PCI DSS—READINESS AND RESPONSE

EMC Consulting Services offers a lifecycle approach to holistic, proactive PCI program management

ESSENTIALS

Partner with EMC Consulting for your PCI program management and benefit from:

- Deep industry understanding and consultants who average 17 years of experience
- RSA's security expertise and industry leadership to accelerate and optimize security strategies and risk postures
- Staying proactive, while continuously improving compliance in the context of evolving business and security program needs
- The development of a PCI program that is aligned with your business objectives
- A comprehensive view of gaps and remediation steps to ensure compliance prior to an annual PCI assessment
- PCI compliance while transforming your IT service organization when you transition to a cloud computing environment

The Payment Card Industry Data Security Standard originated in 2004 through collaboration of American Express, Discover Financial Services, JCB, MasterCard, and Visa to create a common global framework for the management and protection of cardholder information.

SECURED BY RSA®

Any organization that collects, stores, processes, or transmits cardholder data is required to comply with the Payment Card Industry Data Security Standard, a set of best-practice requirements for protecting payment card data. Commonly known as PCI DSS or PCI, this standard focuses on six high-level control objectives, 12 major security requirements with over 240 sub-requirements that support each control objective. Since its release on December, 15, 2004, hundreds of breaches of payment card data and consumer information have been reported by organizations, and with the growing use of Internet banking and e-commerce, the risks and number of reported transgressions are growing.

Organizations struggle to consistently apply PCI DSS controls and demonstrate their ability to maintain a steady state of compliance. This challenge is not limited by geography or industry. Retailers, hotels, local and federal governments, healthcare, universities, and financial institutions have all been forced to report consumer data compromises in recent years.

New guidelines effective January 1, 2011 with PCI DSS version 2.0 offer clarifications and additional guidance and address evolving requirements not previously addressed in PCI DSS version 1.2.1. This new version updates the standards to keep pace with emerging threats, technology evolution, and changes in the market.

A LIFECYCLE APPROACH TO PCI PROGRAM MANAGEMENT

Too often, organizations define their PCI programs based on the strict assessment requirements associated with PCI DSS and overlook the importance of developing a compliance strategy that maps to overall business goals. Truly efficient compliance programs implement policy and procedures that satisfy multiple compliance and regulatory requirements within a common framework. Organizations often look at PCI assessments as a vehicle to identify gaps—rather than an opportunity to evaluate readiness and establish the right policies, security controls, and methods within a larger compliance context. Simply passing a PCI assessment leads some organizations to falsely assume they are safe from a breach and able to respond to an event should one occur.

Taking a holistic, lifecycle approach to PCI program management enables the organization to be proactive, while continuously improving compliance in the context of evolving business and security program needs. EMC® Consulting, leveraging the security and compliance expertise of RSA®, The Security Division of EMC, offers a range of services to help organizations accelerate compliance and respond to events rapidly and effectively. Our PCI program management lifecycle includes three main phases:

- PCI Program Strategy and Implementation
- PCI Readiness Assessments
- Breach Management Advisory and Post-Event Assessments

PCI PROGRAM STRATEGY AND IMPLEMENTATION

Many organizations struggle to demonstrate an approach to PCI program management that is strategically aligned to the business and provides measurable results. EMC Consulting has helped many organizations not only remediate their PCI compliance issues, but also develop a PCI program that is aligned with business objectives. Our PCI team will work with you to develop an entire security and compliance program or provide assistance with specific components to help your program become effective and sustainable. Our PCI Program Strategy and Implementation services include:

- Comprehensive strategy and program development for PCI compliance
- Program management of the end-to-end compliance process—from pre-assessment through PCI DSS compliance assessment performed by a third-party Qualified Security Assessor (QSA)
- Design of strategic frameworks for PCI program management that avoid spot solutions which do not fit within the fabric of your IT security, risk, and compliance program
- Assessment and development of processes, including workflows and reporting structures
- Development and implementation of security best practices included in daily security operational procedures, incidence response plans, and post-incident documentation
- Assigning ownership of the PCI DSS requirements to the appropriate teams
- PCI training to security teams, data owners, key stakeholders, and internal audit teams
- Bridging the gap between written and actual security practices
- Developing processes for event response, integrated with your crisis management, incident response, and security operations center
- Recommending automated platforms for compliance management

PCI READINESS ASSESSMENT

The challenge organizations face is not the PCI assessment process itself; the PCI Security Standards Council establishes clear requirements for self-assessment and the process for annual onsite PCI assessments conducted by PCI-certified QSAs. Rather, the true challenge is achieving readiness for the assessment by putting the right PCI DSS policies and controls in place to ensure compliance and protect cardholders from risk.

The correct approach to PCI compliance validation is a three-step process: assessment, remediation, and compliance. As in the accounting industry, best practice is to have one entity review the environment for compliance and assist the organization with any remediation, and a separate entity to provide review and attestation of compliance. By approaching PCI compliance with a detailed readiness gap analysis and remediation activities before any onsite assessment takes place, you can mitigate the risk of failing an assessment and incurring steep costs of non-compliance.

Deliverable	Description
Readiness Assessment	• Provides a clear understanding of compliance in relation to the PCI DSS • A spreadsheet format covers the exact elements of the PCI DSS to be leveraged as a remediation roadmap should the need arise • Reviews and documents any compensating controls in place
Remediation Roadmap	• Details identifying compliance or non-compliant gaps and sufficient direction to target those systems requiring remediation
Supplemental Findings Report	• Items that do not impact compliance, but are specific suggestions on improving your security posture

EMC Consulting's PCI Readiness Assessment can help you understand your current PCI DSS posture and develop a remediation strategy roadmap prior to undergoing a formal PCI assessment. The scope of PCI Readiness Assessment encompasses your entire cardholder data environment. Its objective is to uncover relevant and pertinent information that will enable management to address any PCI compliance issues and reduce risk and impacts to your cardholder data environment.

