Providing stronger security practices that enable PCI Compliance and protect cardholder data.

Establish and Maintain Secure Cardholder Data with IBM Payment Card Industry Solutions

Highlights

- ***Offers pre-assessment service***
- ***Includes annual onsite PCI assessment with report on compliance (ROC)***
- ***Provides quarterly scanning services***
- ***Determines current vulnerabilities with penetration testing***
- ***Validates payment applications for PCI with application security assessment***

Secure consumer data and trust

For any organization that collects, stores or transmits personal cardholder data, security is vital to earning and maintaining trust. Identity theft, weekly headlines about data breaches and the perception of loose controls over personal cardholder information drove the payment card industry (PCI) to establish standards that would protect cardholder data from theft and misuse.

In September 2006, the PCI Security Standards Council (PCI SSC) was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International to “develop, enhance, disseminate and assist with implementation of security standards for payment account security.” Resulting from the efforts of this group, the PCI Data Security Standard (PCI DSS) has created common industry requirements for safeguarding cardholder data. Card issuers aggressively enforce PCI DSS with financial institutions and merchants. Failure to meet PCI DSS requirements can have widespread economic impacts for merchants and financial institutions.

Billions of credit cards lead to broad PCI compliance impacts

With more than 1.5 billion cards in circulation from Visa alone, PCI compliance requirements impact a large contingent. Merchants, service providers or other organizations that store, process or transmit cardholder data must conform to PCI requirements. Failure to comply can result in fines or increased transaction charges from merchant banks. Impacted industries include:

- *Retail – online sites, brick and mortar businesses, mail/telephone order*
- *Hospitality – restaurants, resorts, hotel chains*
- *Transportation – airlines, car rental, limo services*
- *Financial Services – banks, credit card processors, brokerages and insurance companies*
- *Healthcare/Education – hospitals, doctors, dentists, universities*
- *Telecommunications and Utilities– wireless, cable, electric, gas or water, etc.*

Establish and maintain PCI compliance and secure cardholder data using IBM PCI solutions

Since PCI compliance impacts any organization that touches consumer card data, service providers that process merchants' cardholder transactions are also subject to PCI DSS. While merchants and service providers are held to different standards based on card activity and services provided, they both face two key compliance issues:

1. Establishing and proving initial compliance
2. Maintaining compliance on an on-going basis.

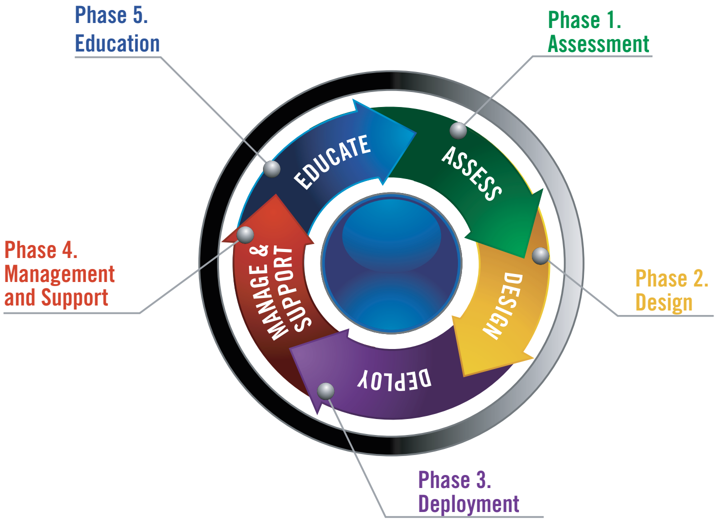
IBM Payment Card Industry solutions are designed to help businesses achieve and maintain PCI compliance in accordance with annual audits. Following best-practice guidelines, IBM supports organizations through the five phases of PCI compliance: assessment, design, deployment, management and support, and education. Using a phased approach helps organizations identify and fix root causes of non-compliance and establish internal controls to promote ongoing compliance year after year.

