

PCI: REQUIREMENTS TO ACTION

Practical guidance for more
efficient, effective compliance

Benjamin Tomhave, MS, CISSP

PROVIDED WITH THE SUPPORT OF:



TRUTH TO POWER
ASSOCIATION



TABLE OF CONTENTS

CONTENTS

- A MORE RATIONAL APPROACH TO PCI COMPLIANCE..... [1](#)**
 - Positioning PCI in the Enterprise..... [3](#)
- PCI FROM THE INSIDE OUT [4](#)**
 - Risk Management [4](#)
 - Network Security and Architecture [6](#)
 - Logging and Monitoring [7](#)
 - Operational Security [8](#)
 - Encryption Key Management [10](#)
 - Secure Development [11](#)
 - Testing and Audit..... [12](#)
 - Identity and Access Management (IAM) [13](#)
 - Policies, Standards, and Procedures [14](#)
 - Training and Awareness [15](#)
- TRANSLATING PCI REQUIREMENTS INTO ACTION [16](#)**
 - The In-Scope Environment..... [16](#)
 - PCI: Indicated Actions..... [19](#)**
 - Requirement 1: Install and maintain a firewall configuration to protect
cardholder data..... [19](#)
 - Requirement 2: Do not use vendor-supplied defaults for system passwords and
other security parameters..... [21](#)
 - Requirement 3: Protect stored cardholder data..... [21](#)
 - Requirement 4: Encrypt transmission of cardholder data across open,
public networks [22](#)

TABLE OF CONTENTS, continued

Requirement 5: Use and regularly update antivirus (AV) software or programs.....[23](#)
 Requirement 6: Develop and maintain secure systems and applications[23](#)
 Requirement 7: Restrict access to cardholder data by business need to know.....[24](#)
 Requirement 8: Assign a unique ID to each person with computer access[25](#)
 Requirement 9: Restrict physical access to cardholder data.....[26](#)
 Requirement 10: Track and monitor access to network resources and
 cardholder data.....[27](#)
 Requirement 11: Regularly test security systems and processes.....[28](#)
 Requirement 12: Maintain a policy that addresses information security for
 employees and contractors[29](#)

APPENDIX A: SECURITY POLICY, STANDARD, AND PROCEDURE MODELS ... [32](#)

PROVENANCE..... [33](#)

NOTES [34](#)

LEGAL NOTICE..... [37](#)

A MORE RATIONAL APPROACH TO PCI COMPLIANCE

The Payment Card Industry Data Security Standard (PCI)¹ is as notable for the guidance it offers as for that it omits. By parsing card data protection into a 12-step program, the standard appears to promise an accessible checklist—perhaps even a roadmap—for reasonably complete information security. Yet, by assuming—and omitting—much of the security- and risk-management context that provides efficiency and effectiveness in enterprise implementations, PCI leaves many opportunities for budgetary gaffes and breach events.

Largely because of these assumptions, PCI has since its first release in 2005 sparked both skepticism and criticism. Critics call the standard a money pit: a mandate of checklist compliance that diverts capital, resources, and strategic focus for only a topical guarantee of card-data protection. Meanwhile, the ongoing evolution of information security as a corporate practice has only served to highlight PCI's limitations as a relatively static programmatic standard

Compliance costs are a particularly sore point, although concrete cost estimates vary widely. Gartner reports that in 2008 the average Level 1 merchant spent \$2.7 million PCI compliance, and the average Level 2 merchant spent \$1.1 million—a fivefold increase over 2006 costs.² Meanwhile, Forrester Research has pegged PCI compliance spending at 2 to 10 percent of annual IT budgets,³ which themselves tend to average 6 to 7 percent of annual revenue. Depending on the merchant, this figure could put compliance spending either higher or lower than Gartner's estimates. Yet, as the 2008 Heartland Payment System breach and other high-profile security incidents⁴ attest, spending on PCI compliance offers no guarantee of card-data security.⁵

Corporate executives and regulators have disparaged PCI for structural faults as well.⁶ Citing the standard's complexity, point-in-time assurance model, and checklist approach to information protection, security experts claim PCI not only fails to fully protect organizations against security threats, but also often displaces effective internal initiatives and investments.

Is PCI fatally flawed? The answer hangs as much on companies' approach to compliance—and security as a risk management practice—as on the rule itself.

Much undue risk, unnecessary work, and excessive costs associated with PCI compliance spring from misconceptions or misapplication of the standard. PCI is primarily a tactical, technical standard; but it is not comprehensive guidance. Nor does it constitute a risk or security management framework.⁷

.....

**Is PCI fatally
flawed? The answer
hangs as much on
companies' approach
to compliance—and
security as a risk
management practice—
as on the rule itself.**

.....

Thus, where PCI fails companies—and vice versa—those failures tend to fall into three categories:

- **Too much compliance, not enough security.** Companies that focus on PCI as a compliance goal, rather than a security means, are bound to miss significant risks that can come back to haunt them. As a security checklist, PCI is not sufficiently detailed to provide comprehensive coverage, even in compliant entities. A letter-of-the-law approach to compliance, such as penetration tests focused only on financial systems, the omission of social engineering vectors, and fix-it-and-forget-it annual assessments, leaves companies exposed. In fact, confusing compliance with security can increase risk potential, since companies may assume more risk than they should when they believe they're protected by a bullet-proof skin of PCI compliance.
- **Static compliance, dynamic environments.** PCI's annual self-assessment requirements leave companies lots of time to reorganize, rearchitect, redevelop, and reconfigure between reporting deadlines. Meanwhile, the threatscape is constantly changing; and, while PCI does require reassessment (or at least rescanning) of the cardholder environment after "major changes," the criteria for this trigger are largely ambiguous. Furthermore, PCI requires routine monitoring of the cardholder environment. However, routine monitoring often fall shorts in its scope and applicability. The entire world could change around the billing environment, drastically altering the threatscape, and PCI would still be relatively happy with the status quo.

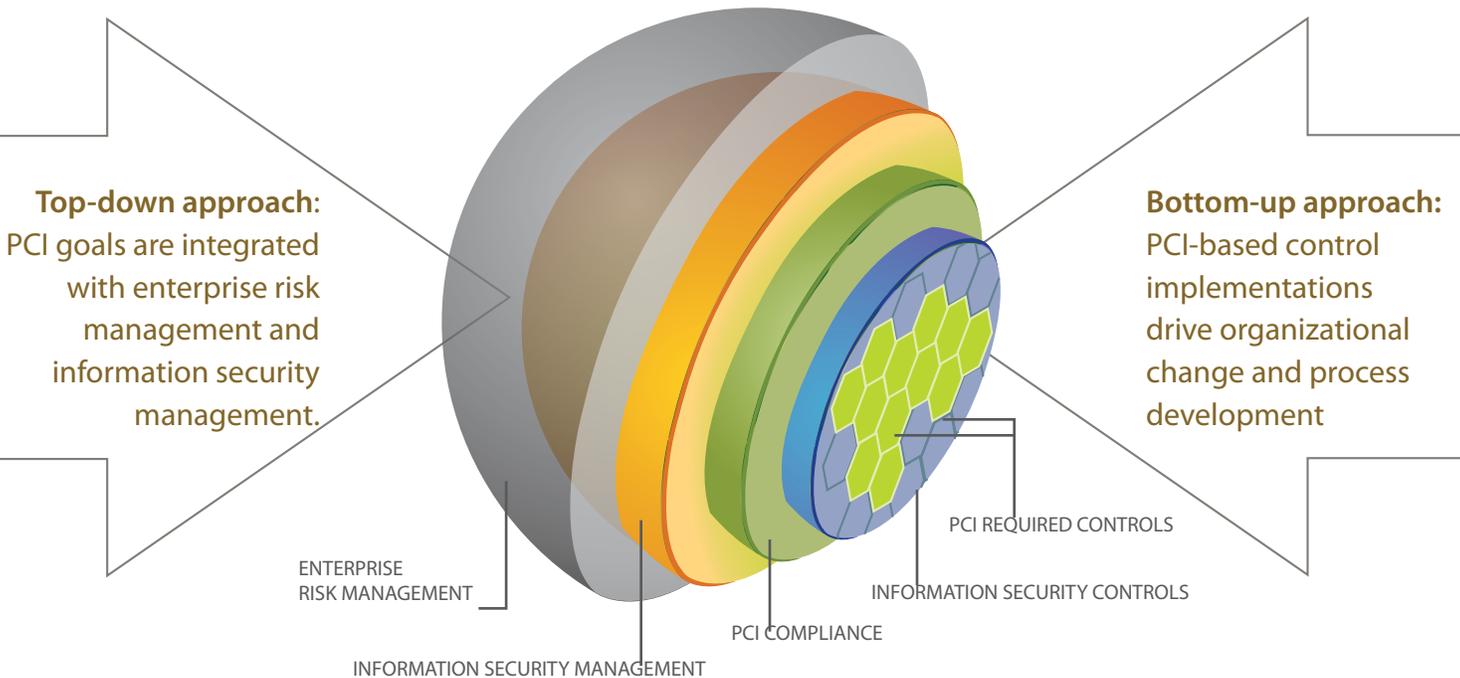
Companies that fail to properly assess and account for the security-risk impact of internal changes—or that fail to keep security controls, such as antivirus definitions, up to speed with external threats—are risk magnets. Every change, from new server purchases to new virus outbreaks, multiplies the likelihood of a breach. Annual security is simply not adequate to protect covered systems, to say nothing of enterprise systems as a whole.

