Security management solutions for merchants
White paper

Tivoli® software

Support PCI security compliance with enhanced solutions from IBM.

September 2007

Contents

Overview

The world has embraced payment cards to support commercial transactions for almost every kind of business. Unfortunately, the data associated with these payment cards is the focus of many identity theft activities, including online hacking, illegal actions by company employees and the physical theft of media such as storage tapes.

The Payment Card Industry (PCI) Data Security Standard (DSS) has been designed to protect the personal information of credit card holders. This white paper briefly describes PCI requirements, the benefits of compliance and the penalties for noncompliance. It shows how IBM supports PCI compliance efforts through a combined offering of software, hardware and services. IBM offers compliance gap analysis, remediation, validation, ongoing testing and reporting, as well as a range of products that help organizations develop integrated, end-to-end processes that encompass each aspect of security planning, management and compliance reporting.

Review PCI requirements

More than one billion people use at least one type of payment card, which supports commercial transactions in almost every business worldwide.[1] Account data and personally identifiable information, referred to in the standard as "cardholder data," is the focus of many identity theft activities, including online hacking, the physical and logical theft of databases stored on a variety of media and other illegal actions by trusted insiders.

The PCI DSS is designed to protect cardholder data. The standard is based on 12 data-centric requirements that are designed to ensure the six objectives listed on the next page.

PCI Data Security Standard	
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across public networks open
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

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

These requirements combine the use of data encryption and end-user access control with activity monitoring and logging. The standard, supporting documentation and a complete description of these objectives are available from the PCI Security Standards Council at www.pcisecuritystandards.org.

Recognize critical PCI compliance deadlines

Today, a significant number of merchants are still not fully compliant. As of December 2006:

- Only 36 percent of Level 1 merchants (six million or more credit card transactions annually) were PCI compliant.
- Only 15 percent of Level 2 merchants (one to six million credit card transactions annually) were PCI compliant.

Highlights

These figures clearly show that in 2007, compliance will be a critical initiative for acquiring banks (acquirers) and their merchants. Deadlines are in place, and the penalties for noncompliance can be severe. The Visa PCI Compliance Acceleration Program (CAP) states that acquirers will be fined between $5,000 and $25,000 a month for each of its Level 1 and 2 merchants who have not been validated:

- By September 30, 2007, for Level 1.
- By December 31, 2007, for Level 2.

In addition, the Visa PCI CAP includes acquirer fines for data compromises involving merchants of any size. In 2006, Visa levied $4.6 million in fines, up from a total of $3.4 million in 2005.

On the other hand, significant incentives for PCI compliance are now available for acquirers. Visa has invested $20 million in an incentive fund payable to the acquirers of the largest U.S. merchants who have already or will validate PCI compliance by August 31, 2007, provided they have not been involved in a data compromise.

Visa is also linking the benefits of tiered interchange rates to PCI compliance, creating an additional security incentive for acquirers of large merchants. Additionally, acquirers whose Level 1 and 2 merchants validate compliance after March 31, 2007, and prior to August 31, 2007, will be eligible to receive a reduced one-time payment for each qualifying merchant.

For merchants, the penalties and incentives regarding PCI compliance are significant

For merchants, the penalties – and incentives – regarding PCI compliance are significant. Failure to comply with the security standard, promptly rectify a security issue or report a compromise can result in:

- Possible restrictions on the merchant by the card associations.
- Permanent prohibition of the merchant's participation in card association programs.
- Violation of applicable federal or state laws.
- Required compensation for fraud losses perpetrated by the use of account numbers associated with the compromise.

By supporting and adhering to the PCI standard, merchants and other organizations can help:

- Encourage stronger customer relationships.
- Reduce lost sales and revenue due to the theft or corruption of cardholder data.
- Build consumer confidence.
- Support the development of new markets, including e-commerce.

Initiate PCI compliance efforts

PCI compliance is a complex, ongoing process. Based on our experience with clients, IBM recommends an approach that includes gap analysis, the implementation of automated, integrated compliance solutions, and ongoing monitoring and assessments.

