RSA®

The Security Division of EMC

White paper

Getting Serious About PCI Compliance

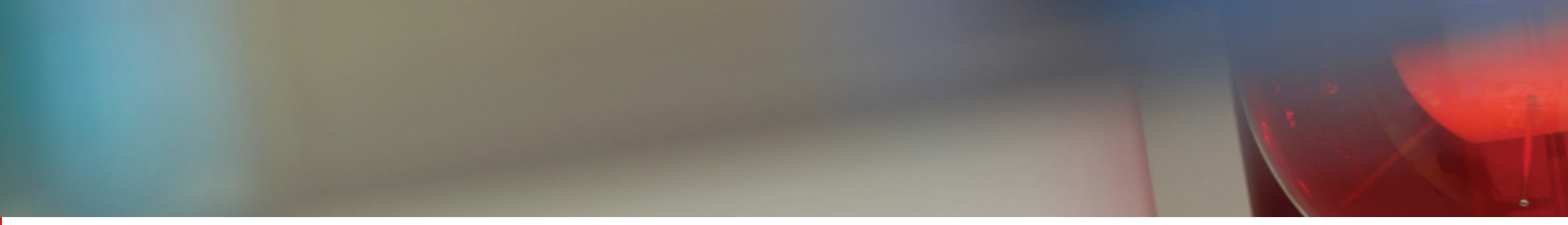
A Comprehensive Resource for PCI Compliance

With so many data breaches in the news and the card brands stepping up enforcement of the Payment Card Industry (PCI) Data Security Standard (DSS), merchants, banks and service providers are increasingly taking information security and compliance more seriously. New fines and incentives help make a strong business case for a PCI compliance program.

Yet many organizations have little experience with meeting comprehensive security requirements and/or managing a formalized compliance program. "Getting Serious about PCI Compliance" is intended to help organizations address PCI compliance and set the foundation for a long-term sustainable program. Companies need to approach compliance as more than just a reactive measure but rather make good security part of how they conduct business.

This paper lays out the rationale for undertaking PCI compliance, outlines seven key steps in developing a compliance program and explains how to avoid some of common pitfalls en route to compliance. For more information on PCI,visit www.rsa.com/pci

Contents



Getting Serious about PCI Compliance Part 1: Why Now?

Payment Card Industry Data Security Standard

If your organization takes credit cards or does anything with card data, by now you have probably heard about the Payment Card Industry (PCI) Data Security Standard (DSS), which was originally introduced in 2004. Perhaps you have not paid much attention to PCI or have been slow to implement a compliance program. As of the end of last year, Visa reported that only 15-36% of even their highest-volume merchants were compliant. But that is set to change dramatically in 2007.

Card Brands Stepping-up Enforcement

Visa and MasterCard, the leaders in this effort, have both indicated that they will get more aggressive in enforcing the PCI standard this year. The PCI DSS was developed by the card brands, Visa International, MasterCard Worldwide, American Express, JCB, and Discover. Previously, each had its own program for data security such as the Visa Cardholder Information Security Program (CISP) and the MasterCard Site Data Protection Program (SDP). The PCI DSS consolidated the individual brand's standards into one international industry standard for securing credit and debit card data.

Any organization that stores, processes or transmits card data is covered by PCI. This means all merchants that accept card payments; banks that manage the merchants and transactions; and service providers that process card data. And all of them have to start getting serious about PCI compliance.

PCI applies to merchants that accept credit cards as well as "off-line" signature debit cards which are processed using the same networks as the credit card transactions. All merchants that accept credit and debit card payments are covered by the PCI standard, even when they do not transact business online.

No Silver Bullet for Compliance

To comply with PCI, merchants and service providers need to have a comprehensive security program in place which includes policies, procedures and technology. No one technology or solution will make an organization compliant. It requires a commitment to evaluating security controls, determining necessary improvements, implementing changes, and then continuing this cycle by assessing controls annually. But the effort will be well worth it.

Non-compliance in the past has not resulted in major consequences for most organizations, even though Visa alone levied almost $5 million in fines in 2006. Until now, fines have been assessed only in cases where actual data breaches occurred. Beginning in the fall of 2007, Visa will be issuing fines for every large merchant that is not compliant. Fines will escalate over time, starting at $5,000 a month and increasing to $25,000 per month for each non-compliant merchant.

Carrot and Stick Approach

These new fines are part of Visa's PCI Compliance Acceleration Program, which not only includes steeper fines but also incentives. Visa's tiered interchange rates—commissions paid for each credit card transaction—will be linked to PCI compliance. Merchants who do not comply with PCI face the prospect of increased rates.

According to Visa, the impact will range from $250,000 to more than $20 million per year, depending on the merchant's qualifying volume. These are the kind of dollar values that will make many merchants take notice. Implementing security measures to comply with PCI will likely be much less expensive in the long run than paying higher rates.

Other incentives include Visa's $20 million program which provides straight monetary rewards for merchants that achieve PCI compliance. It should be noted that the fines are levied against, or incentives paid to, the acquiring banks, which have the direct contractual relationship with Visa. If applicable, merchants will receive the fines or incentives through their acquiring banks.

Protecting the Payment Card System

Increased enforcement of PCI is motivated by the need to protect the integrity and trust of the whole payment card system. Over the last few years, there has been a flood of data breaches involving credit card data, including some cases in which literally millions of account numbers were compromised. If things continue, it could potentially put the whole system at risk. Consumers might start to feel that using a credit card off-line or online is not safe.

The card brands would also like to fend off possible regulatory actions by governments worldwide. For example, because of well-publicized data breaches, the U.S. Congress is considering enacting legislation specifically aimed at the protection of cardholder data. Another big motivator is reducing credit card fraud. Online fraud is approaching $3 billion USD a year in North America alone. Better security will help get this under control.

