

WIPRO PCI DATA SECURITY STANDARD COMPLIANCE SOLUTION



Transactions made
smooth and secure

Business Challenge

A Gartner survey revealed that one in twenty consumers have been the victim of credit card fraud in the past year. According to the Federal Trade Commission, 10 million consumers were victims of identity theft in 2003. The FTC estimates that the total impact associated with these crimes approach \$50 billion per year. Similar studies estimate that the total impact associated with these crimes approach \$50 billion per year. Identity theft, a popular form of credit card fraud, is a growing crime in the US. A study by the Gartner Group suggests these trends will continue, expecting "mass victimization" of consumers over a period of the next two years, and suggests that "consumers be extra careful to monitor all their financial transactions for unexplained account activity, withdrawals, or fund transfers".

Enterprises throughout the world store sensitive, credit card information associated with customers, employees and partners in their information systems. Many of these systems do not have adequate security controls. These systems are not only vulnerable to data thefts and misuse. Many Enterprises do not have privacy policies embedded in their security frameworks on the storage, usage and sharing of personal data. This may lead to legal consequences as cardholder protection laws such as the Visa's Cardholder Information Security Program (CISP) and the Payment Card Industry (PCI) Data Security Standard, which was jointly developed by VISA and MasterCard are being widely enforced around the world.

What is PCI?

PCI is a standard for securing credit cardholder data. It applies to all members, merchants and service providers that store, process or transmit cardholder data. Security requirements apply to all system components, which encompasses any network component, server or application included in or connected to the cardholder data environment. The PCI standard has been endorsed and adopted by payment brands like MasterCard, VISA, American Express, Diners Club, Discover and JCB International. The Cardholders Information Security Program (CISP) uses the PCI Data Security Standard as its framework. It consists of 12 aggregate security requirements and 175 sub-requirements grouped into 6 areas.

PCI Standard Framework

- Build and Maintain Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

Key Challenges in meeting PCI Compliance

- Effective User Authentication and Identification system
- Data classification as a basis for robust access control framework for users
- End-to-end encryption on the media handling cardholders data
- Keeping up-to-date with new vulnerabilities
- Sustainable Event/LOG Monitoring
- Minimizing impact of PCI/CISP Compliance Solution on applications and their performance
- Complying with the new legal requirements such as Privacy Act and Identity Theft Prevention Act for protecting credit card numbers
- Secure Data Management: Storage, Transit and Disposal
- User awareness training to handle compliance and suspicious events
- Realigning existing security framework to meet PCI compliance requirements with minimum operational overheads
- Information Security Policy Management

DRIVER / Regulator VISA and MasterCard

Affected Organization Merchant organizations, service providers and acquirers

Deadlines Merchants (Level 1: 30th Sept 2004, Level 2 & Level 3: 30th June 2005, and Level 4: TBD) and Service Providers (30th Sept 2004)

Cost of Non-compliance Visa imposes a fine on members up to an upper limit of USD 500,000 per incident if their merchant or service provider is found to be non-compliant at the time of security breach. Obviously members may transfer the liability downstream.

Responsibility Flow Members are required to be compliant and ensure the entities downstream are PCI compliant. Acquirers make the provisions of compliance as part of their contractual agreement with merchants and their service providers.



PCI Consulting from Wipro:

Wipro offers PCI compliance readiness solution. This is based on in-house developed PCI methodology – ADAM (see below). The readiness solution comes in the form of a remediation plan, implementation and roadmap document.

Our PCI DSS specialists assess the current security environment from PCI Compliance perspective, work out the gaps and recommend the fixtures in terms of a remediation plan. As a part of this document our consultants also provide the implementation strategies based on the priorities, cost/benefit analysis, risk indicators, leveraging the existing efforts etc. This helps the customer to be ready to comply in the phased manner and in a cost effective manner.

Key areas of assessment

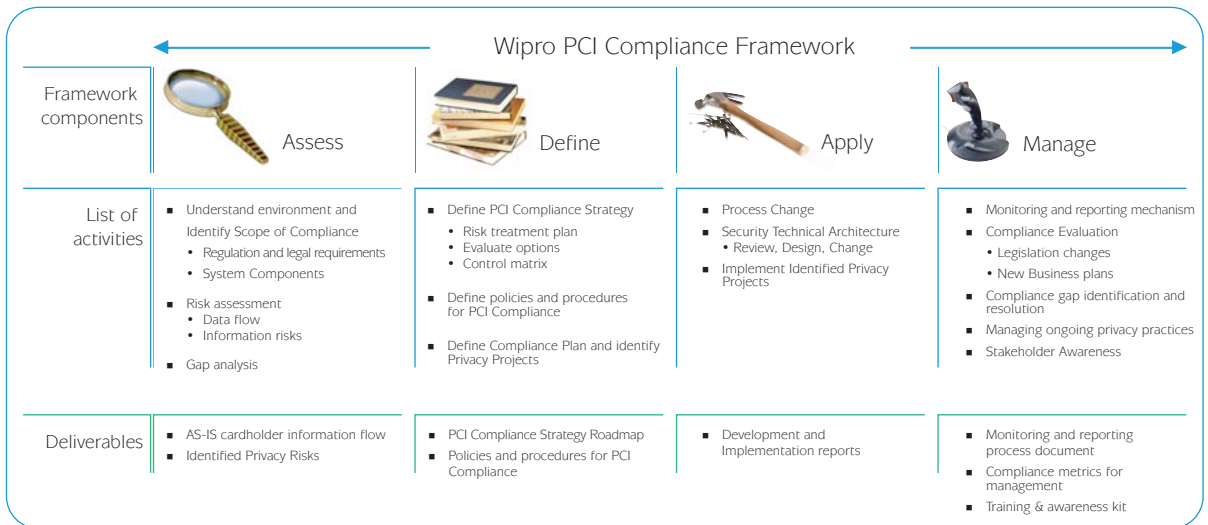
Effectiveness of user access control	User awareness on incident handling suspicious events	Vulnerability Management	Sustainable Event/ LOG Monitoring
Security Policy Management		Data Storage & Retention	Secure Data Management Certified Processors TP Agreements Offsite Vendors
		Data Encryption Payment System Transaction Flow Key Management	

PCI standard requirements and Wipro's security solutions

- | | |
|---|---|
| <p>1 <u>Build and maintain secure network</u>
Install and maintain a firewall configuration to protect data
Do not use vendor-supplied defaults for system passwords and other security parameters</p> | <p>End Point & Gateway Security Solution</p> |
| <p>2 <u>Protect cardholder data</u>
Protect stored data
Encrypt transmission of cardholder data and sensitive information across public networks</p> | <p>Credit Card Information & Protection Solution</p> |
| <p>3 <u>Maintain a vulnerability management program</u>
Use and regularly update anti-virus software
Develop and maintain secure systems and applications</p> | <p>Enterprise Wide Vulnerability Management</p> |
| <p>4 <u>Implement strong access control measures</u>
Restrict access to data by business need-to-know
Assign a unique ID to each person with computer access
Restrict physical access to cardholder data</p> | <p>Global Identity & Access Management</p> |
| <p>5 <u>Regularly monitor and test networks</u>
Track and monitor all access to network resources and cardholder data
Regularly test security systems and process</p> | <p>Security Information Management</p> |
| <p>6 <u>Maintain an information security policy</u>
Maintain a policy that addresses information security</p> | <p>Security Information Management</p> |

Wipro is an end-to-end solution provider

ADAM reflects the full cycle of PCI Compliance - from assessment to gap analysis to remediation plan to implementation to compliance management.



Wipro's PCI Compliance Solution	Standards / Tools Used	Alliances
<p>Key Deliverables:</p> <ul style="list-style-type: none"> AS-IS Assessment Document Gap Analysis Document Remediation Plan Compliance Strategy Document Monitoring & Reporting Solution Training & Awareness <p>Key Features:</p> <ol style="list-style-type: none"> Compliance Framework Integration with existing efforts Consolidation of prevailing compliances <p>Business Benefits:</p> <ol style="list-style-type: none"> Reduced cost Investment protection Easy Management of Compliance 	<p>PCI, BITS, ISO, COBIT</p> <p>Qualys, VM Tools, WebXM, Watchfire, PrivacyScan etc.</p> <p>Wipro's Solutions and Methodology for IM, Data privacy, VM Solutions, SIM Solutions, End point and Gateway Solutions etc.</p>	<p>IM:</p> <p>IBM, Sun, HP, Oracle, Microsoft etc.</p> <p>Data privacy:</p> <p>RSA, Entrust, Ingrian, Vormetric, Synamos and Wipro's data privacy solution</p> <p>VM Solutions:</p> <p>Symantec, McAfee, Trend Micro, CA</p> <p>SIM Solutions:</p> <p>CA.NETIQ, ArcSight, CISCO and Wipro's Log monitoring solutions</p> <p>End point and Gateway Solutions:</p> <p>CISCO, Symantec, McAfee, Checkpoint etc.</p>

For more information,
Please contact Prasenjit Saha
Email: prasenjit.saha@wipro.com
Mob: +91 98457 18830

Wipro Technologies

USA: Wipro Technologies, 1300, Crittenden Lane, 2nd Floor, Mountain View, CA 94043.
Ph(W): 650 316 3555/650 316 3549. Fax: 650 316 3467/3468.

UK: Wipro Technologies Ltd., Third Floor, 137 Euston Road,
London NW1 2AA. Ph: +44 207 387 0606. Fax: +44 207 387 0605.

Head Office

India: Wipro Technologies, Doddakannelli, Sarjapur Road, Bangalore 560 035.
Ph: +91 80 2844 001. Fax: 91 80 2844 0256.

Website: www.wipro.com Email: info@wipro.com