PCI DSS processes in place that each store must follow, the sample can be smaller than is necessary if there are no standard processes, to provide reasonable assurance that each store is configured per the standard process.
- If there is more than one type of standard process in place (for example, for different types of stores), then the sample must be large enough to include stores secured with each type of process.
- If there are no standard PCI DSS processes in place and each store is responsible for their processes, then sample size must be larger to be assured that each store understands and implements PCI DSS requirements appropriately.

Compensating Controls

Compensating controls must be documented by the assessor and included with the Report on Compliance submission, as shown in Appendix C – Compensating Controls Worksheet / Completed Example.

See PCI DSS Glossary, Abbreviation, and Acronyms for the definitions of “compensating controls.”

Instructions and Content for Report on Compliance

This document is to be used by assessors as the template for creating the *Report on Compliance*. The audited entity should follow each payment card company’s respective reporting requirements to ensure each payment card company acknowledges the entity’s compliance status. Contact each payment card company to determine each company’s reporting requirements and instructions. All assessors must follow the instructions for report content and format when completing a *Report on Compliance*:

1. Contact Information and Report Date

- Include contact information for merchant or service provider and assessor
- Date of report

2. Executive Summary

Include the following:

- Business description
- List service providers and other entities with which the company shares cardholder data
- List processor relationships
- Describe whether entity is directly connected to payment card company
- For merchants, POS products used
- Any wholly-owned entities that require compliance with the PCI DSS
- Any international entities that require compliance with the PCI DSS
- Any wireless LANs and/or wireless POS terminals connected to the cardholder environment

3. Description of Scope of Work and Approach Taken

- Version of the Security Audit Procedures document used to conduct the assessment
- Timeframe of assessment
- Environment on which assessment focused (for example, client’s Internet access points, internal corporate network, processing points for the payment card company)
- Any areas excluded from the review
- Brief description or high-level drawing of network topology and controls
- List of individuals interviewed
- List of documentation reviewed

- List of hardware and critical (for example, database or encryption) software in use
- For Managed Service Provider (MSP) reviews, clearly delineate which requirements in this document apply to the MSP (and are included in the review), and which are not included in the review and are the responsibility of the MSP's customers to include in their reviews. Include information about which of the MSP's IP addresses are scanned as part of the MSP's quarterly vulnerability scans, and which IP addresses are the responsibility of the MSP's customers to include in their own quarterly scans

4. **Quarterly Scan Results**

- Summarize the four most recent quarterly scan results in comments at Requirement 11.2
- Scan must cover all externally accessible (Internet-facing) IP addresses in existence at the entity

5. **Findings and Observations**

- All assessors must use the following template to provide detailed report descriptions and findings on each requirement and sub-requirement
- Where applicable, document any compensating controls considered to conclude that a control is in place
- *See* PCI DSS Glossary, Abbreviation, and Acronyms *for the definitions of "compensating controls."*

Revalidation of Open Items

A "controls in place" report is required to verify compliance. If the initial report by the auditor/assessor contains "open items," the merchant/service provider must address these items before validation is completed. The assessor/auditor will then reassess to validate that the remediation occurred and that all requirements are satisfied. After revalidation, the assessor will issue a new *Report on Compliance*, verifying that the system is fully compliant and submit it consistent with instructions (See above.).

Build and Maintain a Secure Network

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

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
1.1 Establish firewall configuration standards that include the following:	**1.1** Obtain and inspect the firewall configuration standards and other documentation specified below to verify that standards are complete. Complete each item in this section			
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration	**1.1.1** Verify that firewall configuration standards include a formal process for all firewall changes, including testing and management approval of all changes to external connections and firewall configuration			
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify that a current network diagram exists and verify that it documents all connections to cardholder data, including any wireless networks			
	1.1.2.b. Verify that the diagram is kept current			
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.3** Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the Intranet. Verify that the current network diagram is consistent with the firewall configuration standards.			
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	**1.1.4** Verify that firewall configuration standards include a description of groups, roles, and responsibilities for logical management of network components			
1.1.5 Documented list of services and ports necessary for business	**1.1.5** Verify that firewall configuration standards include a documented list of services/ports necessary for business			
1.1.6 Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)	**1.1.6** Verify that firewall configuration standards include justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN			
1.1.7 Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented	**1.1.7.a** Verify that firewall configuration standards include justification and documentation for any risky protocols allowed (for example, FTP), which includes reason for use of protocol, and security features implemented			
	1.1.7.b Examine documentation and settings for each service in use to obtain evidence that the service is necessary and secured			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
1.1.8 Quarterly review of firewall and router rule sets	**1.1.8.a** Verify that firewall configuration standards require quarterly review of firewall and router rule sets			
	1.1.8.b Verify that the rule sets are reviewed each quarter			
1.1.9 Configuration standards for routers	**1.1.9** Verify that firewall configuration standards exist for both firewalls and routers			
1.2 Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.	**1.2** Select a sample of firewalls/routers 1) between the Internet and the DMZ and 2) between the DMZ and the internal network. The sample should include the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment. Examine firewall and router configurations to verify that inbound and outbound traffic is limited to only protocols that are necessary for the cardholder data environment			
1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include:	**1.3** Examine firewall/router configurations to verify that connections are restricted between publicly accessible servers and components storing cardholder data, as follows:			
1.3.1 Restricting inbound Internet traffic to internet protocol (IP) addresses within the DMZ (ingress filters)	**1.3.1** Verify that inbound Internet traffic is limited to IP addresses within the DMZ			
1.3.2 Not allowing internal addresses to pass from the Internet into the DMZ	**1.3.2** Verify that internal addresses cannot pass from the Internet into the DMZ			
1.3.3 Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network)	**1.3.3** Verify that the firewall performs stateful inspection (dynamic packet filtering). [Only established connections should be allowed in, and only if they are associated with a previously established session (run NMAP on all TCP ports with "syn reset" or "syn ack" bits set – a response means packets are allowed through even if they are not part of a previously established session)]			
1.3.4 Placing the database in an	**1.3.4** Verify that the database is on an internal network			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
internal network zone, segregated from the DMZ	zone, segregated from the DMZ			
1.3.5 Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment	**1.3.5** Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder environment, and that the restrictions are documented			
1.3.6 Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted) should have the same secure configuration	**1.3.6** Verify that router configuration files are secure and synchronized [for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations]			
1.3.7 Denying all other inbound and outbound traffic not specifically allowed	**1.3.7** Verify that all other inbound and outbound traffic not covered in 1.2 and 1.3 above is specifically denied			
1.3.8 Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)	**1.3.8** Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into systems storing cardholder data			
1.3.9 Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	**1.3.9** Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active, which is configured by the organization to specific standards and not alterable by the employee			
1.4 Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).	**1.4** To determine that direct access between external public networks and system components storing cardholder data are prohibited, perform the following, *specifically* for the firewall/router configuration implemented between the DMZ and the internal network:			
1.4.1 Implement a DMZ to filter and screen all traffic and to prohibit direct	**1.4.1** Examine firewall/router configurations and verify there is no direct route inbound or outbound for Internet			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
routes for inbound and outbound Internet traffic	traffic			
1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ.	**1.4.2** Examine firewall/router configurations and verify that internal outbound traffic from cardholder applications can only access IP addresses within the DMZ			
1.5 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).	**1.5** For the sample of firewall/router components above, verify that NAT or other technology using RFC 1918 address space is used to restrict broadcast of IP addresses from the internal network to the Internet (IP masquerading)			

