Risk & Controls Solutions
Information Security Services

Payment Card Industry standards: Compliance burden or opportunity?

Practical strategies to reduce risk and compliance costs

PricewaterhouseCoopers

Contents

Executive summary

Is your company experiencing compliance fatigue?

Beyond the economic costs of non-compliance, companies could suffer reputational and brand damage if a security breach results in the compromise of payment card data

In response to an alarming increase in the theft of payment card data, including high-profile incidents at multiple organisations, the major credit card brands (i.e., Visa, MasterCard, American Express, Discover, and JCB) collaborated to develop the Payment Card Industry Data Security Standard (PCI DSS) to increase the protection of payment card data. Since its publication in 2004, the PCI DSS has undergone a number of revisions to reflect new threats and to provide additional clarification on the estimated 200-plus controls it addresses.

As a general guideline, any company that accepts debit or credit card payments is required to comply with the PCI standard. In November 2008 Visa announced global mandates for compliance with the PCI DSS. Visa will require confirmation from acquirers by September 30, 2009 that their large and mid-level merchants do not retain sensitive payment card data after transaction authorisation. Visa will require acquirers to provide an Attestation of Compliance for each of their large merchants demonstrating that each has validated full PCI DSS compliance by September 30, 2010. Even though mid-level and smaller merchants currently have to be PCI DSS compliant, compliance validation deadlines have not been announced for them at the time of this writing and are currently being mandated by the acquiring banks upon their discretion.

Companies that fail to comply by the deadlines face substantial fines and penalties as well as potential expulsion from payment card programs. Beyond the economic costs of non-compliance, companies could suffer reputational and brand damage if a security breach results in the compromise of payment card data.

Despite the prospect of fines and penalties, many merchants still are not PCI DSS-compliant. There are multiple reasons for non-compliance.They include a lack of education among merchants, underestimation of the complexity and cost of remediation efforts, and compliance fatigue resulting from the need to respond to a broad range of requirements that impact the average organisation.

There are many ways to achieve compliance with the PCI DSS. PricewaterhouseCoopers believes the most effective approach is to view PCI DSS compliance not as another compliance requirement, but rather as a controls framework that provides the opportunity to reduce risk to the organisation.

Focusing strictly on stand-alone compliance efforts can produce a false sense of security. Consider the recent case of a company that experienced a security breach shortly after passing its PCI DSS compliance assessment. The breach and the resulting millions of dollars in fines, penalties, legal fees, and remediation cost might have been prevented if the company had followed a risk-based approach rather than the compliance-based methods used by many third-party assessors.

PricewaterhouseCoopers has developed a five-phase approach that enables PCI DSS compliance through the identification and remediation of risk associated with payment card data. PricewaterhouseCoopers' approach uses the PCI DSS as a baseline controls framework that is supplemented with leading risk management practices and compliance and threat management experience. Within this framework, merchants can take a number of steps to reduce the size of the payment environment, the risk associated with potential cardholder data loss, and the cost of achieving and maintaining compliance. PricewaterhouseCoopers has developed five strategies to achieve these goals. Once the framework reaches operational compliance, the organisation can begin to integrate PCI DSS compliance within a broader integrated governance, risk, and compliance (iGRC) framework to achieve greater efficiencies and further reduce risk.

An in-depth discussion

Achieve Payment Card Industry standards compliance as an outcome of addressing risk.

Figure 1: Overview of PCI DSS Categories

Build and maintain a secure network 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplier defaults for system passwords and other security parameters	**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
Protect cardholder data 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks	**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 vulnerability management program 5. Use and regularly update antivirus software 6. Develop and maintain secure systems and applications	**Maintain an information security policy** 12. Maintain a policy that addresses information security

Source: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

The standard includes more than 200 individual controls that focus on the confidentiality of payment card data

Companies are facing an increase in compromised credit card data

Credit card fraud is approaching epidemic proportions—affecting 3.2 million people in the United States alone, according to a 2006 study by the Federal Trade Commission.[1] A number of security breaches in recent years, including several high-profile incidents, have exposed large volumes of credit card and other personal data to criminals.

In response to this growing incidence of payment card theft and fraud, the major credit card brands developed data protection programs focused on protecting the confidentiality of payment card data within merchant and service provider environments. In 2001, Visa created its Cardholder Information Security Program (CISP) and MasterCard launched its Site Data Protection (SDP) program. Soon after, American Express developed the Data Security Operating Policies (DSOP) and Discover launched the Discover Information Security & Compliance (DISC) program.

In 2004, the CISP requirements were incorporated into an industry standard known as the Payment Card Industry Data Security Standard, or PCI DSS. In 2006, ownership of the PCI DSS standard was transferred to a newly formed independent body, the Payment Card Industry Security Standards Council (PCI SSC). The council has the mandate to maintain and distribute the PCI DSS and all its supporting documentation and has subsequently also taken responsibility for the training of third-party PCI DSS assessors.

The PCI DSS has become the de facto security controls framework for the protection of payment card and related customer data. (Because of antitrust regulations, all of the major card brands still maintain their own data protection programs, but the brands mandate that their merchants and service providers comply with the PCI DSS.) In addition, PricewaterhouseCoopers has observed wider adoption of the PCI DSS as a controls framework by leading organisations to protect other sensitive data types, such as personally identifiable information (PII), intellectual property (IP), and employee and customer data.

PCI DSS compliance requirements

The PCI DSS consists of 12 requirements in six categories that address security management, policies, procedures, network architecture, and software design for the protection of payment card data (Figure 1). The standard includes more than 200 individual controls that focus on the confidentiality of payment card data. Regardless of their size, all merchants and service providers that store, process, or transmit payment card data are required to fully comply with each of the control requirements that applies to their environment.

On October 1, 2008 the PCI SSC released version 1.2 of the PCI DSS. Version 1.2 provided additional clarity and enhancements around existing controls and evolving threats, without introducing any significant changes that would negatively impact merchants that are currently compliant. Merchants performing assessments beginning after October 1, 2008 should utilize version 1.2 and all merchants must validate against version 1.2 by January 1, 2010.

[1] Federal Trade Commission—2006 Identity Theft Survey Report

As a general rule of thumb, merchants and service providers are classified according to their annual volume of payment card transactions. Each card brand has specific criteria that determines the merchant or service provider level (see Appendix for more details about merchant levels and validation requirements). For example, Visa defines a Level 1 merchant as one that processes more than 6 million Visa credit card transactions annually. Under a reciprocal arrangement, if an organisation is classified as a Level 1 merchant according to Visa's criteria, it is also recognised as a Level 1 merchant by the other card brands.

All service providers and merchants, regardless of their transaction volume, are required to comply with the PCI DSS. The classification levels merely determine the process that must be followed to validate compliance. For example, Level 1 merchants are required to submit a Report on Compliance to their acquiring banks, while Level 2 and 3 merchants are required to submit a Self-Assessment Questionnaire.

Third-party service providers that store, process, or transmit payment card data on behalf of merchants are also required to comply with the PCI DSS. Examples of service providers include payment gateways, outsourcers/ hosting companies, and record storage companies. Additionally, the standard requires that a contract be in place between a merchant and each of its service providers that establishes responsibility (and accountability) for handling payment card data according to the PCI DSS requirements.

Service providers are required to report their compliance with the card brands. Merchants are encouraged to engage only service providers that have reported their PCI DSS compliance to the card brands.

All service providers and merchants, regardless of their transaction volume, are required to comply with the PCI DSS

Each compensating control must be approved by key stakeholders in the certification process, normally including the qualified security assessor (QSA), acquiring bank, and, in certain cases, the card brands

The PCI DSS applies to all processes and system components that store, process, or transmit payment card data. All system components within the cardholder data environment, or with connectivity to the environment resulting from a lack of network segmentation, are within the scope of the PCI DSS. Even if cardholder data is encrypted while at rest or exists in non-electronic form (e.g., printed receipts and handwritten invoices) it is subject to compliance with the standard. All business processes that involve payment card data (including paperbased and manual processes) are within the scope of the PCI DSS.

The PCI DSS allows for compensating controls in cases where an organisation cannot meet a requirement because of a financial, technical, or business constraint. In such cases, the organisation is required to describe in writing the reason the control cannot be deployed, a definition of the risk associated with the control, the proposed compensating controls that will be deployed to mitigate the risk, a description of the validation testing performed against these controls, the processes in place to maintain these controls, and any residual risk associated with the compensating control.

Among other things, compensating controls must meet the intent and rigour of the original stated PCI DSS requirement, and they must be similarly effective in preventing a compromise of payment card data. Each compensating control must be approved by key stakeholders in the certification process, normally including the qualified security assessor (QSA), acquiring bank, and, in certain cases, the card brands. Compensating controls may be classified as “temporary,” pending the deployment of a more permanent solution, or “permanent,” with the condition that they be reassessed annually to determine their effectiveness in light of changes in the environment or evolving threats.

Common Drivers for PCI Compliance

- Increased awareness and general concerns over data privacy
- Significant fines and penalties that can be imposed by credit card brands (including expulsion from programs)
- Potential reputation and brand damage, leading to loss of revenue
- Concerns over civil liability resulting from customer identity theft
- Industry peer pressure
- Proposed changes to the Australian Privacy Act around mandatory disclosure of breaches
- Alignment with corporate risk management guidelines

Penalties and deadlines

Merchants and service providers not complying with PCI DSS requirements may be subject to significant fines and penalties, increased transaction processing fees, and even expulsion from card programs. In the event of a payment card data breach, a merchant can be fined in excess of $500,000 and may be subject to a processing fee increase amounting to millions of dollars, depending on the merchant's transaction volume. If track data (information encoded within the magnetic stripe) is compromised, additional measures, such as Visa's Account Data Compromise Recovery Program, take effect, normally resulting in significant additional penalties to cover assessed exposure and damage.

In addition to being fined, any Level 2 to 4 merchant that is compromised is reclassified automatically as a Level 1 merchant, and will be required to adhere to the same compliance validation procedures as Level 1 merchants (see Appendix).

In the event of a payment card data breach, merchants and their service providers are required to report the loss or theft of cardholder data immediately to the appropriate credit card brands to minimise the impact. The card brands levy a per-incident fine on those who fail to report a suspected or confirmed loss or theft of cardholder data. Additional fines are issued if the merchant was not PCI DSS-compliant at the time of the payment card breach or data loss.

In addition to fines and penalties issued by the card brands, indirect costs (both financial and non-monetary) are associated with payment card data breaches. Those costs may include damage to brand reputation, loss of consumer confidence, and possible class-action lawsuits. Companies whose payment card and customer data are breached also may face substantial government fines and interventions (e.g., following proposed changes to the Australian Privacy Act) if they were found not to have used reasonable and appropriate security measures to prevent unauthorised access to customer information within their environments.

In November 2008, Visa Inc. announced global compliance validation deadlines in an effort to provide a consistent framework for merchants, service providers, and agents around the world. Level 1 and 2 merchants are required to assert that they do not store sensitive data elements by September 30, 2009. Level 1 merchants are required to validate full compliance with the PCI DSS by September 30, 2010.

PCI-specific knowledge proves essential

A major transportation company in the U.S., a Level 1 merchant that processes more than 30 million credit card transactions annually, conducted a PCI DSS assessment. The project team had limited knowledge of the standard and did not accurately identify all the systems and processes that were in-scope. As a result, more than half of the company's controls were later found not to be in compliance, remediation efforts were stalled, the organisation was fined $25,000 per month, and it was facing increased transaction processing fees.

Why companies struggle to comply

Despite the risk of a security breach and the threat of substantial fines and other penalties, many companies that are required to comply with the PCI DSS have not yet done so. In the U.S. as of March 31, 2008, almost one-fourth (23 percent) of the estimated 362 Level 1 merchants, 22 percent of Level 2 merchants, and 43 percent of Level 3 merchants had not yet validated compliance. Statistics for Level 4 merchants were not available.[2]

PricewaterhouseCoopers' professionals have observed the following common challenges to achieving PCI DSS compliance:

- Viewing compliance as "an IT problem"—Because of the numerous technical controls in the standard, many organisations consider compliance to be an "IT problem," and look to the information technology department to "fix it." This approach generally results in a technology-centric approach that often does not give enough consideration to manual or non-IT procedures and controls.

  PCI DSS compliance should be viewed as a business challenge that involves people and processes as well as technology, and should be jointly "owned" and addressed by IT, business leaders and other relevant groups within the organisation. Leading organisations establish a PCI DSS compliance body with representation from business, IT, internal audit, treasury, and legal to oversee compliance efforts and the program once compliance has been achieved.

[2] Visa Inc. Cardholder Information Security Program, PCI DSS Compliance Validation Update as of 3/31/08.

The company brought in a team of PwC security professionals with experience in PCI DSS and the transportation industry to help get the compliance efforts back on track. A key problem was that the company did not have a good understanding of its payment environment. The PwC team helped the company identify the environment, map all payment card process flows, and understand the risks associated with each payment process. Then the team helped to develop controls-based remediation solutions to address some of the key risks identified, such as encryption key management, incident response, enterprise password parameters, and international PCI DSS compliance. With our assistance, the client was able to perform all required remediation and achieve PCI DSS-compliant status.

