KFI WHITE PAPER:
Evaluating Exceptions in a SOC Engagement and Managing the Risk of a Qualified Opinion

One of the most challenging aspects of a System and Organization Controls (SOC) engagement is evaluating exceptions/control failures and determining how they will impact the SOC report and whether they will result in a qualified or adverse opinion. There is a significant amount of judgment involved in this evaluation, but essentially it comes down to responding to the following questions:

- For a SOC 1: Do the exceptions result in a failure to achieve one or more control objectives?

- For a SOC 2: Do the exceptions result in a failure to effectively address one or more Trust Services Criteria (TSC)?

"Yes" responses to the questions above may result in the need to modify the service auditor's opinion. The purpose of this whitepaper is to help service organizations understand the process that service auditors follow to evaluate exceptions and present practical strategies to reduce the impact of exceptions on the service auditor's opinion.

When the service auditor brings exceptions to the attention of the service organization (which should happen as soon as the exceptions are identified), it is important that the discussion about these exceptions includes how they will potentially impact the opinion. At the time that this initial conversation occurs, the service auditor will not have reached a conclusion on the impact of the exceptions because he/she still needs to evaluate:

1. Whether there are compensating controls that are operating effectively.
2. The root cause of the exception(s).
3. Other qualitative aspects of the exception(s) that may reduce the level of risk.

In some cases, the exceptions will pertain to non-key controls and there will be sufficient compensating controls so that there is no impact on the service organization's ability to achieve control objectives (SOC 1) or address TSC (SOC 2). In these situations, the exceptions will not result in a modification of the service auditor's opinion.

Here is a common example of this scenario:

> One of Company X's detective controls related to logical access is that a quarterly access review is performed and unnecessary accounts/ accounts of terminated employees are disabled. The service auditor selects a sample of two quarters and determines that the access review was not performed for one of the quarters. Therefore the control was not operating effectively. However, Company X has a key preventative control that addresses the same risk — *accounts of terminated employees are disabled by IT within 24 hours and are tracked in the ticketing system.* This control was also tested and was determined to be operating effectively. Assuming that other key logical access controls related to new user provisioning, passwords and system authentication are operating effectively, then the exception related to the quarterly access review will not likely have any impact on the service auditor's opinion.

Both of the controls discussed above (quarterly access review and disabling of terminated user accounts) address the same risk — that terminated employees may access data and systems and perform malicious activities. However, disabling system access for terminated employees is considered to be a key preventative control and the quarterly access review is generally considered to be a non-key detective control that is designed as a second level of defense.

Building on the same logical access example, assume that the scenario is reversed.

> The quarterly access review control was operating effectively, but Company X did not disable accounts for three terminated employees out of a sample of 20 within 24 hours. In the absence of compensating controls related to terminations/disabling accounts, the logical access control objective (SOC 1) has not been achieved and logical access TSC (SOC 2) have not been adequately addressed. The quarterly access review is not considered to be a sufficient compensating control in this scenario because it would not detect unauthorized access in a timely manner.

As noted above, there should be an immediate meeting of the minds between the service auditor and service organization when exceptions are identified. This is often a brainstorming session where the service organization and service auditor bounce ideas off of each other about compensating controls. One of the common compensating controls that companies can use when they have a breakdown in their logical access removal controls is the following:

> *On the day of termination, employee card keys to the office facility, VPN tokens, laptops and other company equipment are collected and the IT department completes a termination checklist to document these activities. It is only possible*

to access systems and data from a company workstation or remotely with a company laptop and VPN token.

If this control is in place and operating effectively, it may reduce the risk associated with the system access removal exception described above to an acceptable level and the service auditor's opinion would not be modified.

The evaluation of exceptions should always include consideration of qualitative factors. Using the logical access example, assume that the exceptions were employees in the marketing and sales departments who did not have access to production assets or any sensitive customer data. In this scenario, the risk that the terminated employees could access, steal or destroy sensitive systems and data is considered remote. The service auditor may conclude in this situation that the risk associated with the exceptions is acceptable and will not cause the opinion to be qualified.

Another common example of an exception that we see in SOC control testing is related to the following control:

The Company has installed anti-malware or anti-virus solutions on all critical servers and updates these solutions at least weekly with the latest virus signatures.

Often times, our testing reveals one or more servers that are not running anti-malware or anti-virus solutions or the solutions have not been updated for several months. However, if the organization uses a file integrity monitoring (FIM) tool that would detect changes/issues on servers in a timely manner or they have other compensating controls in place, then the risk associated with the exception(s) may be acceptable and it may not have any impact on the service auditor's opinion. Furthermore, if the servers that were missing anti-malware/anti-virus sit outside the production environment and/or do not house any sensitive data, this could significantly reduce the risk associated with the exception.

The use of a FIM tool can also be an effective compensating control when there is an issue with change management. For example, assume that one of Company X's control is that all software changes are tested and approved before being moved to production. In a sample of 20 software changes, however, there was no evidence that two changes were tested and approved. If a FIM tool is in place, configured properly and operating effectively, then it would identify suspicious changes and alert the appropriate parties immediately so that they could be investigated. This could potentially reduce the impact of the change management exceptions to an acceptable level so that a qualified opinion could be avoided. In addition, if the changes simply involved low-risk cosmetic fixes to the

software and did not impact security, then the risk associated with the exceptions may be deemed to be acceptable.

In conclusion, exceptions in a SOC engagement are challenging for both service organizations and service auditors. But they also provide an opportunity for companies and their auditors to collaborate, strengthen their business relationship and drive improvement in the overall control environment. The key steps that service organizations and their auditors should follow in the exception evaluation process are:

1. Discuss the exception(s) and the impact that they will have on the report and the opinion. This discussion should occur as soon as possible after the exceptions are identified. Sometimes this discussion will help clarify the type of documentation that is required and an alternative form of evidence may be identified that can result in the resolution of the exception(s).
2. Evaluate whether there are compensating controls related to the exception(s). There could be significant controls that the auditor is not aware of that do not appear in the report. Such compensating controls could reduce the risk associated with the exception(s) to an acceptable level.
3. Evaluate the nature and risk level of the exception(s). Qualitative aspects of exceptions are important.
4. Evaluate the root cause of the exceptions (i.e., why the exceptions occurred).

When service organizations and service auditors work together, they can often find strategic ways to minimize the impact that exceptions have on SOC reports and avoid a modified (qualified or adverse) opinion.