Benefits of PCI Compliance

For an individual organization, the benefits of complying with PCI go beyond avoiding fines and increased interchange rates, although these alone are significant. Ultimately the objective of PCI is to protect card information from compromise. Organizations which implement better security measures as per the PCI standard reduce the risk of an actual breach occurring, which safeguards their reputation and customer relationships, and protects them from paying the costs of a breach. Companies with programs in place to protect card data also have the ability to extend these efforts throughout the organization and protect other sensitive business, employee, partner and customer data.

According to a study by the Ponemon Institute, if your organization has a data breach, you could lose up to 60% of affected customers. Their findings indicated that over 40% of individuals affected by a data breach said that they might discontinue their relationship with the company and another 19% had already discontinued their relationship.

Breaches Are Costly

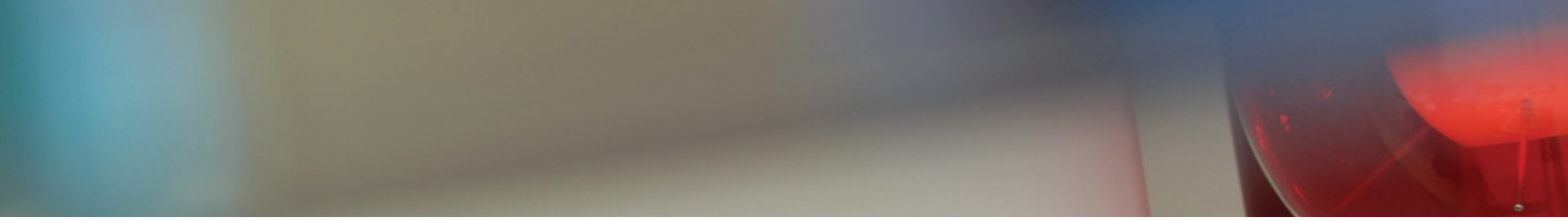
Costs are another reason why companies need to avoid breaches. The ChoicePoint case provides some hard data about just how costly a breach can be. The impact to their business was huge. Back in 2005, this leading data broker exposed information on about 145,000 Americans and was forced to make a disclosure to all those affected. The end result was a stream of headlines detailing the case, creating a wave of bad publicity for the company.

Their direct costs were over $11 million (for communications; credit reports and monitoring; and legal fees). In addition, the sales losses were expected to be about $20 million for the year and their total market capitalization dropped by $720 million right after the incident. In a ruling by the FTC, ChoicePoint was also fined $15 million. On top of this, the company faces pending litigation. In general, privacy and security breaches are expected to fuel many class action lawsuits against many companies in the coming years.

Trust Can Be an Important Differentiator

Consumers are becoming much more discerning and are selecting companies that will protect their information. A study by Privacy and American Business found that 60% of consumers had decided not to do business with a company because they were not sure how their personal information would be used.

The flip side of this is that companies which invest in security have the opportunity to build trusted relationships with their customers. A Javelin Strategy & Research poll showed that 85% of consumers would likely increase their shopping at a store if they knew it was a leader in devoting resources and technology to protecting its customers' personal account data. If clients trust a business with their data, the business can use this trust to build client loyalty and ultimately, increase revenue.



"More than ever before, consumers are demanding that the businesses with which they transact will deliver on their expectations of iron-clad data security… Trust is emerging as one of the critical business issues of the 21st century… Data security must move out of the back office and into the boardroom. Corporate officers must apply the same rigor to data security as they do to their financial controls."

– Visa USA President and CEO John Philip Coghlan, Visa Security Summit, March 2007

Leveraging Your PCI Compliance Program

The PCI DSS is just one of many standards, regulations and legislation that mandate the protection of information. In the US, companies must also meet Sarbanes Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), etc. and about 40 states now have data breach notification laws.

There are also many international regulations including the European Union Data Protection Directive, the Japan Personal Information Protection Act and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), etc.

Although PCI is focused on cardholder data, the PCI standard could be used more broadly. It is one of the most detailed security standards available. Many companies can use it as the basis for their overall information security framework and leverage it to meet other standards and regulations.

Seven Steps on the Road to Compliance

- Step 1: Get the Facts
- Step 2: Form Your Team
- Step 3: Find the Data
- Step 4: Analyze Your Risks
- Step 5: Do a Gap Analysis
- Step 6: Develop and Implement a Remediation Plan
- Step 7: Perform an On-site Audit or Assessment

Getting Serious about PCI Compliance Part 2: Seven Steps on the Road to Compliance

The Compliance Journey

Simply put, to become PCI compliant, an organization must meet the requirements of the Payment Card Industry (PCI) Data Security Standard (DSS) and then prove that it meets the requirements. The standard is managed by the PCI Security Standards Council (SSC). Although the SSC oversees the standard, it is the card brands which still individually enforce PCI compliance and the acquiring banks are contractually responsible for ensuring that their merchants meet PCI requirements.

Validation Depends on the Number of Transactions

How your organization proves compliance to the PCI standard will depend on the number of transactions it processes. Merchants and service providers with higher levels of transactions will have to pass an on-site audit every year. Those with lower levels of transactions must do a self-assessment to validate compliance. (See Step 7: Perform an On-site Audit or Assessment for more details).

The on-site audit must be done by an external auditor which is called a "Qualified Security Assessor" (QSA). Merchants do have the option of using an internal audit team. All merchants and service providers must get a quarterly network scan done by an "Approved Scanning Vendor" (ASV). The PCI SSC is responsible for certifying QSAs and ASVs and provides a list of these on their web site.

