Leading practices

KPMG Government Institute

Issue brief | June 2017

Effectively evaluating SOC 1 reports in the Department of Defense

The Chief Financial Officers (CFO) Act of 1990 drove financial management reform across the federal government. Included in the CFO Act is the requirement that applicable federal agencies obtain audited financial statements. As one of the agencies required to comply with the CFO Act, the Department of Defense (DoD) continues its journey to become the last CFO Act agency to undergo full financial statement audits. The DoD has made crucial steps towards that goal; as of 2016, a significant number of budget items were subject to audit and all military services underwent audits of current and prior year (2015) budgeted activity.

While progress has been made, significant obstacles remain. Each of the independent auditors that audited the military services in 2016 issued disclaimer opinions and hundreds of findings associated with lack of effective internal control and supportable transactions. Among the many noted findings were DoD components' continued challenge of effectively identifying, demonstrating their evaluation of, and mitigating risks related to the myriad of complex and inconsistently documented relationships held with service providers both within and external to the DoD.

As of the end of fiscal year (FY) 2016, 700 IPA findings and recommendations related to the three military services' FY 2015 and 2016 budgetary schedules remained open. (Source: GAO Report GAO-17-317, "High Risk Series")

DoD components' ability to effectively evaluate and establish key controls associated with external entities to which financial transaction processing and reporting have been outsourced (henceforth referenced as "service organizations") is an important element to achieving preparedness to undergo financial statement audits. System and Organization Controls (SOC) 1 reports are reports on controls at service organizations that are relevant to their customers' (also known as "user entities[1]") internal control over financial reporting. SOC 1 reports include an independent auditor's[2] opinion on, among other things, the effectiveness of the service organization's controls and, as such, are an important means by which user entities can conduct these evaluations.

To help user entities effectively address this complex and persistent obstacle to audit readiness, KPMG LLP prepared this issue brief to highlight leading practices associated with the implementation of service organization/SOC 1 report evaluation programs. We prepared this issue brief based on our experiences supporting DoD audit readiness and sustainment initiatives, serving as the financial statement auditor for 8 of the 15 cabinet-level federal agencies, and conducting SOC 1 engagements for commercial and federal service organizations.

Background

An important aspect of a financial statement audit is the auditor's development of an understanding of the control environment of the entity under audit. This includes, among other things, obtaining an understanding of how the entity undergoing audit considers service organizations to whom

[1] A user entity is "an entity that uses a service organization for which controls at the service organization are likely to be relevant to that entity's internal control over financial reporting." (American Institute of Certified Public Accountants (AICPA), Statement on Standards for Attestation Engagements No. 18, Attestation Standards: Clarified and Recoded, Clarified Attestation Section 320 (AT-C 320), Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting, 2016).

[2] An auditor who reports on controls at a service organization is referred to as a "service auditor". That reference is used in this issue brief.

business processes associated with financial reporting have been outsourced.

The audited entity's (i.e., the user entity's) inability to articulate the relationships it has with its service organizations, how it monitors its service organizations, and how it mitigates service organization risks that are relevant to financial reporting may raise an auditor's concerns about the user entity's control environment and, by extension, the risk that control weaknesses will result in misstated financial reports. The auditor also performs his/her own procedures to identify relevant service organization relationships that the user entity has and the level of financial reporting risk associated with those relationships. Specifically, user auditors determine whether a service organization is relevant to the financial statement audit by obtaining an understanding of the services provided by the user entity's service organizations, including internal control, and considering the impact the service organization has on the user entity's financial statements. The user auditor makes such determinations by obtaining an understanding of the user entity's flow of transactions inclusive of relevant controls provided by the service organization, determines the nature of the relationship between the user entity and service organization (including contractual terms that define services provided by the service organization), identifies the nature of transactions processed and their significance to the user entity's financial statements, and the degree of interaction between the service organization and user entity.

DoD service organizations include the Defense Finance and Accounting Service (DFAS), Defense Logistics Agency (DLA), and Defense Information Systems Agency (DISA).

A common means by which user auditors evaluate controls performed by service organizations is by obtaining and reviewing their SOC 1 reports. A SOC 1 report includes important information about service organization controls for use by user entities and their financial statement auditors ("user auditors") and, among other things, the service auditor's opinion, among other things, of the effectiveness of controls provided by the service organization that are relevant to its user entities' financial reporting processes. A SOC 1 report describes business processes performed by the service organization on behalf of user entities and corresponding controls[3], responsibilities user entities have for implementing effective controls that complement those of the service organization (referred to as complementary user entity controls or "CUECs"), the tests performed by the service auditor, and the results of those tests. Often, service organizations employ other service organizations to perform some activities considered relevant to user entities' internal control over financial reporting. These other service organizations are called "subservice organizations". When subservice organizations exist, the service organization's SOC 1 report should, at a minimum, identify the subservice organization and relevant services provided by the subservice organization, including whether the carve-out method or the inclusive method has been used in relation to them.[4]

Because the SOC 1 report scope is defined by the service organization, the user entity and user auditor conduct evaluations to determine applicability to the user entity. Provided SOC 1 reports are properly scoped, user entities and auditors can leverage such reports to assess service organization control weaknesses for risk/impact on the user auditor's financial statement audit. These evaluations, combined with other assessments, help the user auditor form an overall view of financial reporting risk, which is then used to design the approach for the financial statement audit.

Example:

DFAS processes civilian payroll on behalf of DoD components (user entities). Services include, but are not limited to, the preparation of transaction files that user entities import into their accounting systems. If relevant DFAS controls are ineffective, the risk that transaction files and, by extension, user entity financial statements contain misstatements increases.

A thematic finding by user auditors who have conducted DoD financial statement audits and audit readiness examinations to date has been that DoD components do not have effective processes for obtaining an understanding of financially relevant service organizations, have not evaluated such relationships to identify financial reporting risks, and have not implemented effective internal controls to mitigate

[3] The presentation of such processes and other relevant information in SOC 1 reports is included in a section called management's description of the system, whereby the "system" is "the policies and procedures designed, implemented, and documented by management of the service organization to provide user entities with the services covered by the service auditor's report" AICPA (AT-C 320, Reporting an on Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting, paragraph 8).

[4] The AICPA's AT-C 320, Reporting an on Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting, paragraph 8, defines two methods (carve-out and inclusive) of presenting subservice organizations in a SOC 1 report. Interested readers are directed to AT-C 320 to obtain additional information.

such risks. These findings represent a significant obstacle to DoD components being able to achieve readiness to undergo successful financial statement audits.

The remainder of this issue brief outlines leading practices that user entities can consider operationalizing to demonstrate to their auditors and other stakeholders that they understand, have evaluated, and effectively mitigated service-organization-related risks to their financial reporting processes.

Leading practices for DoD component service organization/SOC 1 report evaluations

As outlined in the section above, user entities' ability to establish an effective evaluation program to assess the impact of service organizations on financial reporting processes through, among other means, the use of SOC 1 reports represents a key success factor in the effort to achieve audit readiness. The imperative nature of implementing such capabilities is not lost on the Office of the Undersecretary of Defense (Comptroller) (OUSD(C)). The Financial Improvement and Audit Readiness (FIAR) Guidance, OUSD(C)'s seminal blueprint for achieving a department-wide audit-sustainment infrastructure, provides direction to DoD components for obtaining an understanding of internal control over financial reporting, to include controls associated with relevant business processes outsourced to service organizations.[5]

In our experience as audit readiness advisors, independent financial statement auditors, and independent service auditors, we have often noted that user entities that have established mature, consistently performed, and formally documented service organization/SOC 1 report evaluation programs:

— Can readily describe the relevance of (and reliance placed upon) their service organizations in the context of the user entity financial reporting process

— Are able to effectively respond to control weaknesses described in SOC 1 reports by clearly articulating relevant risks and compensating or mitigating controls

— Realize favorable audit outcomes compared to user entities that have not established such evaluation programs.