- **Bad self-assessment, bad assumptions, and/or bad reporting.** Most merchants are not subject to external audits and may exercise significant discretion in both their internal assessments and the self-assessments they remit to their banks. This aspect of the standard leaves plenty of room for honest mistakes, corner cutting, fudging, and blatant dishonesty. PCI's compliance costs are significant and should be approached with an efficiency posture; however, cost constraints do not justify compliance program that pay only lip service without validation. Companies (and auditors) must, as Ronald Reagan famously said, "Trust, but verify."

In fact, almost all of these failures are allowed under PCI—a perfect indicator of why compliance with the standard cannot rationally be used as either the alpha or omega of security efforts.

PCI lives in a murky twilight of security management. While it provides some concrete milestones, these can be effective only if companies 1) provide a managerial context of appropriate scope, risk relevance, operational integration, and continual improvement; and 2) ensure that more granular controls are working more frequently than the rule absolutely requires. Companies must support PCI from both the

Positioning PCI in the Enterprise



top down and the bottom up, according to their unique risk profiles and risk vectors. Above all, companies must accept managerial responsibility for security decisions.

Given context and structure, PCI can be a critical component of an effective security practice. While the effectiveness of any security investment is notoriously difficult to quantify (what is the cost of a breach that never happened?), the obverse of increased risk in the absence of compliance has been documented. According to the 2009 Data Breach Investigations Report issued by the Verizon Business RISK Team, more than 75 percent of companies that reported experiencing a breach had been deemed noncompliant in the preceding 12 months.⁸ This is a statistically significant correlation between control failures and breach events. In light of this finding, the question is not whether PCI can represent effective security, but how to make compliance make sense in the enterprise context. As indicated earlier, the answer lies in approaching PCI compliance from both the top down and the bottom up:

- **Top-down approach:** Integrate PCI as an assurance checklist within strategic risk- and security-management programs. In general, the only way to do accomplish this efficiency is to integrate security values and procedures into typical operational processes.
- **Bottom-up approach:** Use PCI as a lever to build and advance the overall organizational security program—with the understanding that PCI compliance is not an end goal. Companies can leverage the requirement for changes and process development to improve the entire organization wherever possible rather than only applying these methods and tools to the smaller cardholder environment.

Both of these approaches are needed to support not only efficient, effective compliance, but defensible security practices in the broader scheme of enterprise risk management and rational spending.

The balance of this paper supports both initiatives by providing an analytical perspective on PCI requirements, references to useful resources that support an integrated compliance approach, and practice-based recommendations for implementing PCI controls that makes sense in terms of operational risk, compliance obligations, and business justification. Although this guidance will not allow you to develop a security and risk management program overnight, it supports the first and most critical step: understanding what you need to do to turn PCI compliance from an expensive, pro forma proposition into a comprehensible, pragmatic, and programmatic effort.

PCI FROM THE INSIDE OUT

Risk Management

A risk management approach is not required for PCI compliance. That said, savvy security professionals will tell you that risk management is an essential precursor to efficient compliance, sound security strategy, and effective security operations.

In reality, there's no good way to short-cut the development of a risk management process and approach. You can, however, leverage one or more frameworks to jumpstart your strategy. Robust risk management frameworks like those cited in this section generally cover, to a greater or lesser degree, the categorization and/or rating of information systems or assets; the identification and measurement of security risk; and the selection, implementation, assessment, monitoring, and continual improvement of security controls for risk mitigation. Comprehensive and widely used frameworks include⁹:

- [ISO/IEC 27005:2008 Information technology -- Security techniques – Information security risk management](#), issued by the International Organization for Standardization. Not for the faint of heart, the 27005 standard offers relatively quantitative, heavyweight guidance suitable for very complex environments. As a methodology-neutral standard, it may be more easily adapted for use in conjunction with other standards and information security management and assessment methodologies. However, ISO/IEC 27005 has also been criticized for its inconsistency with most risk management approaches; and, in fact, for its divergence from what is traditionally thought of as “risk management” by the security industry. Moreover, while ISO/IEC 27005 describes some attributes of a risk management approach, it does not set forth hard requirements, leaving it open to the perversion of overall risk management processes and practices.
- [Operationally Critical Threat, Asset, and Vulnerability Evaluation \(OCTAVE\)](#), maintained by CERT, part of the Software Engineering Institute (SEI) at Carnegie Mellon University. OCTAVE

COMMUNITY RESOURCE

THE TEAM MODEL OF FRAMEWORK INTEGRATION

The Total Enterprise Assurance Management (TEAM) Model: A Unified Approach to Information Assurance Management presents one approach to integrating multiple frameworks within an overall enterprise assurance management program.

The TEAM Model breaks assurance management into three programmatic components—enterprise risk management, operational security management, and audit management—that are centered on a single set of requirements. Under each component area, organizations are free to implement the best framework or methodology possible, with the caveat that each implementation interfaces well with the other areas.

comes in three flavors: original; “-S,” for smaller organizations; and –Allegro, for more streamlined assurance. OCTAVE methods are relatively qualitative, team-based, and communication-intensive. The methodology itself tends to be used more in high-level discussions and less in an operational capacity.

- **Factor Analysis of Information Risk (FAIR)**, maintained by Risk Management Insight. FAIR applies Bayesian analysis and quantitative assessment techniques in an effort to make risk measurement more scientific. For companies seeking to put hard numbers behind their risk decisions, FAIR represents one of the most useful available methodologies; however, the relevance of risk decisions reached through FAIR is heavily dependent on the availability and reliability of risk data.
- **NIST Risk Management Framework (RMF)**, maintained by the National Institute of Standards and Technology (NIST), a US government agency. The RMF is a compilation of several NIST 800-Series Special Publications for information security that favor quantitative assessment of operational and technical risks. Although 800-Series standard are primarily published for federal agencies, NIST standards can be adapted for private-sector organizations.
- **Systems Security Engineering – Capability Maturity Model (SSE-CMM)**, maintained by the International Systems Security Engineering Association (ISSEA), is a technical maturity model that includes risk management as an inherent component. The model supports the effective measurement and management of risk on a continual basis.

- **The INFOSEC Assurance Capability Maturity Model (IA-CMM)**, maintained by the US National Security Agency (NSA) through the INFOSEC Assurance Training and Rating program. IA-CMM is based on the Systems Security Engineering Capability Maturity Model (SSE-CMM) and is largely composed of two key methodologies: INFOSEC Assessment Methodology (IAM) and INFOSEC Evaluation Methodology (IEM). The measurement of risk on a given system within the environment is one of the major outcomes of following IAM.

As you can see in the descriptions above, each given framework approaches risk management in its own way. Organizations should choose a framework and approach that melds well with corporate culture and values. Following OCTAVE, for example, requires time and input from many high-level managers, which may be unavailable in some organizations, but preferred in others. NIST and FAIR, by contrast, rely more heavily on the collection and analysis of data that might or might not be readily available.

Risk and security managers should also be sensitive to cultural factors that might indicate one approach over another. For example, executives and other organizational stakeholders in one organization might see a more quantitative, data-dependent framework as divisive; an “ivory tower” approach to risk management. In another organization, a quantitative approach might be preferred. After all, the insurance industry, which is rooted in actuarial science, provides ample evidence of organizational faith in quantitative risk management methodologies.

