RSA ARCHER PCI COMPLIANCE MANAGEMENT - V2

AT-A-GLANCE

- Core solution pre-requisites: RSA Archer Enterprise and Policy Management modules
- Use out-of-the-box policies, control standards, procedures and assessment questions mapped to the PCI DSS 2.0
- Decrease required time to conduct PCI assessments, from weeks to days
- Perform SAQ assessments against a range of in-scope targets, including merchants, applications, facilities, business units and data flows

DATA SHEET

EXECUTIVE SUMMARY

Credit cards have become the payment method of choice for consumers, initiating new opportunities for fraud and identity theft. Fragmentation of the payment process across multiple entities (merchant, service provider, credit processing entity, etc.) creates numerous entry points for criminals to access and misuse customer information. As a result, the Payment Card Industry (PCI) program has placed significant pressure on businesses to establish solid enterprise-level security programs.

The PCI Data Security Standard (DSS v2.0) offers a unified set of security requirements for all credit card types, as defined by Visa and MasterCard and endorsed by other major credit cards. This program provides a clear set of security standards to follow in order to reduce the risk of credit card and identity theft. Organizations that fail to comply may lose their ability to participate in credit card processing programs, which could greatly impact their ability to conduct business.

Costs associated with demonstrating PCI compliance can be substantial. Companies that can reduce these costs and constrain compliance efforts within the operational facets of their business will be much more successful. However, non-compliance could have detrimental business impact.

The challenge for many organizations lies in meeting PCI requirements in the context of the business and clearly articulating control infrastructure scopings. PCI DSS compliance cannot be a point in time exercise. Rather, it must be a continuous assessment effort throughout the year. The extensible PCI DSS 2.0 framework for managing control definition and compliance measurement and reporting allows businesses to efficiently and effectively ensure ongoing compliance.

RSA Archer PCI Compliance V2 value add solution allows your organization to streamline the compliance process, automate assessments and lower test costs. Jumpstart your PCI compliance program by conducting continuous, automated assessments and gain visibility to manage and mitigate risk.

The PCI Compliance V2 value add solution fully integrates with core RSA Archer GRC solutions, allowing customers to implement an efficient, sustainable PCI compliance program.

NEW FOR VERSION 2

- Complete re-write of the PCI solution to enable full support of Archer 5.X platform
- Multiple card holder and CDE data environments per company project
- Mail merge functionality and auto-generated report on compliance (ROC)
- Tighter integration with Archer Compliance Management
- Auto scoping of card holder data environments

POLICY MANAGEMENT

Utilize a pre-loaded library of policies, control standards, procedures and assessment questions mapped to the PCI 2.0 Data Security Standard. Also upload your own policies, standards and procedures, aligning them with the PCI requirements they satisfy.

ENTERPRISE MANAGEMENT

Determine organization assets in scope with PCI compliance requirements, data classification levels for all personal information assets within your organization, and risk-rate enterprise systems that house payment card data.

SYSTEM ADMINISTRATION

Centrally deploy, manage, and monitor the status and progress of all agents and scan groups. Configure nearly everything using GUI controls.

RSA ARCHER GRC PLATFORM

RSA recognizes that no two businesses are alike. Every organization has unique processes for managing compliance, and retrofitting those processes to a rigid solution structure is not practical. To address your needs for point-and-click configuration, the RSA Archer GRC Platform delivers a rich feature set that allows business users to tailor RSA Archer solutions according to your established processes and naming conventions—with no custom code.

Ways in which you can tailor RSA Archer solutions include:

- Modify the solution structure to collect business-specific information from end users
- Creating roles and groups to control information access at the application, record and field level
- Building workflow stages to model your organization's processes, and notify users automatically when tasks enter their queues
- Creating role-specific dashboards through a drag-and-drop interface

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa..