Service Organization Controls (SOC) Reports for Certain Critical Service Contracts – Sample/Draft Language for Requirement Document

# Background

The Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government*, commonly known as the “Green Book”, provides internal control considerations for service organizations. The Office of Management and Budget (OMB) Circular A-123, *Management’s Responsibility for Enterprise Risk Management and Internal Control,* discusses management’s responsibility for oversight of Service Organizations. The American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) No. 18, *Attestation Standards: Clarification and Recodification*, provides the standard for auditing and reporting on service organization controls.

# Discussion

VA may engage external parties to perform critical operational processes such as accounting and payroll processing, information and systems security services, health care claims processing and digitization, etc. These external parties are referred to as *service organizations*. VA management retains responsibility for the performance of processes outsourced to service organizations and will monitor the service organizations’ internal controls. VA also retains responsibility for the risks associated with the outsourced processes. Management should establish user controls—processes and procedures to complement service organization controls, and monitor services provided by the service organizations. The extent of VA’s oversight of service organizations’ controls depends on the nature of the contract or agreement.

VA management should provide increased oversight of a service organization when the service organization’s activity is significant to VA’s financial statements. Accordingly, VA should obtain SOC reports for any outsourced function that is significant to the specific department/office operations and the department/office should have monitoring controls over the review of those reports including implementing compensating controls in the event of control failures noted in those reports. Obtaining and monitoring SSAE -18 reports is a way to limit VA’s risk if the Vendor’s own lack of controls over financial operation and information security may lead to substantial misrepresentation of VA’s financial information, impairment of security controls or breach of privacy data.

If a service organization’s activity is significant to VA’s financial statements, requiring a Service Organization Controls (SOC) 1 Type 2 audit and report may be warranted.

If a service organization’s activity related to information systems (including information security and privacy data controls) could seriously jeopardize VA achieving a substantial mission objective, requiring a SOC 2 Type 2 audit and report may be warranted. Examples include services such as the ability to access electronic health records or ability to pay VA employees in a timely way, etc.

The American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 18, Attestation Standards: Clarification and Recodification (SSAE 18) suggests that management should work with their supporting (VA) contracting officer to establish contractual requirements to obtain independent audit reports attesting to the controls of service organizations and for those organizations performing services that are material to either VA’s financial statements or mission objectives. Service Organization Controls (SOC) (recently renamed System and Organizational Controls (SOC) for Service Organizations) reports most relevant to VA contracts include:

1. SOC 1, Type 2 – Reports on the design and operating effectiveness of controls for a service organization significant to VA’s internal controls over financial reporting throughout a specified period. These reports, prepared in accordance with SSAE 18, section 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting, are specifically intended to meet the needs of entities that use service organizations (user entities) and the CPAs that audit the user entities’ financial statements (user auditors), in evaluating the effect of the controls at the service organization on the user entities’ financial statements.

2. SOC 2, Type 2 – Reports on the design and operating effectiveness of a service organization relevant to Security (of Information and Systems), Availability (of Information and Systems), Processing Integrity, Confidentiality, and Privacy throughout a specified period.  These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users’ data and the confidentiality and privacy of the information processed by these systems.

Initial SOC Reports should cover a minimum of 9 months of performance under the contract.

Subsequent SOC Reports should cover 12 months of performance under the contract.

In the event the service provider is unable to complete their SOC Report timely, VA management should document performance of internal control to avoid over-reliance on contractor processes and contractor-provided data. Management should also ensure the SOC Report(s) cover a substantial portion of the fiscal year and bridge letters are considered.

The sample/draft language below is generic and may be edited to meet the needs of the user organization requesting the service contract.

**Sample/Draft SOC Report/SSAE 18 Requirement**

X.X.X. Service Organization Control (SOC) Reporting

***[Insert this section if SOC 1 Report is needed]*** The Contractor must engage an independent external auditing firm to conduct a Service Organization Controls (SOC) (now called System and Organizational Controls (SOC) for Service Organizations) examination and produce a Report on Controls at a Service Organization Relevant to User Entities Internal Control over Financial Reporting, SOC 1 Type 2 Report, in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 18, Attestation Standards: Clarification and Recodification (SSAE 18). The contractor must provide VA with a written copy of the SOC 1 Type 2 examination report (the “Prime Report”). The independent auditing firm must have prior experience in conducting SSAE audits. In addition, the Contractor must provide a written copy of the SOC 1 Type 2 report, completed in accordance with SSAE 18, for any material subservice organization (the “Subcontractor Report”). The Prime Report and Subcontractor Reports must address the specific services provided by the Contractor to VA under this contract. The current guidance for SSAE 18 was issued in April 2016. Reference: <https://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/SSAE_No_18.pdf> (Section 320, Reporting on an Examination of Controls at a Service Organization

Relevant to User Entities’ Internal Control Over Financial Reporting). SSAE guidance may be updated during the performance of the contract. The contractor must comply with updates to SSAE 18 and provide new reports using the updated SSAE guidance.