Note that, when it comes to choosing a framework, one size does not always fit all—even within a single organization. Managers should plan to assess various frameworks, identify at least one framework that seems like a good fit for the organization, and customize a risk management approach that fits the organization’s unique characteristics.

In fact, many companies pursue a hybridized risk management methodology based on multiple frameworks. While this approach can provide the best fit and coverage, managers should also be aware of potential stumbling blocks a hybridized approach can present in risk management practice. Some frameworks are tied to licensed methodologies; training, assessment, and certification programs; tools; and specialized professional services. Integrating disparate methodologies can complicate the organization’s ability to use or benefit from such supplementary resources down the road. Instead of applying hybridization across the entirety of enterprise, managers should instead look at a tiered approach that ranges from risk-based decision processes to hands-on risk assessment to in-the-trenches risk mitigation.

Network Security and Architecture

PCI’s verbose requirement for network security and architecture is one the more interesting compliance cost centers. PCI Version 1.2, the most recent release at the time of this writing, requires the use of a stateful firewall and bars reliance on basic router access control lists (ACLs). These firewalls are stipulated for the protection of the mandated “demilitarized zone” (DMZ) for systems and applications processing, as well as the transmission of cardholder data.

As a best practice, a dual-DMZ architecture—with a primary DMZ that protects Internet-facing hosts and applications and a sub-DMZ for the storage of cardholder data that accepts only traffic from within the primary DMZ—is highly recommended. The internal sub-DMZ should communicate only with the primary DMZ using specific point-to-point rules for both inbound and outbound connections.

Sustaining compliance with these requirements requires some planning. Scalability and manageability are common issues. Software-based firewalls running on a server (even a stripped-down server) can hit throughput limits. And managing multiple rulesets can quickly become a headache. Firewalls and other network elements should be planned and managed to avoid unique and one-off implementations and instead adhere to a comprehensive, well-managed set of standardized configurations for multiple devices. The same principle applies for routers and intrusion detection systems (IDS).

Logging and Monitoring

PCI Requirement 10, which requires organizations to manage and maintain audit logs, is another potential high-cost requirement. Per PCI v1.2, merchants must: 1) save logs to a central, protected log server; 2) review logs at least daily (automated reviews are OK); 3) retain at least one year of logs; and, 4) ensure that at least the last three months of logs are immediately available on demand (per Requirement 10.7).

The real cost of compliance with PCI’s logging requirements lies in management, security, and review. If you have several systems defined as in-scope for PCI—and particularly if some are externally facing hosts—you must maintain fairly detailed logs for them. On top of this, PCI’s specification of daily log review for “all system components” is one of its most onerous requirements—more so, because manual review and processing of audit logs is a mind-numbing and time-intensive task.

For these reasons, many companies opt to use commercial log-management tools for the collection and analysis of log data. Organizations that cannot budget for log management software can still reduce (but not eliminate) the review burden by instituting scanning scripts that automatically scan logs for new events, system events, suspicious user activities, and known attack indicators. Such scripts can usually be configured to write their findings to a separate log or recording mechanism and/or email findings to designated staff.

.....

Firewalls and other network elements should be planned and managed to avoid unique, one-off implementations and instead adhere to a comprehensive, well-managed set of standardized configurations

.....

.....

Log collection, correlation, and analysis is one area where a checklist approach to compliance can seriously undermine the security purpose.

.....

Companies must also take care to protect the log data itself, since it contains sensitive information about both the systems that store and process cardholder data and servers that perform security functions, such as intrusion detection and access management. Log data builds up quickly, so system managers must ensure that sufficient storage capacity is allocated for logs and other audit records. Some log-management tools can also help in this regard, since they can be configured to reduce the likelihood that log volume will unexpectedly exceed storage capacity.

Beyond requiring daily log review, PCI offers few parameters for what organizations should look for or how they should analyze log data. Notably, because PCI enforcers are mainly concerned with raw log data as a forensic tool, PCI does not require centralized analysis of log data. Moreover, while PCI requires companies to review and correlate physical access logs and monitoring trails, it requires no comparable level of correlation for server logs. This is one area where a checklist approach to compliance can seriously undermine the security purpose. A more strategic approach to log management that looks across systems and events can provide invaluable visibility into system and user activities—a potential treasure-trove of risk indicators.

Even absent this level of coordination, however, meeting PCI's log management requirements requires both planning and managerial strategy. Standards such as [NIST Special Publication 800-92](#) (PDF) can help companies define good-practice steps for log collection, correlation, and realtime analysis. Most of these process steps can be automated, allowing companies to proactively detect information confidentiality and integrity risks, as well as use patterns, server loads, and other trends that might indicate risks to information availability.

Don't forget incident response management in your log management planning. Engaging skilled, competent employees who can perform risk, performance, or forensic analyses on logs is a managerial—not technical—activity. This is another way that PCI can end up costing you more than you might expect. However, omission can be still more costly.

Operational Security

Operational security controls help reduce risks introduced by IT operations themselves. These controls can be simple actions, such as hardening servers. Or they can be more involved activities, such as defining and following good antivirus, patch management, vulnerability management, configuration management, and change management practices. In terms of compliance cost, however, these efforts are usually one of the more nominal areas.

Server hardening is an excellent example of a low-cost technical control. If you use a standard approach, such as the one recommended by the [NSA Security Configuration Guides](#), or even a software solution, your largest expense is most likely to be the time it takes to prepare a server for the tool’s deployment and ensure that applications can operate properly within the hardened environment. Similarly, deploying antivirus is a good and relatively low-cost practice, although you must make sure the software is running properly, ensure the application will perform regular updates, and put processes in place to capture applicable logs.

Patching servers can be straightforward, as long as you don’t break your applications in the process. PCI v1.2 Requirement 6.1 requires organizations to apply “critical” patches within one month of their release and allows organizations to prioritize patch installation according to system criticality. While

.....

While PCI stops short of recommending risk-based patch prioritization, the language in v1.2 at least gives managers a “hook” for defending patching decisions to their auditors.

.....

PCI stops short of recommending risk-based patch prioritization (“An organization may consider applying a risk-based approach to prioritize their patch installations.”),¹⁰ the language in v1.2 at least gives managers a defensibility “hook” for defending patching decisions to their auditors. To be safe, however, it is advisable to document a patch scoring system—such as the one recommended by the [The Security Content Automation Protocol \(SCAP\)](#) from NIST—to your environment, combined with a risk-based approach to scheduling patch implementation.

PCI requirements for configuration management and change management also fall under operational security and have a rather greater potential to give technical staff major headaches. Change review and approval—as well as associated requirements such as versioning, rollback procedures, and segregation of duties—can add time and process to developer and administrator

responsibilities. Companies are likely to incur costs in the short term, with respect to performance efficiency and overall staff morale. These “people” costs should be factored into the overall costs of PCI compliance. Managers should also be sensitive to “techie” tendencies to shortcut procedural requirements. However, change and configuration management should increase operational efficiency over the longer term.

Automated workflows and configuration management tools can help reduce some of the process burdens and risks associated with change and configuration management. A good configuration management system can save your bacon if an upgrade goes awry or if a key piece of networking equipment gives up the ghost.

Change and configuration management policies and procedures are generally enacted as organizational development standards, providing benefits well beyond PCI's in-scope environment. In addition, implementing relevant controls within the context of a service management framework, such as the [Information Technology Infrastructure Library \(ITIL\)](#) issued by the UK's Office of Government Commerce, can improve both the effectiveness and efficiency of control efforts, as well as the IT service delivery process as a whole.

Encryption Key Management

Encryption is one of the more frequently overlooked and poorly understood PCI requirements. PCI requires two types of encryption: one for data "at rest" in databases and one for data "in motion" over public networks.

Encryption of data at rest is by far the more complex requirement. In many cases, developers believe they can write custom code for encryption algorithms and functional key management. In reality, however, such practices can introduce tremendous unmitigated and unmanaged risk to the enterprise. Writing code for encryption and key management is a tricky venture at best, and downright dangerous on average.

Currently, there is one major open source key-management platform that companies can use to meet encryption requirements. StrongKey is the reference platform upon which the work of the [OASIS Encryption Key Management Infrastructure \(EKMI\)](#) Technical Committee is based. EKMI represents the future of key management, converging public key management (PKI) with symmetric key management into a single unified system.

