RISK & ACCOUNTING ADVISORY SERVICES

SOC 2 Services

Validating the Controls You Provide to Your Clients

With more organizations outsourcing significant components of their IT systems and infrastructure to outside service providers, it has become critical for stakeholders (e.g., customers, regulators, business partners) to be confident that those service providers have implemented adequate controls to achieve data security and confidentiality, resource availability, processing integrity and compliance with privacy requirements associated with personal data. A key step to providing this assurance is through a System and Organization Controls ("SOC") 2 or SOC 2+ report - a single management control report that reduces headaches resulting from multiple audit requests from your client organizations.

The primary users of SOC 2 reports are your executive management and the management team of your customers. A SOC 2 audit will include examinations of:

Fair Presentation

How policies and procedures are designed, implemented and documented, including automated and manual functions, support services and report delivery.

Design Effectiveness (for Type I & Type II)

How your company identifies risk and how that risk is mitigated. Understanding transaction flow, and how controls are designed and implemented.

Operating Effectiveness (for Type II only)

How your firm's management monitors controls and independent testing, ensuring controls are applied consistently throughout the reporting period.

Cherry Bekaert LLP
CPAs & Advisors

SOC 2 Reports are Based on AICPA Trust Principles

- **Security** – Is the system protected against unauthorized access (both physical and logical)?
- **Availability** – Is the system available for operation and use as committed or agreed?
- **Processing integrity** – Is the system processing complete, accurate, timely and authorized?
- **Confidentiality** – Is information designated as confidential protected as committed or agreed?
- **Privacy** – Is personal information collected, used, retained, disclosed and destroyed in conformity with the entity's privacy notice and Generally Accepted Privacy Principles ("GAPP")?

In addition, the AICPA allows service providers to incorporate other frameworks into their SOC 2 audit, resulting in what is referred to as a SOC 2+. These reports can be used to demonstrate assurance in areas that go beyond the TSPs in order to include compliance with various regulatory and industry frameworks. Examples include:

- NIST 800-53 or 171
- ISO 27001
- HITRUST (HIPAA Compliance)
- PCI
- Cloud Security Alliance ("CSA")
- Cybersecurity Maturity Model Certification ("CMMC")

Trusted Advisors Throughout the Process

With Cherry Bekaert, we provide the personal attention you deserve whether you are going through the SOC audit process for the first time or the fifteenth. We create a detailed timeline and agenda for each project with specific milestones to be met along the way. Our team does not simply provide audit services. Rather, we are committed to learn your business, provide valuable solutions and guide you through an efficient audit process.

About Cherry Bekaert

v. 05.27.2022 Brochure_RAAS_SOC2-Services_770152250

Let Us Be Your Guide Forward

To speak to a Cherry Bekaert professional about the SOC reporting services, please contact us at **SOC@cbh.com** today.

Steven Ursillo, Jr., CPA, CISA, CISSP, CCSFP
Partner, Risk & Accounting Advisory Services
sursillo@cbh.com
401.250.5605

Dan Sembler, CPA, CISA
Partner, Risk & Accounting Advisory Services
dsembler@cbh.com
919.782.1040

cbh.com/cyber

Cherry Bekaert LLP
CPAs & Advisors