Analyze compliance gaps

Accurate gap analysis lays the foundation for compliance efforts. Based on research, surveys and our work with merchants and acquirers around the world, IBM has found that today's compliance gaps are often based on one, or a combination, of the following factors:

- Lack of segregation of duties
- Lack of adequate access controls (for example, generic, default and shared IDs)
- Lack of network segregation
- Back-end operation networks that often break the isolation of PCI networks
- Too many exceptions to firewall policy with no business justification
- Insufficiently documented policies and procedures
- Unpatched systems
- Unsecured storage of sensitive magnetic stripe data
- Lack of proper log management and user access monitoring
- Lack of encryption for data in motion (e-mails and messaging) and data at rest
- Lack of knowledge about where the data is at rest

Highlights

Without proper automation and integration, PCI compliance can be a labor-intensive process

Automate controls

Without proper automation and integration, PCI compliance can be a labor-intensive process. Gartner predicts that by 2011, companies pursuing a risk-oriented approach to compliance, standardization of controls and automation will reduce their manual process controls by 70 percent.[2] At the same time, companies that select individual solutions for each regulatory challenge they face will spend 10 times more on the IT portion of compliance projects than companies that take an integrated approach.[3]

Accordingly, companies should develop their compliance initiatives based on cost-effective, automated solutions that are tightly integrated to provide holistic, enterprise-wide security and compliance management that is platform agnostic.

Implement ongoing assessments

IBM provides certification, software and services required for ongoing assessments, testing and many of the reports required in the process.

Through IBM Internet Security Systems (ISS), IBM is a Qualified Security Assessor (QSA) and an Approved Scanning Vendor (ASV), having met the requirements to perform PCI data security assessments. IBM assessments are conducted by Qualified Data Security Professionals (QDSPs) who have in-depth experience in compliance requirements.

IBM is also recognized as a Qualified Payment Application Security Company (QPASC) and has met all requirements to perform PCI Application Security Assessments to validate payment applications. These assessments are conducted by IBM experts who are Qualified Payment Application Security Professionals (QPASPs).

The professional service process assisting with PCI compliance includes the following steps:

- **Pre-assessment testing and remediation recommendations.** A customized gap assessment is performed to determine the current level of compliance with specific requirements of PCI standard compliance.
- **PCI assessment with report on compliance.** This assessment delivers a comprehensive evaluation of an 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. If required, the client will also receive a report on compliance, certifying compliance with PCI.
- **Post-assessment comprehensive report.** This report details strategic and tactical recommendations by IBM for maintaining compliance with PCI requirements and industry best practices.
- **Quarterly external PCI vulnerability scanning assessment.** Delivered four times a year, this comprehensive report delivers detailed Quarterly Scanning Assessment data and tactical recommendations for maintaining compliance with PCI requirements and industry best practices.
- **Penetration testing.** IBM assists with the annual penetration testing requirement. An annual penetration test (network and application level) is required as part of Requirement 11.
- **Payment application best-practices validation.** Onsite validation of credit card payment applications delivered by Visa QPASP–certified professionals.
- **Ongoing assessments.** A monitoring system can be implemented to deliver baseline assessments of compliance on a regular basis.

Explore IBM offerings for enhanced PCI compliance solutions

Along with regular testing and revalidation for PCI compliance, organizations naturally want to find more efficient and cost-effective ways to support compliance. This goal can be supported through improved automation, best practices and software solutions designed to help optimize security, accurately gather data and quickly generate comprehensive reports.

Highlights

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 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 offers a unique capability to customers in being able to provide both services and products to support all 12 PCI requirements.

IBM offers both services and products to support all 12 PCI requirements

IBM offers both services and products to support all 12 PCI requirements. Because IBM is a merchant, a service provider, a hosting provider (levels 1–4) and a QPASP, we have broad-based, multilevel expertise that gives us a deep understanding of both the issues facing our customers and the technology solutions that can be used to address these issues.