With these observations in mind, we have drawn upon our aforementioned experience to offer the following leading practices associated with the implementation of service organization/SOC 1 report evaluation processes. These leading practices were identified through our observation of user entities at various stages of implementation of service organization/SOC 1 report evaluation programs. Generally speaking, user entities found to have established evaluation programs demonstrated performance of one or more of these practices, while user entities found to have less established (or no) programs demonstrated performance of few or none of these practices.

Formalize the evaluation program

In our experience, there is a recognized need for user entities to establish the appropriate degree of formality in establishing a service organization/SOC 1 report evaluation program. A formally established program helps provide a consistent methodology for the performance, documentation, and communication of SOC 1 report evaluations and results. A formally established evaluation program is supported through the development and implementation of documented methodologies, tools, and job aids to help identify service organization relationships, validate that responsibilities and audit support requirements are completely and accurately documented in signed agreements, and evaluate SOC 1 reports for impact on user entity financial reporting processes.

Remember: ALL DoD components are user entities!

Based on our experience, user entities that have implemented established service organization/SOC 1 report evaluation programs identify resources who will be responsible for various aspects of the evaluations, assign accountability, and establish and document processes for performing evaluations of service organizations and their SOC 1 reports, as well as tools and templates to document key activities. Establishing formalized processes helps user entities identify activities that are repeatable and predictable and activities that are complex, unpredictable, and require specific subject matter specialty. Understanding the complexity, predictability, and requisite subject matter specialty associated with various evaluation activities can help user entities better sequence and delegate such activities, ultimately contributing to a more effective and efficient evaluation process.

Failing to establish a sufficiently formalized program presents potential audit readiness obstacles, including a user entity's:

— Inability to identify relevant service organization relationships

— Inability to understand the scope of the SOC 1 report

— Misinterpretation of SOC 1 report results due to inadequate understanding of reliance on service organizations

— Failure to implement sufficient compensating or mitigating controls to address relevant risks associated with service organizations.

Our experience informs us that entities who formally establish and deploy processes, tools, and templates are able to stand up their evaluation programs in a more efficient and effective manner than those entities who adopt less formal approaches.

[5] OUSD(C): Financial Improvement and Audit Readiness Guidance, April 2017, Section 4.A.2, Consideration of Service Providers.

Demystify, agree upon, and document service organization relationships, roles, and responsibilities

An evaluation of service organization relationships and SOC 1 reports is dependent upon user entities' understanding of the following:

- Their business processes
- Elements of their processes that have been outsourced to service organizations
- The division of responsibility for business processes and controls between the user entity and its service organizations
- The relevant risks to financial reporting as well as other risks

Therefore, user entities require methods for evaluating business processes considered relevant to financial reporting, identifying and evaluating service organization relationships, and recognizing key risks that the user entity expects the service organization to mitigate through its controls.

The FIAR Guidance requires that service organizations and the DoD components they serve agree upon and document audit readiness roles and responsibilities within existing service level agreements (SLAs) or separate memorandums of understanding (MOUs).[6] Establishing these agreements formalizes key service organization and user entity responsibilities and helps to promote compliance. Establishing these agreements to be sufficiently detailed to describe the specific controls and procedures that each party is responsible for helps to avoid misunderstanding/confusion regarding each party's responsibilities. Beyond their utility as mechanisms to help assure coordination between service organizations and user entities, these agreements can be used to demonstrate the user entity's understanding of service organization relationships/ownership of evaluation responsibilities to their user auditors and other stakeholders.

Based on our experience, audit support roles and responsibilities documented in SLAs or MOUs that are reviewed on an annual basis and reviewed and re-signed by authorizing user entity and service organization officials on a triennial basis or sooner if there are significant changes to the relationship or other relevant elements to the agreement are foundational elements to established service organization/SOC 1 report evaluation programs.

