System and Organization Controls (SOC) Reports

Service organizations are entities that provide services—such as payroll or web-hosting—to other entities. SOC for Service Organizations reports are issued by an independent CPA to assist service organizations in building trust and confidence in the service provided and controls related to those services. There are three types of such services.

SOC 1® – SOC for Service Organization: ICFR

Report on Controls at a Service Organization Relevant to User Entities’ Internal Control over Financial Reporting

Reports prepared in accordance with AT-C 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting, are intended to meet the needs of user entities and user auditors in considering the controls at the service organization and their impact on the user entities’ financial statements. User entities are entities that use the service organizations’ services. User auditors are the auditors of user entities. Use of these reports is restricted to the management of the service organization, user entities, and user auditors.

There are two types of reports for ICFR engagements:

- **Type 1** – Report on the fairness of the presentation of management’s description of the service organization’s system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.
- **Type 2** - Report on the fairness of the presentation of management’s description of the service organization’s system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.

SOC 2® – SOC for Service Organizations: Trust Services Criteria

Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

These reports are designed to meet the needs of users that seek detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users’ data and the confidentiality and privacy of the information processed by these systems. The emphasis within SOC 2 reports is not on ICRF, but the operational fitness of the system. These reports can play an important role in:

- Oversight of the organization
- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight
Similar to a SOC 1 report, there are two types of reports, with similar differences: A type 1 report is on management's **description** of a service organization's system and **the suitability of the design of controls**. A type 2 report is on management's description of a service organization's system and **the suitability of the design and operating effectiveness of controls**. Use of these reports are **restricted**.

**SOC 3® – SOC for Service Organizations: Trust Services Criteria for General Use Report**

These reports are intended to meet the needs of users who seek assurance about the controls at a service organization relevant to security, availability, processing integrity confidentiality, or privacy, but do not seek or have the knowledge required to make effective use of the detail in a SOC 2 Report. Since SOC 3 reports are **general-use reports**, they can be freely distributed. The most common examples of a SOC 3 report are WebTrust and SysTrust.