Throughout each phase of achieving PCI compliance, IBM consultants recognize common pitfalls that impede organizations from meeting PCI standards. Businesses should pay close attention to the following issues that deter successful compliance efforts:

- *Lack of encryption for e-mails and messaging*
- *Lack of encryption for data at rest*
- *Lack of knowledge about where all data resides*
- *Lack of segregation of duties*
- *Lack of adequate access controls (using generic, default and shared IDs)*
- *Lack of network segregation*
- *Back end operation networks often break the isolation of PCI networks*
- *Too many firewall rules with no business justification*
- *Insufficient documented policies and procedures*
- *Un-patched systems*
- *Storing sensitive magnetic stripe data*

From expert consulting, to assessment services, advanced security technology and managed security offerings, IBM solutions are designed to enable enterprise-wide compliance.

IBM's Five-Phased Approach to Achieving PCI Compliance



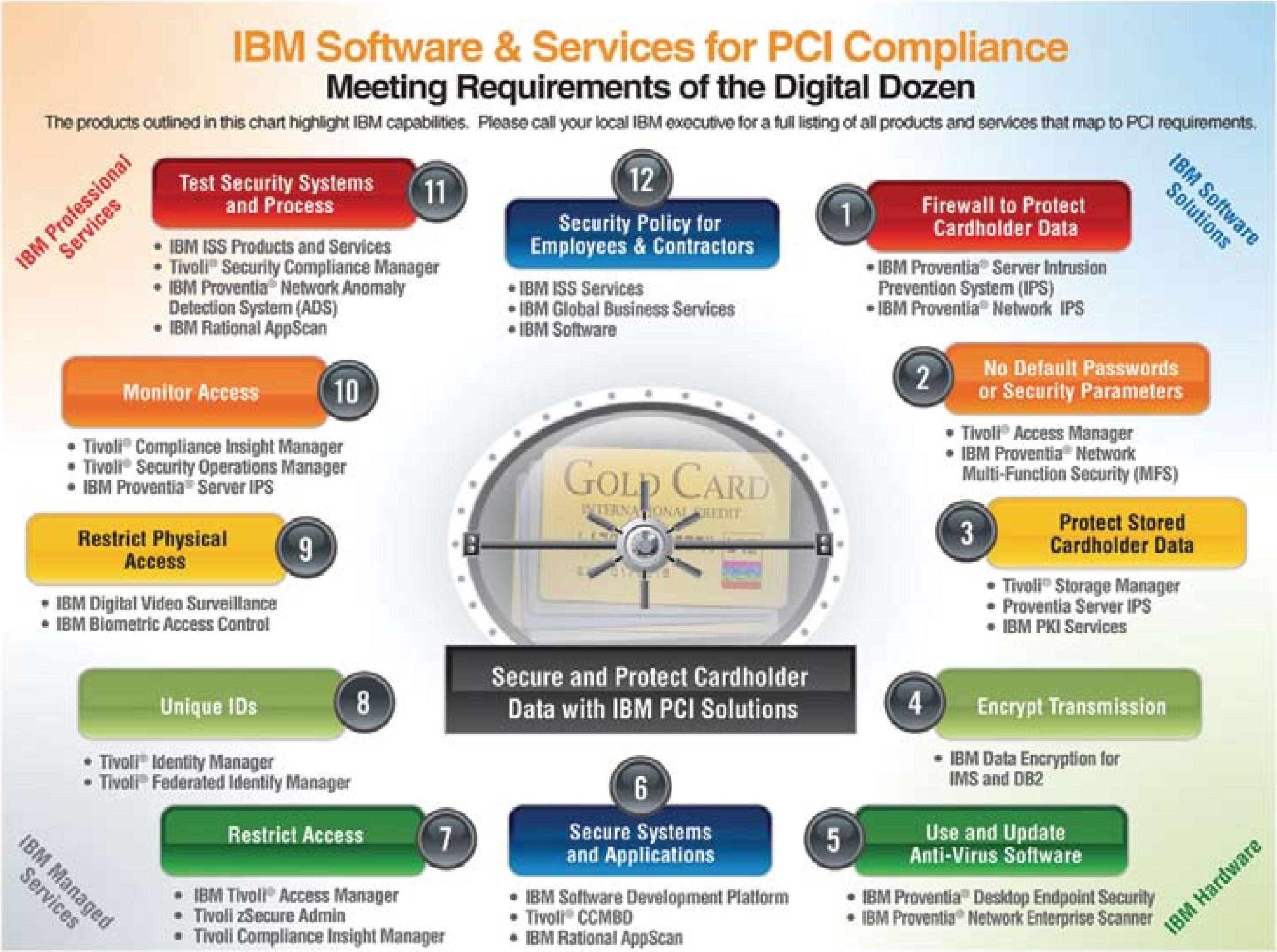
IBM products and services deliver PCI compliance solutions