Consequently, IBM solutions can help organizations streamline and enhance the full range of PCI compliance efforts, as outlined below:

Requirement 1: Install and maintain a firewall configuration to protect cardholder data
This requirement calls for the use of firewalls for all Internet-based traffic regardless of whether the traffic is from customers, business partners or employees. The company must put processes in place to regularly review and

justify the configuration of the firewalls to guard against unknown routes through the firewall that might be exploited. In addition, the standard indicates that "adequate network segmentation" can reduce the size of the cardholder environment and therefore limit the scope of the PCI requirements.

IBM Managed Firewall Service can be used for outsourcing all firewall services, including the firewall management requirements needed to ensure compliance to PCI. For companies that want to manage their own firewalls, IBM Tivoli® Application Dependency Discovery Manager can help create a "network map" of the IT components – including the location of firewalls – as specified by PCI requirements.

IBM Tivoli Change and Configuration Management Database (CCMDB) can be used to standardize the processes for making changes to firewalls. IBM Tivoli Security Compliance Manager can be used to monitor firewall configuration files, ensuring that they have not been modified outside of the standardized processes. IBM Tivoli Security Operations Manager can be used for correlating firewall data.

The IBM Proventia® family of hardware and software products also provides integrated firewall technologies along with intrusion prevention capabilities to assist in blocking attacks to the network, server and desktop end points of a merchant.

Attacks against a system can come from within an enterprise's network as well as externally. The IBM z/OS® Communications Server can safeguard the availability of the system by protecting against denial-of-service attacks. There are built-in defenses and optional services, such as Intrusion Detection Services (IDS), which can defend against attacks from the network.

Highlights

Integrated communications services from IBM Global Technology Services offer a network design solution that can be used to analyze the network environment and help a company design network zones to isolate systems that contain cardholder data. This can possibly help reduce the scope of PCI requirements.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

One of the most commonly exploited vulnerabilities in IT environments concerns vendor default passwords

One of the most commonly exploited vulnerabilities in IT environments concerns vendor default passwords

One of the most commonly exploited vulnerabilities in IT environments concerns vendor default passwords. These default passwords are readily available on the Internet, and criminals regularly test target machines to see if they are configured with the default passwords. Requirement 2 stipulates that the company must put procedures in place to ensure that default passwords are changed. It also requires that tests be performed to ensure that default passwords are not used in the cardholder data environment.

IBM Tivoli Release Process Manager and the IBM Tivoli Provisioning Manager family of products can be used to help ensure that default passwords are changed as part of the deployment process. IBM Tivoli Identity Manager and IBM Tivoli Access Manager for Enterprise Single Sign-On also help in the management of passwords and adherence to password policy. In addition, Tivoli Identity Manager can help by provisioning accounts in a manner that matches organizational security policy, rather than defaulting to vendor-supplied settings, and deprovisions accounts when employees leave – thereby maintaining tight control over access to sensitive data.

For IBM System z™ environments, IBM Tivoli zSecure Audit can be used to ensure that default passwords are not being used. IBM ISS Penetration Testing Services can test deployed IT environments for the presence of default passwords.

In addition, Requirement 2 calls for the enforcement of a "one primary function per server" rule to ensure that each deployed IT component is not compromised by the presence of other software on the server. The IBM Integrated Communication Services Network Design offering can be used to design a network environment that conforms to this principle. Tivoli Security Compliance Manager can be used to monitor software and processes that are present on the server but do not belong there according to the established policy.

Requirement 3: Protect stored cardholder data

Compliance with Requirement 3 involves the secure management of data storage by a company. This includes secure procedures for the storage and use of data, backed by key-based encryption of stored data. The requirement specifies that the keys used for encryption be protected against both disclosure and misuse. It also specifies that companies fully document and implement all key management processes and procedures.

To address these needs, IBM provides an ISS Information Security Assessment service to help with cardholder data discovery. IBM Global Technology Services offers Integrated Lifecycle Management services to help manage the overall usage of data from collection to destruction.