Plan the work and work the plan

DoD service organizations and their service auditors typically issue SOC 1 reports in mid-August of each year. This timing allows DoD report users to consider results that cover a significant portion of the federal fiscal year (i.e., October 1 through June 30) and are available with enough time for use by user auditors in the planning of their financial statement audits.

An effective service organization/ SOC 1 report evaluation program is an annual process that spans the entire fiscal year.

Think marathon, not sprint.

User entities who wish to demonstrate to their auditors and other stakeholders a proactive process for considering relevant service organization risks should not simply wait for SOC 1 reports to be published. Instead, they may consider leveraging the entirety of the fiscal year to stage and update evaluation documentation based on interim updates obtained from communications with service organizations, OUSD(C) Service Provider Working Group (SPWG) meetings, and other channels, as deemed appropriate. OUSD(C) SPWG meetings in particular are valuable forums for obtaining key updates regarding DoD SOC 1 reports. Updates typically communicated include anticipated future reports, changes to the scope of upcoming and/or in-process SOC 1 engagements, and mid-period findings identified by service auditors. SPWG meetings are held three times per year, and, in our experience, DoD components that actively engage in these forums are able to obtain timely updates regarding the status of in-process SOC 1 engagements. The following graphic depicts a notional view of how various activities associated with the performance of service provider/SOC 1 report evaluations may be timed to "leverage the calendar" and reduce risks associated with trying to complete most or all evaluation activities after SOC 1 reports are released in the middle of August of each year.

Effectively planning service organization evaluation activities to span the fiscal year can help user entities complete routine and predictable aspects of service organization/SOC 1 report evaluations in advance of mid-August report issuances. Thus, once the report is issued, user entities may focus on unforeseen/complex report elements, such as control weaknesses identified in the latter stages of the service auditor's examination.

Leverage the network

DoD components' network includes internal organizations as well as external groups, such as the OUSD(C) FIAR Office. User entities that coordinate activities among the various internal organizations that play a role in service organization/SOC 1 report evaluations are able to, among other things, drive consistency in the performance of

[6] OUSD(C): Financial Improvement and Audit Readiness Guidance, April 2017, Section 4.B.4, Methodology - Service Providers.

evaluations across the enterprise, conduct benchmarking, and more efficiently and effectively coordinate responses to various compliance requirements. Coordination across the DoD network and beyond can help user entities identify leading practices related to evaluation processes, tools, and templates implemented by other user entities. Coordination with other DoD components can aid in the identification of innovative ways that other user entities have addressed similar SOC 1 report findings and/or related findings identified by user auditors.

Communication is critical in the evolution of a service organization evaluation program. We see the opportunity for DoD user entities to communicate with other user entities that are similar in nature and use similar service organizations and service organization systems to share knowledge and experiences in the evaluation of SOC 1 reports. User entities may discuss their efforts to establish a service organization/SOC 1 evaluation program and leverage individual lessons learned to make improvements across the DoD.

