Reducing risk in the vendor due diligence process

December 06, 2019

Lenders increasingly contract with third-party vendors to outsource a wide variety of essential services. While outsourcing has many benefits, it generally does not relieve the lender of the liability or regulatory risk associated with a given activity. As a result, a lender should take care to assess a vendor's suitability and capability to perform given services before engaging the vendor to carry out those services for the lender. Due diligence is critical, but what diligence is "due" and how can you trust the information provided? Part of the answer may be a Service Organization Controls (SOC) Report.

SOC Reports are standard reports designed by the **American Institute of Certified Public Accountants** (AICPA) on a service organization's controls over security, availability, processing integrity, confidentiality, and privacy. SOC audits are conducted by independent auditors and are designed to give outside parties the ability to verify a service provider's internal controls. Upon conclusion, the auditors issue formal reports – SOC Reports – identifying the industry standard, the state of the service provider's actual operations, and any material variance between the two.

AICPA recognizes three types of SOC reports:

- **SOC 1** reports review the service provider's financial statements and the financial controls employed in its financial reporting system. These reports also consider the fairness and accuracy of the service provider's description of its financial reporting systems, and the effectiveness of its financial controls.
- **SOC 2** reports look beyond the service provider's financial reporting and provide detailed information about the service provider's operations as they relate to the security, availability, integrity, confidentiality, and privacy of information processed.
- **SOC 3** reports cover the same subject matter as SOC 2 reports but lack detail and do not include descriptions of the auditor's testing methods. For these reasons, SOC 3 reports are referred to as "general use reports" and are designed for broad distribution.

SOC Reports are further distinguished by type. A "Type 1" report reviews the service provider's systems on a specified date, and a "Type 2" report examines its systems over a period of time. While a Type 1 report may answer the question of whether a service provider has internal controls, a Type 2 report will confirm whether the service provider utilizes those controls properly. As a result, Type 2 reports afford a lender a more complete picture of the service provider's internal controls, and not simply a snapshot of its capabilities on a date in time.

When requesting an SOC Report from a service provider, a lender should ensure that it receives the report which best addresses its needs. Because SOC 1 reports emphasize controls over financial reporting, it may not give adequate assurances that the service provider has the internal controls necessary to protect, preserve, and

recover processed transactional or operational information. Similarly, while an SOC 3 report may serve as a starting point, it may not give the level a detail a lender requires. By contrast, the SOC 2 report will provide the lender insight into a service provider's capabilities and practices, to make a more informed choice when selecting a vendor. Finally, lenders should consider the "Type" of report provided. While a Type 1 report will reflect controls maintained by the vendor, a Type 2 report will reflect how the vendor's controls perform over time. In many cases, then, a Type 2 report may be more indicative of actual future performance than a Type 1 report.

Lenders do not need to guess when evaluating the suitability or capability of a potential vendor. Asking for the vendor's SOC Report is an easy step in the due diligence process, and one that may reduce the liability and regulatory risk of outsourcing.

This article was first published on Auto Finance Excellence, a sister service of Auto Finance News, and is reprinted with permission. McGlinchey Stafford is pleased to serve as the official Compliance partner of Auto Finance Excellence, providing insights and thought leadership through webinars, podcasts, and monthly columns.