Outside of StrongKey, numerous commercial solutions offer a range of experiences and value propositions. Many of these solutions are moving toward other key management standards, such as the OASIS Key Management Interoperability Protocol (KMIP), the IEEE P1619.3 draft, and the IETF Keyprov protocol. Commercial solutions seldom come cheap; however, they offer to many companies an accessible path for meeting PCI's strong key management requirement, which must be taken seriously.

Managers should also consider the process requirements of key management, in addition to the technical aspects. Specifically, PCI requires the application of split knowledge, dual control, and separation of duties in the management of encryption keys. These requirements are meant to ensure that no single person can control all of the keys or the key environment. A person who generates keys may not also install them. And a person who installs keys must not be able to generate and install their own key, in order to prevent insertion of an unauthorized key. All of these controls must be supported by periodic checks to ensure that the key system has the highest integrity possible.

.....
Writing code for encryption and key management is a tricky venture at best, and downright dangerous on average.

Secure Development

Bolting security onto applications and projects is not only ineffective, it doesn't meet compliance requirements. Security must be integrated into development process, per PCI Requirement 6. In most cases, companies must institute changes in development practices in order to meet this demand.

The best approach to this requirement is to align development processes with a software development lifecycle. Managers should also encourage developers to engage in programs, such as the [Open Web Application Security Project \(OWASP\)](#),¹¹ which is recommended in the PCI standard. However, as with risk management, companies can leverage available management models to accelerate integration of security practices within development programs. OWASP's [Software Assurance Maturity Model \(SAMM\)](#) and the [Building Security In Management Model \(BSI-MM\)](#), an open resource released by vendors Cigital and Fortify, both represent robust, free resources that can jumpstart secure-development initiatives.

In many cases, developers will need to modify their practices to incorporate security functions, such as input

.....

Where development staff lack experience with secure coding, a team-mentor approach to education can encourage more rapid adoption.

.....

and output validation, elimination of common vulnerabilities, and use of stored procedures. Where development staff lack experience with secure coding, a team-mentor approach to education can encourage more rapid adoption. In this approach, managers identify team members who are interested in application security, encourage skill development, and support these early adopters in leading other team members to improve overall security practices. Sending developers to training courses or engaging external training services that specialize in secure development can further accelerate the absorption of secure coding concepts and practices.

Companies should also ensure that application security is integrated into QA processes. Basic security testing should accompany standard code and functionality test-

ing. QA staff should look for common application vulnerabilities¹² and validate that code functions as expected. QA should also stress-test interfaces that might be subject to brute-force attacks; including, but not limited to, login, registration, and billing screens.

Commercial products and services can help If you're not entirely confident in your company's ability to achieve secure development objectives. Some consultants and service vendors specialize in secure coding and static code analysis, and several software vendors offer products for secure-code analysis.

Testing and Audit

PCI breaks security testing into two areas: vulnerability scanning and penetration testing (“pentesting”). Vulnerability scanning is usually performed by automated tools and has marginal utility in terms of identifying potential unpatched weaknesses in systems. The requirement for vulnerability scanning is accompanied by a requirement to use only an Approved Scanning Vendor (ASV), who must scan your externally-facing systems on a quarterly basis. PCI also requires internal vulnerability scanning, although this can be performed in-house by reasonably skilled staff using well-known tools.

Pentesting can be another thing entirely. While vulnerability scanning is passive in the sense that it seeks only to identify potential security weaknesses, pentesting actively explores the extent of the damages that would be allowed by found weaknesses. These efforts can include both technical and non-technical methods. Although application and network testing are often viewed as technical processes,

the SSC’s [Information Supplement: Requirement 11.3 Penetration Testing](#)¹³ (PDF) also puts social engineering within the pentesting scope.

This broad range of activities requires very diverse skill sets. Obviously, individuals who are qualified to perform software-based application testing might not be equally adept at social engineering tests. Companies should factor the potential cost of multiple staff resources into PCI compliance budgets.

Unlike external vulnerability scanning, pentesting does not require hiring an ASV or Qualified Security Assessors (QSA). Instead, the only requirement is to use “competent staff” to perform these tests on an annual basis. It’s important, however, to note that the use of skilled penetration testers (“pentesters”) is essential to the success of an internal testing program, even if that means engaging an outside resource or hiring additional staff. For this

reason, pentesting can represent a significant line-item expense associated with PCI; however, as with encryption, pentests are a requirement for which it’s dangerous to cut corners. Having your local curious hacker/admin do the job can leave a lot to be desired, fall short of compliance, and fail to meet the security objective of pentesting requirements. In particular, it is important to work with an experienced professional who will write a useful, usable report and who isn’t afraid to tell you what’s broken—hopefully, without breaking your systems in the process.

Because automated pentests are designed to closely approximate hacker methods, application and network pentesting are two of the few areas of compliance where automation is a de facto requirement.

The key to efficiency is to keep your scope refined, document what you do and what you find, and define a remediation plan to address negative findings in a timely fashion.

Whoever performs the test, a broad array of commercial and open source tools are available for vulnerability scanning, network scans, and application security assessment.

Overall, the key to efficient security testing and auditing is to keep your scope refined, document what you do and what you find, and define a remediation plan to address negative findings in a timely fashion. The strong backing of senior management is another implicit need in all of these stages, and on the technical side you may need to build out a toolkit that combines multiple testing applications and procedures.

Incidentally, when implementing an in-house security testing and audit program, be sure that you take the time to properly define different risk levels for your environment (as noted in the previous Risk Management section). NSA’s [INFOSEC Assurance Training and Rating Program](#)—more specifically, [IAM](#) and its associated [INFOSEC Evaluation Methodology \(IEM\)](#)—provides an excellent reference for defining an assessment program, as does the Open Source Security Testing Methodology Manual (OSSTMM) from the Institute for Security and Open Methodologies (ISECOM)

Identity and Access Management (IAM)

PCI stipulates strict limitations on who may access cardholder data and how, based on the principles of default deny and least privilege. What this means is that, by default, nobody should have access to cardholder data. All access must be explicitly authorized and as narrow in scope as possible. Further, access must minimally make use of strong passwords (at least seven alphanumeric characters) that are changed on a regular basis and do not repeat over four change cycles. In cases of remote access to cardholder environments, PCI ups the ante with a requirement for two-factor authentication. All users who access the system must have unique IDs: group accounts and shared login credentials are forbidden.

Without saying as much, these requirements take you down the path of a reasonably robust identity and access management (IAM) system. Each person who accesses the system should have a unique ID against which all access is recorded and tracked. Role-based access controls, (rather than ad hoc discretionary access controls) must be used in authorizing access.

All of this amounts to a potentially complex access management framework that would benefit well from a central tool. Fortunately, there are several automation options to help reduce the inevitable complexity and expense of implementing IAM. Either an open source or commercial product might offer a viable approach, depending on your organization. Solutions can be as straightforward as mandating the integration of all IAM into Active Directory in a Microsoft Windows-based environment; or the solution

.....
**Without saying as much,
 these requirements take
 you down the path of a
 reasonably robust identity
 and access management
 (IAM) system.**

TERMINOLOGY

Policies generally outline fundamental requirements that top management considers to be imperative

Standards provide more detailed rules for implementing the broader policies

Procedures describe the steps or actions required to comply with policies and standards

can take an open source route, leveraging projects such as OpenIAM, Kerberos, and OpenLDAP. Some third-party solutions support hybrid environments, as well.

The bottom line in all of these cases is that, while defining role-based access controls (RBAC) is necessary and vital to the success of PCI compliance and an IAM program, it can also be a nightmare, absorbing great swaths of time that might better be spent elsewhere. Choosing the right tools and assigning the right staff are the keys to meeting IAM goals, while minimizing the unnecessary burn of resources

Policies, Standards, and Procedures

PCI requires companies to document official, managerial rules for technical and operational security. Although the development of policies, standards, and procedures is a critical initiative that supports not just PCI, but organizational risk and security management as a whole, it can also be one of the most time-consuming compliance processes. Even if you opt to outsource part of the work, you must at some point take ownership and manage these critical pieces of internal guidance through necessary approval processes.

Accordingly, the greatest costs associated with this requirement area are time and staff resources. Most policy development projects bog down somewhere along the line, typically during approval rounds. Plan appropriately—and plan on exercising a lot of patience—when you start on these efforts. In addition, remember that periodic review and maintenance are part of the policy management process. Policy reviews should be

COMMUNITY RESOURCE

IT POLICY TEMPLATE WIKIS



Truth to Power's IT Policy Templates Wiki Project is a free repository of structured IT policy models that you can copy, print, customize, and use for your own information governance efforts.

performed at least annually or upon any significant change in operational practices, organizational structures, or the technical environment.