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

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
2.1 Always change vendor-supplied defaults **before** installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).	**2.1** Choose a sample of system components, critical servers, and wireless access points, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)			
2.1.1 **For wireless environments**, change wireless vendor defaults, including but not limited to, wireless equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community	**2.1.1** Verify the following regarding vendor default settings for wireless environments: • WEP keys were changed from default at installation, and are changed anytime any one with knowledge of the keys leaves the company or changes positions			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.	• Default SSID was changed • Broadcast of the SSID was disabled • Default SNMP community strings on access points were changed • Default passwords on access points were changed • WPA or WPA2 technology is enabled if the wireless system is WPA-capable • Other security-related wireless vendor defaults, if applicable			
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).	**2.2.a** Examine the organization's system configuration standards for network components, critical servers, and wireless access points, and verify the system configuration standards are consistent with industry-accepted hardening standards as defined, for example, by SANS, NIST, and CIS			
	2.2.b Verify that system configuration standards include each item below (at 2.2.1 – 2.2.4)			
	2.2.c Verify that system configuration standards are applied when new systems are configured			
2.2.1 Implement only one primary function per server (for example, web servers, database servers, and DNS should be implemented on separate servers)	**2.2.1** For a sample of system components, critical servers, and wireless access points, verify that only one primary function is implemented per server			
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	**2.2.2** For a sample of system components, critical servers, and wireless access points, inspect enabled system services, daemons, and protocols. Verify that unnecessary or insecure services or protocols are not enabled, or are justified and documented as to appropriate use of the service (for example, FTP is not used, or is encrypted via SSH or other technology)			
2.2.3 Configure system security parameters to prevent misuse	**2.2.3.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for their operating systems, database servers, Web servers, and wireless systems			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	2.2.3.b Verify that common security parameter settings are included in the system configuration standards			
	2.2.3.c For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately			
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**2.2.4** For a sample of system components, critical servers, and wireless access points,, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. Verify enabled functions are documented, support secure configuration, and that only documented functionality is present on the sampled machines			
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.	**2.3** For a sample of system components, critical servers, and wireless access points,, verify that non-console administrative access is encrypted by: • Observing an administrator log on to each system to verify that SSH (or other encryption method) is invoked before the administrator's password is requested • Reviewing services and parameter files on systems to determine that Telnet and other remote log-in commands are not available for use internally • Verifying that administrator access to the wireless management interface is encrypted with SSL/TLS. Alternatively, verify that administrators cannot connect remotely to the wireless management interface (all management of wireless environments is only from the console)			
2.4 Hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: "PCI DSS Applicability for Hosting Providers."	**2.4** Perform testing procedures **A.1.1** through **A.1.4** detailed in Appendix A, "PCI DSS Applicability for Hosting Providers (with Testing Procedures)" for PCI audits of **Shared Hosting Providers**, to verify that **Shared Hosting Providers** protect their entities' (merchants and service providers) hosted environment and data.			

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	**3.1** Obtain and examine the company policies and procedures for data retention and disposal, and perform the following • Verify that policies and procedures include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons) • Verify that policies and procedures include provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data • Verify that policies and procedures include coverage for all storage of cardholder data, including database servers, mainframes, transfer directories, and bulk data copy directories used to transfer data between servers, and directories used to normalize data between server transfers • Verify that policies and procedures include A programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or, alternatively, requirements for an audit, conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
3.2 Do not store sensitive authentication data subsequent to authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3*:*	**3.2** If sensitive authentication data is received and deleted, obtain and review the processes for deleting the data to verify that the data is unrecoverable For each item of sensitive authentication data below, perform the following steps:			
3.2.1 Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data *In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.* *Note: See "Glossary" for additional information.*	**3.2.1** For a sample of system components, critical servers, and wireless access points, examine the following and verify that the full contents of any track from the magnetic stripe on the back of card are not stored under any circumstance: • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs • Several database schemas • Database contents			
3.2.2 Do not store the card-validation value or code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions *Note: See "Glossary" for additional information.*	**3.2.2** For a sample of system components, critical servers, and wireless access points, examine the following and verify that the three-digit or four-digit card-validation code printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance: • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	• Several database schemas • Database contents			
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	**3.2.3** For a sample of system components, critical servers, and wireless access points, examine the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance: • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs • Several database schemas • Database contents			
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). *Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point of sale [POS] receipts).*	**3.3** Obtain and examine written policies and examine online displays of credit card data to verify that credit card numbers are masked when displaying cardholder data, except for those with a specific need to see full credit card numbers			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches: • Strong one-way hash functions (hashed indexes) • Truncation • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key management processes and procedures The MINIMUM account information that must be rendered unreadable is the PAN. *If for some reason, a company is unable to encrypt cardholder data, refer to Appendix B: "Compensating Controls."*	**3.4.a** Obtain and examine documentation about the system used to protect stored data, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that data is rendered unreadable using one of the following methods: • One-way hashes (hashed indexes) such as SHA-1 • Truncation or masking • Index tokens and PADs, with the PADs being securely stored • Strong cryptography, such as Triple-DES 128-bit or AES 256-bit, with associated key management processes and procedures			
	3.4.b Examine several tables from a sample of database servers to verify the data is rendered unreadable (that is, not stored in plain text)			
	3.4.c Examine a sample of removable media (for example, backup tapes) to confirm that cardholder data is rendered unreadable			
	3.4.d Examine a sample of audit logs to confirm that cardholder data is sanitized or removed from the logs			
	3.4.e Verify that cardholder data received from wireless networks is rendered unreadable wherever stored			
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must	**3.4.1.a** If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local or Active Directory accounts)			
	3.4.1.b Verify that decryption keys are not stored on the local system (for example, store keys on floppy disk, CD-ROM, etc. that can be secured and retrieved only when needed)			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
not be tied to user accounts.	**3.4.1.c** Verify that cardholder data on removable media is encrypted wherever stored (disk encryption often cannot encrypt removable media)			
3.5 Protect encryption keys used for encryption of cardholder data against both disclosure and misuse:	**3.5** Verify processes to protect encryption keys used for encryption of cardholder data against disclosure and misuse by performing the following:			
3.5.1 Restrict access to keys to the fewest number of custodians necessary	**3.5.1** Examine user access lists to verify that access to cryptographic keys is restricted to very few custodians			
3.5.2 Store keys securely in the fewest possible locations and forms	**3.5.2** Examine system configuration files to verify that cryptographic keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys			
3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:	**3.6.a** Verify the existence of key management procedures for keys used for encryption of cardholder data			
	3.6.b **For Service Providers** only: If the Service Provider shares keys with their customers for transmission of cardholder data, verify that the Service Provider provides documentation to customers that includes guidance on how to securely store and change customer's encryption keys (used to transmit data between customer and service provider)			
	3.6.c Examine the key management procedures and perform the following:			
3.6.1 Generation of strong keys	**3.6.1** Verify that key management procedures require the generation of strong keys			
3.6.2 Secure key distribution	**3.6.2** Verify that key management procedures require secure key distribution			
3.6.3 Secure key storage	**3.6.3** Verify that key management procedures require secure key storage			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
3.6.4 Periodic key changes • As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically • At least annually	**3.6.4** Verify that key management procedures require periodic key changes. Verify that key change procedures are carried out at least annually			
3.6.5 Destruction of old keys.	**3.6.5** Verify that key management procedures require the destruction of old keys			
3.6.6 Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key	**3.6.6** Verify that key management procedures require split knowledge and dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)			
3.6.7 Prevention of unauthorized substitution of keys	**3.6.7** Verify that key management procedures require the prevention of unauthorized substitution of keys			
3.6.8 Replacement of known or suspected compromised keys	**3.6.8** Verify that key management procedures require the replacement of known or suspected compromised keys			
3.6.9 Revocation of old or invalid keys	**3.6.9** Verify that key management procedures require the revocation of old or invalid keys (mainly for RSA keys)			
3.6.10 Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities	**3.6.10** Verify that key management procedures require key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities			

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

Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
4.1 Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).*	**4.1.a** Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks • Verify that strong encryption is used during data transmission • For SSL implementations, verify that HTTPS appears as a part of the browser Universal Record Locator (URL), and that no cardholder data is required when HTTPS does not appear in the URL • Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit • Verify that only trusted SSL/TLS keys/certificates are accepted • Verify that the proper encryption strength is implemented for the encryption methodology in use (Check vendor recommendations/best practices)			
4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN.	**4.1.1.a** For wireless networks transmitting cardholder data or connected to cardholder environments, verify that appropriate encryption methodologies are used for any wireless transmissions, such as: Wi-Fi Protected Access (WPA or WPA2), IPSEC VPN, or SSL/TLS			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
If WEP is used, do the following: • Use with a minimum 104-bit encryption key and 24 bit-initialization value • Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS • Rotate shared WEP keys quarterly (or automatically if the technology permits) • Rotate shared WEP keys whenever there are changes in personnel with access to keys • Restrict access based on media access code (MAC) address	**4.1.1.b** If WEP is used, verify • it is used with a minimum 104-bit encryption key and 24 bit-initialization value • it is used only in conjunction with Wi-Fi Protected Access (WPA or WPA2) technology, VPN, or SSL/TLS • shared WEP keys are rotated at least quarterly (or automatically if the technology is capable) • shared WEP keys are rotated whenever there are changes in personnel with access to keys • access is restricted based on MAC address			
4.2 Never send unencrypted PANs by e-mail.	**4.2.a** Verify that an email encryption solution is used whenever cardholder data is sent via email			
	4.2.b Verify the existence of a policy stating that unencrypted PAN is not to be sent via email			
	4.2.c Interview 3-5 employees to verify that email encryption software is required for emails containing PANs			

Maintain a Vulnerability Management Program

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

Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
5.1 Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers) *Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.*	**5.1** For a sample of system components, critical servers, and wireless access points, verify that anti-virus software is installed			
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.	**5.1.1** For a sample of system components, critical servers, and wireless access points, verify that anti-virus programs detect, remove, and protect against other malicious software, including spyware and adware			
5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	**5.2** Verify that anti-virus software is current, actively running, and capable of generating logs • Obtain and examine the policy and verify that is contains requirements for updating anti-virus software and definitions • Verify that the master installation of the software is enabled for automatic updates and periodic scans, and that a sample of system components, critical servers, and wireless access points servers have these features enabled • Verify that log generation is enabled and that logs are retained in accordance with company retention policy			

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	**6.1.a** For a sample of system components, critical servers, and wireless access points and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed			
	6.1.b Examine policies related to security patch installation to verify they require installation of all relevant new security patches within 30 days			
6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.	**6.2.a** Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities			
	6.2.b Verify that processes to identify new security vulnerabilities include use of outside sources for security vulnerability information and updating the system configuration standards reviewed in Requirement 2 as new vulnerability issues are found			
6.3 Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.	**6.3** Obtain and examine written software development processes to verify that they are based on industry standards and that security is included throughout the life cycle From an examination of written software development processes, interviews of software developers, and examination of relevant data (network configuration documentation, production and test data, etc.), verify that:			
6.3.1 Testing of all security patches and system and software configuration changes before deployment	**6.3.1** All changes (including patches) are tested before being deployed into production			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
6.3.2 Separate development, test, and production environments	**6.3.2** The test/development environments are separate from the production environment, with access control in place to enforce the separation			
6.3.3 Separation of duties between development, test, and production environments	**6.3.3** There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment			
6.3.4 Production data (live PANs) are not used for testing or development	**6.3.4** Production data (live PANs) are not used for testing and development, or are sanitized before use			
6.3.5 Removal of test data and accounts before production systems become active	**6.3.5** Test data and accounts are removed before a production system becomes active			
6.3.6 Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers	**6.3.6** Custom application accounts, usernames and/or passwords are removed before system goes into production or is released to customers			
6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.	**6.3.7.a** Obtain and review any written or other policies to confirm that code reviews are required and must be performed by individuals other then originating code author			
	6.3.7.b Verify code reviews are conducted for new code and after code changes *Note: This requirement applies to code reviews for custom software development, as part of the System Development Life Cycle (SDLC) – these reviews can be conducted by internal personnel. Custom code for web-facing applications will be subject to additional controls as of June 30, 2008 – see PCI DSS requirement 6.6 for details.*			
6.4 Follow change control procedures for all system and software configuration changes. The procedures must include the following:	**6.4.a** Obtain and examine company change-control procedures related to implementing security patches and software modifications, and verify that the procedures require items 6.4.1 – 6.4.4 below			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	6.4.b For a sample of system components, critical servers, and wireless access points, examine the three most recent changes/security patches for each system component, and trace those changes back to related change control documentation. Verify that, for each change examined, the following was documented according to the change control procedures:			
6.4.1 Documentation of impact	**6.4.1** Verify that documentation of customer impact is included in the change control documentation for each sampled change			
6.4.2 Management sign-off by appropriate parties	**6.4.2** Verify that management sign-off by appropriate parties is present for each sampled change			
6.4.3 Testing of operational functionality	**6.4.3** Verify that operational functionality testing was performed for each sampled change			
6.4.4 Back-out procedures	**6.4.4** Verify that back-out procedures are prepared for each sampled change			
6.5 Develop all web applications based on secure coding guidelines. such as the *Open Web Application Security Project Guidelines*. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:	**6.5.a** Obtain and review software development processes for any web-based applications. Verify that processes require training in secure coding techniques for developers, and are based on guidance such as the *OWASP Guidelines* (http://www.owasp.org)			
	6.5.b For any web-based applications, verify that processes are in place to confirm that web applications are not vulnerable to the following			
6.5.1 Unvalidated input	**6.5.1** Unvalidated input			
6.5.2 Broken access control (for example, malicious use of user IDs)	**6.5.2** Malicious use of User IDs			
6.5.3 Broken authentication and session management (use of account credentials and session cookies)	**6.5.3** Malicious use of account credentials and session cookies			
6.5.4 Cross-site scripting (XSS) attacks	**6.5.4** Cross-site scripting			
6.5.5 Buffer overflows	**6.5.5** Buffer overflows due to unvalidated input and other causes			
6.5.6 Injection flaws (for example,	**6.5.6** SQL injection and other command injection flaws			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
structured query language (SQL) injection)				
6.5.7 Improper error handling	**6.5.7** Error handling flaws			
6.5.8 Insecure storage	**6.5.8** Insecure storage			
6.5.9 Denial of service	**6.5.9** Denial of service			
6.5.10 Insecure configuration management	**6.5.10** Insecure configuration management			
6.6 Ensure that all web-facing applications are protected against known attacks by either of the following methods: • Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security • Installing an application-layer firewall in front of web-facing applications *Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.*	**6.6** For web-based applications, ensure that one of the following methods are in place as follows: • Verify that custom application code is periodically reviewed by an organization that specializes in application security; that all coding vulnerabilities were corrected; and that the application was re-evaluated after the corrections • Verify that an application-layer firewall is in place in front of web-facing applications to detect and prevent web-based attacks			

Implement Strong Access Control Measures

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

This requirement ensures critical data can only be accessed by authorized personnel.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	**7.1** Obtain and examine written policy for data control, and verify that the policy incorporates the following: • Access rights to privileged User IDs are restricted to least privileges necessary to perform job responsibilities • Assignment of privileges is based on individual personnel's job classification and function • Requirement for an authorization form signed by management that specifies required privileges • Implementation of an automated access control system			
7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	**7.2** Examine system settings and vendor documentation to verify that an access control system is implemented and that it includes the following • Coverage of all system components • Assignment of privileges to individuals based on job classification and function • Default "deny-all" setting (some access control systems are set by default to "allow-all" thereby permitting access unless/until a rule is written to specifically deny it)			

Requirement 8: Assign a unique ID to each person with computer access.

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
8.1 Identify all users with a unique user name before allowing them to access system components or cardholder data.	**8.1** For a sample of user IDs, review user ID listings and verify that <u>all</u> users have a unique username for access to system components or cardholder data			
8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users: • Password • Token devices (for example, SecureID, certificates, or public key) • Biometrics	**8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder environment, perform the following: • Obtain and examine documentation describing the authentication method(s) used • For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s)			
8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	**8.3** To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that both a password and an additional authentication item (Smart card, token PIN) are required.			
8.4 Encrypt all passwords during transmission and storage on all system components.	**8.4.a** For a sample of system components, critical servers, and wireless access points, examine password files to verify that passwords are unreadable			
	8.4.b For **Service Providers** only, observe password files to verify that customer passwords are encrypted			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:	**8.5** Review procedures and interview personnel to verify that procedures are implemented for user authentication and password management, by performing the following:			
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects	**8.5.1.a** Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to company policy by performing the following: • Obtain and examine an authorization form for each ID • Verify that the sampled User IDs are implemented in accordance with the authorization form (including with privileges as specified and all signatures obtained,.), by tracing information from the authorization form to the system			
	8.5.1.b Verify that only administrators have access to management consoles for wireless networks			
8.5.2 Verify user identity before performing password resets	**8.5.2** Examine password procedures and observe security personnel to verify that, if a user requests a password reset by phone, email, web, or other non-face-to-face method, the user's identity is verified before the password is reset			
8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use	**8.5.3** Examine password procedures and observe security personnel to verify that first-time passwords for new users are set to a unique value for each user and changed after first use			
8.5.4 Immediately revoke access for any terminated users	**8.5.4** Select a sample of employees terminated in the past six months, and review current user access lists to verify that their IDs have been inactivated or removed			
8.5.5 Remove inactive user accounts at least every 90 days	**8.5.5** For a sample of user IDs, verify that there are no inactive accounts over 90 days old			
8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed	**8.5.6** Verify that any accounts used by vendors to support and maintain system components are inactive, enabled only when needed by the vendor, and monitored while being used			
8.5.7 Communicate password procedures and policies to all	**8.5.7** Interview the users from a sample of user IDs, to verify that they are familiar with password procedures and policies			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
users who have access to cardholder data				
8.5.8 Do not use group, shared, or generic accounts and passwords	**8.5.8.a** For a sample of system components, critical servers, and wireless access points, examine user ID lists to verify the following • Generic User IDs and accounts are disabled or removed • Shared User IDs for system administration activities and other critical functions do not exist • Shared and generic User IDs are not used to administer wireless LANs and devices			
	8.5.8.b Examine password policies/procedures to verify that group and shared passwords are explicitly prohibited			
	8.5.8.c Interview system administrators to verify that group and shared passwords are not distributed, even if requested			
8.5.9 Change user passwords at least every 90 days	**8.5.9** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days For **Service Providers** only, review internal processes and customer/user documentation to verify that customer passwords are required to change periodically and that customers are given guidance as to when, and under what circumstances, passwords must change			
8.5.10 Require a minimum password length of at least seven characters	**8.5.10** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long For **Service Providers** only, review internal processes and customer/user documentation to verify that customer passwords are required to meet minimum length requirements			
8.5.11 Use passwords containing both numeric and alphabetic characters	**8.5.11** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters For **Service Providers** only, review internal processes and			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	customer/user documentation to verify that customer passwords are required to contain both numeric and alphabetic characters			
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used	**8.5.12** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords For **Service Providers** only, review internal processes and customer/user documentation to verify that new customer passwords cannot be the same as the previous four passwords			
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts	**8.5.13** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that a user's account is locked out after not more than six invalid logon attempts For **Service Providers** only, review internal processes and customer/user documentation to verify that customer accounts are temporarily locked-out after not more than six invalid access attempts			
8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID	**8.5.14** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for thirty minutes or until a system administrator resets the account			
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal	**8.5.15** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less			
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users	**8.5.16.a** Review database configuration settings for a sample of databases to verify that access is authenticated, including for individual users, applications, and administrators			
	8.5.16.b Review database configuration settings and database accounts to verify that direct SQL queries to the database are prohibited (there should be very few individual database login accounts. Direct SQL queries should be limited to database administrators)			

Requirement 9: Restrict physical access to cardholder data.