The length of time to become PCI compliant is going to depend on many things such as the organization's size and the level of security they already have in place. Typically, the basic process is a pre-assessment, remediation and final assessment or audit, which takes 9 to 18 months or possibly more for a large enterprise.

Required Reading: Examples of PCI Reference Materials

PCI SSC Documents	Card brand web sites
– PCI Data Security Standard Version 1.1 – PCI DSS Payment Card Industry Self-Assessment Questionnaire – PCI DSS Security Audit Procedures – PCI DSS Security Scanning Procedures Available on www.pcisecuritystandards.org	Visa USA usa.visa.com/merchants/risk_management/cisp.html Visa International (links to regional sites) www.corporate.visa.com/pd/security/main.jsp Mastercard www.mastercard.com/us/sdp/index.html

Compliance Is an On-going Process

Once an organization achieves compliance and passes their first audit or self-assessment, they will need to maintain compliance. Organizations will need to continually analyze their risks. New security measures may be required as the business or IT environment changes or the threat landscape evolves over time. PCI expects organizations to assess and possibly improve their security controls every year.

Here are 7 steps which can help your organization's PCI compliance program go more smoothly. This should not replace the advice and guidance of a QSA or another PCI expert or consultant but can provide some insights into the PCI compliance process.

Step 1: Get the Facts

To start, learn as much as you can about the requirements of the PCI DSS by reading the available reference materials. Then prepare to assess your organization's current security posture by collecting your own internal information security documentation.

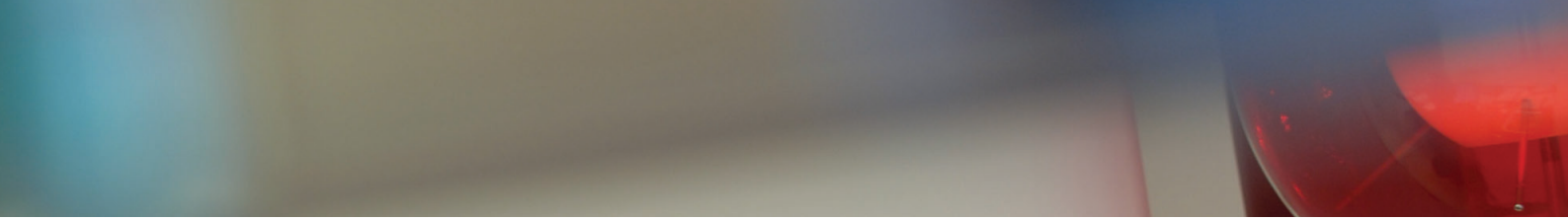
It may seem obvious that the first step is to read the PCI standard itself, but it is also important to read the complete set of supporting documents. Even if your organization plans to use consultants in the PCI process, it is valuable for your team to go through the PCI documents in detail to be able to manage the program effectively. Examples of some of the required reading materials are listed above. The card brands' sites are also an important source of information about their particular enforcement program, etc. Your merchant bank may also have a web site dedicated to PCI compliance.

The PCI standard is quite straightforward. The requirements are organized into 6 logically related groups called "control objectives." These are high level goals that the organization is expected to achieve in order to secure their systems. In the next level of detail, for each of those 6 control objectives, there are 1-3 requirements listed. In all there are 12 requirements. Then for each of those requirements, there are many sub-requirements. In total there are over 200 sub-requirements. It is in the sub-requirements where the PCI standard gets into details, for example, about the policies, procedures and technologies that are required. See the table on page 8 for a list of the PCI requirements.

The PCI Self-Assessment Questionnaire is used by smaller-volume merchants and service providers to validate compliance. The PCI DSS Security Audit Procedures is the actual document used by internal or external auditors for doing the on-site audit required for larger-volume merchant and service providers. The PCI DSS Security Scanning Procedures document explains the purpose and process involved in undergoing a scan. Organizations can use all of these documents as readiness tools.

The Value of the Audit Procedures Document

The PCI DSS Audit Procedures document is an especially useful tool and should be read thoroughly. It can really help to shed light on the audit process. It is laid out as an audit checklist, and for every requirement it lists the actual testing procedures that the auditor must use and expands on the requirements by including details that would not be obvious by reading the standard.



Required Internal Documentation: Collect Whatever Exists

Existing policies and procedures – Security policy – Password policy – Usage policies (i.e. acceptable usage policies – Incident response plan – Log collection and review policy – Log retention and disposal policy – Card data retention and disposal policy – Policies regarding display of card data – Key management policy and procedures – Anti-virus policy – Patch management policy – Physical access control policy – Media distribution policy – Change control policy and procedures – Software development lifecycle policies and procedures	**System configuration standards** – Network components – Servers – Wireless access points **Documented risk analysis** **Data flow diagram** **Samples of audit logs and/or log reports** **User and administrator access lists** – Who has access to cardholder data – Who has access to security systems **Vendor contracts** **Storage system documentation** – e.g., Database documentation **Output from recent vulnerability scans and penetration testing**

For example, requirement 3.1 of the standard is "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."

The Audit Procedures document goes further and describes exactly what the auditor will look for with respect to the policies and procedures. It lists all of the systems that the auditor must check from servers down to bulk data copy directories. It even specifies that the organization must have an automatic process to remove stored cardholder data exceeding retention requirements on a quarterly basis—an important detail about the requirement that would likely not be understood from the standard alone.

The audit or assessment process includes reviewing internal documents representing the current state of your organization's information security controls. Examples of the required documents are listed above. Gathering these documents will be helpful for the pre-assessment phase.

