



PCI DATA SECURITY STANDARD OVERVIEW

According to Visa, "All members, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard."

In order to be PCI compliant, an organization and all its systems involved in the storage, transmission or processing of cardholder information must meet all of the requirements and sub-requirements outlined in the PCI Data Security Standard.

Build and Maintain a Secure Network

- Requirement 1:** Install and maintain a firewall configuration to protect data
- Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Requirement 3:** Protect stored data
- Requirement 4:** Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

- Requirement 5:** Use and regularly update anti-virus software
- Requirement 6:** Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Requirement 7:** Restrict access to data by business need-to-know
- Requirement 8:** Assign a unique ID to each person with computer access
- Requirement 9:** Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Requirement 10:** Track and monitor all access to network resources and cardholder data
- Requirement 11:** Regularly test security systems and processes

Maintain an Information Security Policy

- Requirement 12:** Maintain a policy that addresses information security





REMINGTON PCI SERVICES OVERVIEW

Remington Associates is an information security consulting firm with a consultative and client-service focused approach to information security. As a Qualified Data Security Company (QDSC), Remington is fully authorized to perform PCI compliance audits on behalf of all major credit card brands. Remington's PCI compliance and validation services are made up of five components:

- PCI Counseling and Advisory Services
- PCI Compliance Gap Assessment Services
- PCI Vulnerability Scanning Services
- PCI Readiness and Remediation Services
- PCI On-Site Audit Services

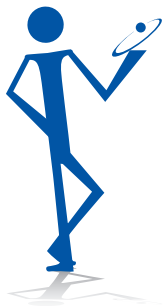
Our clients may use any combination of these services to suit their particular needs. Remington's focus as an organization is 100 percent information security and security regulation compliance. PCI validation and compliance can be the sole focus or part of a larger scope of information security requirements.

PCI COUNSELING AND ADVISORY SERVICES

Often, the biggest challenge in achieving PCI compliance is interpreting the specific requirements in the PCI Data Security Standard and determining whether or not a given security control or configuration would be considered compliant.

Remington Associates will assign a QDSP (Qualified Data Security Professional) to work with your internal team to better understand the intent of each requirement of the PCI Data Security Standard. Through a cooperative review of existing controls, we can provide guidance on whether or not each control or configuration would comply with the Data Security Standard.

PCI Counseling and Advisory services are designed to be flexible with the primary intent being to help clarify aspects of the PCI Data Security Standard and compliance requirements. These services are collaborative and educational in nature, designed to help prepare your organization to move into the more formalized aspects of PCI compliance auditing.





PCI COMPLIANCE GAP ASSESSMENT SERVICES

A PCI Compliance Gap Assessment is designed to uncover elements of the existing environment and security controls that are not in line with the PCI Data Security Standard, without undergoing an in-depth on-site audit.

Using the PCI audit framework as a general guide, this assessment consists primarily of data gathering and interview-style reviews of the existing environment. Normally, hands-on analysis of systems and compliance validation are not included as part of a PCI Compliance Gap Assessment.

By gathering information about the present configuration of systems and security controls, Remington can advise as to which aspects are likely to be found non-compliant according to the PCI Data Security Standard.

Deliverables from the PCI Compliance Gap Assessment will include recommendations for appropriate remediation efforts to bring the PCI-related IT segment into compliance with the PCI Data Security Standard.





PCI VULNERABILITY SCANNING SERVICES

In accordance with PCI compliance validation requirements, Remington can provide quarterly vulnerability scanning of all publicly accessible systems. Remington is available to test (scan) and re-scan your systems with three days advance notice. Upon confirmation of dates and URL(s), Remington will:

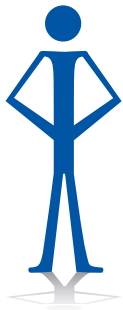
- Perform vulnerability scanning using automated tools on target URL(s)
- Perform platform, perimeter and application level testing from external view
- Identify patterns in scan results and evaluate associated risks
- Perform some manual testing of systems and services with focus on reported vulnerabilities (the objective is to reduce false positives)
- Summarize findings and report
- Package deliverables and report and submit to MasterCard as proof of compliance



Generally speaking, the scope of vulnerability scanning should include, at a minimum, all systems that are accessible via the Internet, whether for public use or for authenticated employees only.

Remington uses the following guidelines taken directly from the Payment Card Industry Security Scanning Procedures document, published by MasterCard:

- Scan all filtering devices such as firewalls or external routers
- Scan all Web servers
- Scan application servers if present
- Scan all custom Web applications
- Scan Domain Name Servers (DNS)
- Scan mail servers
- Scan all load balancers
- Scan virtual hosts
- Scan wireless access points in wireless LANs (WLANs)
- Configure the IDS/IPS to accept the originating IP address of Remington Associates





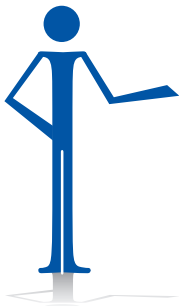
PCI READINESS AND REMEDIATION SERVICES

Upon completion of a PCI Gap Assessment or Counseling Services, Remington's Audit Team will communicate recommendations and transition work efforts to Remington's Remediation Team. The Remediation Team then provides assistance in implementing appropriate security controls or configuration changes to best prepare your organization for compliance validation, specifically for the Self-Assessment Questionnaire, Quarterly Scan or On-Site Security Audit.

The Remington Remediation Team's experience and familiarity with best-in-class security controls combined with our Project Management Office (PMO) ensures smooth implementation of security controls and the changes deemed necessary to bring the PCI segment into compliance.

Remington's PMO is highly trained in the use of its unique Professional Services Framework to implement highly effective security controls and solutions. With Remington's PMO, you receive:

- PMP, CISSP, CISA and QDSP credentials
- Single point of contact for the engagement
- Reduced and managed risk to your projects
- Penta-Constraint management: Scope/Time/Budget/Quality/Risk
- Integrated security management and awareness
- Regulatory and best practice compliance
- Identified accountability for high profile, critical projects



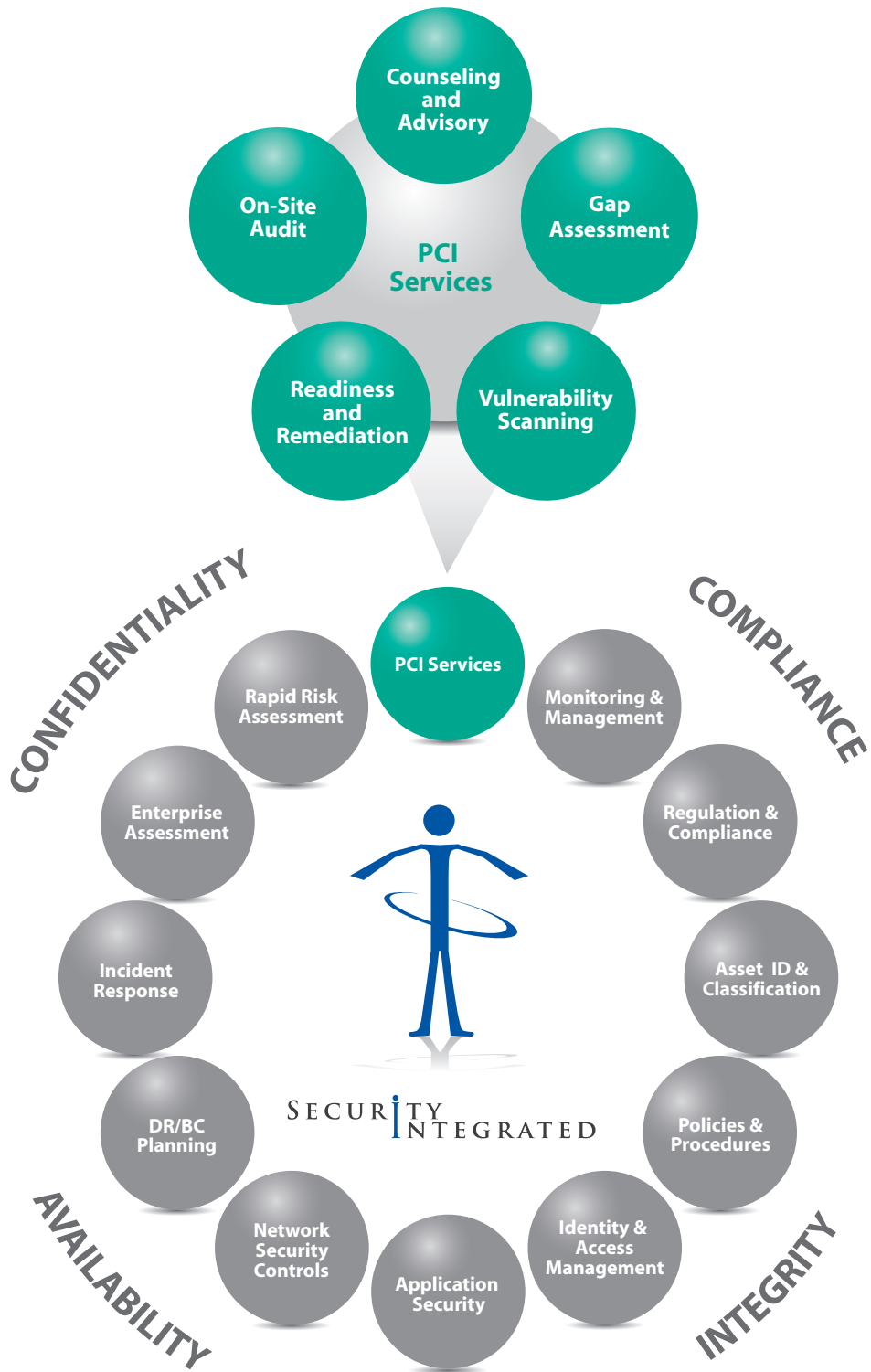


PCI ON-SITE AUDIT SERVICES

For merchants and service providers that require an annual PCI On-Site Audit for PCI compliance validation, Remington is fully qualified and certified to provide this service on behalf of all major credit card brands, including: Visa, MasterCard, American Express, Discover and Diner's Club.

Remington's Audit Team will review all aspects of the environment that store, process or transmit cardholder data to ensure compliance with the PCI Data Security Standard. The auditors will collect data/evidence and perform testing as outlined in the CISP Security Audit Procedures and Reporting document (SAP-R), which is designed to ensure compliance with the PCI Data Security Standard.

Upon completion of the PCI On-Site Audit, Remington will provide full documentation of the results, including the preparation of the Report on Compliance (ROC) for the Visa CISP program. The PCI On-Site Audit requires the results of the last four quarterly vulnerability scans; therefore, scanning may need to be performed in parallel with Remington's PCI On-Site Audit. The PCI On-Site Audit usually follows a PCI Compliance Gap Assessment and/or PCI Readiness and Remediation Services for best results.



REMINGTON ASSOCIATES, LTD.
 SECURITY INTEGRATED