- Lacking a clear definition of the payment environment that is in scope for PCI DSS certification—Many merchants attempt to assess their payment environment without a clear understanding of the in-scope environment. This includes understanding all payment processes (electronic and non-electronic) including how payment card data enters the environment, where the data is processed and stored within the organisation's environment, how the data leaves the environment, and with whom the data is shared. Lack of a clear understanding often results in an incomplete compliance assessment and residual risk.
- Underestimating the extent and complexity of PCI DSS compliance—Many organisations underestimate the extent and complexity of PCI DSS compliance efforts and maintaining an ongoing PCI DSS compliance program. A contributing factor is that management often does not fully appreciate the extent of the payment environment and the number of systems, applications, databases, and technologies that need to be PCI DSS compliant. Remediation, especially in complex, distributed, or legacy IT environments, can come with a hefty price tag that may be difficult to accept. Compliance furthermore requires a cultural change for many organisations, and sometimes this change is met with resistance.
- Controlling logical access to systems containing payment card data—Restricting unauthorised access to payment card data (and systems) is a foundational principle of PCI DSS compliance, and it continues to be a challenge for many companies. A variety of factors add to the challenge, such as data proliferation across disparate systems, the absence of a clear understanding of where data resides in the enterprise, the inability of legacy or home-grown systems to support certain PCI DSS-mandated controls, and the absence of a role-based access control model. Remediation approaches range from tactical point solutions to managing access at the individual payment system level to complex enterprise identity management solutions.

We have observed merchants deploy a variety of solutions ranging from stand-alone manual procedures to fully automated and centralised solutions

- Logging and monitoring events—Logging and monitoring of security-related events on systems that store, process, transmit, or provide access to payment card data is required to aid in detection and prevention of suspicious activity and analysis of activities in the event of a breach. Many systems and applications in a legacy environment do not natively support logging controls mandated by the PCI DSS. Moreover, many of these systems and applications were not designed to handle the additional overhead on system resources in an environment where rapid transactional response time is essential.

  The effective monitoring of massive amounts of log data remains a challenge for many merchants. We have observed merchants deploy a variety of solutions ranging from stand-alone manual procedures to fully automated and centralised solutions. Many merchants with less mature capabilities focus on recording activities associated with access to payment card data rather than proactively monitoring to detect suspicious activity.

- Protecting stored payment card data—The encryption of stored payment card data (data at rest) is a control requirement that many merchants struggle to comply with, primarily because of the complex technical and often intrusive nature of available solutions. The data encryption requirement of the PCI DSS is designed to ensure that even if other data protection mechanisms are breached, the encrypted payment card data will remain inaccessible. Unfortunately, many companies' mainframes, databases, and other legacy systems were not designed to natively support encryption solutions. Data reduction and process reengineering are approaches used by many merchants to reduce the amount and type of payment card data that needs to be encrypted.

- Putting PCI DSS contractual language in place for third-party service providers—Merchants are required to establish contractual agreements with service providers that store, process, or transmit payment card data on their behalf to ensure that their customers' cardholder data is protected in the third-party's environment. Renegotiating contracts with business partners to introduce PCI DSS clauses has proved problematic for most organisations. If merchants are unsuccessful in changing existing contracts, they are required to introduce PCI DSS-related requirements when contracts expire and are renegotiated. Increasingly, merchants are recognising the importance of managing risk in their extended partner network by performing audits or mandating third-party attestations on how well their data is protected.

  Service providers that store, process, or transmit payment card data on behalf of merchants are required to become PCI DSS compliant and report their compliance to the major credit card brands. It is our experience that many service providers are unaware of their PCI DSS obligations, primarily because many do not have a direct relationship with the major credit card brands or acquiring banks. In many cases, service providers do not become aware of PCI DSS compliance requirements until merchants inquire about their compliance status.

- Obtaining management support for scalable remediation solutions—PCI DSS remediation has the potential to be a very costly endeavour. Typical remediation efforts range from implementation of single controls to deployment of big-ticket, enterprise-level security solutions such as encryption, security event management (SEM), access control, and payment infrastructure redesign.

  Although the PCI DSS provides organisations with an opportunity to put these solutions on the executive agenda, caution should be taken to apply the right balance between projects that are tactically important to reach PCI DSS compliance and those that may have a longer-term strategic advantage. Finding this right balance between tactical and strategic remediation programs normally increases management support and helps maintain a focus on timely risk reduction and efforts to reach PCI DSS compliance.

If merchants are unsuccessful in changing existing contracts, they are required to introduce PCI DSS-related requirements when contracts expire and are renegotiated

Placing too much reliance on the QSA's assessment and the resulting certification may create a false sense of security that the risk of a breach has been mitigated

- Taking a siloed approach to compliance—Most organisations take a siloed approach to addressing applicable regulatory, risk management, and compliance requirements. In many organisations, compliance programs focusing on regulations and control frameworks such as PCI DSS, ISO 27001, COBIT are not effectively integrated, even though many of their requirements overlap. Such a siloed approach impairs efficiency and effectiveness, contributing to duplication of effort, inconsistent processes, and ultimately compliance fatigue.
- Placing too much reliance on the QSA—Merchants often rely excessively on their QSA to identify areas of non-compliance and associated risk in the payment and broader enterprise environment. Because of the high-level sampling approach used by many QSAs and their reliance on the merchant to provide information on key payment processes and systems (that may not be known), critical vulnerabilities and associated risks may go undetected. Placing too much reliance on the QSA's assessment and the resulting certification may create a false sense of security that the risk of a breach has been mitigated.
- We have highlighted a number of reasons why organisations struggle to comply with the PCI DSS, and although compliance is essential, it is important to emphasise that it does not provide any assurance against the loss or compromise of payment card data. As this is being written, the payment card industry is grappling with the case of a merchant whose payment card data was breached even though the organisation was certified as PCI DSS-compliant. This case is being watched closely by the industry and, as it unfolds, may likely impact the future state of the standard and related compliance requirements.

What this means for your business

A risk-based, integrated approach can create a more secure and efficient—as well as compliant—organisation.

We believe the most effective approach is to view the PCI Data Security Standard as a framework to help reduce risk to the organisation

The need for a risk-based approach

Merchants can approach PCI DSS compliance in a variety of ways. The prevailing trend, based on our experience, continues to be compliance-focused rather than risk-focused. A compliance-based approach is likely to result in residual risk remaining in the merchant's payment environment even after reaching compliance, as the case cited above illustrates.