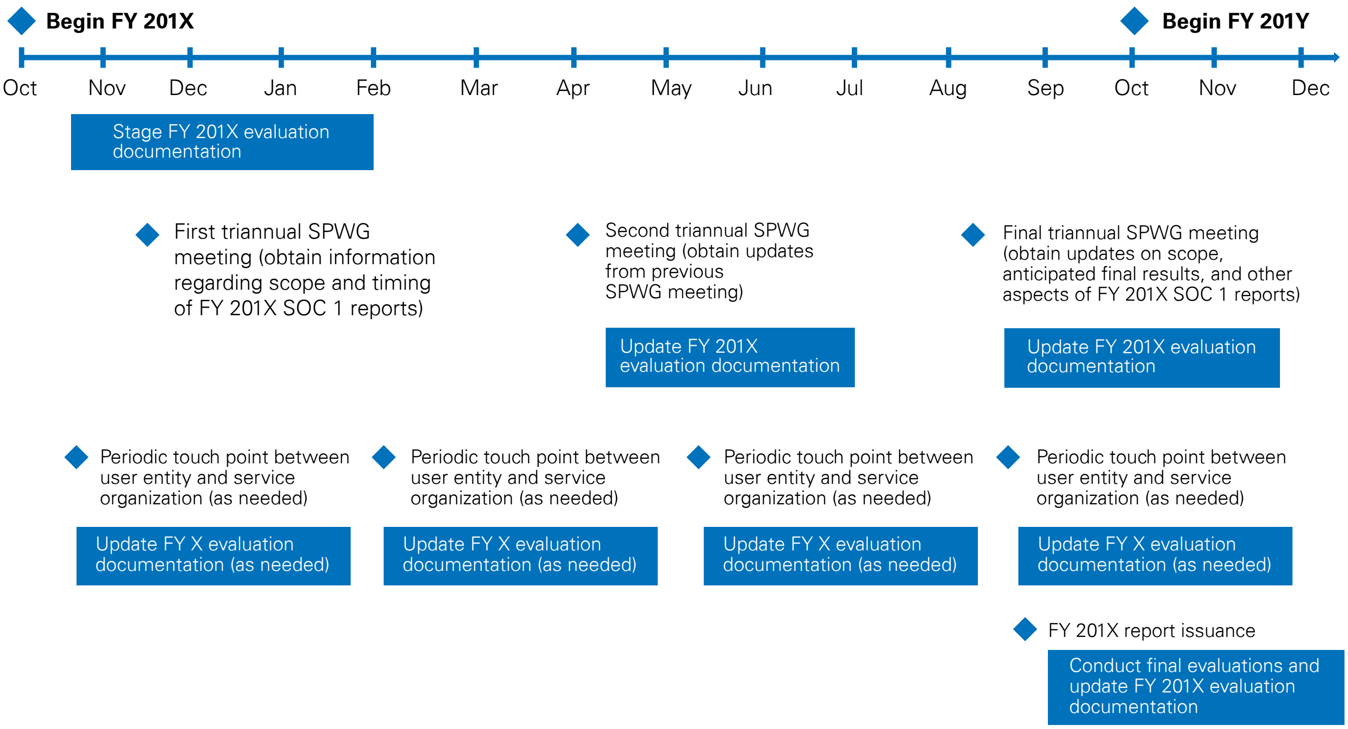
In our experience, DoD user entities who proactively communicate with OUSD(C) FIAR's Service Provider team via individualized communications, SPWG meetings and other Service Provider team-driven interactions represent a leading practice. The individual challenges faced by one user entity have likely been encountered by another, and, because the FIAR Directorate has visibility into audit readiness initiatives across the DoD enterprise, they may be able to provide insight to struggling DoD user entities based on similar challenges faced by others. DoD user entities may also work with OUSD(C) to reach out to private sector user entities that have implemented model capabilities for evaluating service organizations/SOC 1 reports.

Engage your auditors

A user entity is responsible for having internal controls over their financial reporting processes, including (1) internal controls over outsourced activities covered by a SOC 1 report and, if applicable, (2) controls that complement controls provided by the user entity's service organizations (also known as "complementary user entity controls"). As a part of the financial statement audit, a user entity typically provides documentation of its processes and controls to the auditor so the auditor can determine audit procedures. While the auditor is not responsible for the user entity's controls over/associated with service organizations, the user may ask questions regarding the auditor's consideration and treatment of certain conditions, be it the auditor's interpretation of the relevance of service organizations to the user entity's financial reporting processes, the auditor's assessment of SOC 1 report findings, and/or the auditor's assessment of the user entity's service organization/SOC 1 report evaluation process.

