SOLUTION BRIEF

Ensuring Inventory Controls for PCI Compliance

Maintain accurate inventory controls for hardware, software and cloud assets to comply with PCI Data Security Standard

Compliance with the Payment Card Industry Data Security Standard (PCI DSS) is paramount for organizations handling cardholder data. PCI DSS mandates a set of security controls designed to ensure all companies that accept, process, store, or transmit credit card information maintain a secure environment.

A fundamental requirement of PCI DSS compliance is robust inventory control. This involves maintaining a detailed record of all technology assets, particularly those involved in processing, storing, or transmitting cardholder data. Inventory controls are not just about knowing what assets exist within the organization but also understanding the role each asset plays in the handling of cardholder data.

Documentation of All Assets
Every component, from network devices to servers and payment systems, must be accounted for.

Classification of Assets
Identifying which assets are in scope for PCI DSS compliance, based on their involvement with cardholder data.

Regular Updates and Reviews
The inventory must be regularly updated to reflect new, changed, or decommissioned assets.

This inventory serves as the foundation for risk analysis, enabling you to identify and mitigate potential vulnerabilities that could lead to cardholder data breaches. Failure to maintain adequate inventory controls can lead to severe consequences, including security exposures, legal and financial penalties due to PCI violations, reputational damage, and operational disruptions.

Unfortunately, modern enterprise environments, characterized by hybrid and remote work, cloud services, and mobile technologies, have added layers of complexity to maintaining accurate inventory controls and good technology data hygiene.

Traditional IT Asset Management (ITAM) and CMDB-based solutions usually fall short in addressing this evolving technology landscape. Often, IT teams resort to manually pulling information from multiple sources, aggregating it painstakingly via spreadsheets, and contacting users to reconcile duplicate entries or populate gaps.

Challenges

- Keeping up with the fast pace of adoption of diverse user and field devices, SaaS apps and cloud services
- Tracking and managing assets across remote workforce and growing number of locations
- Resource and cost overruns in obtaining and compiling technology inventory data
- Friction between IT and GRC teams due to poor inventory management and inaccurate compliance reporting

Benefits

- Single system for tracking all technology assets across hardware, software and cloud services
- Confidence in inventory controls and compliance with PCI DSS requirements
- Better audit accuracy, efficiency and timeliness with automated workflows to streamline audit preparation tasks
- Cost savings by reducing manual effort, human error and the need for resource intensive IT projects
- Reduced risk of PCI DSS fines and failures
- Improved alignment and collaboration between IT and GRC teams

Ensure PCI DSS compliance through rigorous inventory controls

To enhance the accuracy, efficiency and timeliness of compliance with PCI DSS inventory controls you need to embrace improvements in tools, processes and automation.

Enterprise Technology Management (ETM) solutions provide an integrated platform to manage and monitor your complete technology landscape. This proactive approach ensures compliance with PCI DSS inventory controls as well as other industry standards/frameworks, while also improving your overall security posture.

ETM solutions address the needs of today's dynamic technology environments, overcoming the limitations of traditional ITAM and CMDB solutions by providing:

> "Using Oomnitza, we're able to provide real-time updates on assets and what we have installed, which is a core part of our compliance and certification efforts."
>
> **Nemi George**
> **VP, Information Security Officer & IT Operations**
> ***Pacific Dental Services***

- Centralized inventory of all technology assets by leveraging existing tools and installed agents for comprehensive coverage, ensuring no asset goes untracked.
- Low-code/no-code workflows and pre-packaged workflow applications that are easily configured for your needs, to assess compliance, remediate issues and automate PCI DSS audit preparation tasks.
- Connector integrations with 160+ IT, security and business systems to discover, aggregate, normalize and enrich technology data for single-source audit data.
- Powerful business intelligence, notifications and reporting to keep stakeholders informed and provide evidence for PCI DSS auditors to demonstrate compliance.