Rather than focusing solely on compliance, the PricewaterhouseCoopers approach focuses on reducing the risk of a data breach within the merchant's payment environment. We view PCI DSS compliance as an intended outcome of a systematic, risk-based approach that is designed to:

- Define the relevant in-scope environment
- Assess risks within this environment using the PCI DSS as a controls framework
- Remediate identified vulnerabilities according to risk prioritisation
- Assist in implementation of a program to maintain the controls framework and facilitate certification on an ongoing basis (analogous to implementation of an information security management system for an ISO 27001 certification).

Focusing on risk during the PCI DSS pre-certification as well as the post-certification phase, as opposed to an exclusively compliance-based approach, will enable merchants not only to address compliance, but also to have greater confidence that the likelihood of a payment card data breach has been reduced.

A risk-based approach to PCI DSS compliance also positions an organisation to integrate activities within a broader governance, risk, and compliance framework—thus enhancing the overall risk management process. The requirements of the PCI DSS and other controls frameworks (e.g., ISO 27001, COBIT) overlap in various areas. This presents an opportunity for controls optimisation that can directly translate into reduced compliance costs and an increase in the overall efficiency of the enterprise controls framework.

PricewaterhouseCoopers' approach to becoming PCI DSS-compliant

We believe that a well planned and executed risk-based approach toward PCI DSS will not only reduce risk to the organisation, but will also result in a more effective response to PCI DSS compliance. Our approach consists of five phases: data flow analysis, compliance gap analysis, PCI DSS remediation planning, remediation, and operationalising compliance.

Phase 1: Data flow analysis

The first phase in achieving PCI DSS compliance involves identifying and documenting the entire merchant payment environment, including all processes (electronic and non-electronic) that involve PCI DSS-related data; payment card data entry and exit points; and all systems, applications, data stores, and supporting infrastructure involved in the processing, storage, and transmission of payment card data. Identifying all locations where cardholder data resides and how it flows through (and out of) their systems will enable merchants to accurately determine their scope of PCI DSS compliance requirements.

PCI DSS-relevant data may flow into the merchant environment through e-commerce transactions, customer telephone calls, catalogue sales, field technicians using hand-held devices, payment kiosks, point of sale terminals, physical and electronic mail, third-party business partners, and other payment card acceptance channels. The data may be processed by web applications and supporting systems, payment batch processing systems, and billing systems. And it may exit the organisation in several ways. For instance, it might be sent to an offsite storage facility on backup media or delivered to third-party service providers or business partners for further processing and analysis.

Once all PCI DSS-relevant payment processes and associated data entry, processing, and exit points have been identified, the organisation can map the logical flow of data throughout the environment and identify all the systems, applications, databases, and network infrastructure that support relevant payment processes. For instance, when a customer makes a payment by telephone, a customer service representative enters the credit card information into a payment application. From there, the data may be "swivel-chaired" into another application and then automatically sent to the acquiring bank. Throughout this process, payment card data may be written to transcripts, application logs, and supporting databases. All such interactions between business processes and systems should be recorded.

Understanding the payment environment is crucial

A large healthcare company in the U.S. spent eight months and an estimated $800,000 on PCI DSS remediation without showing any significant progress, largely because it lacked a clear understanding of the payment environment. PricewaterhouseCoopers assisted the client by performing a detailed payment card data flow mapping, which enabled the organisation to get its remediation projects back on track.

Data flow documentation should be updated as payment processes change

It's worth noting that extensive payment card data mapping does not have to be repeated annually. Rather, the initial mapping will establish a foundation for the ongoing PCI DSS compliance program. Data flow documentation should be updated as payment processes change (e.g., when new systems are integrated into the payment environment following an acquisition).

Our experience has shown that in spite of the critical importance of mapping payment data flows and clearly identifying all systems that support PCI DSS-relevant payment processes, the vast majority of companies fail to complete this first phase, primarily because of its complexity and the resources required. Unfortunately, there are no shortcuts to conducting a payment flow analysis.

The exercise can be painstaking in larger, complex environments, but it is essential for determining the people, processes, and technology that fall within the scope of PCI DSS compliance. Companies that choose not to perform this important first phase are unlikely to have a clear picture of their PCI DSS-relevant scope and thus may perform an incomplete and inaccurate PCI DSS compliance assessment. The net result is that unidentified risk may remain in the merchant's environment.

Phase 2: Compliance gap analysis

In this phase, an analysis is performed to identify the gaps between the controls mandated by the PCI DSS and those within the in-scope payment environment. The objective is to identify areas where controls are missing or not up to standard and to quantify these deficiencies within the broader context of risk to the organisation. It is essential to focus on business process controls as well as technology controls (something not all merchants do) and how the two types of controls fit together within the payment processing environment.

It is essential to focus on business process controls as well as technology control

During the analysis, it is useful to develop a "heat map" representation of the organisation's alignment with the controls in the 12 PCI DSS requirement categories to quantify deficiencies in the payment environment. The heat map provides a visual representation of the state of controls according to a predefined set of data points and criteria. The criteria that determine the color for a specific category may vary among organisations based on associated risk (likelihood and impact of control failure), prevalence of the control deficiencies, alternative controls that are in place, and estimated cost and effort to remediate. Quantifying deficiencies in such a manner has multiple benefits. Primarily it provides the ability to prioritise and focus remediation efforts on areas of higher risk that may provide justification for a more strategic enterprise-level solution.

The identification of a comprehensive set of data points can help management make informed decisions on where to focus remediation efforts. This data can be leveraged to identify trends or larger underlying problems within the enterprise such as access control, change control, and provisioning that may provide justification for a more strategic enterprise-level solution.

Our experience across many PCI DSS engagements has shown that most organisations find control deficiencies across all 12 PCI DSS control categories in their initial gap or compliance assessment. PCI DSS categories where many organisations experience higher-risk control deficiencies include:

- Protecting stored cardholder data
- Restricting access to cardholder data by business need-to-know
- Developing and maintaining secure systems and applications.

Prioritising remediation efforts buys time for a client

A telecommunications client in the U.S. planned to replace several systems within two years and had to decide whether to remediate control gaps on these systems or wait to install the new systems and ensure they were PCI DSS compliant. (The company could not afford to immediately address all the control gaps identified.) PricewaterhouseCoopers helped the client to identify which gaps posed the greatest risks to the organisation and thus should be remediated immediately to reduce the likelihood and impact of a breach.

Phase 3: PCI DSS remediation planning

In planning PCI DSS remediation, the organisation can focus on the payment environment (identified in the data flow analysis phase) rather than on the entire company. For a large organisation, this can substantially reduce the time, effort, and cost required to achieve PCI DSS compliance.