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.	**9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems that contain cardholder data • Verify that access is controlled with badge readers and other devices including authorized badges and lock and key • Observe a system administrator's attempt to log into consoles for three randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use			
9.1.1 Use cameras to monitor sensitive areas. Audit collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	**9.1.1** Verify that video cameras monitor the entry/exit points of data centers where cardholder data is stored or present. Video cameras should be internal to the data center or otherwise protected from tampering or disabling. Verify that cameras are monitored and that data from cameras is stored for at least three months			
9.1.2 Restrict physical access to publicly accessible network jacks	**9.1.2** Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized employees. For example, conference rooms used to host visitors should not have network ports enabled with DHCP. Alternatively, verify that visitors are escorted at all times in areas with active network jacks			
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices	**9.1.3** Verify that physical access to wireless access points, gateways, and handheld devices is appropriately restricted			
9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. *"Employee" refers to full-time and part-time employees, temporary*	**9.2.a** Review processes and procedures for assigning badges to employees, contractors, and visitors, and verify these processes include the following: • Procedures in place for granting new badges, changing access requirements, and revoking terminated employee and expired visitor badges • Limited access to badge system			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
employees and personnel, and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.	**9.2.b** Observe people within the facility to verify that it is easy to distinguish between employees and visitors			
9.3 Make sure all visitors are handled as follows:	**9.3** Verify that employee/visitor controls are in place as follows:			
9.3.1 Authorized before entering areas where cardholder data is processed or maintained	**9.3.1** Observe visitors to verify the use of visitor ID badges. Attempt to gain access to the data center to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data			
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees	**9.3.2** Examine employee and visitor badges to verify that ID badges clearly distinguish employees from visitors/outsiders and that visitor badges expire			
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration	**9.3.3** Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration			
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law.	**9.4.a** Verify that a visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted			
	9.4.b Verify that the log contains the visitor's name, the firm represented, and the employee authorizing physical access, and is retained for at least three months			
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility.	**9.5** Verify that the storage location for media backups is secure. Verify that offsite storage is visited periodically to determine that backup media storage is physically secure and fireproof			
9.6 Physically secure all paper and electronic media (including computers, electronic media, networking and communications	**9.6** Verify that procedures for protecting cardholder data include controls for physically securing paper and electronic media in computer rooms and data centers (including paper receipts, paper reports, faxes, CDs, and disks in employee desks and open			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder data	workspaces, and PC hard drives)			
9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data: including the following	**9.7** Verify that a policy exists to control distribution of media containing cardholder data, that the policy covers all distributed media including that distributed to individuals			
9.7.1 Classify the media so it can be identified as confidential	**9.7.1** Verify that all media is classified so that it can be identified as "confidential"			
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked	**9.7.2** Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery mechanism that can be tracked			
9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	**9.8** Select a recent sample of several days of offsite media tracking logs, and verify the presence in the logs of tracking details and proper management authorization			
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.	**9.9** Obtain and examine the policy for controlling storage and maintenance of hardcopy and electronic media and verify that the policy requires periodic media inventories.			
9.9.1 Properly inventory all media and make sure it is securely stored.	**9.9.1.a**Obtain and review the media inventory log to verify that periodic media inventories are performed **9.9.1.b** Review processes to verify that media is securely stored			
9.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows	**9.10** Obtain and examine the periodic media destruction policy and verify that it covers all media containing cardholder data and confirm the following:			
9.10.1 Cross-cut shred, incinerate, or pulp hardcopy materials	**9.10.1.a** Verify that hard-copy materials are cross-cut shredded, incinerated, or pulped, in accordance with ISO 9564-1 or ISO 11568-3e			
	9.10.1.b Examine storage containers used for information to be destroyed to verify that the containers are secured. For example, verify that a "to-be-shredded" container has a lock preventing access			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	to its contents			
9.10.2 Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed	**9.10.2** Verify that electronic media is destroyed beyond recovery by using a military wipe program to delete files, or via degaussing or otherwise physically destroying the media			

Regularly Monitor and Test Networks

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

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	**10.1** Verify through observation and interviewing the system administrator, that audit trails are enabled and active, including for any connected wireless networks.			
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Verify though interviews, examination of audit logs, and examination of audit log settings, that the following events are logged into system activity logs:			
10.2.1 All individual accesses to cardholder data	**10.2.1** All individual access to cardholder data			
10.2.2 All actions taken by any individual with root or administrative privileges	**10.2.2** Actions taken by any individual with root or administrative privileges			
10.2.3 Access to all audit trails	**10.2.3** Access to all audit trails			
10.2.4 Invalid logical access attempts	**10.2.4** Invalid logical access attempts			
10.2 5 Use of identification and authentication mechanisms	**10.2.5** Use of identification and authentication mechanisms			
10.2.6 Initialization of the audit logs	**10.2.6** Initialization of audit logs			
10.2.7 Creation and deletion of system-	**10.2.7** Creation and deletion of system level objects			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
level objects				
10.3 Record at least the following audit trail entries for all system components for each event:	**10.3** Verify through interviews and observation, for each auditable event (from 10.2), that the audit trail captures the following:			
10.3.1 User identification	**10.3.1** User identification			
10.3.2 Type of event	**10.3.2** Type of event			
10.3.3 Date and time	**10.3.3** Date and time stamp			
10.3.4 Success or failure indication	**10.3.4** Success or failure indication, including those for wireless connections			
10.3.5 Origination of event	**10.3.5** Origination of event			
10.3.6 Identity or name of affected data, system component, or resource	**10.3.6** Identity or name of affected data, system component, or resources			
10.4 Synchronize all critical system clocks and times	**10.4** Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:			
	10.4.a Verify that NTP or similar technology is used for time synchronization			
	10.4.b Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.]			
	10.4.c Verify that the Network Time Protocol (NTP) is running the most recent version			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	10.4.d Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). See www.ntp.org for more information			
10.5 Secure audit trails so they cannot be altered	**10.5** Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:			
10.5.1 Limit viewing of audit trails to those with a job-related need	**10.5.1** Verify that only individuals who have a job-related need can view audit trail files			
10.5.2 Protect audit trail files from unauthorized modifications	**10.5.2** Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation			
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	**10.5.3** Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter			
10.5.4 Copy logs for wireless networks onto a log server on the internal LAN	**10.5.4** Verify that logs for wireless networks are offloaded or copied onto a centralized internal log server or media that is difficult to alter			
10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)	**10.5.5** Verify the use of file integrity monitoring or change detection software for logs by examining system settings and monitored files and results from monitoring activities			
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and	**10.6.a** Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
accounting protocol (AAA) servers (for example, RADIUS). *Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6*	**10.6.b** Through observation and interviews, verify that regular log reviews are performed for all system components			
10.7 Retain audit trail history for at least one year, with a minimum of three months available online.	**10.7.a** Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year			
	10.7.b Verify that audit logs are available online or on tape for at least one year			

Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
11.1 Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use.	**11.1.a** Confirm by interviewing security personnel and examining relevant code, documentation, and processes that security testing of devices is in place to assure that controls identify and stop unauthorized access attempts within the cardholder environment.			
	11.1.b Verify that a wireless analyzer is used at least quarterly to identify all wireless devices.			
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	**11.2.a** Inspect output from the most recent four quarters of network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment occurs. Verify that the scan process includes rescans until "clean" results are obtained			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
Note: Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry. Scans conducted after network changes may be performed by the company's internal staff.	**11.2.b** To verify that external scanning is occurring on a quarterly basis in accordance with the PCI Security Scanning Procedures, inspect output from the four most recent quarters of external vulnerability scans to verify that • Four quarterly scans occurred in the most recent 12-month period • The results of each scan satisfy the PCI Security Scanning Procedures (for example, no urgent, critical, or high vulnerabilities) • The scans were completed by a vendor approved to perform the PCI Security Scanning Procedures			
11.3 Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following	**11.3** Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment. Verify that any noted vulnerabilities were corrected. Verify that the penetration tests include:			
11.3.1 Network-layer penetration tests	**11.3.1** Network-layer penetration tests			
11.3.2 Application-layer penetration tests	**11.3.2** Application-layer penetration tests			
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.	**11.4.a** Observe the use of network intrusion detection systems and/or intrusion prevention systems on the network. Verify that all critical network traffic in the cardholder data environment is monitored			
	11.4.b Confirm IDS and/or IPS is in place to monitor and alert personnel of suspected compromises			
	11.4.c Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly. *Critical files are not necessarily only those containing cardholder data. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider)*	**11.5** Verify the use of file integrity monitoring products within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities			

Maintain an Information Security Policy

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

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant system users (including vendors, contractors, and business partners)			
12.1.1 Addresses all requirements in this specification	**12.1.1** Verify that the policy addresses all requirements in this specification.			
12.1.2 Includes an annual process	**12.1.2** Verify that the information security policy includes			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
that identifies threats, and vulnerabilities, and results in a formal risk assessment	an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment			
12.1.3 Includes a review at least once a year and updates when the environment changes	**12.1.3** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment			
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	**12.2.a** Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements			
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:	**12.3** Obtain and examine the policy for critical employee-facing technologies and verify the policy contains the following:			
12.3.1 Explicit management approval	**12.3.1** Verify that the usage policies require explicit management approval to use the devices			
12.3.2 Authentication for use of the technology	**12.3.2** Verify that the usage policies require that all device use is authenticated with username and password or other authentication item (for example, token)			
12.3.3 A list of all such devices and personnel with access	**12.3.3** Verify that the usage policies require a list of all devices and personnel authorized to use the devices			
12.3.4 Labeling of devices with owner, contact information, and purpose	**12.3.4** Verify that the usage policies require labeling of devices with owner, contact information, and purpose			
12.3.5 Acceptable uses of the technology	**12.3.5** Verify that the usage policies require acceptable uses for the technology			
12.3.6 Acceptable network locations for the technologies	**12.3.6** Verify that the usage policies require acceptable network locations for the technology			
12.3.7 List of company-approved products	**12.3.7** Verify that the usage policies require a list of company-approved products			
12.3.8 Automatic disconnect of	**12.3.8** Verify that the usage policies require automatic			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
modem sessions after a specific period of inactivity	disconnect of modem sessions after a specific period of inactivity			
12.3.9 Activation of modems for vendors only when needed by vendors, with immediate deactivation after use	**12.3.9** Verify that the usage policies require activation of modems used by vendors only when needed by vendors, with immediate deactivation after use			
12.3.10 When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access	**12.3.10** Verify that the usage policies prohibit the storage of cardholder data onto local hard drives, floppy disks, or other external media when accessing such data remotely via modem. Verify that the policies prohibit cut-and-paste and print functions during remote access			
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	**12.4** Verify that information security policies clearly define information security responsibilities for both employees and contractors			
12.5 Assign to an individual or team the following information security management responsibilities:	**12.5** Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:			
12.5.1 Establish, document, and distribute security policies and procedures	**12.5.1** Verify that responsibility for creating and distributing security policies and procedures is formally assigned			
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel	**12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned			
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations	**12.5.3** Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned			
12.5.4 Administer user accounts,	**12.5.4** Verify that responsibility for administering user			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
including additions, deletions, and modifications	account and authentication management is formally assigned			
12.5.5 Monitor and control all access to data	**12.5.5** Verify that responsibility for monitoring and controlling all access to data is formally assigned			
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security:	**12.6.a** Verify the existence of a formal security awareness program for all employees			
	12.6.b Obtain and examine security awareness program procedures and documentation and perform the following:			
12.6.1 Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions)	**12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings)			
	12.6.1.b Verify that employees attend awareness training upon hire and at least annually			
12.6.2 Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures	**12.6.2** Verify that the security awareness program requires employees to acknowledge in writing that they have read and understand the company's information security policy			
12.7 Screen potential employees to minimize the risk of attacks from internal sources. *For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	**12.7** Inquire of Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on potential employees who will have access to cardholder data or the cardholder data environment. (Examples of background checks include pre-employment, criminal, credit history, and reference checks)			
12.8 If cardholder data is shared with service providers, then contractually the following is required:	**12.8** If the audited entity shares cardholder data with another company, obtain and examine contracts between the organization and any third parties that handle cardholder data (for example, backup tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes). Perform the following:			
12.8.1 Service providers must	**12.8.1** Verify that the contract contains provisions requiring			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
adhere to the PCI DSS requirements	adherence to the PCI DSS requirements			
12.8.2 Agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses	**12.8.2** Verify that the contract contains provisions for acknowledgement by the third party of their responsibility for securing cardholder data			
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	**12.9** Obtain and examine the Incident Response Plan and related procedures and perform the following:			
12.9.1 Create the incident response plan to be implemented in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing the Acquirers and credit card associations)	**12.9.1** Verify that the Incident Response Plan and related procedures include • roles, responsibilities, and communication strategies in the event of a compromise • coverage and responses for all critical system components • notification, at a minimum, of credit card associations and acquirers • strategy for business continuity post compromise • reference or inclusion of incident response procedures from card associations • analysis of legal requirements for reporting compromises (for example, per California bill 1386, notification of affected consumers is a requirement in the event of an actual or suspected compromise, for any business with California residents in their database)			
12.9.2 Test the plan at least annually	**12.9.2** Verify that the plan is tested at least annually			
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts	**12.9.3** Verify through observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, critical IDS alerts, and/or reports of unauthorized critical system or content file changes			
12.9.4 Provide appropriate training to staff with security breach	**12.9.4** Verify through observation and review of policies that staff with security breach responsibilities are			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
response responsibilities	periodically trained			
12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems	**12.9.5** Verify through observation and review of processes that monitoring and responding to alerts from security systems are included in the Incident Response Plan			
12.9.6 Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments	**12.9.6** Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments			
12.10 All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following	**12.10** Verify through observation, review of policies and procedures, and review of supporting documentation that there is a process to manage connected entities by performing the following:			
12.10.1 Maintain list of connected entities	**12.10.1** Verify that a list of connected entities is maintained			
12.10.2 Ensure proper due diligence is conducted prior to connecting an entity	**12.10.2** Verify that procedures ensure that proper due diligence is conducted prior to connecting an entity			
12.10.3 Ensure the entity is PCI DSS compliant	**12.10.3** Verify that procedures ensure that the entity is PCI DSS compliant			
12.10.4 Connect and disconnect entities by following an established process	**12.10.4** Verify that connecting and disconnecting entities occurs following an established process			

Appendix A: PCI DSS Applicability for Hosting Providers (with Testing Procedures)

Requirement A.1: Hosting providers protect cardholder data environment

As referenced in Requirement 12.8, all service providers with access to cardholder data (including hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that hosting providers must protect each entity's hosted environment and data. Therefore, hosting providers must give special consideration to the following::

Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, as in A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. *Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity* must *comply with the PCI DSS and validate compliance as applicable.*	**A.1** Specifically for a PCI audit of a **Shared hosting Provider**, to verify that **Shared hosting Providers** protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and verify **A.1.1** through **A.1.4** below.			
A.1.1 Ensure that each entity only has access to own cardholder data environment	**A.1.1** If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: • No entity on the system can use a shared web server user ID • All CGI scripts used by an entity must be created and run as the entity's unique user ID			
A.1.2 Restrict each entity's access and privileges to own cardholder	**A.1.2.a** Verify the user ID of any application process is not a privileged user (root/admin).			

Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
	A.1.2.b Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.). IMPORTANT: An entity's files may not be shared by group			
	A.1.2.c Verify an entity's users do not have write access to shared system binaries			
	A.1.2.d Verify that viewing of log entries is restricted to the owning entity			
	A.1.2.e To ensure each entity cannot monopolize server resources to exploit vulnerabilities (error, race, and restart conditions, resulting in, for example, buffer overflows), verify restrictions are in place for the use of these system resources: • Disk space • Bandwidth • Memory • CPU			
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10	**A.1.3.a** Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: • Logs are enabled for common third party applications • Logs are active by default • Logs are available for review by the owning entity • Log locations are clearly communicated to the owning entity			
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	**A.1.4** Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.			

Appendix B – Compensating Controls

Compensating Controls – General

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a technical specification of a requirement, but has sufficiently mitigated the associated risk. See the PCI DSS Glossary for the full definition of compensating controls.

The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments. Each compensating control must be thoroughly evaluated after implementation to ensure effectiveness. The following guidance provides compensating controls when companies are unable to render cardholder data unreadable per requirement 3.4.

Compensating Controls for Requirement 3.4

For companies unable to render cardholder data unreadable (for example, by encryption) due to technical constraints or business limitations, compensating controls may be considered. *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Companies that consider compensating controls for rendering cardholder data unreadable must understand the risk to the data posed by maintaining readable cardholder data. Generally, the controls must provide additional protection to mitigate any additional risk posed by maintaining readable cardholder data. The controls considered must be in addition to controls required in the PCI DSS, and must satisfy the “Compensating Controls” definition in the PCI DSS Glossary. Compensating controls may consist of either a device or combination of devices, applications, and controls that meet **all of the** following conditions:

1. Provide additional segmentation/abstraction (for example, at the network-layer)
2. Provide ability to restrict access to cardholder data or databases based on the following criteria:
    - IP address/Mac address
    - Application/service
    - User accounts/groups
    - Data type (packet filtering)
3. Restrict logical access to the database
    - Control logical access to the database independent of Active Directory or Lightweight Directory Access Protocol (LDAP)
4. Prevent/detect common application or database attacks (for example, SQL injection).

Appendix C: Compensating Controls Worksheet/Completed Example

Example

1. Constraints: List constraints precluding compliance with the original requirement

   Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a 'root' login. It is not possible for Company XYZ to manage the 'root' login nor is it feasible to log all 'root' activity by each user.

2. Objective: Define the objective of the original control; identify the objective met by the compensating control

   The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, shared logins makes it impossible to state definitively that a person is responsible for a particular action.

3. Identified Risk: Identify any additional risk posed by the lack of the original control

   Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.

4. Definition of Compensating Controls: Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.

   Company XYZ is going to require all users to log into the servers from their desktop using the SU command. SU allows a user to access the 'root' account and perform actions under the 'root' account but is able to be logged in the su-log directory. In this way, each user's actions can be tracked through the SU account.

Payment Card Industry (PCI) Data Security Standard

Self-Assessment Questionnaire

Version 1.0

Release: December 2004

How to Complete the Questionnaire

The questionnaire is divided into six sections. Each section focuses on a specific area of security, based on the requirements included in the PCI Data Security Standard. For any questions where N/A is marked, a brief explanation should be attached.

Questionnaire Reporting

The following must be included with the self-assessment questionnaire and system perimeter scan results:

Organization Information

CORPORATE NAME:		DBA(S):	
CONTACT NAME:		TITLE:	
PHONE:		E-MAIL:	

APPROXIMATE NUMBER OF TRANSACTIONS/ACCOUNTS HANDLED PER YEAR:	

Please include a brief description of your business.

Please explain your business' role in the payment flow. How and in what capacity does your business store, process and/or transmit cardholder data?

List all Third Party Service Providers

Processor:		Gateway:	
Web Hosting		Shopping Cart:	
Co-Location:		Other:	

List Point of Sale (POS) software/hardware in use:

Rating the Assessment

After completing each section of the assessment, users should fill in the rating boxes as follows:

IN EACH SECTION IF…	THEN, THE SECTION RATING IS …
ALL questions are answered with "yes" or "N/A"	**Green** - The merchant or service provider is compliant with the self-assessment portion of the PCI Data Security Standard. *Note: If "N/A" is marked, attach a brief explanation.*
ANY questions are answered with "no"	**Red** – The merchant or service provider is not considered compliant. To reach compliance, the risk(s) must be resolved and the self-assessment must be retaken to demonstrate compliance.

Section 1:	Green	Red	**Section 4:**	Green	Red
Section 2:	Green	Red	**Section 5:**	Green	Red
Section 3:	Green	Red	**Section 6:**	Green	Red

Overall Rating: **Green** **Red**

Build and Maintain a Secure Network

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

	DESCRIPTION	RESPONSE
1.1	Are all router, switches, wireless access points, and firewall configurations secured and do they conform to documented security standards?	□ Yes □ No
1.2	If wireless technology is used, is the access to the network limited to authorized devices?	□ Yes □ No □ N/A
1.3	Do changes to the firewall need authorization and are the changes logged?	□ Yes □ No
1.4	Is a firewall used to protect the network and limit traffic to that which is required to conduct business?	□ Yes □ No
1.5	Are egress and ingress filters installed on all border routers to prevent impersonation with spoofed IP addresses?	□ Yes □ No
1.6	Is payment card account information stored in a database located on the internal network (not the DMZ) and protected by a firewall?	□ Yes □ No
1.7	If wireless technology is used, do perimeter firewalls exist between wireless networks and the payment card environment?	□ Yes □ No □ N/A
1.8	Does each mobile computer with direct connectivity to the Internet have a personal firewall and anti-virus software installed?	□ Yes □ No □ N/A
1.9	Are Web servers located on a publicly reachable network segment separated from the internal network by a firewall (DMZ)?	□ Yes □ No
1.10	Is the firewall configured to translate (hide) internal IP addresses, using network address translation (NAT)?	□ Yes □ No

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

	DESCRIPTION	RESPONSE
2.1	Are vendor default security settings changed on production systems before taking the system into production?	□ Yes □ No
2.2	Are vendor default accounts and passwords disabled or changed on production systems before putting a system into production?	□ Yes □ No
2.3	If wireless technology is used, are vendor default settings changed (i.e. WEP keys, SSID, passwords, SNMP community strings, disabling SSID broadcasts)?	□ Yes □ No □ N/A
2.4	If wireless technology is used, is Wi-Fi Protected Access (WPA) technology implemented for encryption and authentication when WPA-capable?	□ Yes □ No □ N/A
2.5	Are all production systems (servers and network components) hardened by removing all unnecessary services and protocols installed by the default configuration?	□ Yes □ No
2.6	Are secure, encrypted communications used for remote administration of production systems and applications?	□ Yes □ No □ N/A

Protect Cardholder Data

Requirement 3: Protect stored data

	DESCRIPTION	RESPONSE
3.1	Is sensitive cardholder data securely disposed of when no longer needed?	□ Yes □ No
3.2	Is it prohibited to store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.) in the database, log files, or point-of-sale products?	□ Yes □ No
3.3	Is it prohibited to store the card-validation code (three-digit value printed on the signature panel of a card) in the database, log files, or point-of-sale products?	□ Yes □ No
3.4	Are all but the last four digits of the account number masked when displaying cardholder data?	□ Yes □ No
3.5	Are account numbers (in databases, logs, files, backup media, etc.) stored securely— for example, by means of encryption or truncation?	□ Yes □ No
3.6	Are account numbers sanitized before being logged in the audit log?	□ Yes □ No

