



Increase Customer Confidence and Peace of Mind with SOC[®] Reports

SOC[®] reports provide a basis for a general set of controls and testing and verify that an organization is adhering to uniform best practices for their IT controls. Having a SOC[®] report allows your organization to be audited just once, instead of repeatedly by every client or business partner that you work with. OCD Tech is a provider of SOC2[®] reports, which can be either type I or type II depending on your organization's needs and timing, as well as SOC3[®] and SOC for Cybersecurity[®] services. Each of these report types are outlined below.

SOC2[®]

Report of controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy.

SOC3[®]

General use report for service organizations.

SOC for Cybersecurity[®]

A framework developed by the AICPA to ensure effective cybersecurity risk communication management.

SOC 2[®] Assessment and Report Types

A SOC 2[®] assessment provides current and potential clients with the assurance that your organization is taking the necessary steps to protect their private information. This helps you gain new clients and retain existing ones thereby allowing you to focus on your business with the peace of mind that you are doing all you can to ensure that customer data is protected and secure.

SOC 2[®] Readiness Assessment

Time spent before the audit where OCD Tech identifies what processes and documentation the client has in place to meet the SOC 2[®] and the gaps where they don't. The client is then responsible for remediating those gaps with OCD-Tech guidance. (1-6 months depending on the number of gaps and the clients availability to remediate them)

SOC 2[®] Type 1 Report

OCD Tech tests each of the processes identified by the client against the supporting policies and procedures and then prepares the supporting documentation. (About 2 weeks) The above is sent through a review process by a proofreader, QA, and CPA for review and sign off (up to 3 weeks).

SOC 2[®] Type 2 Report

The audit period is either 6 or 12 months. OCD Tech tests each of the processes identified by the client by reviewing evidence that the process occurred over the audit period. (testing is usually completed a month after the audit period) The above is sent through a review process by a proofreader, QA, and CPA for review and sign off (up to 3 weeks).

Understanding the Benefits of SOC 2®

SOC 2® reports are intended to meet the needs of a broad range of users that need to understand the internal control at a service organization as they relate to security, availability, processing integrity, confidentiality, and privacy. These reports are performed using the AICPA Guide: Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy and are intended for use by stakeholders (e.g., customers, regulators, business partners, suppliers, directors) of the service organization that have a thorough understanding of the service organization and its internal controls.

Criteria Areas for Security Testing

Control Environment
Communication and Information
Risk Assessment

Monitoring activities
Control activities
Logical and Physical access controls

System operations
Change management
Risk mitigation

Understanding SOC 3®

SOC 3® reports are designed to meet the needs of users who want assurance on the controls at a service organization related to security, availability, processing integrity, confidentiality, or privacy but do not have the need for or the knowledge necessary to make effective use of a SOC 2® report. These reports are prepared using the AICPA/ CPA Canada (formerly Canadian Institute of Chartered Accountants) Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Because SOC 3® reports are general use reports, they can be freely distributed.

Understanding SOC for Cybersecurity®

Companies are facing increasing demands to demonstrate to stakeholders that they are sufficiently managing cybersecurity threats. While the SOC2® and SOC3® frameworks deal with controls as pertaining to Security, Availability, Processing Integrity, Confidentiality, and Privacy, no framework had existed to report on the protections provided by a cybersecurity risk management program – until now.

To address this need, the AICPA has developed a cybersecurity risk management reporting framework that assists organizations as they communicate relevant and useful information about the effectiveness of their cybersecurity risk management programs. The framework is a key component of a new System and Organization Controls (SOC®) for Cybersecurity engagement, through which a CPA reports on an organizations' enterprise-wide cybersecurity risk management program. This information can help senior management, boards of directors, analysts, investors, and business partners gain a better understanding of organizations' efforts.

About Us

OCD Tech is the IT Audit, Security, and Assurance division of O'Connor & Drew, P.C. Comprised of a team of IT industry veterans, OCD Tech utilizes industry recognized frameworks and leading practices to assess your company's technology risks and provide expert analysis and recommendations for actionable improvements to protect your systems, data, and your overall business from cyber threats and attacks. We have provided SOC® services to countless organizations just like yours and would welcome the opportunity to answer your questions and address your specific needs.



Contact Us



Michael Hammond, Principal
CISA, CRISC, CISSP
Phone: 844-OCDTECH
Email: mhammond@ocd-tech.com



Cera Adams, Manager, Assurance Services
CISA, CRISC, AICPA SOC for Cyber Certified
Phone: 844-OCDTECH
Email: cadams@ocd-tech.com

Braintree | Winchester

Tel: 617.471.1120 • www.ocd-tech.com • Twitter: @TheOCDTech