Organizations may require both services and technology in order to meet PCI standards. IBM offers a variety of products and services designed to help businesses meet each of the 12 PCI requirements, referred to as "the digital dozen." IBM's PCI solutions help executives feel secure by establishing complete processes to safeguard cardholder data and satisfy the digital dozen.

The PCI DSS includes 12 requirements – referred to as "the digital dozen" – which organizations must meet each year in order to maintain PCI compliance.

The Payment Card Industry Data Security Standard	IBM PCI Compliance Solutions
Req 1. Install and maintain a firewall configuration to protect cardholder data	✓
Req 2. Do not use vendor-supplied defaults for system passwords and other security parameters	✓
Req 3. Protect stored cardholder data	✓
Req 4. Encrypt transmission of cardholder data sent across open, public networks	✓
Req 5. Use and regularly update anti-virus software	✓
Req 6. Develop and maintain secure systems and applications	✓
Req 7. Restrict access to cardholder data by business need-to-know	✓
Req 8. Assign a unique ID to each person with computer access	✓
Req 9. Restrict physical access to cardholder data	✓
Req 10. Track and monitor all access to network resources and cardholder data	✓
Req 11. Regularly test security systems and processes	✓
Req 12. Maintain a policy that addresses information security	✓

IBM Payment Card Industry solutions offer organizations the following benefits through software products and professional services:



IBM Software & Services for PCI Compliance

Meeting Requirements of the Digital Dozen

The products outlined in this chart highlight IBM capabilities. Please call your local IBM executive for a full listing of all products and services that map to PCI requirements.

IBM Professional Services

IBM Software Solutions

IBM Managed Services

IBM Hardware

11 Test Security Systems and Process
- IBM ISS Products and Services
- Tivoli® Security Compliance Manager
- IBM Proventia® Network Anomaly Detection System (ADS)
- IBM Rational AppScan

12 Security Policy for Employees & Contractors
- IBM ISS Services
- IBM Global Business Services
- IBM Software

1 Firewall to Protect Cardholder Data
- IBM Proventia® Server Intrusion Prevention System (IPS)
- IBM Proventia® Network IPS

10 Monitor Access
- Tivoli® Compliance Insight Manager
- Tivoli® Security Operations Manager
- IBM Proventia® Server IPS

2 No Default Passwords or Security Parameters
- Tivoli® Access Manager
- IBM Proventia® Network Multi-Function Security (MFS)

9 Restrict Physical Access
- IBM Digital Video Surveillance
- IBM Biometric Access Control

3 Protect Stored Cardholder Data
- Tivoli® Storage Manager
- Proventia Server IPS
- IBM PKI Services

Secure and Protect Cardholder Data with IBM PCI Solutions

8 Unique IDs
- Tivoli® Identity Manager
- Tivoli® Federated Identify Manager

4 Encrypt Transmission
- IBM Data Encryption for IMS and DB2

7 Restrict Access
- IBM Tivoli® Access Manager
- Tivoli zSecure Admin
- Tivoli Compliance Insight Manager

6 Secure Systems and Applications
- IBM Software Development Platform
- Tivoli® CCMBD
- IBM Rational AppScan

5 Use and Update Anti-Virus Software
- IBM Proventia® Desktop Endpoint Security
- IBM Proventia® Network Enterprise Scanner

Comprehensive PCI solutions and services – from assessments, consulting, incident response and managed services, IBM combines the skills of security experts with provensolutions to help build effective programs that protect systems and customer data.