User entities should not be shy about seeking auditor feedback regarding previously noted deficiencies in service organization/SOC 1 report processes and/or controls or other audit-related topic areas. It is encouraged that user entities be proactive in coordinating with their auditors to share proposed remediation activities and obtain feedback

Notional service provider/SOC 1 report evaluation time line



Stage FY 201X evaluation documentation

First triannual SPWG meeting (obtain information regarding scope and timing of FY 201X SOC 1 reports)

Second triannual SPWG meeting (obtain updates from previous SPWG meeting)

Update FY 201X evaluation documentation

Final triannual SPWG meeting (obtain updates on scope, anticipated final results, and other aspects of FY 201X SOC 1 reports)

Update FY 201X evaluation documentation

Periodic touch point between user entity and service organization (as needed)

Update FY X evaluation documentation (as needed)

Periodic touch point between user entity and service organization (as needed)

Update FY X evaluation documentation (as needed)

Periodic touch point between user entity and service organization (as needed)

Update FY X evaluation documentation (as needed)

Periodic touch point between user entity and service organization (as needed)

Update FY X evaluation documentation (as needed)

FY 201X report issuance

Conduct final evaluations and update FY 201X evaluation documentation regarding the auditor’s view of whether the remediation would address noted deficiencies.

Additionally, user entities may facilitate auditor-to-auditor communication where possible/appropriate. For example, when the user auditor requests information regarding business processes performed by a service organization, the user entity may provide explanations but may also attempt to establish communication with its service organizations. This activity can help accelerate the user auditor’s understanding of the user entities’ business processes and service organization relationships.

It is our experience that user entities who proactively engage their auditors in the effort to maintain internal controls over financial reporting enjoy more productive relationships than user entities who view their auditors as adversaries bent on identifying “gotcha” findings or hindering other “more critical” entity objectives.

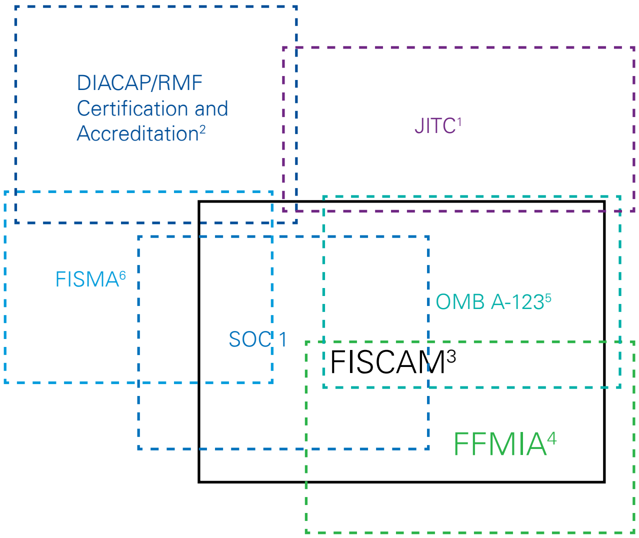
Integrate the evaluation program with agency-wide enterprise risk management

Enterprise risk management (ERM) reflects an organization-wide set of processes for controlling the activities of an entity so that risks threatening the achievement of operational, compliance, and financial reporting objectives are mitigated to an acceptable level. Effective broad-based/agency-wide risk management programs typically encompass a wide range of compliance requirements.

As indicated in the accompanying figure, various compliance programs and efforts have some overlapping requirements. Through proper coordination and implementation, user entities can leverage assessment activities across various compliance activities and minimize redundancy. Governance, risk, and compliance (GRC) technologies can be used to catalog key controls and link them and corresponding testing to various compliance requirements. These linkages can help user entities more readily identify the enterprise-level impact of control weaknesses across all applicable compliance requirements, not just those related to financial reporting objectives.

Integrate SOC 1 report evaluations with other control testing requirements*

*Notional depiction of overlap



1. Joint Interoperating Test Command Certification
2. Defense Information Assurance Certification and Accreditation Process/Risk Management Framework
3. Federal Information Systems Control Audit Manual
4. Federal Financial Managers Integrity Act
5. Office of Management and Budget A-123, Appendix A
6. Federal Information Systems Management Act

Lessons learned take the form of actions to address auditor findings, results of service organization/SOC 1 report evaluations, evaluation process improvements, and enhancements to the tools and templates used to conduct evaluations.