It is very possible that not all of these documents will exist when you begin your PCI program. In fact, you may find that certain policies and procedures need documenting as part of your remediation efforts. Once you are ready for the final assessment or audit, collect the complete set of documents (previously existing and newly prepared) for your assessors in advance, which can help to speed the process along considerably.

Step 2: Form Your Team

Depending on the organization, a number of people will likely be involved in the PCI compliance program, such as security, IT and audit personnel as well as users and administrators, etc. External consultants may be brought in as partners to do the pre-assessment and/or on-site audit.

The Internal Team

The PCI standard itself expects an organization to have a chief security officer (CSO) or assign a security-knowledgeable member of management to be responsible for information security. If that person has not yet been hired or appointed, it may be prudent to do this before a PCI compliance program begins. The CSO or someone on his/her team should probably lead the compliance effort. Some organizations have even created a "PCI Compliance Manager" position.

It is best to have people who implement security controls not actually conduct the pre-assessment and especially not do the on-site audit (in a smaller organization this may not be possible). Just like it makes sense to have different people do code development versus quality assurance testing, it makes sense to have different people do the implementation versus the assessment of security controls.

PCI Requirements

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

Some larger organizations may choose to have a team of internal personnel do the pre-assessment, and then after remediation, have an external auditor come in to do the on-site audit. For other organizations, it may be the same internal team doing the pre-assessment and the self assessment or on-site audit, although, you may also want to separate these duties.

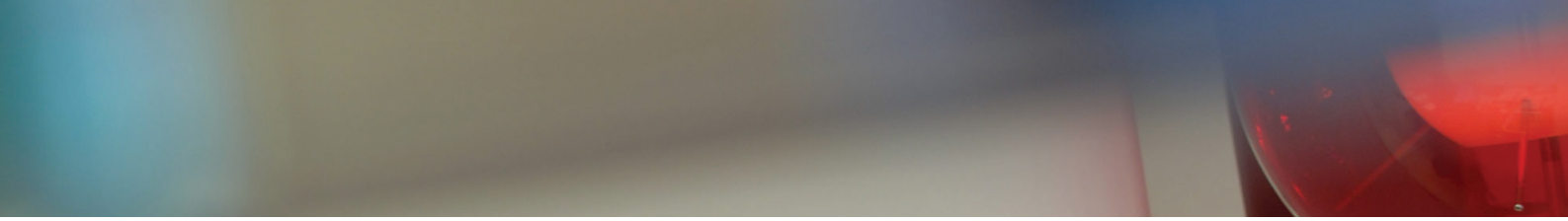
Part of a PCI assessment or audit is interviewing people, in order to, for example, evaluate whether they know and are complying with policies and procedures pertaining to them. Internal personnel to be interviewed during the PCI process include users, network administrators, system administrators, database administrators and software developers.

Working with External Consultants

For merchants and service providers with higher volumes of transactions, the annual on-site audit should be conducted by a QSA. Merchants have the option of using internal auditors. Though they are not required to use a third-party QSA, most find that using an external auditor is very helpful at least for the first year's audit to ensure that the audit is performed correctly. For organizations requiring an on-site audit or even those who will be doing a self-assessment, it may be valuable to work with an outside party on PCI readiness, especially when the consultant has experience in PCI.

However, keep in mind that if you choose to work with a QSA, the external auditor should not perform both the implementation of controls to be assessed and the assessment. As stated earlier, audit functions should be separated from implementation if possible. If someone has implemented a control, either in advance or as part of a remediation effort, it may be hard for them to objectively assess that control. It is not that there is malice; rather it is just difficult for humans to assess self-completed work objectively.

While it is not strictly forbidden yet, the SSC has indicated that they will be looking at possible oversight problems if duties are not being separated and the same QSA performs the readiness assessment, remediation implementation and the final PCI attestation.



Step 3: Find the Data

PCI requirements apply to all system components included in or connected to the cardholder data environment (i.e., any network component, server or application). The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Cardholder data includes cardholder name, primary account number (PAN), and expiration date. Sensitive authentication data is the full magnetic stripe data, personal identification numbers and card validation code numbers.

Data Flow Diagram

One of the first things you need to do en route to PCI compliance is figure out where all your cardholder and sensitive authentication data is. This will define the boundaries of your cardholder data environment and determine the scope of your PCI audit. A diagram showing how card data flows through your organization is very useful in this process. (Be careful not to confuse a data flow diagram with a network diagram; there are differences).

The data flow diagram shows the flow of data from acquisition (either from a customer or third party) to deletion. It shows where the data starts, how it moves around and where it is stored. The diagram should cover data contained in files, applications, databases, including structured, and unstructured data, etc.

The Menace of Unstructured Data

Often organizations will know where their data is in the IT applications, but not in end-user computing applications, such as access databases, spreadsheets word processing documents. Pay special attention to unstructured data since organizations can easily fail PCI audits with the common practice of storing unencrypted data in spreadsheets.

No Storage of Sensitive Authentication Data

Under the PCI standard, cardholder data is treated separately from sensitive authentication data. It is forbidden to store sensitive authentication data (e.g., magnetic stripe data, personal identification numbers and card validation codes) after the authorization process has been completed. This is because, for example, the full magnetic stripe data can be used by attackers to create counterfeit cards.

Therefore, if you find any sensitive authentication data in your environment, you must remove it and ensure that your business processes, systems and applications are not set up to store this data.

Minimal Storage of Cardholder Data

For cardholder data (e.g., names, PANs and expiration dates), even though organizations can store it after authorization, you must keep it to a minimum and have valid business reasons for storing it. (Some retailers use it in processing charge backs and managing dispute resolutions, etc.) If you store cardholder data for any length of time, it must be protected according to the requirements in the PCI standard. Obviously, this is because databases containing large numbers of credit card account numbers are going to be very attractive target to criminals and can be accessed either directly or via an application.

Step 4: Analyze Your Risks

Once you have a good understanding of where cardholder data is within your environment, the next step is to analyze the risks to that data. The PCI standard calls for formal risk assessment to be conducted annually. Risk analysis actually needs to be one of the first things that an organization does when embarking on a compliance program because it will guide decisions regarding the level of security to put in place.

To analyze your risks for every system component in your cardholder data environment, you need to determine: What are the threats and vulnerabilities? What is the likelihood that a threat will occur or vulnerability will be exploited given the current security controls? What would the impact to the organization be? By answering these questions, you can evaluate the nature and level of risk. For system components which face unreasonable levels of risk, you will need to mitigate those risks with additional security measures. The following describes a basic process for analyzing your risks.

Threats and Vulnerabilities

Start with threats, which can be characterized as the potential for agents to cause harm through the unauthorized access, disclosure, misuse, alteration or destruction of information. Threats can arise from a variety of sources either internal (such as malicious or incompetent employees, contractors, service providers, and former insiders) or external (such as criminals, recreational hackers, competitors, and terrorists).

Then, look at vulnerabilities. These are the weaknesses in a system that, if exploited, could result in the unauthorized access, disclosure, misuse, alteration or destruction of information. Vulnerabilities may be either known or expected. Known vulnerabilities are discovered by testing or other reviews of the environment, as well as knowledge of policy weaknesses, inadequate implementations, and personnel issues. Expected vulnerabilities will likely arise in the future. Examples may include un-patched software, new attack methodologies that bypass current controls, employee failures to follow security policy and new technology which introduces security flaws.

Qualitative or Quantitative Methods

Qualitative analysis involves walking through or storyboarding various scenarios in an attempt to determine the likelihood of threats and vulnerabilities and the effectiveness of existing controls; using knowledge, prior experience and industry information.

Quantitative methods come up with numerical values for frequency and probability of threats and vulnerabilities and effectiveness of controls, etc. The problem with quantitative methods is often the lack of reliable and predictive data. Organizations can address this by assigning numeric values based on qualitative judgments.

The next step is to look at the impact of the threats occurring or vulnerabilities being exploited. The impact includes the extent to which the event would affect data integrity, confidentiality and availability; the costs associated with finding, fixing, repairing and restoring a system; lost productivity; financial losses; and other issues affecting the organization's operations and reputation. The impact of certain events may be less significant to the business versus those which would be catastrophic.

Typically, the end result of a risk analysis for PCI is a risk rating for every system component in the cardholder data environment, expressed as, for example "High," "Medium" or "Low" risk, taking into consideration the likelihood of threats and vulnerabilities, the current controls as well as the impact of an event. It is important to thoroughly document the method used to come up with your risk ratings.

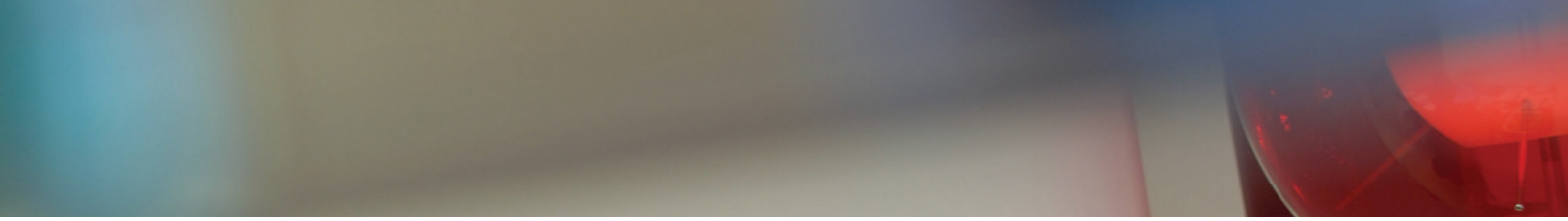
Risk assessment is not a simple task. Organizations may find it useful to consult guidance documents or standards such as NIST SP 800-30 Risk Management Guide for Information Technology Systems (US National Institute of Science and Technology, released in 2002) or BS 7799-3:2006: Information security management systems–guidelines for information security risk management. (British Standard released in March 2006.)

Step 5: Do a Gap Analysis

A gap analysis compares the adequacy of the security measures currently in place to the PCI standard, with the objective of finding the "gaps" between your controls and PCI requirements. It involves inspecting all of the system components in the cardholder data environment while going through the requirements of the PCI standard line-by-line to evaluate how well each requirement is met. The PCI Annual Self-Assessment Questionnaire or the PCI DSS Standard Audit Procedures are useful resources for performing a gap analysis.

The Audit Procedures document is especially useful for organizations which will undergo an on-site audit. It is laid out as an audit checklist. For every requirement, it lists the testing procedures that the auditor must use and indicates whether a particular control is in place and if not, it has a column to keep track of the target dates.

A gap analysis (also called a pre-assessment) can be thought of as similar to taking a practice exam. If your organization were to have a PCI audit done or complete a PCI self-assessment today, with no changes to your current security, how would you fare? In what areas would you already meet the requirements? In what areas would you have to make changes? This pre-assessment can be done by an internal audit team or an external consultant. After the gap analysis is complete, your organization will know what areas to focus on for remediation.



Step 6: Develop and Implement a Remediation Plan

Prioritize the gaps that were identified in the previous step and create a remediation plan with the objective of meeting all of the requirements of the PCI standard. This will include developing a timeline for the implementation of the additional policies, procedures and/or technologies.

