Compliance Manager

General

Industry's Only Automated Compliance Tool that takes the process to the next level by automating the collection of the data, analysing it for you, and providing you with dynamic worksheets that are customized based on your data. Kaseya Compliance Manager is the first and only purpose-built, role-based Compliance Process Automation platform. Combining a wizard-driven workflow engine, automated network and computer data discovery, a web-based management portal, and built-in compliance document generation – to help you maintain and prove compliance.

NIST Cybersecurity Compliance

Compliance Manager uses the NIST Cybersecurity Framework (CSF) as the foundation for a growing number of industry- and application-specific security standards, starting with NY SHIELD, NIST 800-171/CMMC and NYDFS. Customers that work with U.S. Federal or State agencies, including DoD, GSA or NASA, and that process, store or transmit Controlled Unclassified Information (CUI), are required to be NIST 800-171 compliant or risk being excluded from consideration for lucrative government contracts, while companies who store NY citizens private data are required to follow the NY SHIELD guidelines. Our automated data collection and simplified user-driven walkthrough for each standard makes documenting network security for NIST CSF compliance easier than ever.

Automated Scan & Data Collection

- Scan your network and determine if GDPR requirements are being met, and if not, what needs to be done.
- Your list of Compliance To-Dos is maintained for you by the system, and each task is automatically crossed off and marked complete as you go.
- Automatic Data Collection. The system automatically collects a ton of information that you would gather manually with other tools, saving you time.
- The system automatically compares answers to questions with the information it automatically gathers and highlights exceptions where the two don't match.

Remediation & Documentation

- Produce all mandatory reports as required by GDPR and be prepared, in advance, to pass an audit.
- Document and prioritize issues that must be addressed to solve GDPR-related security vulnerabilities.
- Role-based Assignments - Divides the workload into three primary roles: Internal Auditor, Technician, and Site Admin.
- Auditor Checklists - Easily assesses your compliance position and gives you a document to show Auditors to help them see how you are doing.

Compliance Standard Specific Scans

- Scans system looking for information pertinent to the specific compliance standards. Compliance standards require specific deeper scans looking for specific information. For

GDPR, Compliance Manager helps identify where personal data resides. For HIPAA, scans are performed looking for instances of ePHI.

- Performing compliance assessments cannot be done in a vacuum. Subject Matter Experts are oftentimes required to assist in completing worksheets, forms, and providing information that cannot be discovered automatically. Compliance Manager provides a framework for inviting others to assist in the assessment process.
- Compliance Manager presents in-product guidance to help you complete the assessment. Sometimes you need a little help. In-product guidance written by compliance experts helps you answer compliance related questions.

Compliance Guidance

Performing compliance assessments cannot be done in a vacuum. Subject Matter Experts are oftentimes required to assist in completing worksheets, forms, and providing information that cannot be discovered automatically. Compliance Manager provides a framework for inviting others to assist in the assessment process.

Compliance Manager presents in-product guidance to help you complete the assessment. Sometimes you need a little help. In-product guidance written by compliance experts helps you answer compliance related questions.