The encryption infrastructure of the System z mainframe is used by the most demanding enterprise customers to deliver encryption solutions with the simplicity of centralized management. This includes encryption built into every engine, highly resilient encryption key management built into z/OS and an optional tamper-resistant encryption module to protect encryption keys from detection with highest certification at FIPS 140-2 Level 4. Encryption solutions include options for protecting data over the Internet using industry standards

with specialty engine support, IBM DB2® and Information Management System (IMS™) database encryption options to help protect data at rest.

Other IBM system platforms also offer encryption technologies to support encryption over the Internet and encryption of data files.

IBM also offers a wide variety of encryption technologies for different computing environments. IBM System Storage™ TS1120 Tape Drives are designed to protect data on tape. The System z mainframe with tamper-resistant key processing and resilient key management features in z/OS can be used for strong yet flexible key management. IBM Tivoli Storage Manager provides encryption capabilities at the backup/archival object level. IBM also offers DB2 software and IBM Encryption Tool for IMS and DB2 for database-level encryption, as well as encryption cards for IBM AIX® and other servers to further support encryption requirements. For customers who leverage disk-based encryption for PCI compliance, IBM Tivoli Access Manager for Operating Systems can provide the appropriate separation of logical access to support the requirement.

The IBM DB2 Test Database Generator tool can create privacy-enhanced versions of databases to be used in software development and testing so that developers do not have access to sensitive data. IBM also offers powerful document-level encryption through its IBM Lotus Notes® solutions. IBM Tivoli Compliance Insight Manager manages all security logs and enables a proper review of who accessed which cardholder data in storage.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Just as Requirement 3 calls for the protection of cardholder data when it is stored or persisted, Requirement 4 calls for the protection of cardholder

data when it is transmitted – typically using either message encryption or transmission channel encryption.

IBM WebSphere® Application Server provides an implementation of Java™ Secure Socket Extension to encrypt data on TCP connections and Java Cryptographic Extension for more general-purpose encryption needs. These toolkits can be used by applications to protect cardholder data. WebSphere Application Server also provides transmission security at both the data and connection level with its implementation of WS-Security standards.

IBM systems provide support for industry-standard network encryption options including SSL and IPSec. The System z mainframe provides end-to-end encryption (IPSec) across heterogeneous platforms and devices which can use a specialty engine to help reduce the cost of providing this level of security.

Also using XML Web services standards like WS-Security, IBM WebSphere DataPower® XML Security Gateway XS40 can be deployed internally between applications or departments and in a company's perimeter network or DMZ to encrypt, decrypt and digitally sign messages prior to sending to the application server. Like an IP firewall, this provides a hardware-based first line of security enforcement and threat protection for XML, Web services and SOA applications. Additionally, this security can be applied to an entire Web services message or within fields of the message – a credit card field for example – for very granular control. IBM Tivoli Access Manager for e-business can protect access to sensitive data over the Web – through enforcement of access control policy and SSL encryption for data transfers. For IBM WebSphere MQ messaging environments, IBM offers IBM Tivoli Access Manager for Business Integration to provide encryption and access control for MQ-based messages.

Highlights

All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers and viruses

Requirement 5: Use and regularly update anti-virus software

This requirement calls for the use of antivirus software "on all systems commonly affected by viruses." Requirement 5 does not limit its antivirus requirement to systems that actually process cardholder data but includes all systems connected to the network where machines that process cardholder data are present.

IBM Proventia Network Multifunction Security provides network-based protection against virus activity while IBM Proventia Desktop Endpoint Security and IBM Proventia Server Intrusion Prevention System (IPS) can be used to enforce antivirus software policies at the desktop and server level as part of granting access to the internal network. The Tivoli Provisioning Manager family of products can be used to standardize the deployment of antivirus software to machines in your environment. Tivoli Security Compliance Manager can be used as a tool to monitor and audit whether or not the required software and processes are running on the systems, including the appropriate antivirus software version and the proper signature files. Tivoli Security Operations Manager enables correlation of antivirus logs to assist with the demonstration of compliance to auditors.