Compared to other information security regulations or standards, the PCI DSS is very detailed and relatively prescriptive. However there is some flexibility in the standard. It has a concept called "compensating controls." An organization can consider using compensating controls if they cannot meet a technical specification of a requirement but they can sufficiently mitigate the associated risk. Each compensating control must be thoroughly documented and evaluated after implementation and there are strict guidelines for judging its effectiveness.

Compensating controls are only allowed if they meet certain conditions, for example if they meet the intent and rigor of the original requirement and repel a compromise attempt with similar force. Ultimately, the card brands expect organizations to take a risk-based approach. The key when it comes to implementing the compensating controls or any of the controls required by the PCI standard is to analyze the risks (see Step 4: Analyze Your Risks) and use this to make the decisions regarding the level of security required to mitigate the risks.

Step 7: Perform An On-site Audit or Assessment

To complete the PCI compliance cycle, merchants and service providers must validate that they meet all of the PCI requirements either through an on-site audit or self-assessment. Even though PCI is a unified standard for the industry, there is no single compliance and enforcement body. This makes the process of compliance validation a bit more complicated.

Each of the card brands has its own enforcement management program. A merchant or service provider must submit its compliance validation documents for each card brand separately. Generally, although the card brands are the final enforcers, under PCI, the banks are contractually responsible for ensuring that their merchants meet PCI requirements.

Merchant and Service Provider Categories

The method for validating compliance depends on transaction volume. Merchants are categorized into four levels; Level 1 merchants have more than 6 million transactions annually; Level 2 have 1-6 million; Level 3, fewer than 1 million; and Level 4, fewer than 20,000. Level 1 merchants must have an annual on-site audit.

Service providers are categorized in 3 levels: Levels 1 and 2 basically have over 1 million transactions per year, and Level 3 have under 1 million. Level 1 and 2 service providers are also required to have an annual on-site audit. Level 3 merchants and service providers must do a self-assessment. Validation requirements for level 4 merchants are left up to their acquiring bank. (Note: these are the Visa and MasterCard categorizations).

Validation Documentation

The Annual On-Site PCI Data Security Assessment must be completed according to the PCI Security Audit Procedures document. This document is the template for the Report on Compliance (ROC). Merchants and service providers should engage a Qualified Security Assessor (QSA) to do the on-site audit and complete the ROC. For merchants, the report is submitted to their acquiring bank; service providers provide it directly to Visa.

Merchants do have the option of using an internal audit team to perform the on-site audit. It is up to the acquiring bank whether to accept the ROC done by an internal auditor, provided it is accompanied by a letter signed by an officer of the merchant.

Level 1 merchants and all service providers must also submit the Confirmation of Report Accuracy form completed by the assessor. Upon receipt and acceptance of the validation documentation, acquirers then submit the form and a letter accepting the merchant's full compliance validation to Visa.

The Annual PCI Self-Assessment Questionnaire must be completed by Level 2 and 3 merchants and submitted to their acquiring bank. Level 3 service providers submit it directly to Visa. Level 4 merchants may be required to complete the PCI Self-Assessment Questionnaire as specified by their acquirer.

Levels 1-3 merchants and all service providers are required to undergo the Quarterly Network Security Scan. This is an automated tool that checks systems for vulnerabilities. It conducts a non-intrusive scan to remotely review networks and web applications based in the externally facing Internet Protocol (IP) address provided by the organization. These scans must be performed by an Approved Scanning Vendor (ASV).

Audit Should Be a Collaborative Process

To be successful, it is best to work in a non-contentious, partnership model with the QSA or internal audit team. Establish the scope of the audit early on. Go through the Audit Procedures document together and agree which systems will be reviewed. Use the data flow diagram and network maps, etc. to support the rationale for the scope. Prepare in advance all of the documentation the auditor will use in their assessment, including the internal documents listed in "Step Two: Get the Facts" such as policies and configuration settings.

It is important to keep in mind that the intent of PCI DSS compliance is to increase the security of cardholder information, not to fail organizations in a PCI audit which are taking reasonable efforts to comply. For the on-site audit, if there are gaps in compliance, it is best if the auditor is able to indicate that any controls "not in place" have an associated "target date" for remediation. If your organization demonstrates there is a plan with a target date for remediation, the acquiring banks and card brands will know that your organization is committed to correcting the problem and becoming PCI compliant.

PCI Pitfalls

- Lack of awareness and training
- Keeping too much data
- Not segmenting the network
- Not enough focus on third-parties
- Lack of protection for stored data
- Faulty passwords
- Insufficient and/or ineffective logging

Getting Serious about PCI Compliance Part 3: Avoiding PCI Pitfalls

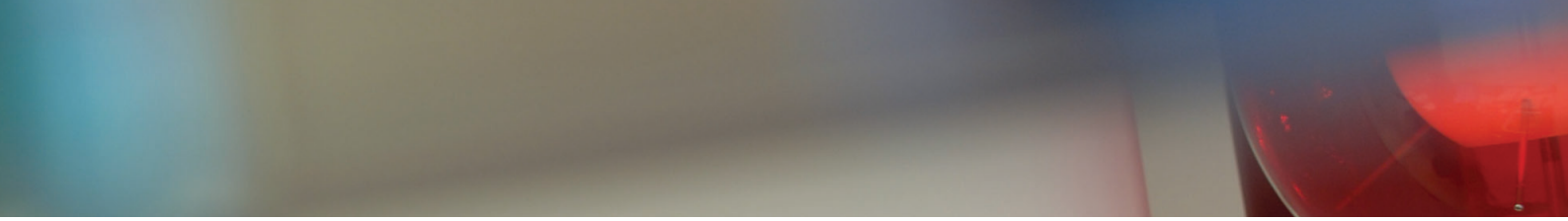
Overcoming PCI Challenges

On the road to complying with the Payment Card Industry (PCI) Data Security Standard (DSS), there are several areas which can present difficulties or be major stumbling blocks. Understanding how best to approach these challenges and knowing about possible solutions can be the key to a successful PCI program. You can better plan and manage your program, determine where to put more focus and head-off potential problems early on. Organizations should also consider that an on-going compliance program should be able to not only meet the PCI requirements but do so effectively and efficiently.