During this phase, the organisation reviews the results of the gap analysis to determine the most appropriate course of action to address identified risks through the remediation of non-compliant controls. The remediation plan normally results in a number of work streams that represent the logical grouping of control categories and corresponding controls, such as with logging and monitoring, vulnerability scanning, data encryption, security awareness training, and network segmentation.

Remediation typically involves short-term, tactical actions as well as longer-term, strategic changes designed to facilitate compliance well into the future. During the remediation planning phase, it is essential to align tactical remediation activities with longer-term, strategic IT and business initiatives. If these initiatives are not aligned, the organisation may risk spending significant resources on controls that are eventually discarded as they are replaced by the longer-term solutions.

During this phase, it may be necessary to propose and champion strategic initiatives as opposed to shorter-term tactical solutions. This proves difficult for many organisations because of the high cost, challenge of deployment, and potentially intrusive and disruptive nature of some longer-term strategic control solutions (such as an enterprise wide identity management solution).

The balancing of tactical and strategic remediation efforts, typically under pressure of an imposed deadline and penalties, often requires close cooperation with third-party assessors, the merchant's acquiring banks, and, in some cases, the card brands as well. In our experience, such external stakeholders often show a good deal of flexibility to accommodate longer-term strategic remediation solutions if the merchant is able to deploy temporary or compensating controls to address associated risks before the longer-term solution becomes operational.

Compensating controls should be a key consideration during the remediation planning phase in cases where the organisation cannot meet a technical specification of a requirement but has the potential to sufficiently mitigate the associated risk. For instance, we have seen compensating controls effectively applied where legacy systems did not support the access controls required by the PCI DSS, or where a required control would have a negative impact on system response time and associated business processes.

Compensating controls must be thoroughly documented in the merchant or service provider's Report on Compliance or Self-Assessment Questionnaire. The controls must be reassessed annually to confirm their effectiveness in an ever-evolving threat landscape.

During this phase, the organisation should also explore the potential for reengineering payment and other processes to reduce the PCI DSS remediation scope, as well as the cost of remediation activities. For instance, if an organisation can remove e-mail transmission of payment card data from a payment process, it can take the e-mail system out of the scope for remediation, thereby avoiding the deployment of a costly e-mail encryption solution.

The PCI DSS remediation planning phase ends with defined solutions for each area of non-compliance, as well as approved projects and project plans and the assignment of project owners. A plan for addressing risks should also be in place for areas where remediation will not be performed or where a temporary control solution will be deployed, such as in the case of compensating controls.

The controls must be reassessed annually to confirm their effectiveness in an ever-evolving threat landscape

Establishing a program management office

After a gap analysis, a large Level 1 merchant struggled to track and manage the remediation of approximately 1,000 instances of non-compliant controls. PricewaterhouseCoopers established a PMO to oversee the remediation process and worked with project owners to ensure that milestones were clearly defined and met, resulting in the project being completed on time. Our role involved constant communication with the project owners and the executive leadership team to relay project slippage and develop resolutions to bring the projects back on schedule.

Phase 4: Remediation

With a sound plan in place, the organisation can begin tactical and strategic remediation. The details of PCI remediation projects will vary by organisation, but in every case, a program management office (PMO) with support from executive leadership is a critical factor for success. Each project team should report on progress to the PMO on a weekly or biweekly basis to make sure that the projects are proceeding on schedule and that all major milestones are met. In the event that milestones slip and impact the overall target date for completion, the PMO should be able to solicit support from leadership to push the project back on schedule (e.g., through the reallocation of resources or budget).

Remediation projects are commonly managed and executed internally, but larger and more complex initiatives are often supported by third party solution providers. Penetration testing, web application security assessments, application source code reviews, and vulnerability scanning are commonly outsourced to third-party providers that specialise in these services.

Leading organisations hold regular status meetings with their acquiring banks to update them on the progress of their remediation activities. These frequent meetings will help to foster a trusted relationship built on transparency and will give the acquiring bank more insight into the efforts being taken to address risk. Such frequent, ongoing communications often result in more flexibility and support for solutions that make more sense for the organisation, even if the initiatives expand beyond stated compliance deadlines.

Phase 5: Operationalising compliance

PCI DSS responsibilities do not cease once an organisation becomes PCI DSS compliant. Merchants are required to maintain their PCI DSS compliance as a continuous state, as opposed to a point in time when the compliance validation and reporting occurs on an annual basis.

It is essential for organisations to assign clear roles and responsibilities for ongoing compliance activities to business units as well as to the IT and security functions. As noted earlier, PCI DSS compliance involves people and processes as well as technology and should be addressed by the organisation as a whole, including IT and business unit leaders.

Maintaining PCI DSS compliance requires the integration of PCI DSS requirements into enterprise systems development. It also requires change procedures to help ensure that new technologies or processes introduced into the payment environment meet PCI DSS requirements, do not introduce risk, and do not negatively impact the organisation's state of compliance. Most mature organisations further establish a compliance program based on a framework that includes establishing metrics, continual monitoring of the current state of compliance, communicating goals and status, and reinforcing management's commitment. This program should be championed by a leader and team with visibility of the entire organisation and the clout to enforce compliance. This function often resides within the internal audit or compliance group. Overall ownership of PCI DSS should remain with the business and is often overseen by the controller, treasury, or payment processing department.

Putting a PCI compliance program in place

A PricewaterhouseCoopers client was concerned about maintaining compliance after it submitted its initial Report on Compliance. Our team helped the client by first transitioning ownership of the PCI DSS compliance program from an information technology team to a business compliance group that already performed similar annual assessments. We then helped transfer PCI DSS-specific knowledge by building a joint PricewaterhouseCoopers client team to run the program and perform site visits. We also helped develop PCI DSS tollgates as part of the systems and software development life cycle to confirm that new processes, systems, and applications did not bring the client out of compliance.

A key objective of any PCI DSS remediation program should be to reduce the scope of the payment environment and other in-scope systems to a minimum

Five strategies to reduce the risks and cost of compliance

We have described PricewaterhouseCoopers' five-phase approach to achieving and maintaining PCI DSS compliance. Within this framework, merchants can take a number of steps to reduce the size of the payment environment, the risk associated with potential cardholder data loss, and the cost of achieving and maintaining compliance.