EMC Consulting uses a combination of interviews, data flow reviews, and site visits to identify systems that are in scope of PCI and to discover gaps and issues with your compliance to the PCI DSS requirement. We also review all documentation required by the PCI DSS, including (but not limited to) all policies, process, procedures, standards, vulnerability scan results, and penetration test results that support the cardholder environment. We then work with you to:

- Prepare a pre-assessment plan
- Determine and identify relevant programs per defined criteria
- Interview various program owners and work with your staff to gather required data
- Document, review, and confirm collected data with program owners
- Analyze collected program data based on defined criteria
- Report finding and recommendations

Findings and recommendations not only provide you with a comprehensive view of gaps and remediation steps to ensure compliance prior to an annual PCI assessment, but also identify measures beyond the standards that will increase your security and compliance posture. (Any recommendations that are not part of the PCI DSS are provided as a supplemental report and are not part of the readiness assessment report.)

EMC consultants provide the onsite and remote services necessary to complete the assessment activities and leverage EMC and RSA subject matter experts to provide as-needed assistance for review, quality assurance, and reporting purposes.

BREACH MANAGEMENT AND POST-EVENT READINESS ASSESSMENT

Even organizations that pass a PCI Readiness Assessment can be impacted by a breach of cardholder information—and discover only then that their incident response and crisis management processes are woefully inadequate.

After a breach occurs, organizations are required to hire a QIRA (soon a QFI) and undergo a breach investigation to determine compliance at the time of breach. Those findings are reported back to the acquiring bank and payment brands. The actions taken can determine the level of financial impact on an organization, yet even the best incident response plans do not provide step-by-step guidance on what an organization needs to do.

In the event of a breach, EMC Consulting's post-breach experts can interpret the findings of the QIRA and enable you to address critical remediation issues by making the best possible informed decisions during times of crisis and in the months that follow. Our Breach Management and Post-Event Readiness Assessment service provides guidance on:

- How to address a breach—even before you call for forensics help
- Addressing the fallout of a breach from both a technical and business perspective
- Addressing ramifications of a breach, weeks or months after the incident has occurred
- Developing and implementing plans to ensure that your organization is compliant going forward

PCI QUALIFICATIONS: EXPERTISE AND EXPERIENCE

EMC Consulting, leveraging the security expertise of RSA, combines deep PCI consulting experience with best-in-class services, products, and partnerships to provide an information-centric approach to proactively managing security for the payment card industry.

EMC Consulting's PCI consultants include former QSAs and current internal security assessors (ISAs), averaging more than 15 years of experience in the industry. Many have held security focused positions in well-known domestic and international enterprises, hold patents for specific process methodologies and internationally recognized certifications (including CISSP, CISA, CISM, and CGEIT), and have authored or contributed to information security books as well as published articles in business and security journals.

In addition, our consultants have participated in the creation of standards, working with bodies such as the PCI Security Standards Council, HITRUST, IETF, UN Pandemic Preparedness, HIMSS, NERC, CDC, and Information Risk Executive Council.

These professionals have a rich set of expertise and experience, including:

- Conducting onsite PCI assessments for some of the largest and most admired organizations in the world—in Level 1 environments of six million credit card transactions annually to over 24 million credit card transactions per day as well as in Level 2, 3, and 4 environments
- Helping manage the fallout for organizations that have experienced some of the largest cardholder data breaches in history
- Leading international remediation efforts requiring the management of global and local resources, and spanning online retailers (card-not-present transactions), brick-and-mortar retailers, travel and entertainment providers, hospitality, payment processors, and major payment brands
- Helping customers retain PCI compliance while transforming their IT service organizations as they transition to cloud computing environments

EMC CONSULTING FOR PCI PROGRAM MANAGEMENT

EMC Consulting understands the many obstacles that organizations face in maintaining and demonstrating PCI compliance and has the experience to help organizations determine areas at risk for failing a PCI assessment and effectively and efficiently remain in compliance. Clients benefit from our thorough review and recommendations on aspects of security programs that are most commonly found to be out of compliance, including:

- Vulnerability management
- Firewall reviews
- Penetration tests
- Monitoring
- Log management
- Change management
- User access
- Newly discovered repositories of cardholder data
- Application security
- Inaccurate data flows

Leveraging the security expertise of RSA, EMC Consulting combines deep PCI consulting experience with best-in-class services, products, and partnerships to provide an information-centric approach to proactively managing security for the payment card industry.

RSA is a global leader in authentication and security event management and GRC management platforms. We benefit from their deep insight into security architectures, concepts, and solutions. We have hundreds of certified security professionals who have delivered thousands of projects within some of the most information-intensive organizations in the world, meeting PCI challenges that other consulting organizations are just starting to consider.

EMC CONSULTING

As part of EMC Corporation, the world's leading developer and provider of information infrastructure technology and solutions, EMC Consulting provides strategic guidance and technology expertise to help organizations exploit information to its maximum potential. With worldwide expertise across organizations' businesses, applications, and infrastructures, as well as deep industry understanding, EMC Consulting guides and delivers revolutionary thinking to help clients realize their ambitions in an information economy. EMC Consulting drives execution for its clients, including more than half of the Global Fortune 500 companies, to transform information into actionable strategies and tangible business results.

CONTACT US

For more information, visit www.EMC.com/consulting, or contact your local EMC Consulting representative.

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

EMC² where information lives®