IT Foundation for SOC2 Compliance

The key IT systems and processes that need to be in place for SOC2 compliance are explained briefly below. Your auditor will guide you in the complete set of policies and processes for compliance, but these capabilities give you the foundation you'll need to avoid wasting your auditor's time and needing to restart the compliance process.

Compliance Management Application

SOC2 compliance is an ongoing process. Over time you'll need to show evidence that you are following the policies and processes you've established. A flexible compliance management application, such as Vanta, can integrate with the various enterprise systems to collect data on compliance and trigger alerts. You may need to be compliant with more than one set of regulatory or industry requirements. KalioTek is a Vanta partner and uses the Vanta application in many of our SOC2 projects. We also use it ourselves to track our SOC2, PCI and HIPAA compliance.

Contact us for more information about preparing for secure operations and SOC2 certification.

Security Awareness Training

Employee login credentials are the weakest link in securing company assets. Training and testing company employees to protect these, as well as tracking course completion and acceptance of policies, is a key part of any compliance regimen. A specialized application can help you do this at low cost, while keeping your staff up to date on the latest threats and counter measures.

Endpoint Security

Last decade's antivirus solutions that operate on individual devices don't cut it anymore. Coordinated real-time protection across multiple devices from Viruses, Malware, Ransomware and Phishing attacks is now needed. Choosing a leading provider will put you on the right path to counter evolving threats for years to come.

Endpoint Management

The remote workforce with distributed, mobile employees is here to stay, leaving employees outside the visibility and control of the company network. A strong endpoint management solution is now a must. They give you visibility into the state of all user devices and enable centralized management to an extent not possible in the past. Features include: granting conditional access at a granular level, remote lock and remote wipe, separation of personal data vs. corporate data, preventing sensitive data from leaving the device/network, pushing security patches, validating encryption and backup, etc. All this is great for demonstrating compliance as well as peace of mind.

Inventory of Authorized Company Hardware and Software

The Center for Information Security (CIS) cites these as their top security concerns. You need to know what should be in your environment and when something new and unauthorized appears. With the number of on-premise and remote devices and apps in today's companies, an automated application is required to track these assets and trigger alerts.

Password Management

No one can remember all the passwords required for access to all the systems they need for modern work, especially if passwords are all different and complex, as recommended. An application can manage passwords for you while keeping them secure and automating logins.

Employee Onboarding and Offboarding Processes

You'll need solid processes to ensure that each employee gets the right tools and permissions within those tools. An audit trail of who approved access is important for compliance and security. The process is reversed when an employee is terminated. You'll audit active users regularly to ensure that access by former employees or temporary contractors has been appropriately terminated.

(408) 550-8007 • sales@kaliotek.com

kaliotek.com • 4340 Stevens Creek Blvd., Ste. 250 • San Jose, CA 95129

KalioTek™

Contact us for more information about preparing for secure operations and SOC2 certification.

IT and Security Policies

Your policies are the foundation of your security program, your detailed plan to safeguard your data and operations. They're also the first thing an auditor will ask for in a compliance assessment or in the event of a breach. While templates are available to help you create your policies, these are more than rote tasks to check off. There are real choices to make that will define your exposure and impact your employees' daily work.

Vendor Management Process

You rely on a core set of vendors and service providers to run your business – your digital supply chain. They may have access to some of your systems and share data. You need to know which are authorized and that they follow strong security practices. As 3rd-party solutions proliferate in our companies at the individual and department level, we need tools and processes to stay on top of this.

About KalioTek

KalioTek's mission is to partner with growing life sciences organizations to provide access to a wide range of IT and security expertise in a flexible, as-needed, and affordable model. Since 2002, our team has served hundreds of emerging and midsize companies. Our client base requires that we stay on top of IT and security technologies as they evolve and understand the solutions that are appropriate for this specific market.

For more information or to inquire about how KalioTek can help your company with some of the solutions described above, contact us at 408.550.8007 or sales@kaliotek.com.