Significant presence and reach in vertical industries – proven experience serving a wide variety of vertical industries makes IBM well-suited to helping all types of organizations meet PCI compliance requirements.

Access to security expertise – IBM's elite team of security experts comprises senior security professionals who have honed their skill through corporate security leadership, security consulting, investigative branches of the government, law enforcement, research and development.

Customized solutions – IBM consultants partner with the client's key staff and management members to design a customized plan that meets the client's specific security goals.

Specialized skills and tools – IBM consultants combine proprietary and industry-leading security assessment tools with in-depth analysis of vulnerability data to evaluate and build an effective security program.

Leading managed services – IBM delivers one of the most comprehensive managed security services portfolios in the industry designed to transfer the burden of managing security in-house to a trusted security expert.

IBM solutions for PCI Compliance begin with an assessment

Often, organizations are too close to their own systems to identify all compliance items that qualified independent security assessors routinely evaluate. A better approach uses qualified third party assessors to conduct an initial assessment of the IT environment against PCI standards. From there, consultants can help organizations remediate problems, enhance security technology and improve security policies in order to meet PCI DSS requirements.

IBM Professional Security Services deliver expert security consulting to help organizations of all sizes reduce risk, achieve regulatory compliance, maintain business continuity and reach their security goals. IBM Internet Security Systems (ISS) is globally recognized as a PCI Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV), and is well-qualified to help enterprises comply with the PCI DSS requirements.

As the logical first step to compliance, the IBM PCI assessment offering comprises the following services:

Pre-assessment – a customized gap assessment determines the current level of compliance and outlines the specific steps required to effectively achieve PCI DSS compliance before performing the formal assessment.

Annual onsite PCI assessment with report on compliance (ROC) – provides a comprehensive evaluation of the organization's information security program according to PCI specifications for networks, servers and databases involved in the transmission, storage and processing of credit card data.

Quarterly scanning services – includes a vulnerability assessment to help ensure and validate that proper security precautions are in place.

Penetration testing – demonstrates a real-life network attack to determine current vulnerabilities and analyze how attackers significantly impact a business.

Application security assessment for payment application providers – validates payment applications for PCI (as a Qualified Payment Application Security Company, IBM ISS has met the requirements to perform PCI payment application security assessments)

IBM Internet Security Systems PCI Certifications and Expertise

- *Qualified Data Security Company (QDSC)*
- *Qualified Security Assessor (QSA)*
- *Approved Scanning Vendor (ASV)*
- *Qualified Payment Application Security Company (QPASC), having met the requirements to validate payment applications.*
- *Qualified CISP Incident Response Assessor. IBM ISS is qualified to provide incident response and forensic analysis in the event of a security emergency.*

IBM ISS solutions for PCI compliance

Products and services from IBM Internet Security Systems™ (ISS) help to create stronger security practices that enable PCI compliance and protect cardholder data.

IBM Professional Security Services – deliver comprehensive, enterprise-wide security assessment, design and deployment services to help build effective network security solutions. Using the penetration testing services to meet requirement 11, PSS simulates covert and hostile network attacks to identify specific vulnerabilities in the protection of an organization's sensitive data. IBM Professional Security Services help clients quickly set security roadmaps and identify steps required for PCI compliance.

IBM Proventia® Server Intrusion Prevention System (IPS) – identifies and blocks known and unknown threats and helps enforce corporate security policies for servers. Proventia Server IPS combines a local firewall, intrusion detection and prevention system, and application integrity monitoring to protect servers and help clients adhere to regulatory compliance standards. Proventia Server IPS assists with PCI requirements 1, 5, 6, 10 and 11.

IBM Proventia Network Enterprise Scanner – helps clients manage the vulnerability lifecycle, from initial scanning through remediation. Proventia Network Enterprise Scanner provides internal security departments with the same tools external auditors use when assessing the network for risk. Proventia Network Enterprise Scanner assists with PCI requirements 6 and 11.

IBM Proventia Desktop Endpoint Security – combines a personal firewall, intrusion prevention, buffer overflow exploit prevention, application protection and virus prevention in a single agent. It protects desktops and helps clients adhere to corporate standards while blocking attacks before they can cause outages, employee downtime and excessive calls to the helpdesk. Proventia Desktop assists with PCI requirements 5 and 6.

IBM Protection Platform Products – integrated products complement and support the family of IBM products. Proventia Management SiteProtector provides centralized command, control and correlation of a broad array of network security agents and appliances including Proventia Network Anomaly Detection System, Proventia Network Multi-Function Security (MFS), and IPS products.

IBM Managed Security Services – assist customers by providing 24x7x365 management and monitoring of firewalls and IDS/IPS devices, directly addressing PCI requirement 1 with a service option. IBM's Managed Security Services include IBM Vulnerability Management Service, the IBM Security Event and Log Management service and IBM Managed Protection Services. Clients can access reporting and workflow through the MSS Customer Portal. The portal can also be used to correlate security and network events to more easily address PCI requirements 1, 5, 6, 10, 11 and 12. IBM Managed Security Services along with IBM products can aid PCI compliance efforts.

IBM Tivoli Security and Compliance Software Solutions

Tivoli products assist with a variety of PCI requirements. Tivoli software enables organizations to deliver service excellence in support of business objectives through integration and automation of processes, workflows and tasks.

IBM Tivoli® Access Manager for e-business and IBM Tivoli Identity Manager – help businesses define and manage a centralized authentication, access and audit policy. The solutions also establish a new audit and reporting service that collects audit data from multiple enforcement points as well as from other platforms and security applications to assist with PCI requirements 6, 8 and 12.

Tivoli Compliance Insight Manager – serves as a key component of IBM's compliance management offering that helps clients monitor the activity of privileged users. The product collects, centralizes and archives relevant security log data from heterogeneous sources, filtering collected information against requirements and corporate security policies, and provides consolidated viewing and reporting through a central, compliance-oriented dashboard. Tivoli Compliance Insight Manager can help you to reduce audit preparation time and meet monitoring requirements to assist with PCI requirements 10 and 11.

Tivoli Identity Manager (TIM) – provides a security-rich, automated, policy-based user management solution. It helps enterprises set up new accounts and passwords quickly for employees and customers, validate every user account on every resource, and allows for users to reset and synchronize their own passwords to efficiently gain access to valid resources. With TIM, clients can address PCI requirements 2 and 8.

Tivoli Security Compliance Manager – acts as an early warning system by identifying security vulnerabilities and security policy violations. Tivoli Security Compliance Manager helps organizations meet PCI requirement 6 to define and monitor consistent security policies. Security policies can be based on both internal security requirements and industry-standards.

Tivoli Security Operations Manger – centralizes and stores security data throughout the IT and operations infrastructure and provides a platform from which to automate incident recognition and response, streamline incident handling, enable policy monitoring and enforcement, and provide comprehensive reporting for regulatory compliance. The end result is an efficient, cost-effective approach to security operations that addresses PCI requirement 10.

Tivoli zSecure suite – helps ensure the security of mainframe systems by automating administration and auditing. Consisting of modular components, the zSecure suite enable enterprises to administer a mainframe, monitor for threats, audit usage and configurations, and enforce policy compliance. Tivoli zSecure Audit, a component of the Tivoli zSecure suite, offers the capability to fingerprint sequential log data residing on both tape and direct access storage device (DASD) media to check the integrity of System Management Facility (SMF) logs. Tivoli zSecure provides critical reporting about compliance efforts for PCI requirements 1, 2, 10, 11 and 12.

Learn how IBM Payment Card Industry solutions can secure cardholder data

With a broad product and service portfolio, industry expertise and a deep understanding of PCI requirements, IBM delivers the level of support organizations need to achieve and maintain PCI compliance. With its combined solutions, IBM helps companies evaluate their overall security posture and implement proper controls and security technology to meet the PCI DSS regulations.

For more information on IBM software and services for PCI compliance:

- *Visit ibm.com/itsolutions/governance*
- *Contact Ask Security Solutions at askss@us.ibm.com*
- *Call 1-800-IBM-4YOU*

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
09-07

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.