



OBTAINING BENEFIT FROM PCI



Security Connected

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.

Manual security and operational controls have a higher likelihood of failure and are a primary cause of increased compliance violations and costs.

PCI Compliance Drives Other Business Advantages

Challenges

Globalization. Economic uncertainty. Geopolitical risk. Cyberhacking. These are very serious issues that executives must manage in today's business environment. Add in the dynamic nature and growing set of requirements for regulatory compliance, and it's a wonder that any organization is able to thrive in today's market. In recent years, many cybercriminals have focused on accessing and stealing consumer credit card information from any retailer, merchant, bank, processor, or company. If your company accepts or stores credit card information, that data can be vulnerable to cyberthieves.

To address the increasing challenge of protecting sensitive customer credit card information, the Payment Card Industry Data Security Standard (PCI DSS, or PCI) was developed. It is a set of requirements designed to ensure that any company that processes, accepts, stores, or transmits credit card information maintains a certain level of security within its IT environment to appropriately protect cardholder data. PCI defines the following 12 high-level requirements under its category objectives:

Build and maintain a strong 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 antivirus software or programs.
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 for all personnel.

To meet these requirements, companies have invested significant time and resources implementing new processes and controls, along with point technologies, to ensure that they can demonstrate compliance. Overwhelmingly, the processes and controls were manual, and, as companies grew and the regulatory environment expanded, these manual controls were unsustainable and very costly to support. Companies remained in a tactical, reactive mode trying to maintain compliance, often failing as compliance violations and associated fines continued to increase. Point technologies tended to extend the challenge, as they often did not support critical IT systems, lacked coverage across the entire enterprise, and lacked analytic capabilities with a simple management console.



The PCI DSS Council manages the ongoing evolution of the PCI standards and is an independent body created by major payment card companies, including Visa, MasterCard, American Express, Discover, and JCB.

Solutions

The benefits of compliance management can be realized when you take a strategic approach to your compliance program. Since PCI provides prescriptive guidance on information security requirements, it is good starting point on which to build an effective compliance management program. The key is building a process that focuses on assessment, responsiveness, and monitoring; taking an enterprise view to ensure all critical, in-scope systems are covered; implementing management analytics for insights and prioritization; and automating key IT controls to minimize overlap and reduce cost.

This approach unifies fragmented processes, controls, and technologies and provides operational efficiencies across any compliance program. An effective program proactively and automatically assesses compliance, responds to issues or violations, and continuously monitors controls to ensure that you are constantly compliant. This moves you away from reactive tactics where you respond to violations that have already occurred to a strategic model where you identify and mitigate potential compliance violations.

Automate key controls

Manual controls are costly due to the high resource requirements and only provide “point in time” coverage that leaves you exposed to potential violations. By automating assessment, monitoring, and reporting controls, you can significantly reduce resource requirements and costs. Automated monitoring controls help maintain a continual state of compliance, ensuring that controls remain effective all the time. Finally, automated reporting provides immediate time-to-value and cost efficiencies in supporting regulatory and policy compliance requirements. Standardized templates feed PCI compliance reports that automatically compile data across agent-based and agentless systems, for a comprehensive,

efficient analysis on the state of compliance for an executive, manager, or auditor.

Ensure enterprise coverage

PCI covers myriad systems that are in scope for compliance, including point-of-sale systems, payment applications, ATMs, and databases where sensitive customer financial data is stored. An effective program delivers a technology platform that supports all of these systems, ensuring that controls can be assessed and managed across the infrastructure and ensuring that you will not be exposed to a potential violation due to lack of coverage.

An enterprise platform approach also helps consolidate a fragmented, point-product infrastructure and aligns core assessment, monitoring, and reporting functionality into a single management console. It drives efficiency by leveraging integrated, automated systems; reduces the complexity of multiple, overlapping systems and controls for individual regulations; and cuts costs.

Build management insight

Depending on the threat and the impacted system, potential compliance violations, issues, and threats can be prioritized and treated in multiple ways. Management analytics deliver insight into the priority, impact, risk, and associated cost of a potential violation. Drag-and-drop analytic dashboards enable anyone to automatically analyze and manage security threats and potential risks from a single user interface, across any device that is in scope for PCI.

Rather than spending resources trying to “fix” every violation or issue, you can now leverage automated analytics to get a deeper understanding of the root cause of an issue and the potential impact to your organizational strategy and performance, so you can make better decisions on how to best mitigate these threats.

Best Practices Considerations

- Focus on aligning and unifying fragmented compliance processes and controls
- Invest in automated capabilities to assess, respond, and monitor
- Consolidate your view and management of controls across your IT infrastructure
- Ensure your compliance program covers all in-scope systems and devices
- A single management platform pulls together all compliance information across the enterprise, allowing more efficient and effective management
- Continuous monitoring can help prevent any future compliance violation or risk event

Compensating controls can provide adequate coverage for any PCI or compliance requirement in the event that a key control fails. Management analytics help ensure that the compensating controls maintain the right level of effectiveness.

Value Drivers

PCI compliance may cost you time and money, but you can realize savings and competitive benefits by:

- Establishing a centralized control framework funded by PCI efforts that can be used for consistent auditing controls across a range of regulatory mandates and internal governance
- Prioritizing remediation based on PCI tasks and tracking that demonstrate success
- Leveraging PCI remediation to justify investments, rollouts, and new technologies
- Driving shareholder value through remediation. If new technologies cut remediation efforts in half because of mitigating controls, you save time, resources, and money
- Taking advantage of PCI as a differentiator: a track record of successful PCI audits is a competitive advantage

Related Material from the Security Connected Reference Architecture

Level II

- Controlling and Monitoring Change
- Protecting the Data Center
- Protecting Information

Level III

- Essential Protection for PCs
- Securing Removable Media
- Enforcing Endpoint Compliance
- Protecting Intellectual Property

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected.

About the Author



Dave Anderson is Senior Director of Security and Risk Management for McAfee, responsible for the global product marketing strategy for the McAfee risk and compliance business unit. Dave has nearly 20 years of global experience in information security, risk management, and strategy at leading enterprise technology and services companies, including SAP, ArcSight, KPMG, and VeriSign, where he has developed market and product solutions that integrate risk, compliance, security, and strategy into unified governance and risk frameworks. Dave's experience includes implementing and delivering IT governance solutions based on COSO, CobiT, ISO 27001, and ITIL standards. Dave has been published in multiple leading industry and technical journals and is a frequent speaker on risk management, corporate governance, and security strategy. Dave holds an MBA from Duke University with a specialty in global management and strategy.

dave_anderson@mcafee.com

