Achieve ISO 27001 Certification with Effective IT Asset Management

With information security being a continual concern, organizations have expanded initiatives to monitor and maintain their internal controls. For organizations looking to achieve the highest level of international security standards, ISO 27001 is a benchmark representing best practices around security measures and a commitment to protecting client information. ISO 27001 is internationally recognized, giving current and potential clients reassurance that their information is safeguarded. Achieving ISO 27001 is a sizable project requiring a high level of commitment from organization executives. While the process of achieving ISO 27001 certification can be an overwhelming task, it can lead to potential new buyers and improved internal practices.

Organizations are more vulnerable to data breaches than ever before, and ISO 27001 creates a framework to quickly detect and react to potential risk. Certification ensures that an organization is able to appropriately respond to these challenges and remain compliant as it scales. Leading up to a certification audit, organizations must inspect current controls and address the steps needed to achieve ISO 27001 standards. While ISO 27001 audits observe several components of an organization's information safety practices, effective IT asset management is an essential factor to achieve certification.

Under the ISO 27001 certification, there are 14 different subcategories of control sets outlining the requirements that organizations must satisfy. Although asset management has its own subcategory, other categories such as human resource security, cryptography, and access control all require effective asset management. Under these control sets, devices must be assigned to users, returned during offboarding, encrypted and prohibited from being accessed by unauthorized users. For organizations with thousands of IoT assets, this can be a major challenge.

Oomnitza's platform assists organizations in achieving ISO 27001 standard information security through centralized and automated asset management. Within Oomnitza's asset module, organizations can access a comprehensive asset record which shows assigned users, installed software, access controls, and service tickets over that asset's lifetime. Having this information in a centralized location also allows for HR teams to easily meet security compliance standards as well. During offboarding, organizations can ensure all IoT devices are returned to the appropriate teams. Oomnitza also

brings automation to asset management with customizable workflows; through the construction of workflows, organizations can set automated triggers that generate corresponding actions. In the case of unauthorized access or an unencrypted device being detected, workflows can be built to automatically create a service ticket that alerts IT.

For organizations with manual asset management processes and siloed IoT asset data, ISO 27001 compliance can be an overwhelming challenge. Manual processes and asset information located across different platforms can lead to discrepancies and human error. Oomnitza provides a platform to resolve this issue, help organizations centralize their IoT asset data, react quickly to security risk, and ultimately achieve ISO 27001 certification.