Requirement 6: Develop and maintain secure systems and applications

All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers and viruses. This requirement covers topics such as secure coding practices to ensure that the developed software does not have vulnerabilities that can be exploited by hackers.

IBM offers the IBM Rational® Software Development Platform family of products to help ensure secure coding practices across the software development lifecycle. The development platform includes a suite of

testing tools to create both automated and manual test environments. The development platform also includes IBM Rational Purify,® which can be used to look for application vulnerabilities even when the source code is not available. To help create a wall of separation between development and production environments, IBM DB2 Test Database Generator creates privacy-enhanced versions of databases.

IBM ISS provides an Application Security Assessment service to examine the design of software applications for vulnerabilities and provides multiple products that can identify unpatched systems for remediation. IBM Global Technology Services offers a Secure Solution Design solution that isolates and identifies security issues across the entire application lifecycle.

To manage the transfer of software assets from the development team to the production environment, IBM offers Tivoli CCMDB and Tivoli Release Process Manager solutions that govern the deployment of software into the production environment based on IT Infrastructure Library® (ITIL®) best practices.

Tivoli Provisioning Manager as well as Tivoli Security Compliance Manager can be used to verify that the proper software patches are installed – and if they are not, Tivoli Provisioning Manager can schedule the installation. Tivoli Security Compliance Manager can provide an ongoing monitoring solution for software and security patch compliance.

When exposing legacy applications as Web services or SOA components, WebSphere DataPower Integration Appliance XI50 can provide secure SOA enablement of mainframe systems, instantly connecting them to enterprise SOA and Web services while providing access control and policy enforcement as well as XML Web services encryption, decryption and digital signatures.

Highlights

IBM offers a variety of products that can be used to control access to data and monitor user patterns for violations of policy

Requirement 7: Restrict access to cardholder data by business need-to-know

This requirement covers access control issues at all levels of the IT environment. It specifies the adoption of a default, "deny all" policy for accessing data via any mechanism, as well as a policy that identifies the conditions under which cardholder data may be accessed and used.

IBM offers a variety of products that can be used to control access to data and monitor user patterns for violations of policy. The IBM Tivoli Access Manager family of products provides an industry-leading authentication and authorization framework that can be used to control access to applications where cardholder data is accessed. WebSphere DataPower XML Security Gateway XS40 is a power security and policy-enforcement point for controlling access to XML Web services, enabling the XS40 to seamlessly integrate with all types of access control architectures, such as IBM Tivoli Access Manager or Tivoli Federated Identity Manager. For System z environments, IBM Tivoli zSecure Admin can be used to manage access control policies. IBM Tivoli Identity Manager can automate the provisioning and deprovisioning of user accounts to ensure that access control policy is enforced and maintained.

IBM offers the Tivoli zSecure family of products and Tivoli Compliance Insight Manager to monitor privileged-user database access activity and compare these behavior patterns against acceptable use and security policies. In addition, for database-level protection, IBM offers IBM DB2 Audit Management Expert. For document- and process-level controls, Lotus Notes and IBM FileNet offerings protect sensitive information accessed as part of business processes.

Requirement 8: Assign a unique ID to each person with computer access

Covering the accountability aspect of controlling access to cardholder data, Requirement 8 specifies that every person's activities on a network containing cardholder data be uniquely identifiable. This helps identify users who abuse access to cardholder data. Tivoli Federated Identity Manager can perform credential validation, mapping and translation across an SOA environment, so that all transactions can be directly traced back to the user requesting them across a wide variety of new and legacy systems.

Tivoli Identity Manager can help standardize the processes for provisioning users with credentials and access based on policy established by the organization. Tivoli Identity Manager can create and provision accounts in a wide variety of systems commonly found in IT environments. IBM also offers Tivoli zSecure Admin to address the specific needs of System z environments. Additionally, Tivoli Compliance Insight Manager aggregates the logs from operating systems, applications and databases. These logs are correlated to user information, showing whose IDs are being used and how.

