



# PAYMENT CARD INDUSTRY (PCI) DATA SECURITY SOLUTIONS

## Payment Card Industry (PCI) Data Remediation Solutions

**If your organization accepts or processes credit cards, you need PCI Data Remediation Solutions.**

To protect sensitive customer information and to maintain consumer confidence, most major credit card associations have adopted the Payment Card Industry (PCI) Data Security Standard, which was jointly developed by VISA and MasterCard.

All merchants and payment-processing firms with internal systems that store, process, or transmit cardholder data must comply with the PCI Data Security Standard. In certain cases, self-assessment and quarterly network scans may be the only formal requirements. However, for high-volume merchants and service providers, compliance must be demonstrated by means of an annual assessment that is conducted by a certified third-party assessor.

Details of SAVVIS' assessment process are provided in the separate "Payment Card Industry Data Assessment Solutions" overview, which is available from your SAVVIS Account Executive. This overview focuses on the steps of the PCI Compliance process that follow PCI Assessment, including PCI Remediation and ongoing Compliance.

## Non-Compliance Penalties

When an organization is found to be in non-compliance with PCI standards, penalties can be severe. In rare instances, merchants or service providers who do not comply with requirements may be forbidden to store, process or transmit credit card information. Failing to meet required PCI deadlines can result in financial penalties, more stringent audit requirements and possible exclusion from the payment card program. State privacy laws may require public reporting of security breaches that involve customer information, significantly impacting your organization's reputation and brand identity.

To facilitate our customers' PCI Compliance activities, SAVVIS has teamed with a Qualified Data Security company (QDSC) to provide the first end-to-end PCI compliance program, which is geared to all merchant and service provider levels. By engaging the SAVVIS Security team, your organization will be able to safeguard customer data and protect your brand identity.

## A Full Service Offering for Cardholder Data Protection

The joint offering from SAVVIS is unique in that it provides a single stopping point for completion of the entire PCI Data Security process – from assessment, to remediation, to ongoing compliance analysis. Additionally, we deliver many years of experience in the Information Security realm, ensuring that not only the letter, but also the spirit, of the mandate are followed.

With a broad suite of services that expands far beyond PCI, SAVVIS can easily show your firm how to leverage an investment in PCI, and assist you with other mandated security programs.

For a summary of services that are offered in addition to PCI Assessment & Remediation, refer to the list below. In some cases, the services are offered solely on servers that are managed by SAVVIS. Since each organization's security environment is unique, please contact your SAVVIS Account Executive for additional details.

## PCI SOLUTIONS FROM SAVVIS ENABLE YOUR ORGANIZATION TO:

- Simplify PCI process & achieve annual deadlines by working with experts in the PCI space
- Rely on trusted partners with years of experience in serving hundreds of the world's leading retailers
- Choose from annual assessments or ongoing assessment services
- Leverage end-to-end solutions that include PCI Assessment, Gap Remediation, and ongoing Compliance Analysis

For more information about SAVVIS, visit [www.savvis.net](http://www.savvis.net) or call 1-800-SAVVIS-1.

## SAVVIS Services

In addition to PCI Compliance services, SAVVIS offers a broad range of Managed Security Services and Security Consulting Services to help your organization maintain organizational security.

- Application Security Review
- Assurance Manager
- Content Integrity Monitoring (CIMS)
- Host-based Intrusion Detection (HIDS)
- Incident Response (IR)
- Managed Firewall
- Managed Vulnerability Scanning (MVS)
- Network-based Distributed Denial of Service (DDoS) Mitigation
- Network Penetration Testing
- PCI-Ready Managed Infrastructure
- SAVVIS Intelligent Monitoring (SIM)
- Security Architecture Design & Review Service
- Security Assessment
- Security Assurance Manager
- Security Code Review
- Security Policy Design & Deployment

## Proven Methodologies Ensure Accurate Results

Both SAVVIS and SAVVIS' QDSC partner have extensive experience with VISA's Cardholder Information Security Program (CISP) and MasterCard's Site Data Protection Program (SDP), the precursors to the joint PCI Data Security Standard. We deliver solutions that combine a wealth of experience related to methodologies, tools and templates that drive cost-effective implementation of PCI standards.

SAVVIS' QDSC partner for PCI Assessment is a Qualified Payment Application Security Company and an Approved Scanning Vendor for VISA and MasterCard, and its approach to PCI compliance has been validated by engagements with numerous merchant and payment processing firms throughout North America.

When the assessment process is complete, SAVVIS can assist your organization in developing ongoing solutions that ensure compliance with PCI requirements, going forward. The complete assessment and compliance process consists of eight steps, which are summarized in the chart to the right. The steps for the complete Assessment & Remediation process include:

- Establish team charter and project kickoff meeting
- Review baseline PCI materials
- Create remediation snapshot
- Prepare high-level data protection assessment
- Develop accessibility assessment
- Prioritize remediation tasks
- Create remediation plan
- Develop supplementary task documents and plan execution

For more details regarding specific tasks that are completed in each of the phases, refer to the sections that follow. It is also important to remember that engagements are customized to achieve your organization's goals, and to meet your specific needs.

### Establish Team Charter & Project Kickoff Meeting

In this phase, your organization will identify a project team, who will collaborate with SAVVIS during the course of the PCI engagement. To ensure maximum project success, a team charter will be established, and a project kickoff meeting will take place, ensuring that stakeholders are aware of their responsibilities and understand the required stages of the project plan.

Customers are generally supported by a Project Manager, Security Architect and a Retail Systems Specialist during this phase, and SAVVIS' responsibilities are outlined in a customized Statement of Work.

The overarching goal of this phase is to evaluate the current state of your firm's compliance activities, and prioritize the project tasks that are necessary to achieve compliance.



### Review of baseline PCI Materials

In the next phase, SAVVIS reviews the following types of documentation, to determine the state of PCI readiness at your organization:

- IT governance requirements
- Corporate and store-level technology standards
- Store-level operational requirements, including management controls, merchandising, loss prevention and sales audit procedures
- Network topologies, encompassing corporate and store-level networks
- Cardholder dataflow diagrams
- Existing remediation projects, if applicable
- Current policies & procedures
- Remediation Roadmap and Report of Compliance

To supplement document review, SAVVIS will perform an on-site assessment of at least one retail storefront location, at a site agreed upon by both SAVVIS and the customer. At the storefront location, SAVVIS will conduct interviews with store personnel, perform a review of the facility (and its retail systems), and document potential risks to cardholder data.

In addition, SAVVIS may evaluate potential data security risks at your headquarters, with a focus on contacts who have regular access to cardholder information, such as store operations, loss prevention and sales audit staff.

Working with your remediation contacts, the primary goal is to identify team members who can supply required information, to schedule and conduct follow-up interviews, and to report on key findings.

### Creation of Remediation Snapshot

Based on the documents that have been reviewed and the interviews that have been conducted in the previous phase, a Remediation Snapshot is prepared for your organization. The remediation snapshot identifies all potential remediation tasks, and documents their status. The snapshot also provides the basis for additional documentation, which will be described in further detail below.

### Preparation of high-level Data Protection Assessment

The goal of this phase is to identify the primary risks to the confidentiality of cardholder data in your organization's environment.

Examples of vulnerabilities that may place your organization at risk include (but are not limited to) the following:

- Potential breaches of the network perimeter in stores and in corporate environments.
- Potential breaches of system access controls, by corporate insiders, or by intruders.
- Potential breaches of encryption controls.
- Potential breaches of physical access, including systems access, or access to physical media that houses cardholder data.
- Exposure to Worms, Trojan Horse attacks, or other malicious code.

When the analysis is complete, a high-level risk stratification document is prepared for your organization.

### Development of Accessibility Assessment

At this point, SAVVIS evaluates the "accessibility" of tasks that were identified in the Remediation Snapshot phase, and vulnerabilities that were identified in the High-Level Data Protection phase. In this context, "accessibility" may be defined as "...the ability to accomplish a particular task, when analyzing time, cost and available resource skills."

To determine the accessibility of a particular remediation task, SAVVIS evaluates the task's duration, potential material costs, and the resource skills that are available.

