Iceberg PCI Program Manager for ServiceNow® (GRC)

Overview

For any Merchant the impact of not complying with the Payment Card Industry Data Security Standard (PCI DSS) is very costly. There are fines upwards of $500,000 per data security incident and $100,000 per month for non-compliance. Additionally, Merchants are suffering a loss of brand valuation through tarnished reputations when losses or breaches occur. Therefore, the need for companies to remain in compliance is high value both financially and reputationally. But managing to this is in Level 1 Merchants (those with greater than 6 Million transactions annually) has become a serious challenge.

Not only is the cost of non-compliance very expensive, the cost for a company to become compliant and sustain compliance has become excessive.

Specifically, getting ready for an audit and ensuring that you have either collected everything that the auditors will require access to, or know exactly where to get information or evidence they require at the time of the audit is arduous and time -consuming. Most organizations manage this data in spreadsheets or different tools across the organizations. This manual approach cannot scale to keep up with sustainment needs.

Our Solution

Iceberg PCI Program Manager (IPM) for ServiceNow GRC is an out of the box configured PCI Management solution targeted directly at PCI Level 1 Merchant organizations. It allows organizations to rapidly organize, manage and store annual PCI Assessments by Qualified Security Assessor (QSA). It provides continuous management and PCI compliance reporting through actionable remediation alerts by Internal Security Assessor (ISA) and the team. By readily providing complete visibility into corporate PCI Program compliance status the organization can provide accurate and detailed communication to all stakeholders.

Iceberg PCI Program Manager addresses the following challenges faced by Level 1 Merchants:

- Proper scoping of all Cardholder Data Environment (CDE) and subsequent validation that the scope has been correctly defined and documented (this accounts for at least 50% of the effort on an annual Assessment by the QSA)
- Organized collection and storage of evidence, including version control, used to support control assessments (this is the second largest consumer of time)

The Credit Card Industry regulates companies dealing with customer information and mandates the infrastructure is secure and the right policies and controls are in place to manage privacy and risk.

Companies know they must have a process in place for continuous monitoring of compliance with the Payment Card Industry (PCI) Data Security Standard (DSS).

Key risk areas are specific to each line of business and are

important for establishing performance standards against regulations and compliance requirements.

Iceberg PCI Program Manger allows for better reporting and managing attainment and sustainment of compliance. Enabling organizations to sustain compliance and avoid costly penalties and fines, all the while having better reporting to all stakeholders including the QSA.

Iceberg

- Continuous management of controls assessments during the year and leading up to the annual assessment
- Managing the remediation activities to address any gaps, as well as the re-test of the associated controls when not in compliance
- Connecting the ASV scan details with the internal Vulnerability Management Program while having traceable evidence that specific failed scan results are linked to Vulnerability Response activities and re-scan confirmations
- Accurately completing the annual assessment by/for the QSA with specific detail captured on 'how' the control was verified
- Program reporting using centrally available active information

Key Features and Benefits

Feature	Benefit
Cardholder Date Environment (CDE) Definition	Defining the CDE accurately using the populated Configuration Management Database (CMDB) or simple asset listing are used to define total possible CDE quickly using bulk search functions
CDE Scoping	Bulk scoping (or individually) each CDE defined asset is annotated as 'in-scope' or 'out-of-scope' with justifications by ISA and QSA, removing e-mail and attachments from the process, significantly reducing time and improving the ability to defend scoping and segmentation
Sampling Support	The DSS allows assessors to sample during assessments. Sampling management during the CDE definition and scoping expedites the assessment process dramatically. Both manual selection and random % of the total population are supported, increasing QSA confidence in results
PCI Profiles and Controls Generation	Full sets of Profiles and Controls automatically generated for each scoped item within any CDE, reducing manual administration and maintenance of the CDE data
PCI Data Content Pack Accelerator	The full DSS 3.2.1 has been decomposed and mapped to control templates and related test templates aligned with the Report on Compliance (RoC)
Data Model Supports RoC Template	All captured information has been mapped to the official RoC Template, ensuring it will be possible to quickly generate an accurate RoC Report for QSA review
Evidence Collection and Location	All evidence is either collected within CDE metadata or locators are recorded for external sources of information (e.g. SharePoint, or other systems). This capability will significantly reduce burden on PCI management team prior to and during an assessment

ABOUT ICEBERG

Iceberg helps organizations plan, deploy and support successful implementations of Governance, Risk Management & Compliance (GRC) solutions, decisions. Headquartered in Ottawa, Canada and serving all of North America, Iceberg's team of consultants, developers and subject matter experts offers a full lifecycle of services, including executive workshops, implementation and integration, and support services. We are also a value-added partner for North America's leading GRC software platforms.

icebergnetworks.com

420-515 Legget Drive, Ottawa, Ontario K2K 3G4 | Toll Free: 855-595-0808 | info@icebergnetworks.com

Iceberg