On the bright side, many freely available policy-development resources reduce the need to develop governance documents from scratch. There are many non-commercial and commercial sources of policy models that can expedite internal drafting processes. [Appendix A: Security Policy, Standard, and Procedure Models](#) provides pointers to several robust resources.

Training and Awareness

Training is the primary mechanism for integrating PCI and other security requirements and responsibilities into employees' day-to-day activities. Fortunately, of all the PCI requirements, training and awareness can also be one of the most cost-effective. At a minimum, all it requires is an internal resource with solid topical knowledge and good presentation skills.

Alternatively, companies may wish to engage a vendor specializing in technical training; particularly in security policies. Online training, instead of in-person training courses, can also be an effective mechanism. Both of these approaches require additional investments.

Do not, in any case, underestimate the importance or effectiveness of well-designed and well-delivered training programs. Awareness training can significantly reduce bad-security practices that can (and often do) undermine or circumvent even the best technical controls. Bear in mind, however, that training must be provided at least on an annual basis and should be provided more frequently in companies and internal organizations that experience heavy staff turnover. Network operations centers and call centers tend, for example, to experience relatively high staff churn. As such, security awareness training should be part of the mandatory orientation process for these organizations. Moreover, training should be re-run at least every six months, to ensure that people are keeping security best practices in the forefront of their minds.

In developing security awareness training, it is important to involve more than just technical resources in the development and approval of the training materials. You may even be able to piggyback PCI training on existing human resources and new-employee training programs, if you can keep course material concise and on-point. For longer training classes, be sure to schedule breaks if the class runs much longer

.....

You may be able to piggyback PCI training on existing human resources and new-employee training programs, if you can keep course materials concise and on-point.

.....

than an hour. A light, interactive approach to course delivery will hold employees' attention and encourage better knowledge retention than straight lecture/dictation.

Courses that are developed and delivered internally tend not to incur much in the way of cost, although it can be beneficial to have the training staff themselves trained on presentation skills and/or course development techniques. You can also incur additional costs related to the use of specialized technologies (such as software and infrastructure for online training); and the cost of course development, trainer training, training vendors, and class infrastructure (even if it's all outsourced) must also be factored into compliance budgets.

TRANSLATING PCI REQUIREMENTS INTO ACTION

Now that we've spent some time interpreting PCI's requirements generally, let's dig deeper into what attaining compliance actually entails.

Unfortunately, PCI Version 1.2 is not written for implementers; rather, it's structured more like an audit-procedures guide. While this might make the requirements easier to comprehend from a goals standpoint, it would be helpful to have an implementation guide that sets forth action items against which the organization's employees can execute.

This section seeks to provide one form of implementation guide by summarizing the actionable requirements of the PCI standards. All of the statements and action items listed hereafter are derived directly from PCI DSS 1.2.¹⁴

The In-Scope Environment

Defining the "in-scope" environment for PCI controls is one of the most important compliance factors—and one of the least well-understood strategic steps. Companies must take care to fully and accurately scope their PCI environments, especially when planning remediation investments based on prior assessments.

The PCI supporting document [PCI DSS Security Audit Procedures](#) (PDF) includes a section that clarifies which systems and components are covered by PCI requirements. Check your assumptions. On the one hand, cardholder data has a nasty habit of finding its way into unauthorized caches and uses. On the other hand, PCI itself does not necessarily or explicitly cover all enterprise systems.

PCI's privacy and security requirements apply mainly, but not exclusively, to cardholder data. Some non-cardholder data is also considered in the PCI standard; notably:

- **Authentication Credentials** passed over wireless networks. PCI Version 1.2 guides covered entities to also consider the security of access to systems covered by the PCI DSS. User authentication data passed over wireless networks is of particular concern and must be considered in PCI compliance.
- **Out-of-scope data on PCI-covered systems.** PCI requirements apply to systems that contain, access, or interface with cardholder data. These systems may contain out-of-scope data that is nevertheless covered by PCI.

Where does your PCI data live? Diagramming data flows can be a good first step in defining the in-scope environment. Map where card data enters the enterprise, which systems it touches and where the data flows between organizational applications, databases, and other systems. The discovery (and eradication) of rogue card-data in departmental systems is one of the most valuable potential outcomes of the mapping process. Make a particular effort to think of the less-than-obvious organizational consumers of cardholder data within your organization. Marketing spreadsheets, sales databases, activity reports, log files, and development testing files are common culprits in the unwanted and unnecessary expansion of PCI-covered environments.

System segmentation is another common, cost-driven scoping strategy. This entails the logical or even physical isolation of the systems to which you are required to apply the most intensive and expensive controls. The approach can be particularly effective when it's too expensive to execute PCI-required security controls on an enterprise scale, or when those controls would hobble legitimate and materially-significant business functions (for example, cross-site scripting used for a Web-based marketing function).

Unfortunately, PCI v1.2 still leaves wiggle room for Level 1 merchants and their Qualified Security Assessors to variously define network segmentation; however, the recommended practices of using routers with stateful ACLs, switches with virtual local area network (VLAN) configurations, and firewalls to segment networks reduces the chance that you and your QSA will disagree.

Management should be aware that scoping for the wrong reasons—usually just to get as much information as possible out from under PCI's contractual thumb—can defeat compliance, cost-containment, and organizational objectives. Network segmentation should be planned cautiously and intelligently to support maximum ongoing alignment of segmented systems. Without this strategic constraint, siloed PCI implementations are much more likely to introduce redundant, inconsistent, and incompatible controls and technologies that are expensive to implement and nearly impossible to scale or sustain. Companies should also consider the cost and risks associated with managing and enforcing a separate strain of policies, standards, and procedures for PCI silos.

Merchants can also reduce the in-scope environment by outsourcing or engaging vendors for transactional processing and card-data storage. Many companies choose this route simply to offload the risk and complexity of PCI compliance. It should, however, be noted that PCI enforcers still theoretically hold merchants responsible for the failures of processing vendors. Although this enforceability of this provision is questionable, it is nevertheless in the best interest of merchants to validate and enforce to whatever

degree possible the compliance of vendor environments and services. In fact, this assurance (and a right to audit) should always be built into vendor contract.

Finally, it must be noted that segmenting PCI systems does not relieve the organization of its general obligations to protect and secure sensitive customer and business data. Managers taking a strategic approach to PCI scoping should evaluate the cost of architecting and enforcing segmentation against the benefits of the control requirements that are *inconsistent or incompatible* with the organization's general information security regime—not the costs and benefits of PCI as a whole. Bottom line: mapping data flows is an essential step in understanding enterprise risk, even irrespective of the impact on scoping.

PCI: Indicated Actions

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

Summary:

Companies must implement a DMZ for cardholder environments. A DMZ is effectively a security bubble that contains the database wherein cardholder data is stored. Protection for the DMZ includes formal processes for approval and testing all firewall and router configurations and changes that impact the integrity of the DMZ. From an architectural best practice perspective, it is highly recommended that a secondary DMZ be embedded within the primary DMZ, with tightly restricted communication between the two. The secondary DMZ holds the cardholder data, separating it from the applications,

As part of this process, the company must develop and maintain a current network diagram; documentation of roles and responsibilities for PCI compliance; and documentation of all authorized services and ports that are exposed, along with a justification and description of the security measures that protect covered systems. In general, all “untrusted” network connections—including access from the Internet, partner networks, and wireless environments¹⁵—must pass through firewalls. Firewall rules must be narrowly focused, limiting both ingress and egress traffic.

Access controls into the cardholder environment must be IP-specific and must not expose internal addresses (per RFC1918¹⁶). Servers should not be allowed to open new egress connections; users must not be able to bypass firewalls to get to the Internet; and the firewalls must perform stateful inspection, evaluating the state, context, and content of data packets. All rule sets must be reviewed at least every six months.

Action Items:

- Establish firewall and router configuration standards.
 - Maintain a current network diagram.
 - Document formal process for approving and testing all connections and changes.
 - Implement a firewall at each Internet and DMZ connection point.
 - Document roles and responsibilities for network management.
 - Document, justify, and secure all network services and ports.
 - Reviewed firewall configurations and rule sets at least once every 6 months.
- Institute firewalls between covered systems and untrusted networks, including the Internet and wireless networks.
 - Implement a DMZ for cardholder applications with an additional internal DMZ containing the cardholder data itself.
 - Use IP-specific configuration rules that restrict both ingress and egress traffic based on a default deny-all stance.
 - Use stateful-inspection firewalls.¹⁷
 - Disallow bypassing of the firewall.
 - Route internal traffic internally, rather than through the Internet.
 - Use NAT with IP masquerading¹⁸ to limit exposure of the RFC19¹⁹ IP space.
 - Properly secure, synchronize, and back up router and firewall configurations.
 - Ensure that database servers within the internal DMZ can only access other servers in the external DMZ, and nowhere else.¹⁸ Such a requirement could, if strictly interpreted, introduce interesting challenges for patch and vulnerability management.
- Institute firewall software on mobile and employee-owned computers with direct Internet access.
 - Institute and manage policies and procedures for the configuration, use, and maintenance of personal firewall software.
 - Install and configure personal firewall software, per firewall policies, on mobile and employee-owned devices with direct Internet access.

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

Summary:

PCI requires companies to change all default passwords, SSIDs, SNMP strings, and other security elements on vendor-provided software that could be used to expose cardholder data. Additionally, companies should develop system configuration standards based on known good practices, as described below.

Action Items:

- Change default passwords, wireless SSIDs, and SNMP strings prior to production deployment.
- Develop system configuration standards based on known good practices that address the following:
 - One primary function per server
 - Disable unnecessary and insecure services and protocols
 - Configure security parameter as appropriate
 - Remove unnecessary files and components
- Remote administration must use a secured protocol.

Requirement 3: Protect stored cardholder data

Summary:

Wherever possible, do not store cardholder data. Some types of data— including the full magnetic strip (also known as *magstripe*) data, the card-verification code/value, and the PIN or encrypted PIN block— may not be stored at all. Although companies may store the cardholder's name, the primary account number (PAN), the expiration date, and the service code, the storage and display of such data must be secured in the ways described below.

Action Items:

- Minimize the storage of cardholder data through the development and enforcement of a data retention policy.
- Strictly limit the data that is stored and displayed.
 - You may store cardholder names, Primary Account Numbers (PANs), expiration data, and service codes

- Do not store full magnetic strip data, card verification codes/values (sometimes called CVV2s), or PINs or encrypted PIN blocks
- If the full PAN is stored, mask display to only the first six and last four digits (and preferably less). Display restrictions may be relaxed for cases of privileged access by personnel authorized to view full card numbers for specific business needs.
 - Render the PAN unreadable in storage using hashing, truncation, index tokens and pads, or strong encryption using good key management practices.
 - If disk encryption is used, logical access must be independent of the OS. Do not tie keys to user accounts. Institute and fully document key management practices, addressing key generation, secure distribution, secure storage, at least annual key rotation, and retirement of old or compromised keys. Key management practices must also enforce split knowledge and dual control of keys, as well as preventing the unauthorized substitution of keys.
 - Key custodians must sign a custodian agreement that certifies the custodian's understanding and commitment to comply with of key management policies and procedures.
- Restrict access to stored cardholder data on a need-to-know basis.
- Implements secure storage of cardholder data with minimal replication or duplication.
- Require all personnel with access to key materials or systems to sign a key custodian form that describes their role and responsibilities.

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

Summary:

Cardholder data must be protected with strong encryption when transmitted across public networks, such as Internet, wireless, GSM, and GPRS networks. Industry best practices for wireless networks must be applied. Unencrypted PANs must never be transmitted using end-user messaging technologies (including email, instant messaging, and chat).

Action Items:

- Implement strong cryptography²⁰ to protect the transmission of cardholder data over public networks, including the Internet, wireless networks, GSM, and GPRS.
- Use industry best practices for securing wireless networks (WEP²¹ is no longer a trusted standard).

- Never allow unencrypted PANs to be transmitted via end-user messaging technologies, such as email, instant messaging, and chat (IRC).

Requirement 5: Use and regularly update antivirus (AV) software or programs

Summary:

AV software from a reputable vendor must be installed and working on any systems that are commonly afflicted with malware. AV and AV audit logs must be addressed in security policy, in accordance with PCI Section 10.7.

Action Items:

Deploy a reputable AV solution to systems commonly afflicted with malware.

Ensure that AV installations are current, active, and generating audit logs in accordance with relevant security policies and standards.

Retain audit logs for at least one year

Ensure that at least three months of logs are immediately accessible through online interfaces.

Requirement 6: Develop and maintain secure systems and applications

Summary:

Companies must build security and privacy controls into development lifecycles. These controls generally fall into the broad categories of patch management, secure coding practices, separation of duties, segregation of development environments, configuration management, change management, access management, and vulnerability management. Public-facing Web applications, which are presumed to run in more hostile security environment than internal applications, are subject to special security measures.

Action Items:

- Deploy a vulnerability management plan that results in timely updates to configuration standards.
- Develop, document, and implement patch and vulnerability management policies and procedures.
 - Prioritize patches using a risk-based approach and apply them as appropriate

- Ensure that all critical security patches are applied within one month of release.
- Institute secure coding practices as part of a well-defined software development lifecycle, complete with quality assurance and code review capabilities.
 - Segregate development, testing, and production environments.
 - Enforce separation of duties between development/testing and production personnel.
 - Test all patches and configuration changes for input validation, error handling, secure storage of cryptographic materials, secure communication, and effectiveness of role-based access controls (RBAC).
 - Ensure that live production data is not used in application development or testing.
 - Remove all test data and accounts, custom application accounts, user IDs, and passwords from application prior to production deployment.
 - Review custom code for vulnerabilities:
 - Follow secure web application security practices, such as those advocated by OWASP.²²
 - Ensure code protects against cross-site scripting (XSS) attacks, SQL injection, malicious file execution, insecure direct object refers, cross-site request forgery (CSRF), information leaks and improper error handling, broken authentication and session management, insecure cryptography management, insecure communication, and failure to restrict URL access (enforced workflow, etc.).
- Implement and following robust change control/management procedures.
 - Document and assess the impact of all proposed changes.
 - Develop and enforce a change review process that includes impact assessment and managerial sign-off for all changes.
 - Test operational functionality prior to deployment.
 - Develop and document roll-back procedures (the ability to revert to a prior “good” application state or version).
- Provide additional security for public-facing Web applications with either regular (at least annual) code reviews or deployment of a Web application (proxy) firewall.

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

Summary:

Companies must limit access to cardholder data to only those individuals with a legitimate and recognized business need. Access management should be automated, be based on user roles, and cover all system components.

Action Items:

- Configure access controls for “default deny,” allowing only individuals with explicitly authorization to access covered systems. Authorization should be granted only to individuals with a legitimate business need to access cardholder data.
 - Access management should conform to role-based permissions (a user account must be assigned an authorized role to gain access to covered systems) and the principle of least-privilege access (the user must be able to access only such information and resources that are necessary to their legitimate business purpose).
 - The role-based access control systems must cover all system components.

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

Summary:

Companies must be able to uniquely identify, authenticate, and control access for all users of covered systems. Access rights and privileges should reflect the current role or status of a user, such as termination of employment or a change in role that impacts the user’s need for access.

This PCI section indicates fairly stringent password management requirements. Passwords must be obfuscated in backend systems and kept current through required rotation. Each individual password must be unique within four rotations and consistent with secure-format criteria.

Action Items:

- Assign all users a unique ID and a password, passphrase, or two-factor credentials.
 - Authenticate all individual access to cardholder databases.
 - Require two-factor authentication for remote access.
 - Do not use group, shared, or generic accounts or passwords.
- Implement proper, well-documented identity and access management.
 - Disable or remove accounts assigned to terminated personnel immediately upon termination.
 - Disabled or remove accounts after 90 days of inactivity.
 - Disable vendor maintenance accounts that are not in active use.
 - Lock out or disabled accounts after a maximum of six failed login attempts. Set lock-out for a minimum of 30 minutes, unless overridden by an administrator.
 - Enforce password rules and management

- Set first-time passwords to a unique value and enforce an immediate password change upon the first login.
 - Verify user identities prior to resetting passwords or accounts.
 - Protect passwords in backend systems using strong cryptographic methods (hashing is acceptable).
 - Require passwords to be changed at least once every 90 days.
 - Require passwords to be a minimum of seven alphanumeric characters in length.
 - Require the unique passwords for four consecutive change cycles (the user may not use the same password more than once in every four password rotations)
 - Communicate all password policies and procedures to applicable personnel.
- Set session timeouts for a maximum of 15 minutes, requiring the user to re-login for continued access.

