Prepare for a SOC 2 Audit with Oomnitza

As more organizations rely on SaaS and service providers, the number of offerings in the market continues to grow, increasing both opportunities and competition. SaaS and service provider organizations have been forced to adapt – taking on new initiatives to separate themselves in a crowded field. Many organizations have looked to improve internal controls in order to do so.

For organizations obtaining a SOC 2, certification represents achieving the highest standards of international controls and reflects a commitment to protecting client data. Achieving SOC 2 certification is a sizable project that requires a high level of commitment from organization executives, in order to successfully complete a SOC 2 audit. These audits take a comprehensive view of an organization's controls and are centered around the trust principle of information security, availability, processing integrity, confidentiality and privacy.

The SOC 2 audit process typically begins with a six- to twelve-month preparation period; this is when executives develop policies and procedures and implement security controls to meet compliance standards. When a registered CPA comes on site, they will conduct interviews and review artifact

SOC 2 TYPE II CERTIFIED

documents. The bulk of the SOC 2 audit – called the Common Criteria – is where the CPA reports on the security controls an organization has in place. Here, the CPA will look into a SaaS or service provider's organization and structure, communication, risk management, monitoring of controls, logical and physical access controls, system operations and change management.

There are also two certification options available when completing a SOC 2 audit – type I and type II. While type I audits look to see if the necessary controls are in place at the particular time of the audit, type II looks to see if compliant controls have been in place over a period of time, which usually takes six months.

While SOC 2 audits observe several components of an organization's security practices, effective IT asset management is an essential part of reaching certification. Assets must be encrypted, protected against unauthorized use, retrieved during employee offboarding, and reliably assigned to users. For many organizations, these tasks require referencing data from different locations and systems. With siloed data, doing this efficiently can be difficult due to discrepancies and human error.

Oomnitza's approach to IT asset management seeks to resolve the challenges that result from leveraging several systems for device management. The platform centralizes asset data, bringing greater visibility and

automation capabilities to asset management. By unifying several databases into one single source of truth using Oomnitza, organizations can:

Have a comprehensive view into each IoT asset including its ownership, ticket history, encryption, installed software and more.

Automate the creation of tickets when devices do not have an assigned user, are not encrypted or accessed by an unauthorized user.

Create service tickets automatically when employees are offboarding, allowing IT to know what devices need to be returned.

While obtaining SOC 2 Certification comes with several challenges, its benefits are worthwhile: improved internal policies and procedures, security practices, and risk management aid organizations in continual growth. For organizations with manual asset management processes and siloed IoT asset databases, information discrepancies and ineffective procedures hinder both productivity and security. The Oomnitza platform provides a solution to resolve these issues, helping organizations create streamlined IT asset management systems to achieve SOC 2 certification.