The final step of this phase involves assigning an "accessibility index" to each of the remediation tasks, which identifies tasks that will have the highest potential impact. Tasks that are assigned the highest accessibility (based on low time commitments, low cost, and low resource requirements) will be prioritized. Tasks with the lowest accessibility, based on high time commitments, high cost and high resource requirements, receive the lowest level of prioritization.

### Prioritization of Remediation Tasks

Utilizing the accessibility weightings that were established in the previous phase, each task is prioritized according to its accessibility. The end result is a prioritized task listing that will serve as the basis of the Remediation Plan, which is described below.

### Creation of Remediation Plan

Once each task has been prioritized, the results are incorporated into a Remediation Plan, which provides the detailed steps that are required for your organization to implement and complete the PCI Remediation Program. The plan includes critical project tasks, anticipated delivery timeframes, required resources, potential risks and critical interdependencies. In addition, SAVVIS will prepare an Executive Remediation Program Report, which outlines the planned remediation strategy, and actions required to achieve and maintain compliance. At your organization's request, key elements of the report may be synthesized and presented to key members of your Executive Management Team, and/or to third-party vendors who are engaged in your PCI compliance efforts, such as VISA. The Remediation Snapshot (created in the third phase) and the Remediation Plan will also serve as important "compliance gauges," as the project moves forward.

### Development of Supplementary Task Documents & Plan Execution

Once the Remediation Plan is complete, SAVVIS develops supplementary task documents, which are used to execute various components of the plan. Your organization may choose to outsource these tasks, or leverage internal resources instead. The supplementary task documents include:

- PCI requirements that are to be satisfied by completion of tasks in the Remediation Plan
- Goals and objectives that correspond to the tasks in the plan
- Deliverables and task milestones that will be met through task completion
- Project risks and rewards
- Resource requirements, including potential costs for staffing, materials and capital investment
- Employee training and knowledge transfer requirements, to ensure that your organization maintains future compliance
- Interdependencies between project tasks and between stakeholder groups

From your organization's perspective, PCI compliance is the primary goal of the comprehensive project.

### Applying PCI Remediation Knowledge to other Compliance Mandates

The PCI Remediation program will actually improve the management of your business, by establishing controls and documenting processes that define your corporate security program. This focus will reduce the amount of time and effort involved with other compliance audits, and will enable you to maintain and enhance your security program over time, even if you encounter personnel changes. SAVVIS recognizes that many organizations are required to comply with information security compliance requirements that are in addition to the PCI standards. Our unique approach to PCI will enable your firm to leverage our collective experience, to assist with other mandates such as:

- **Retail Banking** – Gramm-Leach-Bliley Act, FFIEC, USA Patriot Act
- **Retail Drug and Pharmacy** – HIPAA, the Health Alert Network
- **Publicly-Owned Organizations** – Sarbanes-Oxley Act, ITIL

While PCI compliance may seem like a challenge, it is mandatory, and it is essential to protect data integrity, meet customer service expectations and preserve your organization's reputation.

#### BENEFITS OF ONGOING PCI COMPLIANCE

Leverage SAVVIS' Expertise in PCI Compliance

- Protect brand equity & reputation
- Maintain high levels of customer service & efficiency
- Avoid potential loss of revenue due to costly and embarrassing service interruptions
- Keep payment process as efficient as possible
- Maintain customer and investor confidence
- Avoid potential fines, negative press attention, and potential litigation
- Focus corporate attention on importance of ongoing compliance

## About SAVVIS

SAVVIS, Inc. (NASDAQ: SVVS) is a global leader in IT infrastructure services for business applications. With an IT services platform spanning North America, Europe, and Asia, SAVVIS leads the industry in delivering secure, reliable, and scalable hosting, network, and application services. These solutions enable customers to focus on their core business while SAVVIS ensures the quality of their IT systems and operations. SAVVIS' strategic approach combines virtualization technology, a global network and 24 data centers, and automated management and provisioning systems.

For more information about SAVVIS, visit [www.savvis.net](http://www.savvis.net) or call 1-800-SAVVIS-1.