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

	DESCRIPTION	RESPONSE
4.1	Are transmissions of sensitive cardholder data encrypted over public networks through the use of SSL or other industry acceptable methods?	□ Yes □ No
4.2	If SSL is used for transmission of sensitive cardholder data, is it using version 3.0 with 128-bit encryption?	□ Yes □ No □ N/A
4.3	If wireless technology is used, is the communication encrypted using Wi-Fi Protected Access (WPA), VPN, SSL at 128-bit, or WEP?	□ Yes □ No □ N/A
4.4	If wireless technology is used, are WEP at 128-bit and additional encryption technologies in use, and are shared WEP keys rotated quarterly?	□ Yes □ No □ N/A
4.5	Is encryption used in the transmission of account numbers via e-mail?	□ Yes □ No □ N/A

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

	DESCRIPTION	RESPONSE		
5.1	Is there a virus scanner installed on all servers and on all workstations, and is the virus scanner regularly updated?	□ Yes	□ No	

Requirement 6: Develop and maintain secure systems and applications

	DESCRIPTION	RESPONSE		
6.1	Are development, testing, and production systems updated with the latest security-related patches released by the vendors?	□ Yes	□ No	
6.2	Is the software and application development process based on an industry best practice and is information security included throughout the software development life cycle (SDLC) process?	□ Yes	□ No	□ N/A
6.3	If production data is used for testing and development purposes, is sensitive cardholder data sanitized before usage?	□ Yes	□ No	□ N/A
6.4	Are all changes to the production environment and applications formally authorized, planned, and logged before being implemented?	□ Yes	□ No	
6.5	Were the guidelines commonly accepted by the security community (such as Open Web Application Security Project group (www.owasp.org)) taken into account in the development of Web applications?	□ Yes	□ No	□ N/A
6.6	When authenticating over the Internet, is the application designed to prevent malicious users from trying to determine existing user accounts?	□ Yes	□ No	□ N/A
6.7	Is sensitive cardholder data stored in cookies secured or encrypted?	□ Yes	□ No	□ N/A
6.8	Are controls implemented on the server side to prevent SQL injection and other bypassing of client side-input controls?	□ Yes	□ No	□ N/A

Implement Strong Access Control Measures

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

	DESCRIPTION	RESPONSE
7.1	Is access to payment card account numbers restricted for users on a need-to-know basis?	□ Yes □ No

Requirement 8: Assign a unique ID to each person with computer access

	DESCRIPTION	RESPONSE
8.1	Are all users required to authenticate using, at a minimum, a unique username and password?	□ Yes □ No
8.2	If employees, administrators, or third parties access the network remotely, is remote access software (such as PCAnywhere, dial-in, or VPN) configured with a unique username and password and with encryption and other security features turned on?	□ Yes □ No □ N/A
8.3	Are all passwords on network devices and systems encrypted?	□ Yes □ No
8.4	When an employee leaves the company, are that employee's user accounts and passwords immediately revoked?	□ Yes □ No
8.5	Are all user accounts reviewed on a regular basis to ensure that malicious, out-of-date, or unknown accounts do not exist?	□ Yes □ No
8.6	Are non-consumer accounts that are not used for a lengthy amount of time (inactive accounts) automatically disabled in the system after a pre-defined period?	□ Yes □ No
8.7	Are accounts used by vendors for remote maintenance enabled only during the time needed?	□ Yes □ No □ N/A
8.8	Are group, shared, or generic accounts and passwords prohibited for non-consumer users?	□ Yes □ No
8.9	Are non-consumer users required to change their passwords on a pre-defined regular basis?	□ Yes □ No
8.10	Is there a password policy for non-consumer users that enforces the use of strong passwords and prevents the resubmission of previously used passwords?	□ Yes □ No
8.11	Is there an account-lockout mechanism that blocks a malicious user from obtaining access to an account by multiple password retries or brute force?	□ Yes □ No

Requirement 9: Restrict physical access to cardholder data

	DESCRIPTION	RESPONSE
9.1	Are there multiple physical security controls (such as badges, escorts, or mantraps) in place that would prevent unauthorized individuals from gaining access to the facility?	□ Yes □ No
9.2	If wireless technology is used, do you restrict access to wireless access points, wireless gateways, and wireless handheld devices?	□ Yes □ No □ N/A
9.3	Are equipment (such as servers, workstations, laptops, and hard drives) and media containing cardholder data physically protected against unauthorized access?	□ Yes □ No
9.4	Is all cardholder data printed on paper or received by fax protected against unauthorized access?	□ Yes □ No
9.5	Are procedures in place to handle secure distribution and disposal of backup media and other media containing sensitive cardholder data?	□ Yes □ No
9.6	Are all media devices that store cardholder data properly inventoried and securely stored?	□ Yes □ No
9.7	Is cardholder data deleted or destroyed before it is physically disposed (for example, by shredding papers or degaussing backup media)?	□ Yes □ No

Regularly Monitor and Test Networks

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

	DESCRIPTION	RESPONSE
10.1	Is all access to cardholder data, including root/administration access, logged?	□ Yes □ No
10.2	Do access control logs contain successful and unsuccessful login attempts and access to audit logs?	□ Yes □ No
10.3	Are all critical system clocks and times synchronized, and do logs include date and time stamp?	□ Yes □ No
10.4	Are the firewall, router, wireless access points, and authentication server logs regularly reviewed for unauthorized traffic?	□ Yes □ No
10.5	Are audit logs regularly backed up, secured, and retained for at least three months online and one-year offline for all critical systems?	□ Yes □ No

Requirement 11: Regularly test security systems and processes

	DESCRIPTION	RESPONSE
11.1	If wireless technology is used, is a wireless analyzer periodically run to identify all wireless devices?	□ Yes □ No □ N/A
11.2	Is a vulnerability scan or penetration test performed on all Internet-facing applications and systems before they go into production?	□ Yes □ No
11.3	Is an intrusion detection or intrusion prevention system used on the network?	□ Yes □ No
11.4	Are security alerts from the intrusion detection or intrusion prevention system (IDS/IPS) continuously monitored, and are the latest IDS/IPS signatures installed?	□ Yes □ No

Maintain a policy that addresses information security

Requirement 12: Maintain a policy that addresses information security

DESCRIPTION		RESPONSE	
12.1	Are information security policies, including policies for access control, application and system development, operational, network and physical security, formally documented?	□ Yes	□ No
12.2	Are information security policies and other relevant security information disseminated to all system users (including vendors, contractors, and business partners)?	□ Yes	□ No
12.3	Are information security policies reviewed at least once a year and updated as needed?	□ Yes	□ No
12.4	Have the roles and responsibilities for information security been clearly defined within the company?	□ Yes	□ No
12.5	Is there an up-to-date information security awareness and training program in place for all system users?	□ Yes	□ No
12.6	Are employees required to sign an agreement verifying they have read and understood the security policies and procedures?	□ Yes	□ No
12.7	Is a background investigation (such as a credit- and criminal-record check, within the limits of local law) performed on all employees with access to account numbers?	□ Yes	□ No
12.8	Are all third parties with access to sensitive cardholder data contractually obligated to comply with card association security standards?	□ Yes	□ No
12.9	Is a security incident response plan formally documented and disseminated to the appropriate responsible parties?	□ Yes	□ No
12.10	Are security incidents reported to the person responsible for security investigation?	□ Yes	□ No
12.11	Is there an incident response team ready to be deployed in case of a cardholder data compromise?	□ Yes	□ No