COMPLIANCE MANAGER GRC™
A Kaseya COMPANY

Kaseya **Cybersecurity** Fundamentals Standard

Get started with IT security assurance with the Kaseya Cybersecurity Fundamentals Standard

Get Up And Running With Automated Cybersecurity Risk Management.

In the realm of cybersecurity, the need for a standardized approach to IT security controls cannot be overstated. The Kaseya Cybersecurity Fundamentals standard is a testament to this philosophy.

Drawing inspiration from the globally recognized NIST Cybersecurity Framework (CSF), we've curated a "short list" of IT Security Controls that every organization should implement -- regardless of size or maturity level. This list is a curated list of NIST CSF controls that reflect the specific needs of modern IT infrastructures. The five areas covered by our controls include:

Identify - Understand and manage cybersecurity risks to systems, assets, data, and capabilities.
Protect - Implement safeguards to ensure delivery of critical infrastructure services.
Detect - Identify the occurrence of a cybersecurity event in a timely manner.
Respond - Take action regarding a detected cybersecurity incident, ensuring minimal impact and swift resolution.
Recover - Restore any capabilities or services that were impaired due to a cybersecurity incident.

By focusing on the most pivotal controls, we ensure that security assessments are expedited, making them more manageable and less time-consuming to act upon.

Set the stage for adhering to all of your IT security and privacy requirements – regardless of the source.

If you have a cyber risk insurance policy, it likely incorporates all of the Kaseya Cybersecurity Fundamental controls. If you have any government regulation or industry rules that you must follow, they likely incorporate the Kaseya Cybersecurity Fundamental controls. If you process, store, or access customer or employee personal identifiable information (PII) of any kind, you'll want to implement the Kaseya Cybersecurity fundamental controls.

Best of all, once you get started with the Kaseya Cybersecurity Fundamentals, you can easily map progress against other standards, and add on additional IT requirements as you go.

Key Benefits for IT Professionals and MSPs:

- **Effortless Onboarding:** Designed for rapid adoption, enabling both IT professionals and MSPs to establish a standardized and automated IT security assurance program swiftly.
- **NIST Cybersecurity Framework:** Built on the pillars of the NIST Cybersecurity Framework, ensuring a solid foundation for comprehensive security practices that resonate with industry standards.
- **Faster Data Collection:** Leveraging Compliance Manager GRC's automated data collection capabilities, making the process seamless and efficient for all users.
- **Customization for MSPs:** Tailored to address the unique needs of Managed Service Providers, enabling them to offer enhanced cybersecurity services to their clients.
- **Value-Added Service:** For MSPs, the framework becomes a powerful tool to differentiate their offerings, attracting clients who prioritize robust cybersecurity measures.

Featured Product Highlights For This Standard

You can use your existing IT security and privacy tools to implement the required Kaseya Cybersecurity Framework controls, but Compliance Manager GRC includes some additional value-added features to help you become more cyber resiliant:

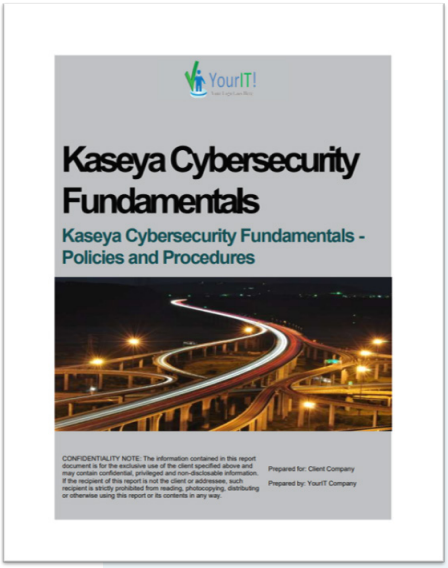
- **Rapid Baseline Assessments –** Quickly identify gaps in cybersecurity according to the Kaseya Cybersecurity Fundamentals standard.
- **Technical Risk Assessments –** Full risk assessment (based on five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover.)
- **Policies & Procedures Manual –** Detailing all of the controls included in the standard and methods of complying.
- **Employee Security Awareness Training Portal –** Includes built-in portal that end-users can log-into, watch short but informative security awareness training videos, quizzes them on their knowledge and records the results.
- **Customizable Standards and Controls –** Modify your procedures to match your specific way of complying with any given control.
- **Role-Based Access –** Helps involve subject matter experts within an organization who can directly input any information required for compliance with Kaseya Cybersecurity Fundamentals
- **Automated Documentation & Reporting –** Provides full documentation, including specific eviidence of compliance with the Kaseya Cybersecurity Fundamental controls

Best of all, you can use this same platform to manage compliance with all your other IT requirements -- including compliance other government and industry rules and regs, with the security terms of your cyber insurance policy, and even compliance with your own internal IT policies.

COMPLIANCE MANAGER GRC™
A Kaseya COMPANY

COMPLETE: ALL-IN-ONE SOLUTION

Kaseya Cybersecurity Fundamentals allows users to track the validity of your cyber risk insurance policy, or making sure your own IT policies and procedures are being followed, Compliance Manager GRC helps you Get IT All Done at the same time, and in the same place. No other Compliance Management software gives you this kind of flexibility.



AUTOMATED ASSESSMENTS & REPORTS

Performing automated assessments with the Kaseya Cybersecurity Fundamentals – while managing all your other IT requirements – is easy with Compliance Manager GRC. You can get more work done with less labor, thanks to automated data collection, automated management plans, and automated document generation.

AFFORDABLE FOR ALL

Compliance Manager GRC is priced to be affordable for the smallest organizations, yet boasts the power and functionality most often found in expensive, enterprise-class governance, risk and compliance platforms. Whether you are managing compliance for your own organization or are an MSP delivering compliance-as-a-service, there's a sensible subscription for you.

Request a Demo today

and discover the advantages of Compliance Manager GRC — the purpose-built compliance process management platform for multifunctional IT professionals.