Requirement 9: Restrict physical access to cardholder data

Summary:

Companies must implement controls to protect physical devices from unauthorized access and retain, unless otherwise restricted by law, records of access. Control and monitoring mechanisms must themselves be physically protected.

Companies should correlate physical access logs (video records and physical sign-in logs, for example), and log content must be periodically reviewed for evidence of breach attempts or events.

In addition to protecting data internally, companies must ensure that appropriate managers review and approve all physical movement of cardholder data and at least annually inventory PCI-covered data stored electronically and physically. When cardholder data is no longer required, the company must render it unreadable and unrecoverable. Required practices must consider all types of media, including paper.

Action Items:

- Implement facility access controls.
 - Implement a badge system that allows employees and/or access devices to easily distinguish between employees and visitors.
 - Issue a physical token, such as a badge or sticker, that clearly indicates access rights and require visitors to surrender of the token at the end of their visits.
 - Define visitor-handling procedures that explicitly grant and, when indicated, revoke authorization for accessing the cardholder environment.

- Establish and retain for a minimum 3 months, unless otherwise restricted by law, a visitor log that captures any visitor's name, the entity they represent, and the name of the employee who is authorizing their visit.
- Monitor access to facilities.
 - Deploy video cameras or other access control mechanisms to monitor access to covered facilities, areas, or machines.
 - Review and correlate collected data, and retain log or other audit data for at least three months, unless otherwise restricted by law.
 - Protect cameras and other mechanisms from tampering or being disabled.
- Physically protect network access points, sensitive media, paper records.
 - Restrict access to enabled network jacks, wireless access points (APs), gateways, and handheld devices.
 - Store backup media in a secure location (preferably offsite) and at least annually review the security controls for stored media.
 - Physically secure all paper and media containing cardholder data throughout its lifecycle
 - Publish, ensure understanding of, and enforce physical security policies and procedures.
 - Clearly classify and label confidential materials.
 - Maintain inventory logs for all media and at least annually audit the inventory.
 - Require management approval for all physical relocation of devices, records, or media that contain cardholder data
 - Use a secured courier or other trackable delivery method for any shipping or offsite relocation of records, or media containing cardholder data
 - If cardholder data or records are no longer required, securely destroy them by shredding, incinerating, or pulping physical media and/or otherwise rendering electronic media unrecoverable.

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

Summary:

Companies must monitor and retain audit logs for all access to and activity in the cardholder environment. Logs should record both who accesses the environment and what they do while within it. Logs must be retained for at least a year, with 3 months of data immediately accessible. The minimum details to be logged include user identification, type of event, date and time, event disposition (success/failure), origination of the event, and identity of the name of the affected data, system component, or resource.

To support analysis, all servers should be synchronized to a proper, reliable time source (also known as an *NTP server*, which must be locked down and explicitly allowed). Logs must be reviewed on a daily basis, although the use of automated tools is allowed under requirement.

Action Items:

- Implement and secure detailed audit trails.
 - Capture all individual access to cardholder data, all root/administrator actions, all access to audit trails, invalid logical access attempts, use of identification and authentication mechanisms, initialization of audit logs, and the creation and deletion of system-level objects.
 - Ensure that access audits logs minimally capture user identification, the type of event(s) initiated by the user, the date and time of access, event disposition (success/failure), event origination; as well as the name of the affected data, system component, or resource.
 - Secure audit and log records, limiting access on a need-to-know basis, protecting the integrity of the logs (including using of log-integrity monitoring software), and backing up logs to a central server or media.
 - Require users of externally facing systems to log to an internal server in order to access protected cardholder data.
 - Synchronize all log-generating systems to a common time source that has been set up in an approved manner and that is explicitly authorized to receive time updates from authorized external sources.
- Review and retain audit logs.
 - Review audit logs daily, either manually or through the use of automation tools.
 - Retained audit logs for at least one year.
 - Ensure that at least three months of audit logs are available online and can be immediately accessed by authorized users.

Requirement 11: Regularly test security systems and processes

Summary:

Companies must assess the security of the PCI-covered environment both quarterly and annually. They should quarterly check for rogue wireless access points and scan for external and internal vulnerabilities. In addition, they should perform annual penetration testing (internal and external) that target both networks and applications. Note that companies are not required to engage a Qualified Security Assessor (QSA) or Approved Scanning Vendor (ASV) for penetration testing, although engagement of an ASV is required for external vulnerability scans.

Companies must also implement intrusion detection systems (IDS) or intrusion prevention systems (IPS) to monitor access to cardholder data, systems, and networks, in addition to file-integrity monitoring software.

Action Items:

- Perform mandatory quarterly tests:
 - Scan for rogue wireless access points.
 - Engage an ASV to perform external vulnerability scans.
 - Perform internal vulnerability scans, remediate any found issues, and rescan until scan results show all issues are resolved.
- Perform mandatory annual tests. (You are not required to engage a QSA or ASV for this requirement; however, the tester must be qualified to perform the assessments.):
 - Perform internal network and application penetration tests.
 - Perform external network and application penetration tests.
- Deploy IDS/IPS and file-integrity monitoring software to monitor access to cardholder data and to protect associated systems.

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

Summary:

Although this requirement seems to demand just one policy, a policy framework or multiple policies are often more effective in meeting security control objectives. In general, the goal is to draft, maintain, and enforce security policies that cover all PCI DSS requirements. Policy development should include formal risk assessment, risk management, and plans for annual review and update processes. Policies must cover the development of daily operational security procedures and must clearly define roles and responsibilities.

Managers must explicitly review and approve usage policies for individuals and devices, and they must explicitly inventory and track what is approved for whom, including labeling devices with owner, contact, and approved purpose(s). The policies themselves must set forth acceptable device uses and network locations and codify the security requirements indicated in PCI's other 11 sections.

The development of good usage policies that expressly prohibit remote users from copying, moving, and locally storing cardholder data is particularly important, since the requirement cannot be enforced through technological means.

To support policy integration, the company must develop and execute a formal security training and awareness program. And finally, if you share data with service providers, you must apply all of these controls to them, as well. Make sure to write it into your contracts.

Action Items:

- Develop and publish security policies, standards, and procedures.
 - Address all applicable PCI requirements.
 - Require an annual process for formal risk assessment and risk management.
 - Perform annual policy reviews and incorporate appropriate updates in published policies.
 - Clearly define roles and responsibilities in security policies.
 - Document roles and responsibilities for daily operational security procedures.
 - Document and require roles and responsibilities for incident response.
 - Document and require background check as part of candidate screening.
 - If cardholder data is shared with vendors or service providers, ensure that all policies and procedures outlined in the security program are applied and enforced for those third parties.
- Develop usage policies for critical employee-facing technologies.
 - Address remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail, and Internet usage.
 - Require explicit managerial authorization and authentication of usage.
 - Require per-person device inventories. Require devices to be labeled with owner, contact, and purpose.
 - Require devices to be authorized for specific uses and network locations.
 - Maintain a list of company-approved products.
 - Require automatic disconnect for idle remote connections and the default disabling of vendor remote access.
 - Prohibit remote users from copying, moving, or storing cardholder data on local drives and media.
 - Assign security management responsibilities.
 - Define roles and responsibilities for the monitoring and control of all access to data.
 - Define roles and responsibilities for the establishment, documentation, and distribution of security policies, standards, and procedures.
 - Define roles and responsibilities for the monitoring and analysis of security alerts and information.
 - Define roles and responsibilities for user account administration.

- Establish, document, and distribute incident response and escalation policies and procedures.
- Implement a formal security awareness program.
 - Run the program at least annually
 - Require staff to acknowledgment in writing that they have read and understood relevant security policy and procedures.

APPENDIX A: SECURITY POLICY, STANDARD, AND PROCEDURE MODELS

Security Policy Frameworks

- [ISO 27001/27002²³ \[Commercial\]](#)
- [GAO Executive Guide: Information Security Management \(GAO/AIMD-98-68\) \(PDF\)](#)
- [Educause: A Primer on Policy Development for Institutions of Higher Education](#)

Security Policies

Free Resources

- [Computer and Network Security Taskforce IT Security Guide: Security Policies and Procedures](#)
- [SANS Security Policy Project](#)
- [IT Security Policy The Information Security Policies / Computer Security Policies Directory](#)
- [Truth to Power IT Policy Template Wikis](#)

Commercial Resources

- IT Governance 2009 Policies & Procedures by Geraint H. Jenkins, Michael Wallace, Larry Webber. Aspen Publishers, Inc. Sep 2008.
- Information Security Policies Made Easy, Version 10 by Charles Cresson Wood. Information Shield. Feb 2009.
- Info-Tech Research Group: The Complete IT Policy Kit.

