KFI WHITE PAPER:
Risk Assessment in a SOC 2

SOC for Service Organizations: Trust Services Criteria

One of the challenges that many service organizations face while completing a SOC 2 engagement is addressing the risk assessment and risk mitigation criteria found in *TSP Section 100: 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (TSC). In a similar respect, one of the challenges that service auditors face is gathering adequate evidence that the service organization's risk assessment addresses all of the relevant criteria. Just because a risk assessment is performed annually does not mean that the TSC related to risk assessment have been effectively addressed. And if any of the criteria which we will discuss 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.

The objectives of this whitepaper are to:

- Identify the risk assessment and risk mitigation criteria that must be addressed in every SOC 2 and provide practical guidance to service organizations on how to address them

- Provide guidance to service auditors on the types of controls that they should look for to address the risk assessment and risk mitigation criteria

By Jamie Kilcoyne, CPA, CISA, CITP, CIA, CFE - K Financial

The risk assessment criteria found in the TSC are as follows:

CC3.1	The entity specifies objectives with sufficient 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

How to Address the Risk Assessment and Risk Mitigation Criteria

CC3.1:

In order to address CC3.1 in a SOC 2, the service organization should specify its objectives as part of its risk assessment. The reason that this criteria is listed first is that it is the most important part of the risk assessment process. All risk assessments should be built around and upon an organization's specified objectives. According to paragraph .14 *of TSP Section 100,* "objectives" for service organizations receiving SOC 2 reports should include meeting commitments to customers. There can be other operational, compliance and financial objectives in the risk assessment as well, but meeting customer commitments should always appear in a service organization's risk assessment. Example customer commitments that are common for service organizations are:

- 99.5% up-time / system availability
- Maintain confidentiality of customer data

CC3.2

Once the service organization's objectives have been clearly specified, the risks to the achievement of the objectives should be analyzed. Building on the example above:

Objectives	Risks
99.5% up-time	A natural disaster may take down the data center where the service is hosted
Maintain confidentiality of customer data	An employee may steal sensitive customer data and sell it

CC3.3

CC3.3 can only be addressed if the service organization specifically considers the potential for fraud and the related risks to the achievement of objectives. Building on the previous example:

Objectives	Risks	Fraud considerations
99.5% up-time	A natural disaster may take down the data center where the service is hosted	No specific fraud factors identified
Maintain confidentiality of customer data	An employee may steal sensitive customer data and sell it	There are certain employees currently employed by the organization with access to significant amounts of customer data. Some of these employees are in jobs that do not pay very well so they may have an incentive and pressure to capitalize on customer data that they can access.

CC3.4

In order to address CC3.4, the risk assessment should include the identification and assessment of changes that could significantly impact the system of internal control. Examples of changes that may be relevant to the risk assessment include:

- External Environment – Changes in the regulatory, economic and physical environment in which the entity operates
- Business Model – New business lines acquired or divested business operations, rapid growth and new technologies
- Leadership – Changes in management and respective attitudes and philosophies on the system of internal control
- Changes in systems and technology
- Changes in vendor and business partner relationships

CC9.1

This criteria can be addressed in either the risk assessment or in separate business continuity (BC) / disaster recovery (DR) plans. The risk mitigation activities required by CC9.1 include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the entity's objectives during response, mitigation and recovery efforts.

CC9.2

In order to address CC9.2, the risk assessment should include a very specific analysis of the risks associated with vendors and business partners. This starts with an identification of key vendors and business partners and an analysis of how the loss of key vendors and business partners will be handled. Some companies perform a separate vendor risk assessment and this is an effective manner to address CC9.2.

Conclusion:

Service Organizations – Seize the opportunity to review your risk assessment methodology / process and update it if necessary to include the TSC discussed above. This is a chance to improve your risk assessment and make it more meaningful.

Service Auditors – Seize the opportunity to help your clients improve their risk assessment process. If you identify instances where the TSC discussed above are not addressed in your clients' risk assessments, help them to close the gaps by providing recommendations on how to address the TSC in an efficient and effective manner.

Remember that there is not a "one size fits all" for risk assessment. The risk assessment TSC are only guidelines. Each organizations' risk assessment should be carefully tailored to suit their needs and address the unique risks that they face.