PCI Pitfall: Keeping Too Much Data

PCI has specific requirements regarding what data can and cannot be stored. Storage of sensitive authentication data after the authorization process is complete is strictly forbidden. Sensitive authentication data is the full magnetic stripe data, personal identification numbers and card validation code numbers.

Cardholder data which includes cardholder name, primary account number (PAN) and expiration date can be stored after authorization but it must be kept to a minimum. PCI requires an organization to have a data retention and disposal policy which limits the storage amount and retention time based on actual business, legal and/or regulatory purposes.



Scale Back Cardholder Data

Companies that have been able to achieve compliance more quickly are those that look at how to scale back the data in their systems. It is important to evaluate whether you really need to pass around and/or store the cardholder data. Is there a way to minimize it? For example, would it be possible if you need the account number to go back to the transactional system and look it up instead of passing it to your marketing or customer service systems? Another thing to consider is that often the need to store the card's transaction history is confused with the need to store the number itself.

Historically, cardholder data has just been readily passed throughout a company's network, since it is easy and storage space is relatively inexpensive. And most companies do not regularly purge their systems of information that is no longer needed. But if you can keep the amount of stored data to a minimum, the scope of the PCI on-site audit or assessment can be reduced. By storing less credit card data, you also reduce the risk of a data breach.

PCI Pitfall: Not Segmenting the Network

To limit the scope of a PCI audit, organizations are encouraged to segment their networks to isolate systems that store, process or transmit cardholder data from those that do not. Adequate network segmentation can reduce the scope of the cardholder data environment. Technologies that can help provide segmentation include firewalls, routers with access control lists, physical security and two-factor authentication. The auditor or assessor must verify that the segmentation is adequate to reduce the scope of the audit.

Decrease the Chance of Compromise

By reducing the scope of the cardholder data environment, segmentation can not only reduce the scope of the PCI audit but also decrease the chance that the data will be compromised. When compromises occur, it is organizations with the least-segmented networks that suffer the most. Although network segmentation can be demanding and time-intensive, it is worth the effort to design and build a network so that even if another part of the network is compromised the cardholder data environment is protected.

PCI Pitfall: Not Enough Focus on Third Party Providers

If your organization passes card data to third parties for handling, storing or processing, under PCI, your organization has an obligation to ensure these companies protect the data. The PCI DSS requires a contractual arrangement whereby your service providers must agree to adhere to the PCI DSS requirements. The agreement must include an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses.

Know What Will Happen To Your Data

In general, as part of selecting an out-sourcer or third-party provider which will handle your card data, you should assess the third-party's security policies and practices to determine if they will meet the PCI requirements. Before you sign a contract, find out exactly what will happen to your data after it goes to the third-party. Sometimes, in an out-sourcing or third-party arrangement, your provider out-source to yet another provider. Be cautious in situations whereby you will not have a direct contractual relationship with a vendor downstream which is handling your card data.

PCI also requires organizations to implement an incident response plan. One area often overlooked is ensuring that third-party providers have an adequate incident response plan should your card data be compromised.

PCI Pitfall: Lack of Protection for Stored Data

If an organization stores cardholder data for any length of time, the data must be protected according to the requirements in the PCI standard. At a minimum, primary account numbers must be rendered unreadable anywhere they are stored, which generally involves encrypting the data.

Under PCI, encryption is a critical component of cardholder data protection. It is also key to implementing a "defense in depth" security strategy. With a layered approach to security, even if the other layers (such as access control and authentication mechanisms) fail and a hacker gains access to the data, the data will be unreadable since it will be encrypted.

Challenge of Encryption

Encryption of stored data is one of the top five challenges in implementing the PCI DSS, according to Visa. One of the reasons is that unfortunately many companies store card data on legacy systems that were never designed for encryption. Companies have several options, including retrofitting the application so that encryption is built-in to application functions, using an encryption appliance which sits between the application and the database and off-loading encryption to the storage mechanism or database.

Encryption is an area that has gotten a lot of attention when it comes to the use of compensating controls. When an organization is not able to implement the encryption requirements because of technical constraints or business limitations, it may be possible to use other ways to render cardholder data unreadable, such as one-way hashes, and truncation and masking, etc. Any compensating controls must be able to sufficiently mitigate the risk, be thoroughly documented and evaluated by the auditor or assessor as effective.

Key Management

In addition to legacy systems, another stumbling block when it comes to encryption can be key management. The PCI DSS has many specific key management requirements, including generation of strong keys, secure key distribution, periodic key changes, destruction of old keys, dual control of keys, the replacement compromised keys and the revocation of old or invalid keys. Ensuring that all of these requirements are met for multiple applications can be a daunting task, yet effective key management is essential in encryption deployments.

Keys must be accessible for the data to be accessible. Yet this must be balanced with the fact that if keys are too accessible, i.e. not properly secured, you run a higher risk of compromise. Reliability is also critical, since an outage in the system will prevent the business from functioning. To address these kinds of challenges, organizations can centralize the provisioning and lifecycle management of encryption keys. Centralized key management can help simplify key management for multiple applications, alleviating the difficulties and inefficiencies of having a separate infrastructure for each application.