To help develop the organizational policies that guide the provisioning processes, IBM offers the Role-Based Access Control (RBAC) Role Definition Service and the Security Policy Definition service.

Requirement 9: Restrict physical access to cardholder data

Any physical access to the data center allows access to both cardholder data and the systems that house it or even the opportunity to remove system components or hard copies. Consequently, physical access should be properly restricted. Accordingly, Requirement 9 specifies the use of appropriate facility entry controls to limit and monitor physical access to all systems that store, process or transmit cardholder data.

Highlights

IBM provides services that can help companies analyze, change and manage their physical environments in accordance with compliance requirements

To help address this requirement, the IBM Physical Security Services/IBM Digital Video Surveillance solution provides integrated video surveillance and security capabilities that enable authorized security personnel to view, monitor and digitally record activity throughout an environment.

IBM also provides site and facilities services, including the Data Center Strategy and Planning service as well as the Data Center Risk Analysis service. These services can help companies analyze, change and manage their physical environments in accordance with compliance requirements.

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical. This requirement mandates a process for linking all access to system components to an individual user. It also specifies the implementation of automated audit trails to reconstruct individual access and other activities.

For a central security audit log management capability that spans applications, operation systems, databases and the mainframe, many customers turn to Tivoli Compliance Insight Manager. From a single dashboard with strong drill-down capability, this solution enables companies to track, monitor and report on access to cardholder data across the enterprise.

IBM solutions also provide deep support in several other areas. At the data-repository level, IBM DB2 Audit Management Expert provides the ability to selectively audit inserts, updates, deletes and reads in DB2 systems. For servers, IBM Proventia Server IPS provides automated, real-time intrusion protection and detection by analyzing events, host logs, and inbound and outbound network activity on critical enterprise servers.

At the event infrastructure level, Tivoli zSecure Audit delivers a comprehensive mainframe compliance and audit solution that enables you to quickly analyze and report on mainframe events, and automatically detect security exposures through extensive status auditing. Tivoli Security Operations Manager provides a centralized platform for monitoring, analyzing and investigating security incidents and policy violations in real time. The Tivoli Security Operations Manager platform analyzes and correlates logs from across the IT infrastructure – including intrusion detection systems, firewalls, hosts and servers. The IBM ISS Security Event and Log Management Service compiles, archives, analyzes, correlates and trends security and network events, while managing your response and remediation workflow.

For networks, IBM Proventia Network Anomaly Detection System delivers a clear view of network behavior while automatically detecting active security threats, risky user behavior, performance issues and noncompliant activities, such as policy violations and unapproved network changes.

Requirement 11: Regularly test security systems and processes

This requirement specifies regular scanning and testing of systems, processes and custom software frequently to ensure security is maintained over time and through changes. Is a vulnerability scan or penetration test performed on all Internet-facing applications and systems before they go into production? Is an intrusion detection system/intrusion prevention system (IDS/IPS) used on the network? Are security alerts from the IDS/IPS continuous?

To maintain regular checks on the security status of the network – based on the rules established in the last assessment – a combination of Tivoli Security Operations Manager, Tivoli Compliance Insight Manager and Tivoli CCMDB can be used. Through powerful dashboards and reports, security administrators can quickly assess the security performance of the network.

IBM Proventia Network Enterprise Scanner can be used to support quarterly, external PCI vulnerability scanning assessments. The solution identifies network devices and analyzes the configurations, patch levels, operating systems and installed applications to find vulnerabilities that could be exploited by hackers trying to gain unauthorized access. Proventia Network Enterprise Scanner also includes vulnerability management and workflow for remediation activities and tracking, along with vulnerability checks specifically developed for PCI compliance.

For the development of an IDS/IPS solution, IBM offers an impressive range of solutions. IBM Proventia Server IPS applies built-in signatures and sophisticated protocol analysis with behavioral pattern sets and automated event correlation to prevent known and unknown attacks. The server security software offers multilayered protection for Microsoft® Windows,® Linux,® AIX, Hewlett-Packard HP-UX, Sun Solaris and VMware servers, keeping data and applications reliable, available and confidential. These solutions can be complemented in the System z mainframe environment with IDS provided in the z/OS operating system.

IDS/IPS solutions are also supported by IBM Proventia Management SiteProtector™, which helps enable PCI compliance efforts at several levels throughout the business. IBM Proventia Multifunction Security (MFS) combines industrial-strength intrusion prevention with firewall, virtual private network, behavioral and signature antivirus, Web filtering and antispam technologies. In addition, IBM Proventia Network Intrusion Prevention System offers preemptive protection for networks made possible by a unique combination of line-speed performance, multifaceted protection and unparalleled security intelligence.

For security testing, IBM provides Ethical Hacking – or penetration testing – services that can help reduce the risk of a hacker causing damage to the network by performing a range of intrusion tests with the same techniques known to be used by the most common hackers. Furthermore, IBM ISS Penetration Testing service can help determine a network's current vulnerabilities while demonstrating how attackers can significantly impact the business. ISS Penetration Testing is a safe and controlled exercise, performed by security experts, to validate existing security controls and to quantify real-world risk.

Requirement 12: Maintain a policy that addresses information security

Designed to establish a clear, strong security tone for the whole company, Requirement 12 specifies that companies establish, publish, maintain and disseminate a security policy that addresses all PCI requirements. Among other items, the requirement states that security policies must be formally documented and regularly reviewed. Roles and responsibilities need to be clearly defined, and background investigations need to be carried out on all employees with access to sensitive information.

The IBM Security Policy Definition service includes a careful review of PCI requirements and the associated priorities for the company, then the creation of a custom security policy to clearly demonstrate management's commitment to compliance. The IBM Security Standards Definition service can be used to develop custom security standards in accordance with PCI requirements.

Addressing a wide range of regulatory and business control challenges, the IBM Workplace™ for Business Controls and Reporting solution helps provide a common platform for companies to easily document, evaluate and report the status of controls management across multiple initiatives in the company.

In addition, the IBM Security Process Development service helps companies define and document the processes that support their PCI compliance efforts. The processes can be developed based on the organization's predefined information security standards in conjunction with the PCI standard.

Summary

IBM offers a unique capability to customers in being able to provide both services and products that support all 12 PCI requirements. IBM services include compliance gap analysis, remediation, validation, ongoing testing and reporting; and its software and hardware solutions contribute toward PCI compliance efforts and support other security needs by providing:

- Centralized security access monitoring and management.
- Detailed auditing and reporting on a quarterly and ongoing basis.
- Integrated security management across multiple, heterogeneous environments.

With IBM, organizations can develop integrated, automated, end-to-end processes that encompass a full range of security planning, management and compliance reporting. Consequently, IBM solutions can help organizations streamline and enhance their PCI compliance efforts.

For more information

To learn more about IBM solutions and support for PCI, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/itsolutions/security

About IBM solutions for enabling IT governance and risk management

IBM enables IT organizations to support governance and risk management by aligning IT policies, processes and projects with business goals. Organizations can leverage IBM services, software and hardware to plan, execute and manage initiatives for IT service management, business resilience and security across the enterprise. Organizations of every size can benefit from flexible, modular IBM offerings that span business management, IT development and IT operations and draw on extensive customer experience, best practices and open standards–based technology. IBM helps clients implement the right IT solutions to achieve rapid business results and become a strategic partner in business growth. For more information about IBM Governance and Risk Management, visit **ibm.com**/itsolutions/governance

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
9-07

[1] PCI Security Standards Council.

[2] Gartner: “The 2007 Compliance and Risk Management Planning Guidance: Governance Becomes Central” by French Caldwell, April 12, 2007.

[3] Gartner: “Audits and Events Drive Governance, Risk and Compliance Spending” by Tom Eid, French Caldwell, March 2, 2007.

Disclaimer: Each IBM customer is responsible for ensuring its own 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 its business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its products or services ensure compliance with any law or regulation.

TAKE BACK CONTROL WITH **Tivoli.**

TIW10409-USEN-00