How to Properly Review a SOC Report

There continues to be a great deal of confusion over the new service organization reporting structure and which reports are the best to obtain. The basic intentions of the reports are as follows:

SOC 1 – Related to Internal Control over Financial Reporting
SOC 2 – Related to testing over the Trust Services Principles of Security, Availability, Processing Integrity, Confidentiality and Privacy
SOC 3 - A simplified report on the same principles in a SOC 2 and available for public use

In this article we won't go into the details of what report you need to obtain. That information can be found in the post titled "Which SOC Report is Right for You?" Here we'll help answer the question of what you should be doing once you get the report in your hands. Properly reviewing these reports is an essential part of the vendor management and risk management functions, and should be taken very seriously. You are only as strong as your weakest link, which could indeed be your vendors.

Obtaining the Correct Report:
When obtaining the report, make sure it is the correct one. There are vendors that issue anywhere from 1 to sometimes more than 30 reports for different areas of their business. To increase the efficiency and effectiveness of your review, ensure you have the correct one. If you are reviewing card issuance procedures, the item processing report will not suffice.

Time Period of Report:
The time period of the report should be reviewed to ensure it covers the needs of the user. Reporting periods vary and often don't cover full calendar years (i.e. reporting period of October 1, 2013 – September 30, 2014). Make sure the time period meets your needs. If there is a gap between the report and the time period you require for your review, you can obtain what is called a bridge letter or comfort letter stating what has occurred since the issuance of the report. It is a best practice to ensure the report you obtain covers a time period of at least six months, with nine to twelve months being ideal.

Auditor Performing the Report:

When reviewing the report elements, make sure a reputable firm such as The Mako Group performed it. We have noticed a great deal of "bargain-basement" reviews being performed that don't properly cover the elements needed for a complete report. If the report and firm are not doing a comprehensive review, reliance on that report could severely affect your risk profile.

Report Coverage:
The controls tested in the report should cover the services you rely on the service provider for. The level of specificity varies based on scope, auditor and service provider control structure. Review the report in detail to ensure your areas of concern and reliance are covered. If they are not, alternative procedures may be necessary.

The service auditor's opinion on the operating effectiveness of the controls:
The auditor will opine in the report on the operating effectiveness of the controls as being Effective or Ineffective. If an Ineffective opinion is given, serious investigation should be put into why. Ineffective controls at a key service provider could have serious consequences on your own control environment.

Management's opinion on the operating effectiveness of the controls:
Like the service auditor, management also opines on the operating effectiveness of controls. The same considerations should be taken as were done with the auditor's opinion. If the two opinions differ, investigation of why should be performed.

Inclusion of control environment in reports:
An aspect of reports that may have not been included in the past is description of the service organization's control environment. This description can provide valuable insights and should be reviewed if present.

Control Exceptions:
Each report contains a section listing out the controls tested and the results of that testing. Any exceptions noted should be investigated for possible impacts on your process. This especially holds true for controls being relied upon. Vendors who have mature risk management and internal control functions have a minimal amount of exceptions in these reports. If you are seeing a high number, your level of caution should be raised.

User Control Considerations:
Most reports contain a section listing controls that should be in place at the user (your) organization. These sections are typically called User Control Considerations, Complementary User Entity Controls or Description of Client Considerations. These are

controls the service organization is assuming you have in place. They may not all be applicable to your business, but this section provides some great insight and may point out gaps in your control structure. Each user control consideration should be reviewed and addressed as applicable.

Subservice Providers:
Your service providers may be outsourcing part of the service they provide you. This could include hosting, helpdesk and other essential functions. The report you are reviewing should list what activities are outsourced. The term used in the report is most typically "subservice provider". You should determine if you rely on that subservice and if you need to obtain a report from the subservice provider or perform any other sort of investigative activities. Remember, you are only as strong as your weakest link.

Controls Relied Upon & Reports Relied Upon:
As was mentioned before, it is a good idea to keep a running listing of reports and controls you rely upon at your service organization. This will increase the efficiency and effectiveness of your review and will help manage your risk.

Performing your reviews with the proper amount of rigor will ensure you are practicing proper risk management. It is a best practice to create an internal checklist for reviewing the reports to ensure all areas are covered. We hear stories every week regarding weaknesses at vendors and resulting control breakdowns and in some cases data breaches. The Mako Group can assist you with your reviews and also the establishment of a proper Vendor Management program. Reach out to us at any time. Making our clients stronger is our reason for being.

Shane M. O'Donnell, CISA, CPA, MSA
Chief Audit Executive
March, 2014