1. Reduce or eliminate the use of payment card data

A common challenge for merchants during the PCI DSS remediation phase is securing payment card data at rest. A key objective of any PCI DSS remediation program should be to reduce the scope of the payment environment and other in-scope systems to a minimum. Scope reduction will decrease the number of technologies and processes that have to be remediated and under normal circumstances may also minimise risk. One of the most effective ways to shrink the payment environment is through the reduction of payment card data. The PCI DSS specifies data protection requirements for the various payment card data elements that are retained, the most important of which is the primary account number, or PAN. The reduction of PANs across the enterprise, plus the consolidation and centralisation of payment card data in a well-controlled environment, is the most effective way to reduce the scope and risk for the payment environment as well as the associated cost of remediation and maintenance. The reduction and elimination of payment card data may require significant process, system, and architecture reengineering, but the benefits in most cases outweigh the costs and short-term impact on the organisation.

The following techniques are commonly used to reduce payment card data and the scope of the payment environment:

- Truncation—A process of redacting the PAN by storing only the first six and last four digits of a payment card account number. Payment card account numbers that are truncated are no longer considered PANs and fall out of scope for PCI DSS compliance. Organisations should ask business unit leaders: "Do you need the full PAN to perform your business function?" If the answer is no, consider the possibility of no longer recording PANs or truncating the numbers.
- Hashing—The one-way mathematical conversion of text into a new value. Hashing produces a number that is equivalent to the PAN but cannot be reversed to reproduce the PAN. Hash values of PANs are not in scope for PCI DSS compliance. (Note that hashing is different from encryption because encrypted data can be decrypted.) Securely hashing PAN data using a "salt" for increased cryptographic complexity will enable an organisation to remove systems and applications from the scope of PCI DSS compliance.
- Tokenisation—An approach used by a number of large organisations that involves replacing the PAN with a unique identifier that does not qualify as a payment card data element. Tokenisation may be a viable option for PCI DSS scope reduction for companies with legacy systems that do not support encryption solutions, and for organisations that maintain distributed (often complex) payment environments that pass payment card data among multiple systems. (In many organisations, payment card numbers stored in several applications may turn up in sales reports, customer databases, and many other places where they are not required. Each new copy of the data increases the security threat and the scope of compliance efforts.) Although tokenisation projects typically are complex and require intrusive application and database changes, they can substantially reduce the payment environment, the number of controls that must be deployed and maintained on an ongoing basis, and the enterprise risk associated with a large payment card data footprint.

Securely hashing PAN data using a "salt" for increased cryptographic complexity will enable an organisation to remove systems and applications from the scope of PCI DSS compliance

Reengineering payment processes

A large entertainment company in the U.S. that grew through a series of acquisitions was plagued with disparate payment processes across the organisation. During the assessment phase, PricewaterhouseCoopers identified a business process where customer service representatives would write down customers' payment card information (including sensitive authentication data) on paper forms and then manually key the data into the billing system. All paper forms were archived in a data storage facility for an indefinite period of time. PricewaterhouseCoopers helped the client develop an approach to purge all of the retained payment card data (while still retaining the remainder of non-payment card data) and reengineer the process so that payment card information would no longer be written to paper, thus removing thousands of paper forms from the scope of PCI DSS compliance.

- Process reengineering—Streamlining or changing payment, or other processes to reduce the number of payment card data repositories. We often observe merchants retaining PCI DSS relevant data for processes such as chargebacks, customer loyalty programs, and marketing/sales analysis. Modifying such processes not to collect and retain PCI DSS relevant data can have a significant scope reduction impact.
- Encryption of payment card data in transit—End-to-end encryption of payment card data is another approach that can be used to reduce the scope of payment environments. If the PAN and associated payment card data is encrypted at the source and decrypted at the destination, and if encryption/decryption keys are tightly controlled, all intermediary systems that handle the data between those transaction points potentially may be removed from scope (if the organisation can prove that the payment card data will remain protected if the intermediary systems are compromised).

2. Purge payment card data

Another approach commonly used to reduce the payment environment is to purge payment card data after the authorisation process or to delete historical payment card data that is no longer required. Organisations should ask themselves why PANs and associated payment card data are retained; this is a very important step in the initial assessment, ongoing systems development, and integration process. Two reasons for retention of this data are commonly accepted: Organisations hold data for (more efficient) bulk processing of transactions and because of regulatory requirements. Three other reasons may be valid but should be evaluated to determine if they are required:

From a technical standpoint, organisations need a credit card number only to authorise a transaction

- Managing chargebacks and disputes—From a technical standpoint, organisations need a credit card number only to authorise a transaction. Historically, many companies have felt that they should retain credit card numbers in the event a customer has a chargeback return. The recommended approach to facilitate returns is to retain only the transaction ID and authorisation number, along with a subset of less sensitive cardholder data that could serve the same purpose from a transactional perspective. Even if organisations decide to retain credit card numbers for return and chargeback purposes, the typical time for dispute resolution is 90 days, in which case any retained transactional card data could be discarded.
- Data mining—Many retailers retain payment card data, including other sensitive personal information, to gain insight into the purchasing habits of their customers. This practice often increases the merchant's risk, perhaps needlessly, whereas a voluntary customer loyalty program could serve the same purpose and be more beneficial to the merchant. If there is a justifiable business need to retain such payment card and customer data, merchants should refrain from retaining the data in its native or even an encrypted format but should rather explore options to modify the data through hashing, truncation, or other means of obfuscation.
- Returning purchased goods and services—Some retailers allow returns without a receipt through a lookup of the purchase record by the credit card used to pay for it. This may be more convenient for customers seeking to return items, but retaining payment card data for this purpose typically brings additional systems into scope and increases the compliance cost and the potential risk associated with a data breach. Merchants should explore options such as oneway data hashing and truncations to convert payment card data to alternate unique values that may be used for the same purpose.

In summary, we believe that in certain situations, the direct and indirect costs of retaining payment card data for the business reasons outlined above may outweigh the benefits. Fortunately, merchants have various options to consider to reduce their PCI-relevant footprint without negatively impacting business processes.

A centralised solution gives the merchant one collection of key systems that must be secured, which has the potential to significantly reduce the PCI DSS-relevant payment environment and associated risk

3. Redesign the payment environment

Another approach used to reduce the PCI DSS scope and accelerate PCI DSS compliance efforts is to redesign the payment environment. For example, PricewaterhouseCoopers assisted a large merchant with the redesign of its payment switch solution, whereby all payment requests are forwarded from a variety of processes such as retail and pharmacy locations, to the payment switch, where transactions are processed, authorised for payment, and forwarded to the appropriate financial institution.

By allowing organisations to centrally store, authorise, and process cardholder information, a payment switch may reduce the cost and effort to comply with PCI DSS requirements in the long run, while also increasing the efficiency of processing, settling, and reconciling card payments. This centralised approach also provides the ability to process other forms of electronic payments, as well as the scalability and flexibility to support future applications.

A centralised solution gives the merchant one collection of key systems that must be secured, which has the potential to significantly reduce the PCI DSS-relevant payment environment and associated risk. Finally, centralising payments allows merchants to aggregate their transactions and may enable them to reduce their per-transaction cost through better negotiated rates and other efficiencies.

4. Outsource payment processing

Outsourcing payment functions to a third-party service provider is another effective approach to reducing the size of a payment environment, the related PCI DSS compliance burden, and the potential risk to the organisation. One such outsourcing solution involves forwarding transactional data directly to a third-party when a customer swipes a credit or debit card. With the subsequent authorisation and settlement process handled by a third-party, the organisation may be able to remove most payment data and systems from their environment, eliminating many of the PCI DSS requirements from their scope.

The potential value and benefit of outsourcing the payment process must be analysed on a case-by-case basis, with the organisation carefully weighing the related costs and benefits. In some cases, the analysis may reveal that the potential medium- and longer-term cost savings from outsourcing are substantial. For instance, our analysis for one client concluded that it would cost the company $5 million to $7 million to remediate its payment environment, compared with an estimated annual outsourcing cost of $250,000. This accelerated remediation solution was further projected to eliminate fines and higher interchange fees associated with not complying with key deadlines. The solution was also projected to significantly reduce the ongoing costs of maintaining inhouse payment systems and complying with the PCI DSS.

It is important to note that although an organisation may outsource its payment processing functions, it will still have PCI DSS compliance obligations. Merchants will be required to have a contractual agreement with the service provider that obligates the third party to comply with the PCI DSS and to ensure payment card data is protected within its environment. Other requirements may still apply if PCI DSS-relevant data flows back into the merchant's environment and if the merchant accesses PCI DSS-relevant data in the service provider's environment.

This accelerated remediation solution was further projected to eliminate fines and higher interchange fees associated with not complying with key deadlines

We have observed some organisations having up to 500 merchant IDs and multiple contracts with acquiring banks

5. Consolidate and centralise

Many organisations maintain a multitude of disparate applications, |systems, and technologies that process, store, or transmit payment card data within their environment. As noted earlier, consolidating such systems and associated data can have significant benefits for organisations, such as increased efficiency of transaction processing, reduced operational and compliance costs, and reduced risk associated with the retention of payment card data.

One area where organisations often realise cost savings and an improved PCI DSS controls environment is through the consolidation of merchant accounts held with third-party acquiring banks. We have observed some organisations having up to 500 merchant IDs and multiple contracts with acquiring banks. Excessive and often decentralised agreements and payment infrastructure commonly result in significant administrative and transactional overhead. Perhaps more importantly, they represent a lost opportunity for the business to consolidate agreements and leverage the resulting higher transaction volume to negotiate more favourable transaction processing rates.

Integrating PCI DSS compliance within an iGRC framework

When an organisation becomes compliant with the PCI DSS, it should look for opportunities to integrate its PCI DSS program into the enterprise governance, risk, and compliance framework. Ideally, such integration should be planned during the PCI DSS compliance remediation phase; in reality, most organisations prefer to perform this integration once the tactical objective of becoming PCI DSS-compliant has been met.

Most organisations have similar, and often duplicative, activities across compliance programs such as PCI DSS, ISO 27001 and COBIT. Rather than operating in silos and addressing each standard or regulation in isolation, companies can be far more efficient and cost-effective by identifying and rationalising overlapping controls and addressing these through a centralised process and organisation.

For instance, we assisted a large client with integrating its PCI DSS compliance efforts within an iGRC framework. Now, when the internal audit department audits one of the many operating entities, it covers PCI DSS, ISO 27001 and COBIT and also performs penetration testing to meet PCI DSS and other requirements.

Establishment of an integrated compliance function with responsibility for multiple regulatory and other requirements has the potential to significantly reduce the cost and impact of ongoing compliance activities, reduce risk, and increase efficiency.

Rather than operating in silos and addressing each standard or regulation in isolation, companies can be far more efficient and cost-effective by identifying and rationalising overlapping controls and addressing these through a centralised process and organisation

Conclusion

The PCI Data Security Standard is regarded by many organisations as one of the most challenging compliance standards. Merchants often overcome their initial concern as they become more aware of the various techniques and approaches available to them to secure payment card data, as well as the flexibility that the standard provides. Leading merchants have further illustrated that the PCI DSS not only provides the opportunity for enterprise risk reduction, but may also serve as a change agent for greater efficiency, lower costs, and more effectiveness.

Appendix

Payment Card Industry Relationships

Figure A provides a simplified representation of the common players in the payment card industry.

Issuing Banks—Organisations that issue credit and/or debit cards to cardholders.

Card issuers are primarily banks, credit unions, and other financial institutions, as well as some merchants that issue their own cards. In recent years, issuers have increasingly offered co-branded payment cards with non-financial organisations such as airlines, department stores, and universities. The issuing bank has the direct relationship with the customer, serves as the party that authorises a transaction during a purchase, and bills the customer for the amount that was settled with the merchant.

Card Brands—The major credit card companies, including Visa, MasterCard, American Express, Discover, and JCB, which maintain their own data protection programs because of antitrust regulations.

The card brands play a key role in establishing compliance requirements, levels, timelines, and penalties for non-compliance with the PCI DSS as reflected in their individual data protection programs.

Acquiring Banks—Card brand members that initiate and maintain relationships with merchants that accept payment cards.

Their main function is to process payments from merchants and to communicate with issuing banks through the payment brand networks to authorise and settle payment card transactions. Acquirers are also responsible for monitoring and reporting merchants' PCI DSS compliance to the credit card brands.

Figure A: Common relationships of PCI DSS compliance role players

Note: Arrows represent primary PCI DSS compliance-driven relationships; other relationships may exist.

An "Open Loop" payment system is depicted; other payment process configurations and associated relationships may exist.

Merchants—A merchant is any organisation that accepts branded credit, debit or charge card payments. Merchants are classified based on transaction volume as one of four merchant levels in Visa and MasterCard's program, or as one of three merchant levels in American Express' program. Discover does not currently classify merchants according to levels and JCB has two merchant levels.

PCI Security Standards Council (SSC)—An open forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection.

The group's primary responsibility is to establish and maintain the PCI security standards and to certify third-party security assessors. The SSC does not conduct assessments and does not issue penalties for non-compliance. The council, which maintains the PCI DSS, was established by the payment industry as a separate and independent legal entity.

Assessor/Consultant—Individuals that perform validation of merchants' or service providers' PCI DSS compliance.

