SOC Risk Assessment

One of the challenges that many service providers face while completing a SOC 2 engagement is addressing the risk assessment criteria found in TSP Section 100: 2017 Trust Services Criteria (TSC) for Security, Availability, Confidentiality, Processing Integrity, and Privacy. Performing an annual risk assessment does not mean the TSC related to risk assessment have been effectively addressed.

If any of the criteria listed below are not addressed in the risk assessment, the service auditor's opinion may need to be modified in the SOC 2 report. In order to address the TSC, many organizations will need to update their risk assessment methodology / process.

Risk Assessment Overview

Risk assessment criteria found in the TSC are as follows:

CC3.1	The entity specifies objectives with enough clarity to enable the identification and assessment of risks relating to objectives
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions
CC9.2	The entity assesses and manages risks associated with vendors and business partners

Methodology

With over a decade of experience working on SOC reports, we have developed a risk assessment methodology to address all the requirements of the 2017 TSP criteria.

Our framework utilizes traditional risk assessment methods where inherent risk is calculated by multiplying impact by likelihood. Our process is focused on the SOC 2 trust services criteria and the underlying COSO and AICPA report guidance.

AuditOne LLP will work with your management team to evaluate your relative risk across all relevant trust services criteria. When completed you will have SOC 2 compliant risk assessment and a detailed relative risk analysis of your information security controls.

About AuditOne LLP

AuditOne LLP provides a cost-effective program to deliver globally recognized third-party security audit reports. Our SOC audit reports establish confidence in your organization, can be used as a sales tool, and are often required by larger companies for due diligence purposes. The AuditOne LLP audit process is simpler, and a far less time consuming compared to other third-party security audits.

Robert Kluba CISM CISSP
Managing Director
Phone: 408.656.9300
Robert.Kluba@AuditOneLLP.com

https://www.AuditOneLLP.com