Reflect, revise, and optimize

User entities that take note of, assess, and respond to lessons learned throughout the audit cycle are able to leverage opportunities for improvement in their service organization/SOC 1 report evaluation programs. Depending on the nature of such items, user entities may find it appropriate to implement adjustments to processes as they are identified or defer implementation of adjustments until the end of the audit cycle. User entities that record and track deferred items help ensure opportunities to improve are leveraged.

Based on our experience, user entities that take stock of the effectiveness of their service organization evaluation program to identify successes, challenges, lessons learned, and action items for adjusting the process going forward at the conclusion of each audit cycle are better positioned to improve such programs than user entities that do not. If the identification and evaluation of lessons learned and opportunities to improve involves all relevant stakeholders, including members of the user entity’s audit readiness/audit support organization, representatives of the user entity team responsible for conducting/coordinating service organization/SOC 1 report evaluations, as well as the user entity’s business areas that outsource processes to service organizations, the user entity will more likely benefit from a broader set of perspectives. As needed, lessons learned sessions may also be conducted with relevant service organizations and the user auditors. Lastly, user entities may share lessons learned, opportunities to improve, and actions taken with their network, to include other user entities of similar composition and service organization reliance profiles and the OUSD(C) FIAR Directorate's Service Provider team.

Final thoughts

DoD continues the march towards audit readiness targets. In 2017, the Army and Air Force are undergoing independent audits of their Statement of Budgetary Resources, and an unprecedented number of military services and components are engaging auditors to perform examinations of various financial statement line items in anticipation of future financial statement audits. These activities speak to remarkable gains the Department is making in advancing its FIAR initiatives.

Because the web of interdependencies that exist between DoD user entities and their service organizations is complex and pervasive, there is a notable dependency associated with Department-wide efforts to improve internal control that is posed by user entities' ability to establish effective service organization/SOC 1 report evaluation programs. This is because such programs enable user entities to:

- Articulate complex service organization relationships in terms of user entities' reliance on service organizations, user entity financial reporting risks associated with support provided by service organizations, and the division of relevant responsibilities between user entities and service organizations
- Evaluate the results of SOC 1 reports to determine whether they have been scoped to meet user entity needs and, if they include weaknesses in controls provided by service organizations, identify relevant financial reporting risks and identify and/or implement mitigating controls that address such risks
- Demonstrate to user auditors and other stakeholders that the user entity has formally documented and consistently performed sufficient and effective processes for performing service organization/SOC 1 report evaluations.

With discipline and focus, the military services and DoD support components alike can position themselves and the Department as a whole to achieve audit readiness targets through, among other things, the implementation of service organization/SOC 1 report evaluation programs. The leading practices outlined in this issue brief provides the DoD with accelerators to help execute that process.

Contact us

Geoffrey Weber
Principal, Federal Advisory
KPMG LLP
T: 703-286-8480
E: glweber@kpmg.com

Mary Stauffer
Director, Federal Advisory
KPMG LLP
T: 571-535-7735
E: mstauffer@kpmg.com

Stephen Camara
Managing Director, Federal Advisory
KPMG LLP
T: 804-782-4445
E: scamara@kpmg.com

The KPMG Government Institute was established to serve as a strategic resource for government at all levels and for higher education and not-for-profit entities seeking to achieve high standards for accountability, transparency, and performance. The institute is a forum for ideas, a place to share leading practices, and a source of thought leadership to help governments address difficult challenges such as performance management, regulatory compliance, and fully leveraging technology.

Visit www.kpmg.com/us/governmentinstitute.

Jeffrey C. Steinhoff
Managing Director, KPMG Government Institute
T: 703-286-8710
E: jsteinhoff@kpmg.com

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.