Organisations can assess their environment by using an independent internal organisation, such as internal audit, or a third-party qualified security assessor (QSA). All merchants and service providers are required to use an approved scanning vendor (ASV) for external vulnerability scanning. Both QSAs and ASVs are trained and certified by the PCI Security Standards Council and must renew their credentials annually.

Merchants must have a contract with their service providers requiring them to be compliant with the PCI DSS

Service Providers—For PCI DSS purposes, a service provider is a business entity that provides services to merchants or acquirers, including the processing, storage and/or transmission of payment card data.

Qualifying service providers must achieve and maintain full compliance with the PCI DSS and are required to report their compliance to the card brands. Merchants must have a contract with their service providers requiring them to be compliant with the PCI DSS.

Service providers are similar to merchants, classified by level. Visa's Account Information Security (AIS) program has three service provider levels.

PCI DSS Compliance Classifications and Requirements

The PCI Security Standards Council is responsible for maintaining the PCI DSS. The various card brands, however, maintain their own data protection programs, and compliance is validated by QSAs, ASVs, or self-assessments. The card brands are also responsible for the enforcement of compliance with their own respective program. Figure B illustrates merchant levels.

Figure B: PCI DSS merchant levels (Visa)

	Level 1	Level 2	Level 3	Level 4
Level qualifiers	• Greater than 6M credit card transactions per year • Any company that has been compromised	• Between 1-6M credit card transactions per year	• Between 20K and 1M e-commerce credit card transactions per year	• Less than 20K e-commerce credit card transactions per year • Less than 1M traditional credit card transactions
PCI DSS requirements	• Annual on-site PCI Data Security Assessment • Quarterly external network vulnerability scans	• Annual PCI DSS Self-Assessment Questionnaire • Quarterly external network vulnerability scans	• Annual PCI DSS Self-Assessment Questionnaire • Quarterly external network vulnerability scans	• Annual PCI DSS Self-Assessment Questionnaire • Quarterly external network vulnerability scans
To be validated by	• Qualified Security Assessor or Internal Audit (with report signed by company officer) • Approved Scanning Vendor	• Merchant • Approved Scanning Vendor	• Merchant • Approved Scanning Vendor	• Merchant • Approved Scanning Vendor

Source: http://usa.visa.com/merchants/risk_management/cisp_merchants.html

Service provider levels

Service providers are organisations that store, process, or transmit cardholder data on behalf of members, merchants, or other service providers. Both issuing and acquiring banks must use, and are responsible for ensuring that their merchants use, service providers that are compliant with the PCI Data Security Standard.

Although there may not be a direct contractual relationship between merchant service providers and acquiring members, Visa members may be responsible for liability that may occur as a result of non-compliance or a payment card data breach. Service providers must be registered with Visa prior to inclusion on the list of CISP-compliant service providers.

Most card brands have adopted Visa's service provider definitions and validation requirements, which are highlighted in the table on the next page.

Figure C: PCI DSS service provider levels (Visa)

	Level 1	Level 2	Level 3
Level qualifiers	• All VisaNet processors (member and nonmember) and all payment gateways	• Any service provider that is not a Level 1 and stores, processes, or transmits more than 1M Visa accounts/ transactions annually	• Any service provider that is not a Level 1 and stores, processes, or transmits fewer than 1M Visa accounts/ transactions annually
PCI DSS requirements	• Annual on-site PCI Data Security Assessment • Quarterly Network Scan	• Annual on-site PCI Data Security Assessment • Quarterly Network Scan	• Annual PCI DSS Self-Assessment Questionnaire • Quarterly Network Scan
To be validated by	• Qualified Security Assessor • Approved Scanning Vendor	• Qualified Security Assessor • Approved Scanning Vendor	• Service Provider • Approved Scanning Vendor

Source: http://usa.visa.com/merchants/risk_management/cisp_service_providers.html

Figure D: Effective February 1, 2009, service providers will be classified in two levels according to Visa's CISP program:

	Level 1	Level 2
Level qualifiers	• VisaNet processors or any service provider that stores, processes and / or transmits over 300,000 transactions per year	• Any service provider that stores, processes and / or transmits less than 300,000 transactions per year
PCI DSS requirements	• Annual on-site PCI Data Security Assessment • Quarterly Network Scan • Attestation of Compliance Form	• Annual PCI DSS Self-Assessment Questionnaire • Quarterly Network Scan
To be validated by	• Qualified Security Assessor • Approved Scanning Vendor	• Service Provider • Approved Scanning Vendor

Source: http://www.corporate.visa.com/md/nr/press873.jsp

Contacts

To have a deeper conversation on the industry or on any of the topics mentioned, please contact:

Andrew Elsworth
Partner

National and Melbourne Information Security Services Lead
+61 (3) 8603 6179
andrew.elsworth@au.pwc.com

Adelaide

Kim Cheater
Partner

+61 (8) 8218 7407
kim.cheater@au.pwc.com

Brisbane

David Harley
Director

+61 (7) 3257 8307
david.harley@au.pwc.com

Canberra

Mark Ridley
Partner

Canberra Lead
+61 (2) 6271 9215
mark.ridley@au.pwc.com

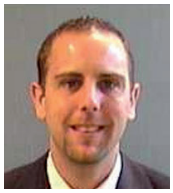
Patrick Kevin
Executive Director

Canberra
+61 (2) 6271 9267
patrick.kevin@au.pwc.com

Melbourne

Steve Ingram
Partner

Melbourne Forensic Technologies Services Lead
+61 (3) 8603 3676
steve.ingram@au.pwc.com



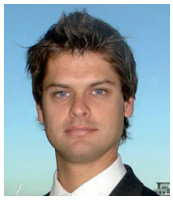
Rich Sands
Senior Manager

Melbourne
+61 (3) 8603 2619
rich.sands@au.pwc.com

Sydney

Jan Schreuder
Partner

Sydney Lead
+61 (2) 8266 1059
jan.schreuder@au.pwc.com



Michael Cerny
Director

Melbourne
+61 (3) 8603 6866
michael.cerny@au.pwc.com

Tom McCann
Director

Sydney
+61 (2) 8266 9616
tom.mccann@au.pwc.com

Malcolm Shackell
Partner

Sydney Forensic Technologies Services Lead
+61 (2) 8266 2993
malcolm.shackell@au.pwc.com

Peter Chapman
Director

Sydney
+61 (2) 8266 8478
peter.chapman@au.pwc.com

Perth

Shane Devitt
Executive Director

Perth
+61 (8) 9238 3473
shane.devitt@au.pwc.com

pwc.com/au/security