***[Insert this section if SOC 2 Report is needed]*** The Contractor must engage an independent external auditing firm to conduct a Service Organization Controls (SOC) (now called System and Organizational Controls (SOC) for Service Organizations) examination and produce a Report on Controls at a Service Organization Relevant to Security (of Information and Systems), Availability (of Information and Systems), Processing Integrity, Confidentiality, and Privacy, SOC 2 Type 2 Report, (the “Prime Report”) in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 18, Attestation Standards: Clarification and Recodification (SSAE 18). The contractor must provide VA with a written copy of the SOC 2 Type 2 examination report (the “Prime Report”). In addition, the Contractor must provide a written copy of the SOC 2 Type 2 report, completed in accordance with SSAE 18, for any material subservice organization (the “Subcontractor Report”). The Prime Report and Subcontractor Reports must address the specific services provided by the Contractor to VA under this contract. The current guidance for SSAE 18 was issued in April 2016. Reference: <https://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/SSAE_No_18.pdf> (Section 320, Reporting on an Examination of Controls at a Service Organization

Relevant to User Entities’ Internal Control Over Financial Reporting). SSAE guidance may be updated during the performance of the contract. The contractor must comply with updates to SSAE 18 and provide new reports using the updated SSAE guidance.

The independent external auditing firm may be the same firm that provides the SOC 1 Type 2 Report***[Remove this sentence if SOC 1 is not required]***. The report must cover all trust principles to include: Security (of Information and Systems), Availability (of Information and Systems), Processing Integrity, Confidentiality, and Privacy ***[Remove the* *remainder of this sentence if the contractor will not have access to HIPAA data];*** and ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) under those principles.

X.X.X. Service Organization Control Reporting - Specifications and Deliverables

VA’s fiscal year begins October 1 and ends on September 30. The Contractor must submit an initial Prime Report and Subcontractor Reports – ***[insert SOC 1, SOC 2, or SOC 1 and SOC 2]*** for all current business and financial operations, or address specific services provided by the Contractor to VA under this contract. The initial report must cover a minimum of nine months of contract performance in accordance with the Schedule of Deliverables. Any deviation to the initial report minimum period must be approved by VA.

Subsequent Prime Reports and Subcontractor Reports must cover twelve month periods and be submitted in accordance with the Schedule of Deliverables. Such subsequent reports must cover the specific services provided by the Contractor to VA under this contract.

All Prime Reports and Subcontractor Reports must clearly indicate the services, systems, and locations covered by the review, as well as the nature and type of control testing performed. The Contractor must also account for controls over subservice organization (Subcontractor) services and performance. The Contractor must include a cover letter on all Prime Reports and Subcontractor Reports affirming that the Contractor is performing services in accordance with the contract. The cover letter must be addressed to VA and must summarize the results of the audit and the audit tests performed. The letter must highlight unusual items, deficiencies, qualifications, and any inconsistencies with professional standards and provide an indication of actions being taken to address, remedy, or mitigate these or other weaknesses noted in the applicable report.

In the event a Prime Report or Subcontractor Report includes any deficiencies material to the Contractor’s performance under this contract or significant to VA’s internal controls over financial reporting or operational controls to achieve the VA mission, as determined by VA in its sole discretion, VA will notify the Contractor in writing of the need for a Corrective Action Plan (CAP) within thirty (30) days of receipt of the Prime Report. The Contractor must submit the CAP to VA in accordance with the Schedule of Deliverables. The CAP must describe, in detail, actions that will be taken by the Contractor to resolve the deficiencies and the timeline (begin and end dates) for completing each action. The Contractor must implement recommendations from its auditor and the audit report within ninety (90) days from report issuance and must cure any deficiencies to VA’s satisfaction within a reasonable period, but no later than ninety (90) days from report issuance, and at no additional cost to VA.

The Contractor must provide a Bridge Letter in accordance with the Schedule of Deliverables to cover the dates between the applicable Prime Report’s and Subcontractor’s Report period end date and VA’s fiscal year end date (September 30) or the end date of all performance under the contract.

The Contractor must address the Bridge Letter to VA from Contractor senior management and must specify the coverage begin and end dates. The letter must include Contractor management’s assertion whether the processes and internal controls that were in effect during the period covered by the applicable Prime Report and Subcontractor Reports remain in effect, and/or summarize any material changes in the control environment and the impact to VA. The Bridge Letter is not a replacement for the actual Prime Report or Subcontractor Reports.