Crowe

Third Party Controls Attestation

Introduction

Enhanced focus on Internal Controls over Financial Reporting (ICFR) has raised the bar on quality of operating controls. This brings into play the question of control efficacies at service organisations (Vendors) who provide services of a nature that have a bearing on ICFR of their Clients. Vendors with deficiencies in service related internal controls and protocols could negatively impact their existing or prospective clients, and thereby suffer business loss.

Vendors are sometimes requested for SOC certification by their clients, currently mainly clients based in USA. The certification is codified as System and Organization Controls (SOC) attestation reports, mandated by SSAE 16 and SSAE 18. Internationally, this requirement is codified in the International Standard on Auditing 402 - Audit Considerations Relating To Entities Using Service Organizations. Such requirements are not mandatory in India.

This note draws attention to potential benefits for listed companies, public interest entities and businesses with significant Vendor operations in aspects that encompass ICFR. The note also highlights action steps for Vendors to prepare for such certification

The requirement could be from audit or governance perspective

What is SOC attestation

SOC or equivalent reports address effectiveness of operating controls and service protocols of Vendors; these are not an audit on financial statements of the Vendors. To illustrate, if a Vendor processes payroll for its Client, or provides an HR management system, or cloud platform for the Client to process payroll, the Client and its auditor would be interested in satisfying the internal controls of the Vendor relating to the payroll processing, payroll management system, or cloud platform as the case may be.

The SOC audit reviews the compendium of safeguards built within the control base of the data and processes, and reports on the effectiveness of those safeguards.

A SOC report from Vendors dealing with high-risk operations of Clients business would help the Client towards regulatory compliance assistance (e.g. ICFR audit) or as a GRC measure.

SOC Reports – different scope & coverage

SOC reports could be SOC1, SOC2 or SOC3. The differences are fundamental; it is not that SOC2 and SOC3 are higher versions – there is a difference in scope and coverage.

Further, SOC1 and SOC2 reports have Type I and Type II report options. Type I reports cover controls as at a point of time; Type II reports covers a minimum test period of 6 months for the subject matter.

SOC1 Report

SOC1 reports focus only on Vendor controls relevant to the Client's financial reporting. SOC1 reports are best suited for evaluating the effect of controls at the service organization on the user entities' financial statements. These help create confidence in the controls and safeguards the Vendor exercises over clients' financial data, and thereby support the ICFR and governance needs of the Client and the Client's auditor. Use of these reports is restricted to the management of the Vendor, Client, and Client's auditors.

SOC1 Type I report pertains to controls testing at a point of time, i.e. on a specific single date. SOC1 Type II reports are more rigorous and are based on testing of controls operation over a period of time; for this reason, these carry greater reliability of internal controls.

SOC2 Report

SOC2 is the most sought-after report in this domain and a must for services from Vendors in an IT based ecosystem. The scope of SOC2 is different in that it deals with examination of the Vendor's controls over one or more Trust Service Criteria (TSC). The TSC are Privacy; Confidentiality;

Processing Integrity; Availability; and Security.

SOC2 is built around the definition of a consistent set of parameters for technology driven services which a Vendor provides its Client. It enables the Client to understand and satisfy the metrics for the 5 key attributes or TSC, concerning the Vendors services. A Client who needs satisfaction on these 'trust principles' must seek a SOC2 report.

SOC2 also has two report types. Type I confirms that controls concerning the TSC exist on the audit date. Type II report affirms that the controls are in place, and are working well for a minimum period of 6 months. Obviously, the Type II is a better representation of how well the Vendor is doing for protection and management of client data.

SOC3 Report

SOC3 is a summarised report of the SOC2 Type II report; it is not as detailed as SOC2 reports are. A SOC3 report is designated to be a less technical and detailed audit report, with a seal of approval which could be put up on the website of the Vendor. However, because it is less detailed and less technical, it does not contain the same extent of controls audit which a Client might require.

Besides ICFR, SOC reports help risk management - protect your business, data and reputation

Value, Beyond Compliance

The process of preparation and audit towards SOC certification helps the Vendor identify, correct and smoothen control shortcomings that may have crept in – a periodic examination is always valuable. Enhanced Client comfort from a SOC report will smoothen any operating concerns, enable continued use, or deeper use, of Vendor's services. The benefit percolates to Client and Vendor.

Preparing For SOC Certification

There is always a first time when a Vendor is asked for a SOC report – either by an existing client, or a prospective client. Or a Vendor may choose to be proactive to get the services certified, possibly as a valuable tool to support business prospects. In the first situation, one is often scrambling for a response; in the latter situation, one is planning ahead. The broad process in each case is the same – preparation based on anticipation helps a smoother and more effective completion, as against preparation under compliance time-lines. You need to

a. Define the Audit Objectives
b. Determine the Scope of Audit
c. Address regulatory compliance concerns
d. Document / update policies procedures
e. Establish controls in lines with the Trust Service Criteria
f. Perform a Readiness Assessment
g. Hire a professional to do the audit

The process is time consuming and throws up surprises – addressable matters generally, but these need time which is often not available.

Advance planning and action helps avoid a sudden scramble; and address inevitable surprises

Caution – Restrict Report Distribution

SOC1 & SOC2 reports may contain sensitive information about the Vendor; hence these are considered restricted use reports and should be shared only at management level for the Vendor, Client and Client's auditors (if needed to support ICFR requirements). On the other hand, SOC 3 may be considered as general use reports, possibly for wider circulation.

Professional Services

Crowe Advisory Services India has a team to

- Provide SOC audit and certification
- Assist in preparation for SOC reporting

Cross-border engagements can be executed on remote basis, together with Crowe offices in different countries

About Crowe India:

Crowe Advisory Services (India) LLP provides Risk Advisory, Corporate Finance, Taxation, Business Advisory, Digital Security Consulting, Data Sciences and Business Process Outsourcing services. We have offices in eight cities in India.

We are a member of Crowe Global, the eighth largest accounting and consulting network worldwide, with 765 offices across 146 countries.

Key Digital Security Contacts:

Anil Aravind, Director, Digital Security Services
anil.aravind@crowe.in

Abhijeet Nath, Director, Digital Security Services
abhijeet.nath@crowe.in

Narasimhan Elangovan, Senior Consultant
narasimhan.elangovan@crowe.in

Crowe Advisory Services (India) LLP
1105 Embassy Centre, Nariman Point, Mumbai 40021
+91 22 6631 1480
www.crowe.in