Security Standards

- [NIST 800-Series of Special Publications \(800-Series\)](#)
- [The Center for Internet Security](#)
- [Common Criteria for Information Technology Security Evaluation](#)

Security Procedures

- [Computer and Network Security Taskforce IT Security Guide: Security Policies and Procedures](#)

PROVENANCE

Author: Benjamin Tomhave, MS, CISSP

Ben Tomhave is Technical Director of Information Security and Compliance for a high-tech firm in Phoenix, Arizona. An author, commentator, and community contributor on information security issues, Ben is an Expert Core Guide in the Truth to Power research community and manages his own blog, The Falcon's View, at <http://www.secureconsulting.net>. He is also currently developing books on enterprise risk management and data retention.

Ben holds a Master of Science in Information Security Management from The George Washington University, in addition to memberships in the American Bar Association Information Security Committee and eDiscovery and Digital Evidence Committee, the OASIS EKMI and KMIP technical committee, ISSA, Infragard, and the IEEE Computer Society.

Prior to his current position, Ben worked in a variety of information security roles for companies including BT Professional Services, AOL, Wells Fargo, ICSA Labs, and Ernst & Young.

Ben may be reached at Truth to Power via his Knowledge Core at <http://www.t2pa.com/cores/security-and-privacy/practical-security>. Registered T2P Members may also contact him directly via his member profile under Ben Tomhave.

NOTES

- 1 The current iteration of the Payment Card Industry Data Security Standard (PCI, or PCI DSS) was originally released in the fall of 2008. Version 1.2 is the third iteration of PCI and represents the standard's continuing evolution. The official document is available at <https://www.pcisecuritystandards.org>.
- 2 Litan, Avivah "PCI Compliance Remains Challenging and Expensive." Gartner. May 16, 2008.
- 3 Kindervag, John. "Confessions of a QSA: The Inside Story of PCI Compliance." Forrester Research. Sep 11, 2008
- 4 For example, Heartland Payment Systems and RBS Worldpay reported massive data breaches in 2008, although they were both recognized as PCI compliant. Following breach investigations, the PCI Security Standards Council removed both companies from its list of compliant payment processors. (Kaplan, Dan. "[Visa: Heartland, RBS WorldPay no longer PCI compliant.](#)" SC Magazine. Mar 13, 2009.) However the implicit gaps between PCI compliance and complete information security have fueled resistance to what some merchants see as an overbearing and overly expensive regulatory regime.
- 5 According to the [2009 Data Breach Investigations Report](#) issued in April 2009 by the Verizon Business RISK Team, almost 20% of companies reporting a breach had been found to be PCI compliant prior to the breach.
- 6 Many of these criticisms were encapsulated in a March 2009 US Congressional hearing held by a subcommittee of the Department of Homeland Security. Recorded proceedings are available on demand at <http://www.homeland.house.gov/hearings/index.asp?ID=185>.
- 7 While the PCI Security Standards Council (SSC) recommends a risk-based approach to information security, it acknowledges risk management is not a prerequisite for PCI compliance. Indeed, neither the standard nor its supporting documents offer substantive guidance on either programmatic security management or risk management. Thus, it comes as no surprise that many companies institute PCI controls as they are presented: in a vacuum and as a checklist security program.
- 8 2009 Data Breach Investigation Report. Verizon Business RISK Team. Apr 19, 2009. http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf (PDF)
- 9 This short list represents only a small subsample of information and risk management frameworks available through a variety of organizations. In fact, many documents that do not self-identify as information or risk management frameworks offer relevant, complementary, or overlapping guidance. Truth to Power catalogs many of these documents in its Rules & Standards Hub. See the Hub's [Information & Operational Protection, Governance & Risk Management, and Maturity Models](#) sections for more information.

- 10 Per PCI v1.2 Requirement 6.1: "An organization may consider applying a risk-based approach to prioritize their patch installations."
- 11 PCI v1.2 specifically references OWASP in its recommended testing procedures for Requirement 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 guide (<http://www.owasp.org>)."
- 12 For examples, see CWE/SANS TOP 25 Most Dangerous Programming Errors. <http://www.sans.org/top25errors>
- 13 Information Supplement: Requirement 11.3 Penetration Testing. PCI Security Standards Council. Apr 15, 2008. https://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf (PDF)
- 14 The author is not a PCI Qualified Security Assessor (QSA). When in doubt, it is best to err on the side of caution. If you're subject to external assessment by a QSA, you should work closely with them to ensure your questions are suitably answered, especially in the context of planned compensating controls.
- 15 In general, An *untrusted* network is any network not directly owned, controlled, or managed by your organization.
- 16 Y. Rekhter, et al. Address Allocation for Private Internets. <http://tools.ietf.org/html/rfc1918>
- 17 For more information on stateful-inspection firewalls, see the Wikipedia entry at http://en.wikipedia.org/wiki/Stateful_firewall
- 18 For more information on Network Address Translation (NAT) and IP masquerading, see the Wikipedia entry at http://en.wikipedia.org/wiki/Network_address_translation.
- 19 This action is based on PCI Section 1.3.5, which states "Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ." Although the requirement seems to be poorly written, it is most likely intended to indicate that database servers in the bubble within the overall cardholder DMZ should be allowed access only to servers in the DMZ, and to nowhere else.
- 20 With PCI Version 1.2, the PCI Security Standards Council has clarified its definition of strong cryptography. The full definition and further explanation are included in the "Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms," viewable at https://www.pcisecuritystandards.org/security_standards/glossary.shtml.

- 21 In PCI Version 1.2, WEP (wired equivalent privacy) is recognized as an insufficiently secure wireless protocol. Although the use of WEP is not absolutely banned, PCI sets deadlines after which WEP may not be implemented or used. Complete information is available in the Data Security Standard document, available at available at <https://www.pcisecuritystandards.org>.
- 22 The Open Web Application Security Project (OWASP) is an open source community that provides free tools and guidance for application security. In particular, PCI recommends that all covered entities adhere to practices recommended in the OWASP Top 10: a list of the most serious web application vulnerabilities, recommendations for protection, and additional support resources. The OWASP Top 10 for 2007 (the latest stable version) can be read online or downloaded at http://www.owasp.org/index.php/Top_10_2007.
- 23 The official ISO site is one of the least useful resources for security managers seeking to interpret and apply the ISO/IEC 27000-series standards. Sites such as ISO 27001 Security (<http://www.iso27001security.com/>) offer deeper insight and support.

LEGAL NOTICE

The information contained in this document does not constitute legal advice. When assessing any compliance or legal matter, seek advice from your own corporate counsel or other qualified legal advisors familiar with your unique situation and environment.

The information in this publication is provided by Truth to Power, LLC (T2P) for educational purposes on an “as is” basis and without warranty of any kind. T2P disclaims any and all liability that might arise, directly or indirectly, from the access or reference to this work or the use or application of the information it contains.

T2P seeks to provide accurate, timely, and complete information in all of our published content; however, we cannot guarantee the accuracy or completeness of the content in this publication at any given time. Further, we assume no responsibility for the quality of included content supplied by underwriters, sponsors, and other third-party organizations. Such content is clearly marked and is solely the responsibility of its provider(s).

COPYRIGHT 2009 TRUTH TO POWER LLC. ALL RIGHTS RESERVED.



PCI Compliance

across your virtual and physical infrastructures.

www.tripwire.com/pci

Tripwire helps you achieve and maintain PCI compliance - from your central systems out to your POS terminals. Automate PCI compliance by combining the required configuration control with Tripwire's enhanced file integrity monitoring. This enables immediate detection and response to security issues across your infrastructure, including virtual environments built with VMware ESX and Microsoft Hyper-V.

And because Tripwire generates a continuous audit trail, auditors can see proof of your PCI compliance across all virtual and physical infrastructures.

Hundreds of leading merchants in transaction-intensive environments rely on Tripwire® Enterprise to ensure the security of their customer's sensitive credit card data.

Check out our PCI Resource Center at:

www.tripwire.com/pci

tripwire[™]