PCI Pitfall: Faulty Passwords

Passwords are another area in which organizations have difficulties in meeting PCI requirements. Under PCI, using vendor-supplied defaults for system passwords and other security parameters is strictly forbidden. Vendor-supplied default passwords are well-known to hackers and can easily be used to break into your systems.

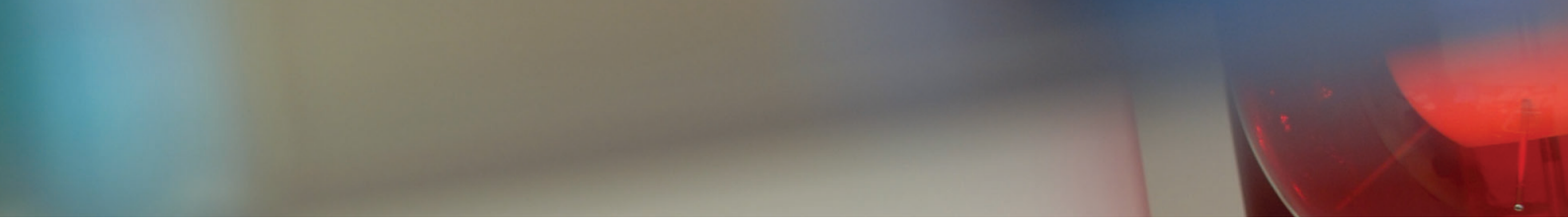
As well, PCI has specific requirements regarding the use of password authentication. Users must be uniquely identified and authenticated to gain access to systems in the cardholder environment. In addition to passwords, authentication methods can include tokens, certificates, or biometrics. The strength of an authentication method depends on the number of "factors" it uses. Factors used to verify identities are: something the user knows, such as a personal identification number (PIN), something the user has (e.g., a token or smart card) and something the user is (e.g., biometric data such as a fingerprint). Combining factors increases the strength of the authentication.

Selection and Management

Passwords are a single-factor method of authentication. They are the most common method because they are the easiest to implement, but they are also the most prone to compromise, because they can be easily shared, stolen or guessed. Passwords seem simple but actually require careful selection and management to be an effective security mechanism.

Therefore, the PCI standard has a number of specific requirements regarding password selection and management. It requires strong (complex) passwords which are a minimum of seven characters in length and consist of both numeric and alphabetic characters. It also has detailed requirements regarding issuing and resetting passwords, revoking passwords for terminated users, removing inactive accounts, periodically changing passwords, limiting password reuse, locking out users after failed logons and requiring re-authentication after inactivity.

Using an automated system to manage passwords can make it much easier to meet these requirements. It is especially helpful to use an interactive method of enforcing strong password selection by users.



Solving Password Problems

To help ease the password burden on users, organizations may decide to implement single sign-on (SSO) systems so that users do not have to remember multiple complex passwords. When users have so many passwords, it can lead to user-created weaknesses such as writing passwords down or it can cause users to constantly forget passwords, jeopardizing the timely availability of information. Password systems must balance the password strength with the user's ability to maintain the password as a shared secret.

Two-factor authentication is another solution that could help here. The PCI DSS requires two-factor authentication for remote access to systems. Organizations may also consider using two-factor authentication for internal access to solve the problems of passwords.

PCI Pitfall: Insufficient and/or Ineffective Logging

Companies can fail PCI audits because of improper log collection, monitoring and retention. The PCI DSS requires more intensive tracking and monitoring than most organizations currently do, including logging all access to network resources and cardholder data. Logging is a central pillar of any security program. It is essential for identifying that a compromise has occurred and then determining the cause. Log information is also used to determine whether processes and security systems are working as expected.

Detailed Tracking and Monitoring

Many events must be logged under PCI including all individual access to cardholder data, administrative actions, invalid logical access attempts and creation and deletion of system level objects, to name a few. And for every event, details such as user ID, date and time, etc. must be logged. To meet the requirements, logs must be reviewed (otherwise they are not useful) and must be protected (otherwise they are not reliable).

Review procedures should include analyzing logs for all system components at least daily. Log reviews must include security systems such as intrusion detection systems (IDS) and authentication and authorization servers (for example, RADIUS). Protection requirements include ensuring only authorized users have access and backing up audit trails to a centralized server.

Organizations have difficulties meeting the logging requirements because of several reasons. Most organizations have many different systems generating logs including operating systems, security systems and applications. Reviewing logs from many disparate systems is difficult, inefficient and can create voids. Attacks often involve multiple assets; if you watch only one in isolation, a single activity may not seem threatening.

Centralized Logging

Overall, monitoring and reviewing logs is a daunting task. Some companies collect logs but they do not review them simply because it is too hard. Others have staff who spending inordinate amounts of time reviewing logs from all of the different systems manually.

But if logs are collected, normalized and aggregated at a single point, analysis becomes easier and review occurs more frequently. With a centralized logging system, managing and securing the logs also gets easier. And it can include an automated, interactive system to track what has been reviewed. More automated review methods can free personnel from manual review, allowing them to do higher-value tasks. Log aggregators and security event management tools offer these kinds of capabilities.

PCI Pitfall: Lack of Security Awareness and Training

Organizations need to consider that having security policies, procedures and technology in place will make no difference if the users and administrators do not take the controls seriously or circumvent them. Security awareness and training must be a key part of PCI compliance program and your security program in general. Part of the problem is that many users probably simply do not know or believe that a threat exists.

Educate your users about the risks to your systems, including the threats and vulnerabilities. Also make sure that your user population not only knows the security policies but also understands them. To help ensure your users do not hinder security, combine strong enforcement mechanisms with ongoing security awareness and training programs.

About RSA

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC