3.B METHODOLOGY – SERVICE PROVIDER

Approximately four years ago, the American Institute of Certified Public Accountants (AICPA) issued Statement on Standards for Attestation Engagements (SSAE) No. 16, *Reporting on Controls at a Service Organization*, to address examination engagements undertaken by service organizations. The AICPA defines a service organization as "an organization or segment of an organization that provides services to user entities, which are likely to be relevant to those user entities' internal control over financial reporting."[12]

The Department utilizes many service organizations, also referred to as service providers, to improve efficiency and standardize business operations. Among the many service providers within the DoD are the Defense Finance and Accounting Service (DFAS), Defense Information Systems Agency (DISA), Defense Logistics Agency (DLA), and Defense Contract Management Agency (DCMA). These service organizations provide a variety of accounting, personnel, logistics, system development and/or operations/hosting support services.

Additionally, DoD has designated executive agents as service providers. DoDD 5101.1 "DoD Executive Agent" section 3.1, defines an executive agent as "the head of a DoD Component to whom the Secretary of Defense or the Deputy Secretary of Defense has assigned specific responsibilities, functions, and authorities to provide defined levels of support for operational missions, or administrative or other designated activities that involve two or more of the DoD Components." An example of an executive agent is an entity (or segment of an entity) that owns an information system and operates that system on behalf of a reporting entity (e.g., the Defense Civilian Personnel Advisory Service (DCPAS) maintains the Department's civilian personnel system software (DCPDS), which is used to initiate, approve, and process personnel actions for reporting entity civilian employees). As service providers, Departmental executive agents also must follow the service provider methodology to determine the extent they impact relevant internal controls over financial reporting for customer organizations.

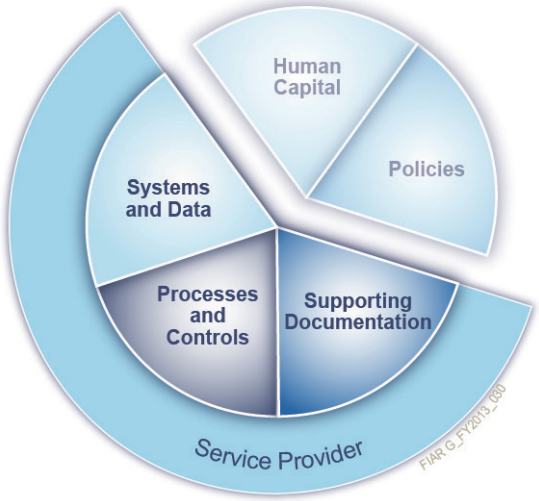

Figure 35. Service providers are responsible for their systems and data, processes and internal controls, and supporting documentation that affect a reporting entity's audit readiness

For the reporting entity to achieve auditability, it is critical that service providers support their customers and execute numerous tasks, including documentation of processes and controls, testing, and remediation. To assist service providers in delivering this support, this section of the Guidance highlights roles and responsibilities, defines some key terms, discusses service provider audit readiness strategies, and provides the detailed methodology that service providers must follow.

3.B.1 Roles and Responsibilities

Reporting entities are ultimately responsible for ensuring that all key processes, systems, internal controls and supporting documentation affecting their financial reporting objectives are audit ready. However, as shown in **Figure 35** service providers working with reporting entities are also responsible for executing audit readiness activities surrounding service provider systems and data, processes and internal controls, and supporting documentation that have a direct effect on the reporting entities' audit readiness state. Since the tasks of service providers are integrated into the end-to-end business processes of a reporting

[12] Source: AICPA Statement on Standards for Attestation Engagements No. 16, *Reporting on Controls at a Service Organization*, paragraph .07

entity, both the service provider and reporting entity are responsible for supporting each other during the audit readiness process. The mutual responsibilities include:

- Maintaining open communications and coordinating with one another
- Establishing common expectations in writing
- Providing additional system and financial information within agreed upon timeframes
- Providing access to subject matter experts or contractors supporting those organizations within agreed upon timeframes
- Working together to discover and correct audit impediments
- Establishing a common, detailed understanding of the method for obtaining assurance

To ensure successful completion of audit readiness tasks, the reporting entity and service provider must agree on the roles and responsibilities for the authorization, initiation, processing, recording, and reporting of transactions, and/or information technology (IT) controls affected by the service provider. **A shared understanding and agreement between the service provider and reporting entity on these roles and responsibilities must be documented in a Service Level Agreement (SLA) or Memorandum of Understanding (MOU). In addition to defining the basic strategy and approach for achieving audit readiness (including scope, required FIAR deliverables, and timelines), the SLA or MOU will also specify whether the service provider and/or executive agent will prepare its own FIP or whether its audit readiness activities will be included in the reporting entity FIP.** See FIAR Guidance website for the ***standard FIP template*** and ***FIP Preparation and Submission Instructions*** document.

An existing SLA may be in place between the reporting entity and service provider, which covers day-to-day operations but may not explicitly include a comprehensive listing of risks of material misstatements, a listing of financial reporting objectives to be achieved, and/or a listing of key supporting documentation to be developed and retained by the service provider. Reporting entities and their service providers can choose to update the existing SLA, or prepare a separate MOU to address the aforementioned audit readiness requirements. (Note that DFAS refers to this agreement as the "FIAR Concept of Operations.")

The SLA/MOU should also identify the types of supporting documentation that should be retained for each business process and transaction type, which organization will retain the specific documents, and the retention period for the documentation. Furthermore, the service provider must provide a description of its control environment, risk assessment process, control activities, information and communication tasks and monitoring activities that may affect the reporting entity's financial reporting objectives. The description of internal controls should be at a level of detail that provides the reporting entity with sufficient information to assess the risks of material misstatement and determine whether these risks have been mitigated; however, the internal control descriptions need not address every aspect of the services provided to the reporting entity. Refer to Appendix D for additional information on reporting entity level controls.

The service provider methodology presented in section 3.B.4 incorporates the inter-relationships between the reporting entity's end-to-end processes and the service provider's processes, systems, controls, transactions and documentation. As an example, **Figure 36** provides a representative illustration of the Civilian Pay end-to-end process. The illustration is a notional example, depicting the processes, systems, internal controls, and documentation within both the reporting entity and the service provider. Note that control activities may be manual or automated and documentation may be retained by either reporting entity. In addition, transactions may be executed within either the reporting entity portion of the process or service provider portion of the process. **Both organizations must be able to provide supporting documentation for their respective portions of the end-to-end process to demonstrate that control activities are suitably designed and operating effectively and transactions are properly posted to the accounting records.**

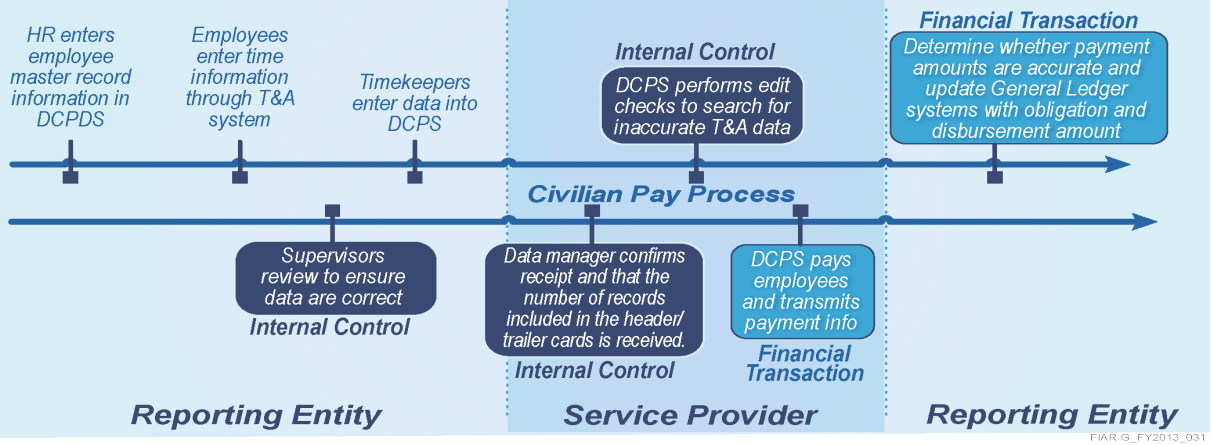

Figure 36. Reporting entities and service providers are responsible for different segments of end-to-end processes in the Department

The complexities inherent in DoD reporting entity and service provider relationships and associated audit readiness inter-dependencies make it essential to establish a common, detailed, written understanding regarding the mutual roles and responsibilities incumbent upon the reporting entity and service provider.

3.B.2 Definitions

Before proceeding, the following definitions will aid in the discussion of the service provider strategy and methodology that follows:

- User Entity – The reporting entity that has outsourced business tasks or functions to a service organization and is either working to become audit ready or is undergoing an audit of its financial statements.
- User Auditor – The financial statement auditor who issues an audit report opining on the financial statements of the user entity.
- Service Organization (or service provider) – The entity (or segment of an entity) that performs outsourced business tasks or functions for the reporting entity that are part of the reporting entity's manual and/or automated processes for financial reporting.
- Service Organization's System – 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.
- Subservice Organization – A service organization used by another service organization to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting.
- Service Auditor – The auditor retained by the service organization to issue an opinion on the service provider's controls that are relevant to a reporting entity's internal control over financial reporting (e.g., SSAE No. 16 examination report), as it relates to an audit of the reporting entity's financial statements.

As the role of these entities is explained throughout this section of the guidance, keep these definitions in mind to avoid confusion when developing audit readiness strategies, which is the next topic.

3.B.3 Strategy

As required by OMB Bulletin No. 14-02, service providers must support their reporting entities' financial statement audits by providing the reporting entities with an appropriate SSAE No. 16 examination report, or by allowing user auditors to perform appropriate tests of controls at the service organization.

Therefore, once systems and/or business processes and reporting entities have been identified, service providers must develop a high-level strategy for supporting the reporting entities' financial statement audits employing one of two options:

- Undergoing an examination in accordance with SSAE No. 16, where the service auditor reports on internal controls at service providers that provide services to reporting entities when those controls are likely to be relevant to reporting entities' internal control over financial reporting (ICOFR); or
- Participating in and directly supporting the reporting entity's financial statement audit, where the service provider's processes, systems, internal controls and supporting documentation are incorporated into the reporting entity's audit.

The process for eliminating audit impediments and known service provider exceptions is to follow the Service Provider Methodology whereby the service provider evaluates the design and operating effectiveness of control activities, and corrects material deficiencies either before an SSAE No. 16 examination begins, or, for service providers directly supporting a reporting entity, within a timeframe that fits the reporting entity's audit readiness timeline.

Accordingly, service providers must develop a sound strategy for identifying and documenting control objectives and control activities, testing control activities and identifying gaps, and designing and implementing corrective actions, in coordination with reporting entities. The strategy must include identification of control objectives, business processes, IT and manual controls, relevant systems, user controls, documentation, and personnel performing the controls. These tasks are essential for the service provider, whether preparing for an SSAE No. 16 examination or opting to provide direct support to the reporting entity and its user auditor. This section discusses many of the strategic elements that should be considered, including service provider/reporting entity relationships, SSAE No. 16 and direct support considerations, user controls, audit readiness dealbreakers, and work products.

In order to develop an appropriate strategy for achieving audit readiness, a service provider initially must identify all reporting entities for which services are provided, and work with those reporting entities to develop a list of the services provided for each reporting entity. In addition, the service provider and the reporting entity must determine which of the services provided are "material" to the reporting entity's financial statements.

Materiality is defined in the FAM as "the magnitude of an item's omission or misstatement in a financial statement that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the inclusion or correction of the item." (FAM Glossary, Page 12)

The concept of relevance and materiality is primarily subjective and involves several qualitative factors, which must be evaluated by the service provider and reporting entity. For example, both parties should consider whether:

- **Relevant information regarding the service providers processes or systems has been omitted or distorted**
- **Relevant aspects of the service provider's operations related to the processing of significant transactions have been included**
- **Controls identified are designed to provide reasonable assurance that control objectives would be achieved**[13]

Accordingly, service providers and reporting entities must coordinate to assess the relevance of services provided in the context of materiality. Ultimately, service providers should subject to audit readiness only those processes, controls and documentation that is deemed material to the reporting entities.

[13] From the AICPA's SSAE No. 16, paragraph A26

Once initial tasks are complete, the service provider must contact each reporting entity and begin coordination of audit readiness efforts, identifying the reporting entity's assessable units and mapping them to the service(s) provided. **Figure 37** depicts a decision tree that a service provider can use to help tailor its approach to service provider audit readiness at an assessable unit level (see Section 3.A.3 for more detailed information on assessable units).

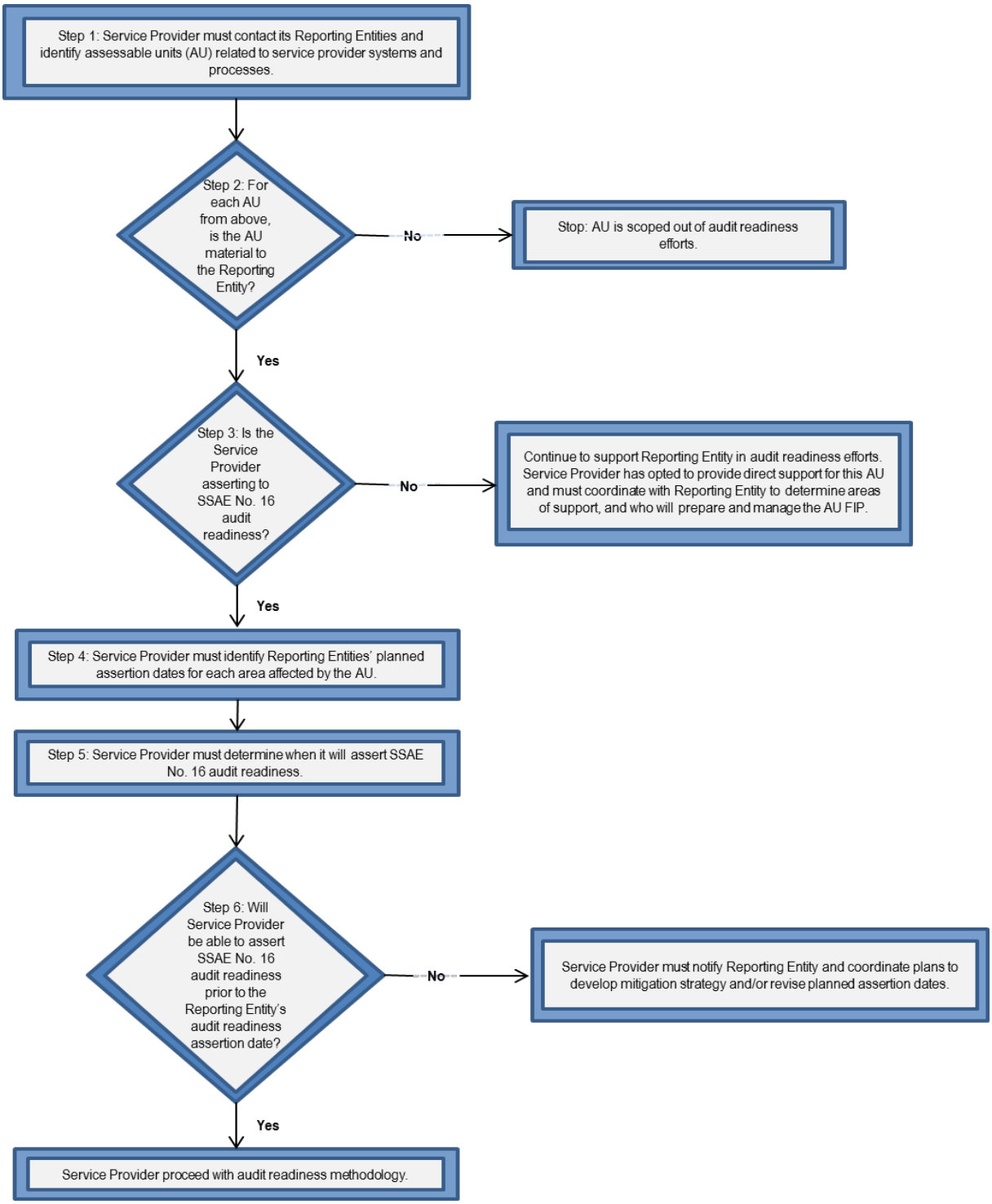

Figure 37. Service Provider decision tree for determining audit readiness strategy

Overall Approach

Most service providers will likely choose to prepare for and undergo an SSAE No. 16 examination because the examination report can be used by the financial statement auditors of multiple reporting entities. However, service providers serving fewer than three reporting entities may opt to directly support those reporting entities where it is more efficient and cost beneficial to do so. Additionally, service providers with unique sets of controls, e.g. different manual processes across reporting entities, may decide to forgo an SSAE No. 16 examination for those services and provide direct audit support to the reporting entity (combining the two options). **Whether or not a service provider opts for an SSAE No. 16 examination, Phases 1 and 2 and Phase 3, Task 3.1 of the service provider methodology need to be completed (discussed in Sections 3.B.4 and 3.B.5).**

As service providers begin to formulate strategies and implement the methodology, the preferred approach will likely include pursuit of an independent examination of service provider controls based on AICPA Statements on Standards for Attestation Engagements (SSAE) No. 16,[14] *Reporting on Controls at a Service Organization*. Accordingly, at this point it is appropriate to address various report options and emphasize the report type required for audit readiness.

Types of Service Organization Control Reports

The AICPA has designed multiple Service Organization Control (SOC) reports to meet the evolving assurance needs of service organizations and their customers. The SOC reports are based upon SSAE No. 16; Professional Standards Section AT 101, *Attest Engagement;* and Trust Service Principles.

Each type of SOC report has been purposefully developed to address a specific assurance need regarding either (a) internal controls that affect user entities' financial reporting; or (b) internal controls that affect the security, availability, and processing integrity of the systems or the confidentiality or privacy of the information processed for user entities' customers. The applicable SOC report will vary depending on the subject matter.

The three SOC reports are:

1. SOC 1 Report – Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting

These reports, prepared in accordance with SSAE No. 16, are specifically intended to meet the needs of the reporting entities that use service providers and their user auditors. The SOC 1 report is used in evaluating the effect of the controls of the service provider on the reporting entity's financial statements. SOC 1 reports do not address non-financial reporting-related control objectives, such as control objectives related to compliance with laws and regulations.

The SSAE No. 16 guidance defines two SOC 1 reports, Type 1 or Type 2.

1a. SOC 1 – Type 1 Report – Report on Management's Description of a Service Organization's System and the Suitability of the Design of Controls

These reports encompass:

- the service auditor's report in which the service auditor expresses an opinion on:
  - the fairness of the presentation of management's description of the service organization's system as of a specified date
  - the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date
- management's description of the service organization's system
- management's written assertion

[14] SSAE No. 16 superseded Statement on Auditing Standard (SAS) No. 70, effective for reports with an issue date of June 15, 2011 or later.

1b. SOC 1 – Type 2 Report – Report on Management's Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

These reports encompass:

- the service auditor's report in which the service auditor expresses an opinion on:
  - the fairness of the presentation of management's description of the service organization's system throughout a specified period
  - the suitability of the design **and** the operating effectiveness of the internal controls to achieve the related control objectives included in the description throughout a specified period
- management's description of the service organization's system
- management's written assertion

Once a determination has been reached that an SSAE No. 16 is the appropriate course of action, the FIAR Directorate requires service providers to obtain Type 2 reports as these reports provide an opinion on both the design and operating effectiveness of internal controls. Since the Type 2 report is the recommended and more commonly used of the SOC reports, when a SOC 1 report is discussed in the remainder of the guidance, the reference is to the Type 2 report.

2. SOC 2 Report – Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

These reports are intended to meet the needs of a broad range of users seeking information and assurance about the controls at a service organization that affect the security, availability, and processing integrity of the systems the service provider uses to process the reporting entity's data, and the confidentiality and privacy of the information processed by these systems. Engagements resulting in SOC 2 reports are performed in accordance with AT 101. SOC 2 reports are typically used for compliance purposes and are not required for financial statement audit readiness.

3. SOC 3 Report – Trust Services Report for Service Organizations

These reports are designed to meet the needs of users seeking assurance about the controls at a service provider related to the security, availability, processing integrity, confidentiality, or privacy. They are similar to SOC 2 reports, but SOC 3 reports are prepared for general use distribution and report on whether the reporting entity meets Trust Services criteria; SOC 3 engagements also are performed in accordance with AT 101. SOC 3 reports are typically used for compliance purposes and are not required for financial statement audit readiness.

As noted above, the SOC 1 – Type 2 report is the report that should be obtained to satisfy FIAR requirements for audit readiness, if the service provider chooses to pursue an SSAE No. 16 examination, because it provides an opinion on the suitability of the design **and** operating effectiveness of controls impacting user entities' financial reporting. A SOC 1 – Type 2 report includes the following sections, as defined in SSAE No. 16:

1. Section 1 – Service Auditor's Report
2. Section 2 – Service Provider Management's written assertion
3. Section 3 – Service Provider Management's description of its system(s)
4. Section 4 – Service Auditor's description of tests of operating effectiveness of controls and test results
5. Section 5 – Optional other information provided by Service Provider Management

The service provider methodology focuses on Sections 2 and 3 of the Type 2 report as well as testing of controls to properly prepare the service provider for either an SSAE No. 16 examination or interaction with the user auditor when providing direct support to the reporting entity. Having now defined SSAE No. 16 report types, it is time to discuss examination considerations.

SSAE No. 16 Examination Considerations

Important matters should be considered when deciding whether to pursue an SSAE No. 16 examination in addition to the number of reporting entities serviced and commonality of controls imbedded in financial reporting processes. These matters include timeliness of the examination, the period covered by the examination, and the treatment of sub-service organizations.

If an SSAE No. 16 examination occurs too soon before the reporting entity's fiscal year end, its usefulness to the user auditor will be diminished. For example, an SSAE No. 16 report covering a six month period ending March 31 may not provide sufficient evidence for a user auditor in that fiscal year, and the user auditor will likely need to conduct additional testing of the service provider's controls (relevant to the reporting entity's ICOFR) to meet his/her audit needs. Similarly, an SSAE No. 16 report issued after September 30 may be of diminished value to the user auditor for that fiscal year, as it would not be available for audit planning and the internal control phase of the audit. **Accordingly, it is imperative that service providers and reporting entities effectively communicate regarding the timing of planned SSAE No. 16 examinations and audit readiness assertions.**

The period of time covered by an SSAE No. 16 examination (with respect to a Type 2 report) is also significant for the service provider and reporting entity. If the SSAE No. 16 opinion covers a sufficient period of time in relation to the fiscal year under audit, the financial statement auditor likely can reduce the nature and extent of internal control and substantive testing (i.e., supporting documentation testing) required for the audit; six months is recognized as the minimum period of coverage.[15] As noted above, effective communication between service provider and reporting entity is essential to maximize the utility of an SSAE No. 16 report.

A final consideration is the treatment of subservice providers. The AICPA's SSAE No. 16 recognizes that a service organization may rely on services provided by another service organization, referred to as a subservice organization (or subservice provider). As an example, consider a reporting entity's Civilian Pay assessable unit. DFAS may provide services to the reporting entity as the service organization that processes its bi-weekly payroll through the Defense Civilian Pay System (DCPS). However, DFAS does not provide application hosting services for the DCPS software; those services are provided by DISA. In this example, DISA is considered a subservice organization with respect to the Civilian Pay assessable unit for this reporting entity.

In these circumstances, SSAE No. 16 allows a service provider (DFAS in the above example) to use one of two methods in presenting information about the subservice organization's system and controls:

- **Carve-out Method.** With the carve-out method, service provider management identifies the nature of the services provided by a subservice organization, but excludes ("carves out") the subservice organization's relevant control objectives and related internal controls from the description and scope of the service provider's SSAE No. 16 report. Management's description of the service organization's system and the scope of the service auditor's engagement will include controls at the service organization that monitor the effectiveness of controls at the subservice organization, which may include management of the service organization's review of a service auditor's report on controls at the subservice organization. (Note that this is the method used by DFAS in the DCPS SSAE No. 16 report issued August 15, 2013.)
- **Inclusive Method.** The other option is referred to as the inclusive method, in which the subservice organization's relevant controls are included in the scope of the service provider's SSAE No. 16 report. In this method, the service organization includes a description of the services provided by the subservice organization, and the subservice organization's relevant control objectives and related controls.

With the carve-out method, although service provider management's description of the service provider's system will exclude the subservice organization's relevant control objectives and related internal controls, the description should contain sufficient information concerning the carved-out services and controls to enable the user auditor to understand what additional information he/she will need pertaining to the

[15] See SSAE No. 16, paragraph A.42.

subservice organization to assess the risk of material misstatement of the reporting entity's financial statements. Service providers will include all available subservice organization SSAE No. 16 reports in their assertion documentation.

When using the carve-out method, instances may exist in which achieving one or more control objectives depends on one or more controls performed by a subservice organization. In such instances, management's description of its system would identify the controls performed at the service provider and indicate that the related control objectives would be achieved only if the subservice organization's controls were suitability designed and operating effectively throughout the period. The service provider may include a table in its description that identifies those instances in which control objectives are met solely by the service provider, and those in which controls at the service provider and at the subservice provider are needed to meet the control objective.

With the inclusive method, the subservice provider's relevant control objectives and related controls are included in the service provider management's description of its system. The service auditor conducts the SSAE No. 16 examination incorporating the two sets of control objectives and activities into his/her testing procedures. The inclusive method is typically used when the service organization and subservice organization are related parties.

Whether the service provider uses the carve-out or the inclusive method, communication between service providers and their subservice organizations, as well as a documented SLA or MOU, is critical to ensure that all essential controls are addressed.

User Auditor Considerations and SSAE No. 16 Control Objectives

The user auditor will consider many factors when relying on an SSAE No. 16 examination report, including the period of time covered by the report, control objectives and control activities addressed in the report, and results of the tests of controls and the conclusions of the service auditor. Service providers should consider user auditor needs in relation to the SSAE No. 16 report whenever possible. For this reason, when defining the control objectives for the SSAE No. 16 examination, the service provider should use existing guidance and best practices.

For business process controls, the AICPA's SSAE No. 16 Implementation Guidance outlines high level control objectives and includes illustrative examples of control objectives to be used for various service provider processes (for example, payroll processing). When IT General and Application Controls are included in the scope of the SSAE No. 16 examination, use the GAO's Federal Information System Controls Audit Manual (FISCAM) to define control objectives. A recommended list of standardized control objectives, aligned to the FISCAM, is presented in **Figure 38**.

IT General Control Objectives (CO)
Security Management
Controls provide reasonable assurance that management has established, implemented, and monitors <***application***> security management programs.
Access Controls
Controls provide reasonable assurance that logical access to <***application***>, as well as logical and physical access to <***application***> (programs and data) is reasonable and restricted to authorized individuals.
Configuration Management
Controls provide reasonable assurance that changes to <***application***>, application programs and database structures are authorized, tested, implemented and documented.
Segregation of Duties
Controls provide reasonable assurance that management has identified, periodically reviewed, and mitigated risks of incompatible duties across <***business operations and IT operations***>.
Contingency Planning
Controls provide reasonable assurance that contingency planning, back-up and recovery procedures exist for <***application***> and are tested on a periodic basis.

Business Process Control Objectives (CO)
Setup
Controls provide reasonable assurance that <***assessable unit transaction / master data***> are authorized, set up, and updated completely, accurately, and timely.
Input
Controls provide reasonable assurance that <***assessable unit transactions***> are received from authorized sources and are input into the application completely, accurately and timely.
Processing
Controls provide reasonable assurance that <***assessable unit transactions***> are processed completely, accurately, and timely; deviations from the schedule are identified and resolved timely.
Output
Controls provide reasonable assurance that <***assessable unit outputs***> are authorized and transmitted completely and accurately, and are processed timely.

Figure 38. IT General and Business Process Control Objectives

For additional information, refer to the FIAR Guidance website for FISCAM control activities and techniques that are highly relevant for addressing key financial reporting risk areas and other ***FISCAM control activities and techniques*** that should be considered by reporting entities and their service providers in their audit readiness efforts.

Complementary User Entity Control Considerations

A service provider's applications and business processes are designed with the understanding that certain complementary user entity controls have been implemented by the reporting entity. Complementary user controls are those controls that management of the service provider, in designing the service(s) provided, assumes are implemented by the user/reporting entity. Complementary user control considerations should relate to the control objectives specified in management's description of the service provider system. Accordingly, the service provider must communicate and confirm its user control assumptions with the reporting entity.

Typical control activities the reporting entity should implement to complement the controls of the service provider include, but are not limited to:

- Control activities that provide reasonable assurance that any changes to processing options (parameters) requested by the reporting entity are appropriately authorized and approved.
- Control activities that provide reasonable assurance that output received from the service provider is routinely reconciled to relevant reporting entity control totals.
- Control activities that provide reasonable assurance over passwords needed to access the systems resident at the service provider through computer terminals.

SSAE No. 16 Audit Readiness Dealbreakers

Service providers working towards an SSAE No. 16 examination are responsible for addressing the dealbreakers listed in **Figure 39** below. These separate dealbreakers are necessary because, unlike financial statement audits, which are focused on determining whether the financial statements are fairly presented in accordance with GAAP, the purpose of an SSAE No. 16 examination is to express an opinion on the effectiveness of internal controls in meeting specific control objectives relevant to financial reporting. Accordingly, tests of key supporting documentation (KSDs) for tests of account balances (task 1.6) are not required by service providers to support SSAE No. 16 readiness assertions. For SSAE No. 16 assertion, service providers will only need to evaluate KSDs that provide evidence that controls are designed and operating effectively. Separate from the SSAE No. 16 assertion, service providers may be requested by reporting entities to assist them with tests of KSD for individual assessable units.

However, service providers preparing for an SSAE No. 16 examination need to address these dealbreakers. During the Assertion/Evaluation phase, the FIAR Directorate will provide feedback to the

service provider on the dealbreakers and recommend additional procedures to make improvements prior to an examination.

SSAE No. 16 Audit Readiness Dealbreakers	FIAR Guidance Reference
1. All material business processes and information systems (including micro-applications) are not defined or included in the scope of the SSAE No. 16 examination.	**3.A.2 Consideration of Service Providers** **3.A.4 Financial Systems Considerations**
2. All relevant business process and information technology control objectives that address information technology general control and transaction setup/input/processing/output risks are not included in the scope of the SSAE No. 16 examination.	**3.A.2 Consideration of Service Providers** **3.B.4 Methodology - Service Provider**
3. All relevant service provider performed controls, user control considerations, and sub-service provider roles and responsibilities that address in-scope control objectives have not been identified and included in-scope for testing.	**3.A.2 Consideration of Service Providers** **3.B.4 Methodology – Service Provider**
4. Testing conducted to assess the design and operating effectiveness of business process and information technology controls is not extensive enough to conclude as to whether the related control objectives have been satisfied.	**3.A.2 Consideration of Service Providers** **3.B.4 Methodology - Service Provider**
5. For areas where control deficiencies have been identified during testing, the service provider has not provided sufficient documentation indicating that corrective actions have been implemented.	**3.A.2 Consideration of Service Providers** **3.B.4 Methodology - Service Provider**

Figure 39. SSAE No. 16 Audit Readiness Dealbreakers

Direct Support Considerations

A service provider may decide to directly support a reporting entity if the service provider has a small customer base (less than three reporting entities), or employs unique control activities within a process (system) for individual reporting entities. Additionally, if a service provider cannot successfully prepare for and undergo an SSAE No. 16 examination within the required timeframe, it should notify its customers (reporting entities) immediately so that those customers and the service provider can work together on mitigation plans (such as direct support) and/or revise planned FIP milestone dates for this key audit readiness dependency. In such situations, the FIAR Directorate must be notified of these changes.

The direct approach will require the service provider to develop an appropriate audit infrastructure with which to support the reporting entity's user auditor in assessing risk, testing controls and transactions, providing documentation, and accommodating potential site visits to service provider locations.

When a service provider is supporting less than three reporting entities (and when the reporting entity is subject to a financial statement audit and the service provider does not receive an SSAE No. 16 examination report), the service provider's processes and internal controls that affect the reporting entity's financial transactions are audited as part of the reporting entity's financial statement audit. As a result, the service provider will need to complete the key tasks and activities of the FIAR Methodology and coordinate with the reporting entities to develop the required FIAR work products (i.e., risk assessments, controls assessments, process narratives, test plans, etc.) to become audit ready.

As noted earlier in this section, OMB Bulletin No. 14-02 requires service providers to support reporting entity financial statement audits by either providing an SSAE No. 16 SOC 1 report, or allowing user auditors to perform appropriate tests of controls at the service organization.

To support this testing, both the reporting entity and the service provider must work together to provide:

- **Transaction-level downloads of reporting entity transactions, accompanied by reconciliations of the transaction level detail to the general ledger and financial statements;**
- **Supporting documentation for requested sample items; and**

- **Personnel/responses to questions asked about trends, variances and specific financial transactions.**

To satisfy user auditor requests, both the reporting entity and service provider will need to ensure they each have an infrastructure of processes and resources established and available to quickly and effectively respond to these requests.

Other Considerations

Other strategic considerations for service providers include:

- SSAE No. 16 explicitly does not apply when the service auditor is reporting on controls at a service provider that are not relevant to reporting entities' ICOFR, such as controls related to regulatory compliance or privacy. For audit readiness purposes, the service provider is not required to provide the reporting entity with an SSAE No. 16 report on controls that are not relevant to ICOFR. The SOC 1 report is the most common type of SSAE No. 16 report used and the SOC 1 – Type 2 report is required for financial statement audit readiness purposes.
- If the reporting entity requests information on compliance or regulatory controls not related to ICOFR and the service provider has not completed a SOC 2 or SOC 3 report, the service provider may provide the reporting entity with results from internal reviews, such as the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), Federal Information Security Management Act (FISMA), or FFMIA reviews.
- **Service providers must prepare, evaluate, and remediate weaknesses in their processes, systems, internal controls and supporting documentation to effectively support the reporting entity audit. This requires the service provider to understand the reporting entity's audit readiness dependencies, including scope, timeline, expected deliverables, etc., and coordinate its audit readiness activities with those of the reporting entity prior to engaging a service auditor to perform an SSAE No. 16 examination.** Coordination and communication between the service provider and reporting entity is essential throughout the audit readiness process.
- **The service provider has lead responsibility for coordinating SSAE No. 16 attestation engagements of its processes and internal controls.**
- **The service provider and reporting entity must work together to discover and correct audit impediments.**

The key to achieving auditability is focusing on the entire end-to-end processes from the time a transaction is initiated to the point when financial data is reported and supporting documentation is retained and stored for future retrieval. Any gaps will likely impede progress for both the reporting entity and service provider. The service provider methodology discussed below is meant to work in concert with the reporting entity methodology to detect and correct, or avoid such gaps.

3.B.4 Methodology – Service Provider

Service providers are responsible for the initiation, authorization, recording, processing or reporting of financial transactions on behalf of the reporting entity. Service providers must have effective processes and control activities to assist the reporting entity in meeting its financial reporting objectives. Consequently, service providers play a key role in ensuring that the reporting entity achieves audit readiness. This section of the Guidance describes the Department's methodology that service providers must follow to support their customers' efforts to achieve audit readiness, as well as Departmental efforts to develop a common strategy by bringing together service providers and reporting entities to identify risks, develop common control and financial reporting objectives, and ensure control activities are designed to meet those risks and are operating effectively.

Figure 40 presents the FIAR methodology that service providers must follow to assist the reporting entity in achieving audit readiness.

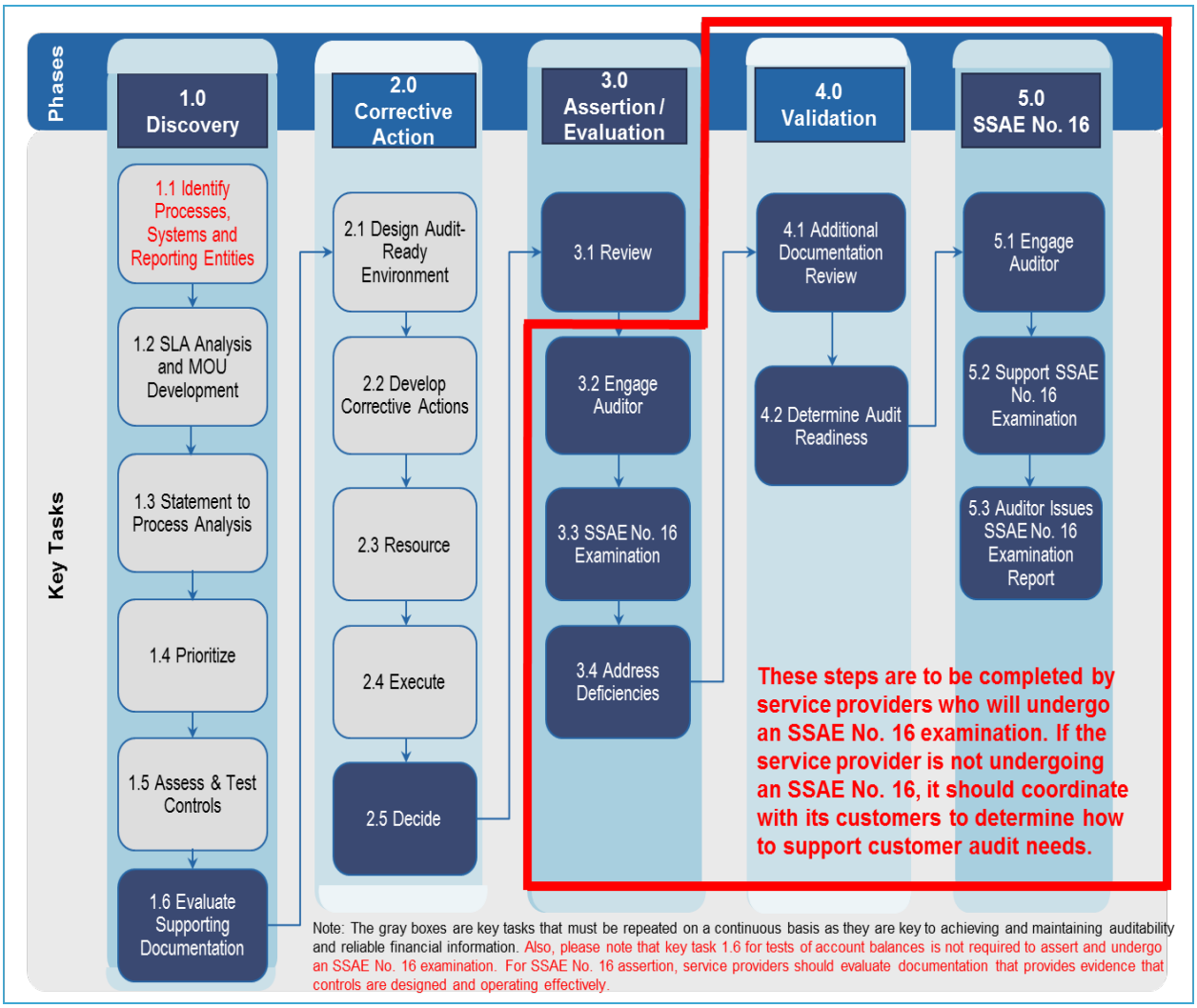

Figure 40. Service Provider Phases and Key Tasks to Achieve Auditability and Reliable Financial Information

3.B.5 Phases and Key Tasks

All service providers must complete each Key Task of the Discovery and Corrective Active phases as well as Key Task 3.1. Furthermore, those service providers that determine to undergo an SSAE No. 16 examination will also need to complete the remaining Key Tasks in the Assertion/Evaluation, Validation, and SSAE No. 16 phases. It should be noted that the SSAE No. 16 examination focuses on determining the design and operating effectiveness of the control activities and the service auditor does not perform documentation testing to support account balances. However, for the purpose of the FIAR Methodology, service providers are required to complete Key Task 1.6, whether they intend to undergo an SSAE No.16 examination or provide direct support to their customers. Successfully completing Key Task 1.6 provides assurance that in the event that the service provider is not able to undergo a SSAE No. 16 examination, the service provider will be able to support its customer's audit readiness requirements through alternative procedures.

The five phases and key tasks of the Methodology are as follows:

1. Discovery
   a. Service provider identifies reporting entities, relevant business processes, systems and assessable units.
   b. Service provider coordinates with the reporting entity (and any subservice organizations) to document understanding of audit readiness roles and responsibilities, and establish an agreed-upon timeline for completion of joint audit readiness activities and/or SSAE No. 16 examination, either within the existing SLA or in a separate MOU.
   c. Service provider documents its business processes and the financial environment, and supports the reporting entity in developing the statement to process analysis.
   d. Service provider coordinates with the reporting entity to define and prioritize the service provider's processes into assessable units.
   e. Service provider identifies risks, control objectives and control activities, and tests the design and operational effectiveness of control activities.
   f. Service provider evaluates the sufficiency and accuracy of documentation to support financial transactions, account balances and financial statement line items **only when supporting the reporting entity's assertion of audit readiness (for asserting to SSAE No. 16 readiness, service providers should evaluate documentation providing evidence that controls are designed and operating effectively).**
   g. Service provider identifies and classifies any deficiencies in control activities and/or supporting documentation.
2. Corrective Action
   a. Service provider defines and designs audit readiness environment, to include requirements for remediating deficiencies in internal control and supporting documentation.
   b. Service provider develops concrete corrective action plans to resolve each deficiency identified during the Discovery phase.
   c. Service provider develops budget estimates of required resources (i.e., funding and staffing levels) to execute corrective actions.
   d. Service provider executes corrective action plans and verifies that corrective actions were implemented.
   e. Service provider determines strategy for supporting reporting entity's audit readiness efforts (i.e., proceed with SSAE No. 16 examination or provide direct support during reporting entity's financial statement audit) and coordinates audit readiness timeline with the reporting entity.

3. Assertion/Evaluation
   a. FIAR Directorate evaluates documentation submitted by service provider to determine audit ready state and provides feedback to the service provider on its status of audit readiness. If the service provider is supporting the reporting entity directly (i.e., no SSAE No. 16 examination), continue to communicate and coordinate with the reporting entity, update timelines as needed and ensure sustainment of service provider's audit readiness activities.
   b. Service provider provides a management assertion letter to the FIAR Directorate on the fairness of the description of its system, the suitability of the design of controls, and the operating effectiveness of controls to meet control objectives.
   c. Service provider engages an auditor to perform an initial SSAE No. 16 examination resulting in a SOC 1 – Type 2 report.
   d. Service provider evaluates nature and extent of deficiencies noted in the SSAE No. 16 report and implements corrective actions to remediate deficiencies.
   e. Service provider performs procedures to verify that corrective actions successfully remediated auditor-identified deficiencies.
   f. Service provider submits the SSAE No. 16 examination report, and additional documentation demonstrating successful remediation of auditor-identified deficiencies to the FIAR Directorate and DoD OIG.
4. Validation
   a. FIAR Directorate reviews the SSAE No. 16 examination report and additional documentation supporting successful remediation of deficiencies.
   b. FIAR Directorate determines service provider's audit readiness state.
5. SSAE No. 16 Examination
   a. Service provider engages auditor to perform SSAE No. 16 examination.
   b. Service provider supports the SSAE No. 16 examination.
   c. Auditor issues SSAE No. 16 examination report.

In the following charts, the key tasks are numbered to coincide with the standard FIP Template. For example, the Discovery Phase of the FIP template includes key tasks beginning with section 1.1, while the Audit Phase begins with section 5.1 of the template.

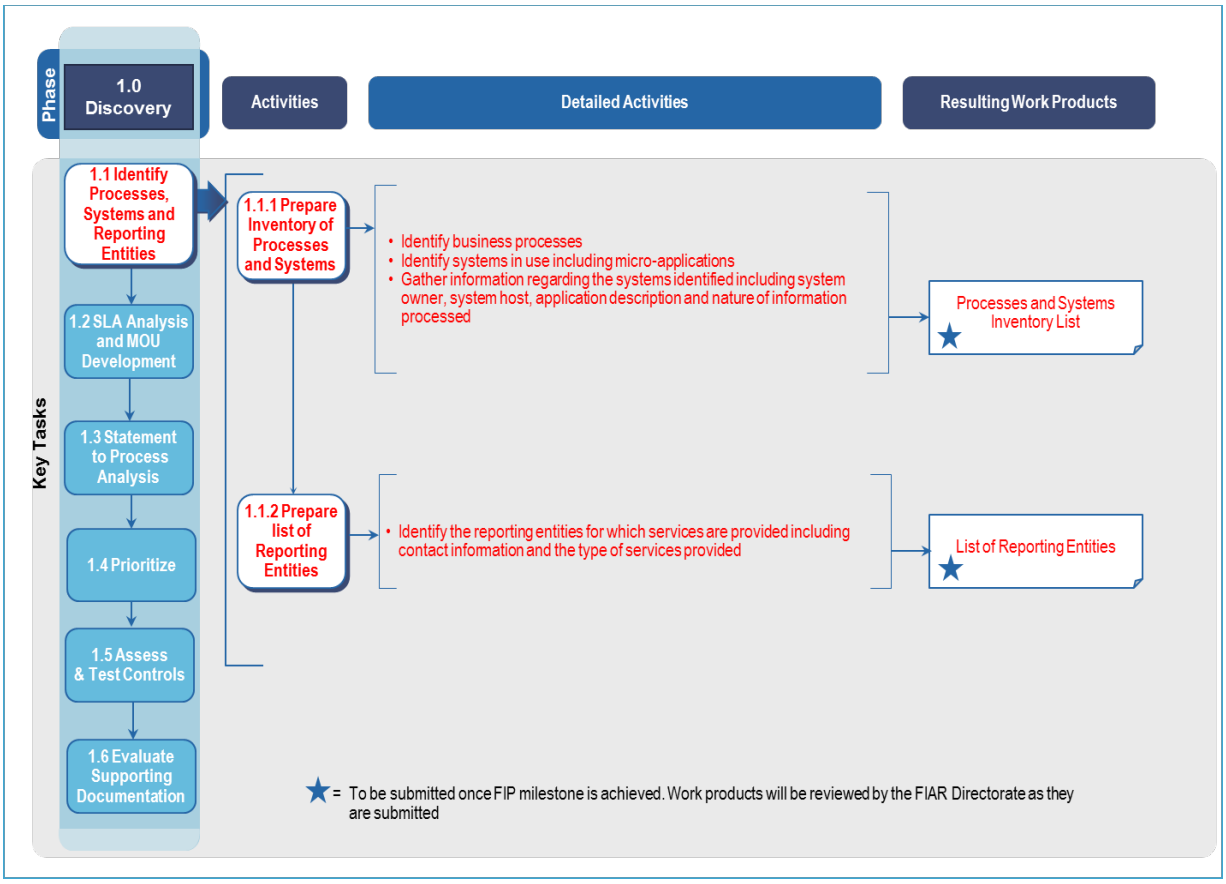

Figure 41. Discovery Phase – Identify Systems and Reporting Entities

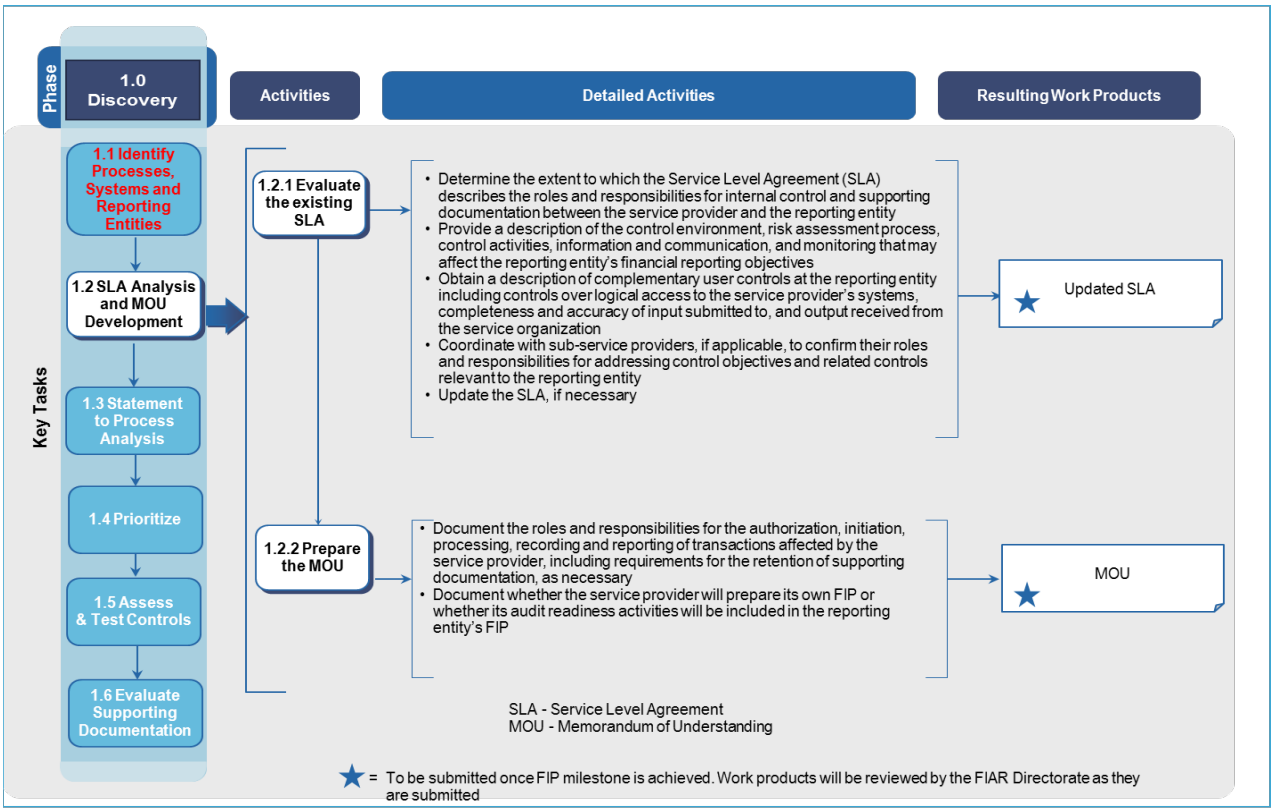

Figure 42. Discovery Phase – SLA Analysis and MOU Development

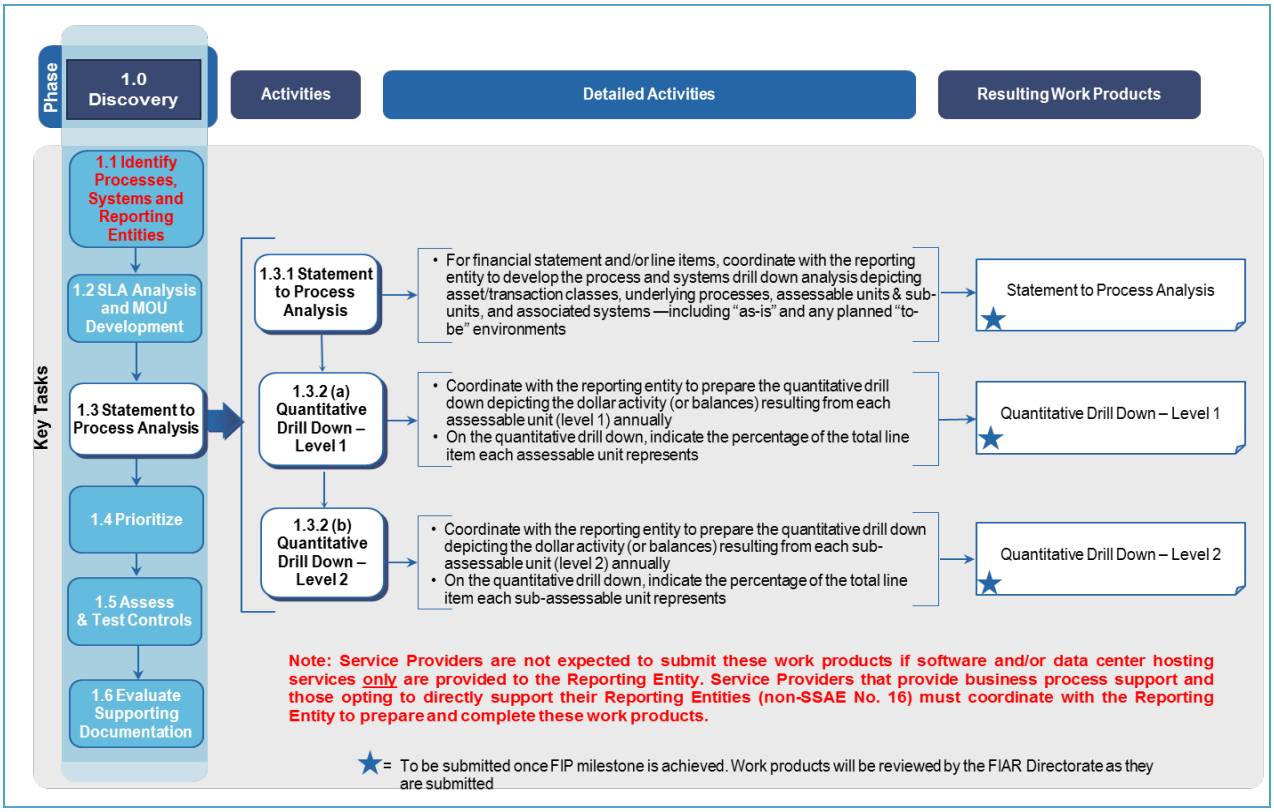

Figure 43. Discovery Phase – Statement to Process Analysis

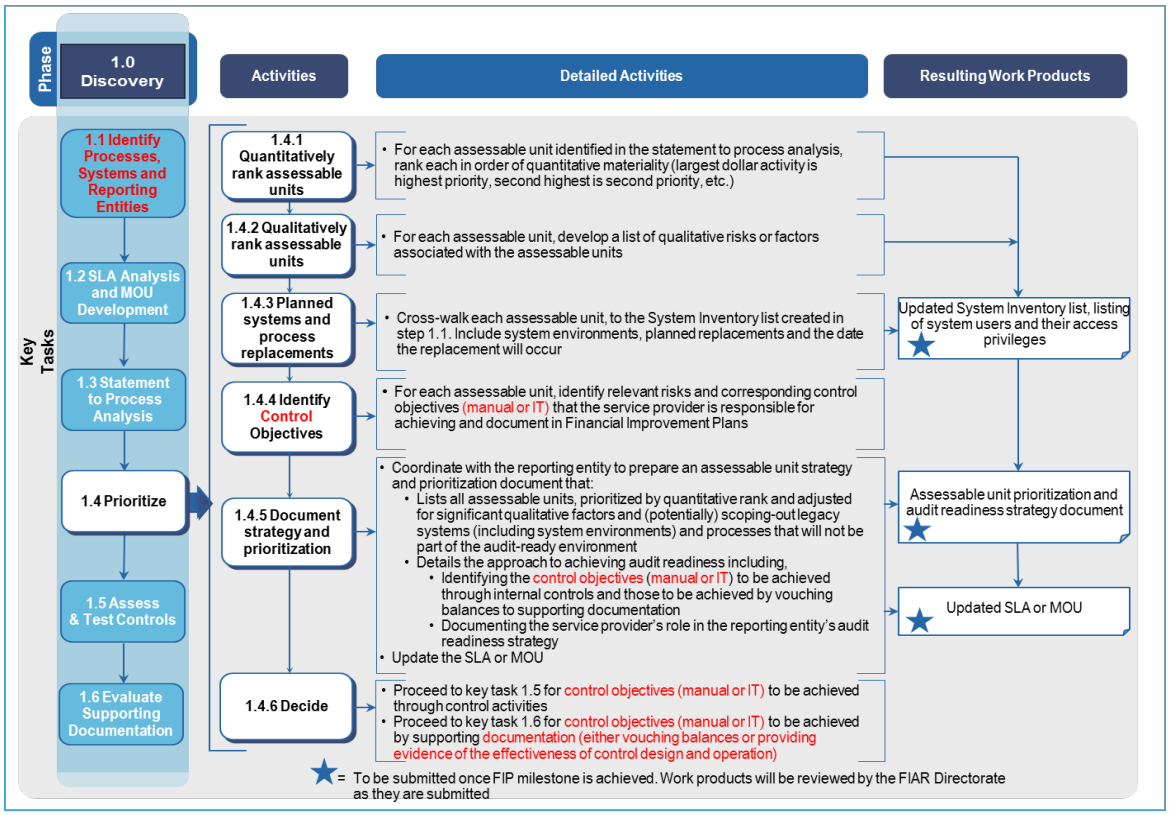

Figure 44. Discovery Phase – Prioritize

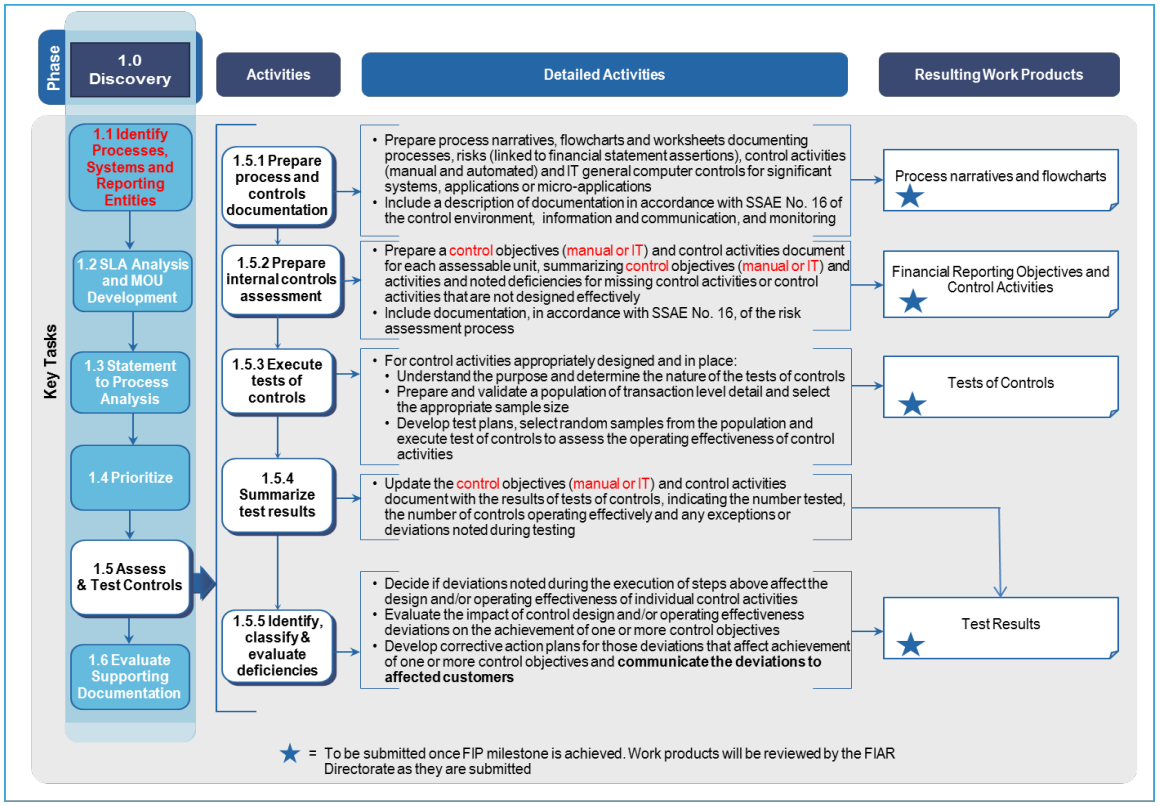

Figure 45. Discovery Phase – Assess & Test Controls

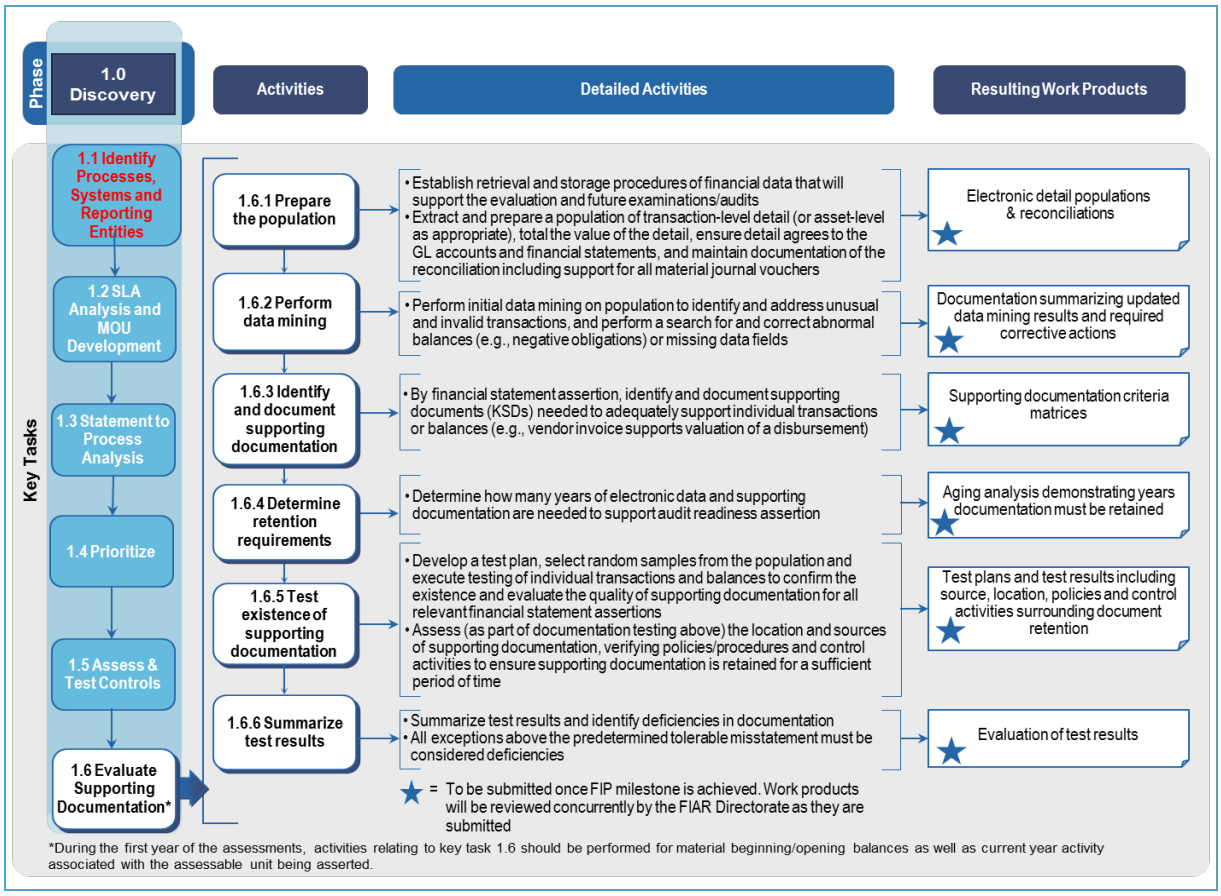

Figure 46. Discovery Phase – Evaluate Supporting Documentation

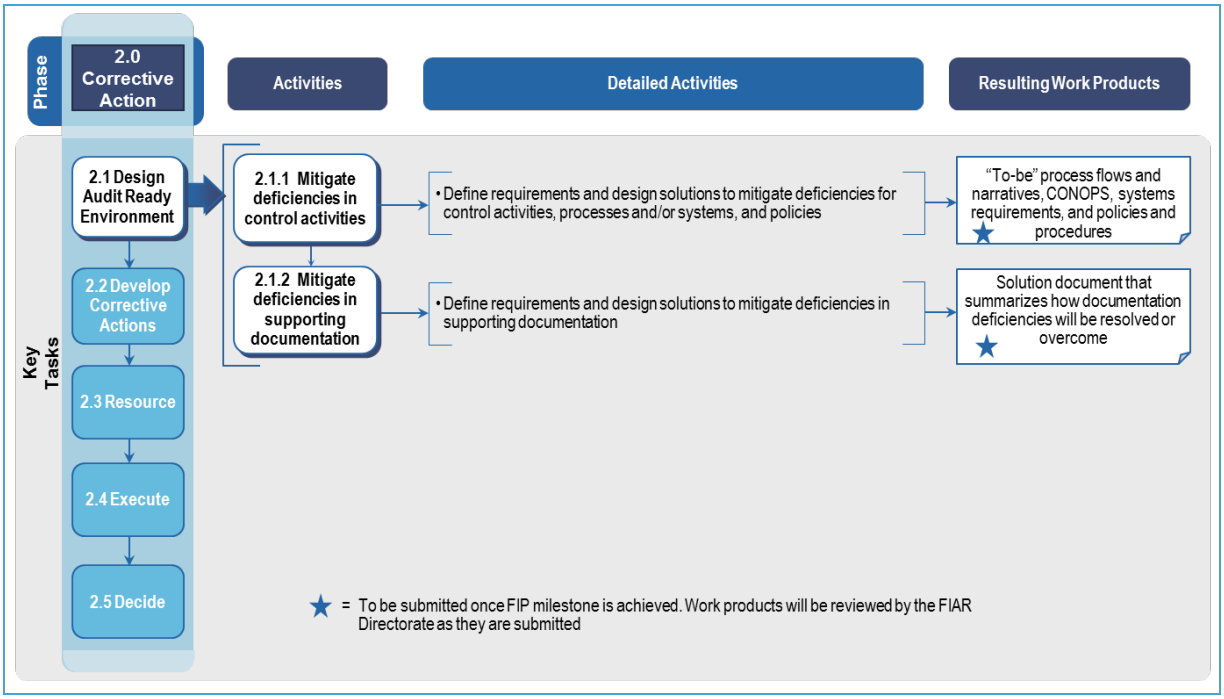

Figure 47. Corrective Action – Design Audit Ready Environment

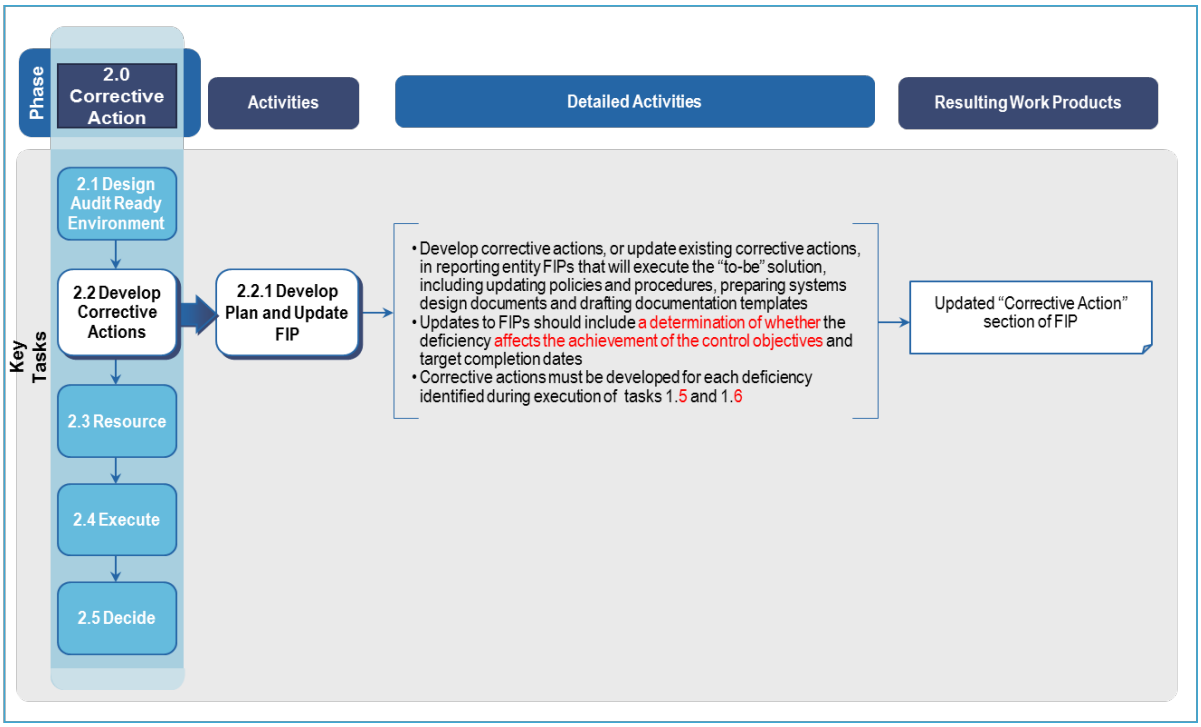

Figure 48. Corrective Action – Develop Plan and Update FIP

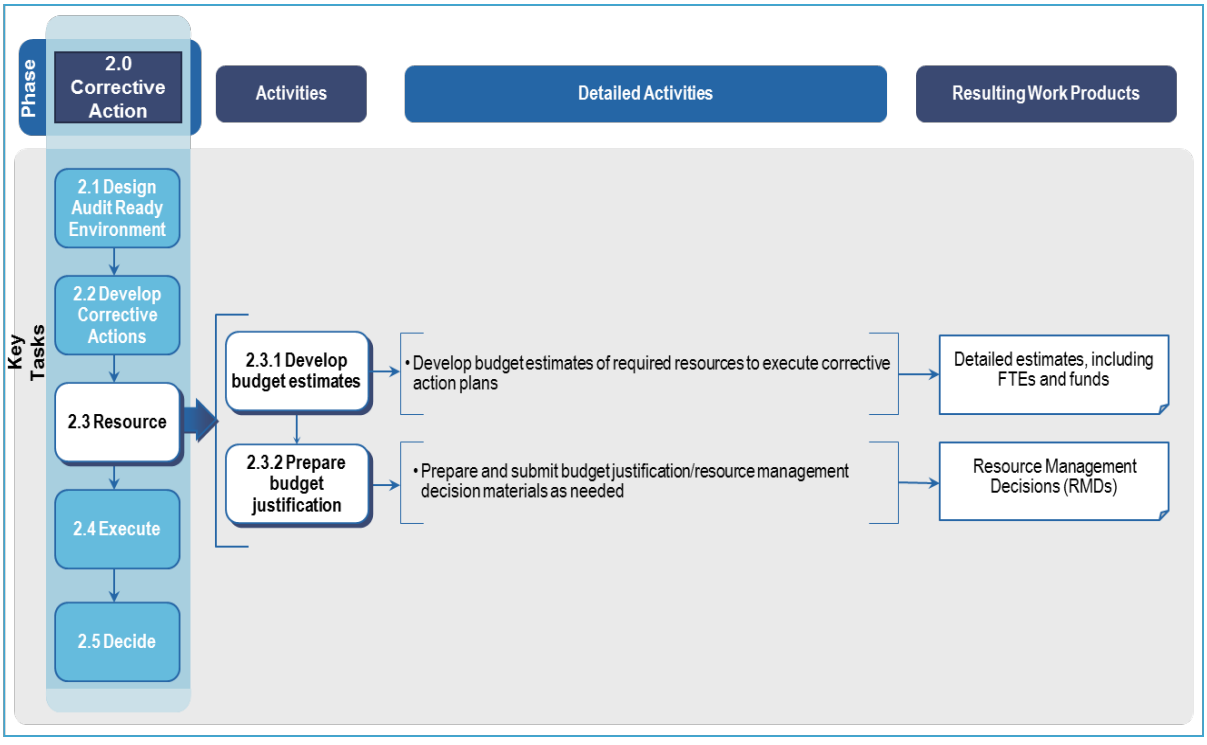

Figure 49. Corrective Action – Resource

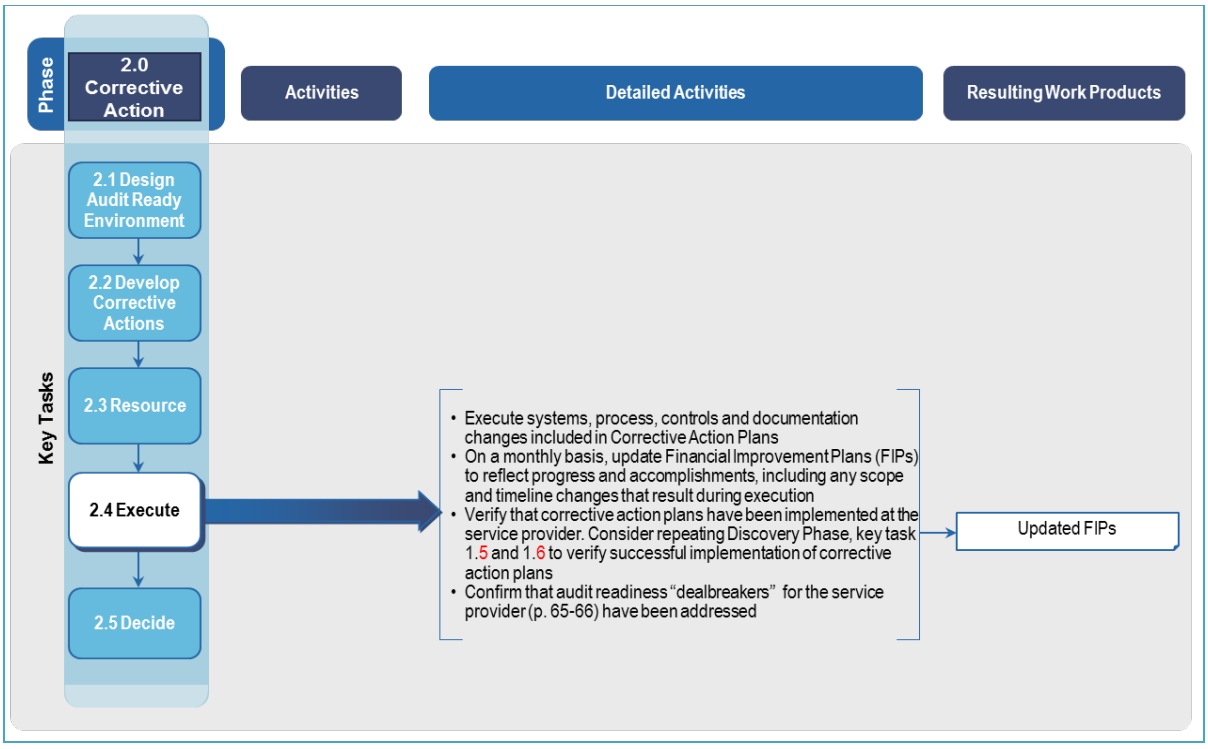

Figure 50. Corrective Action – Execute

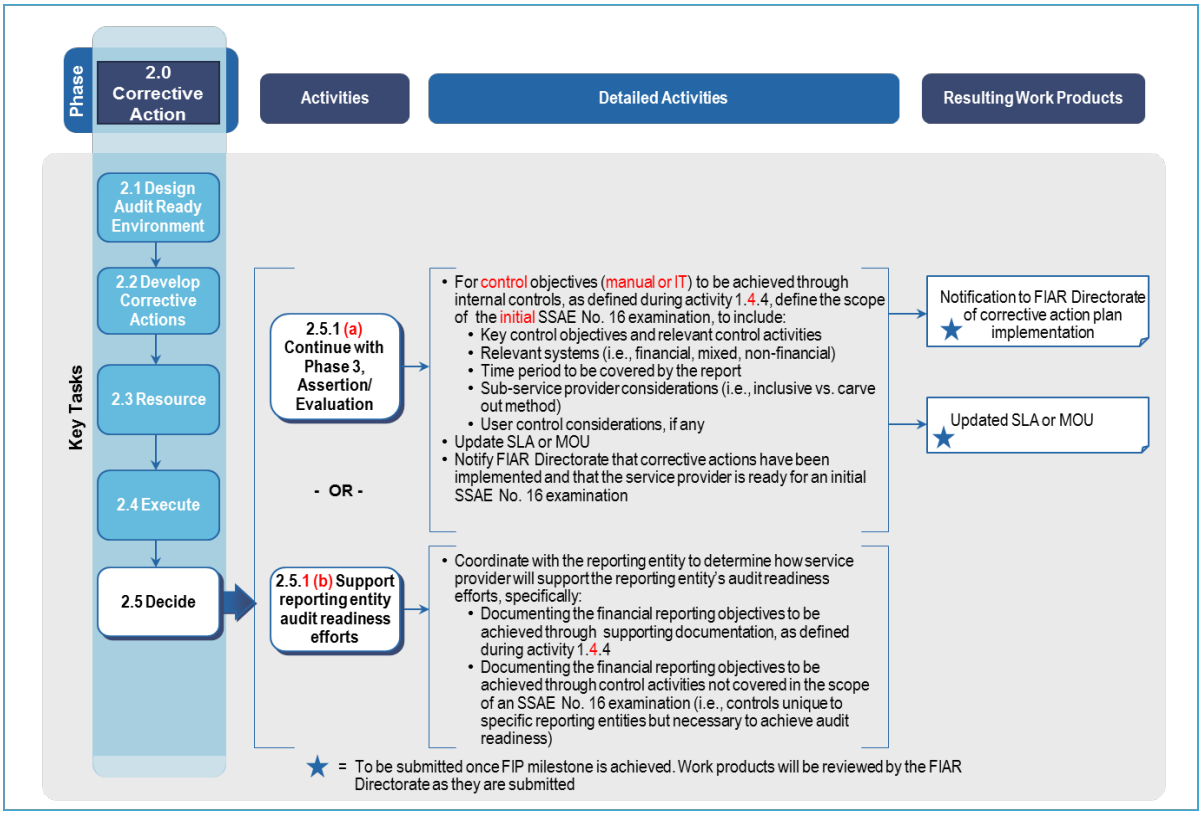

Figure 51. Corrective Action – Decide

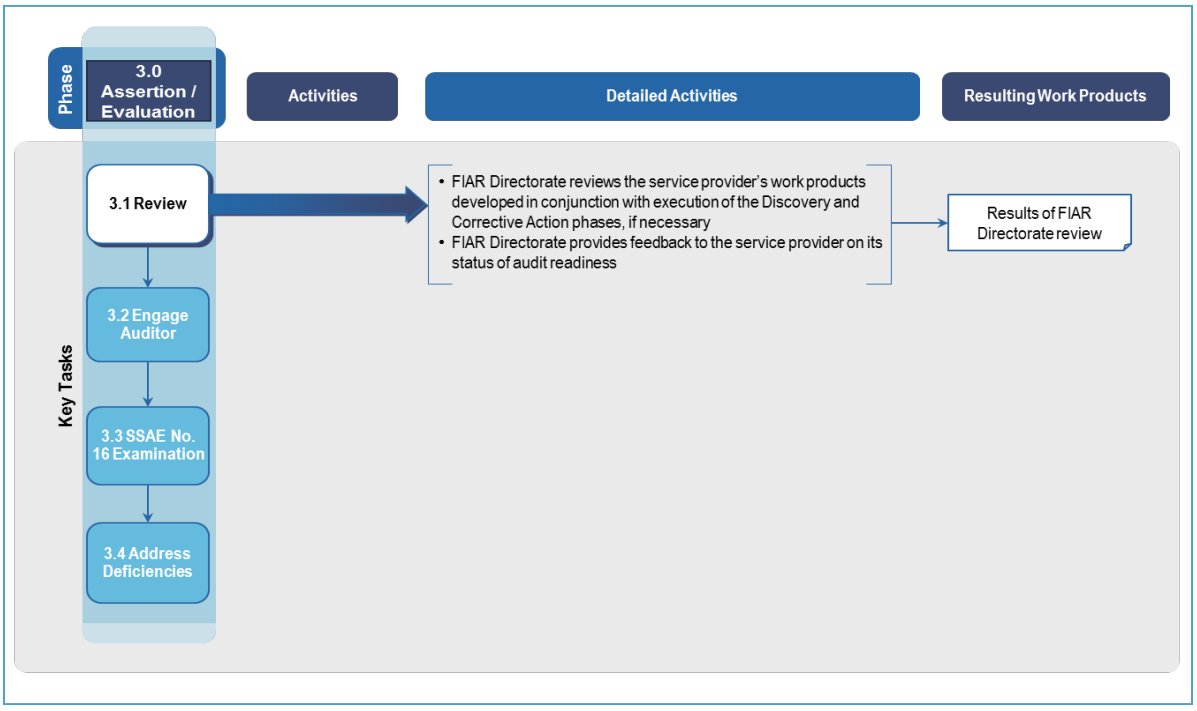

Figure 52. Assertion/Evaluation – Review

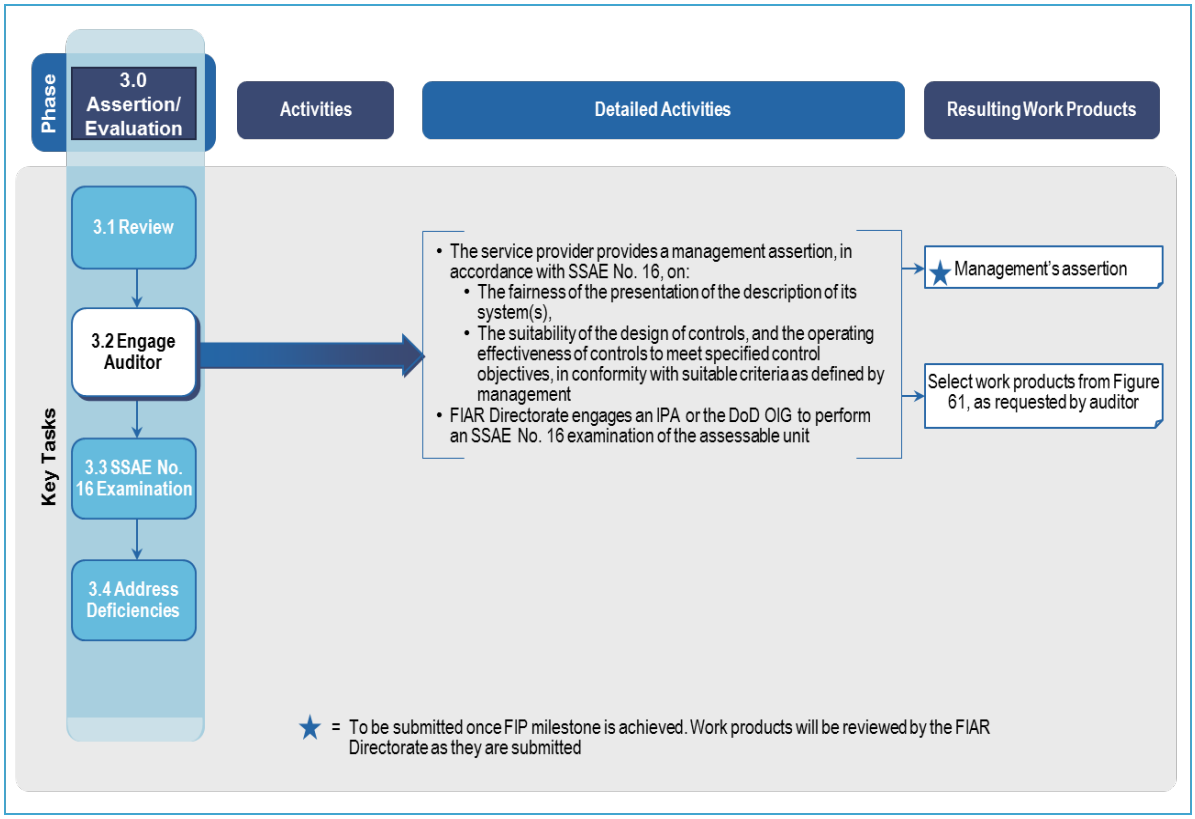

Figure 53. Assertion/Evaluation – Engage Auditor

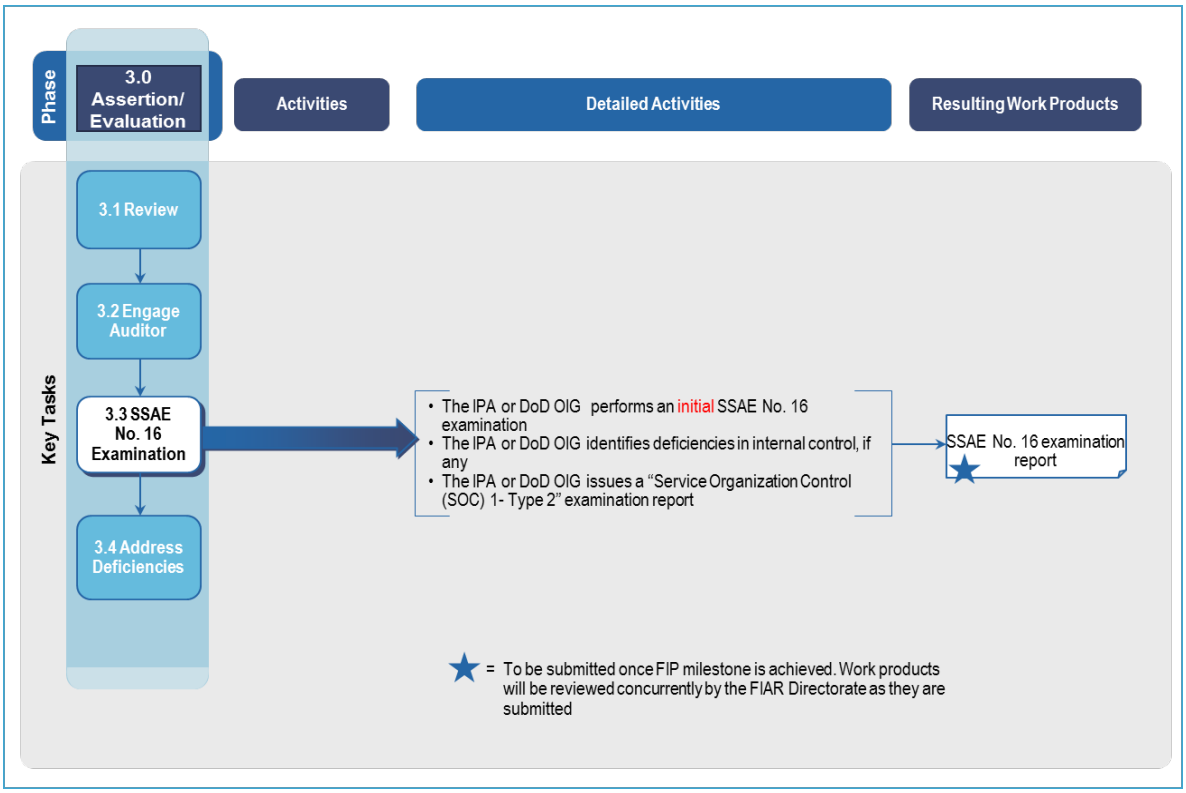

Figure 54. Assertion/Evaluation – SSAE No. 16 Examination

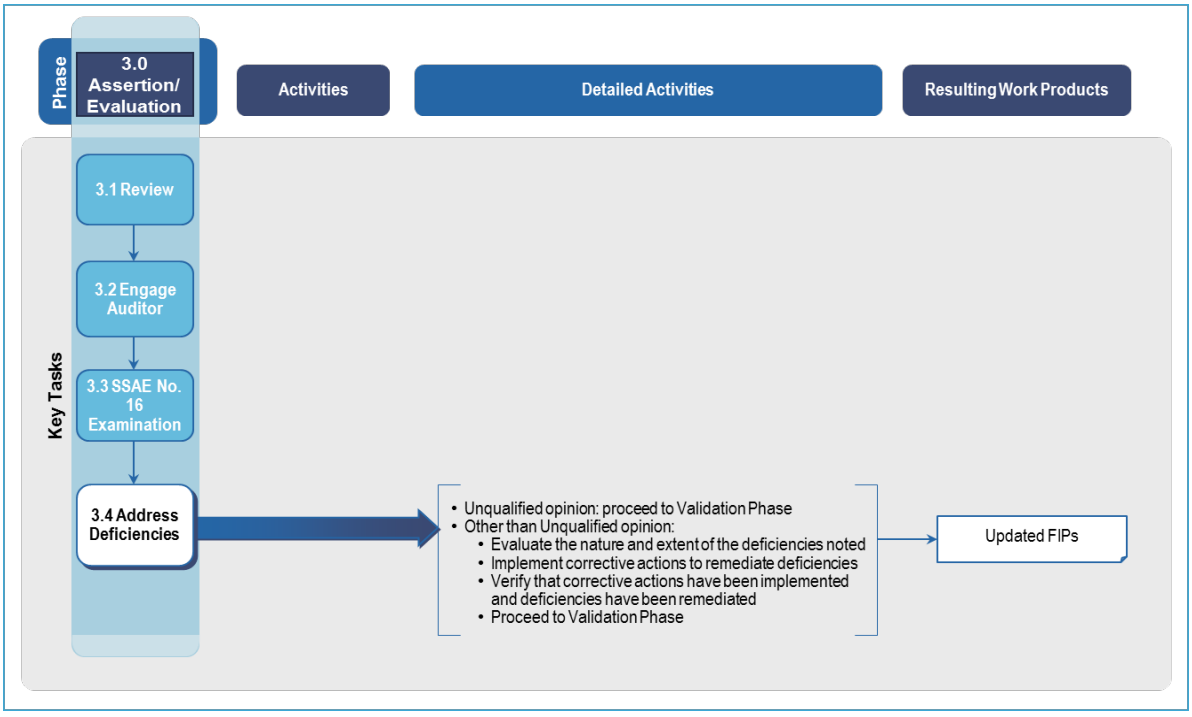

Figure 55. Assertion/Evaluation – Address Deficiencies

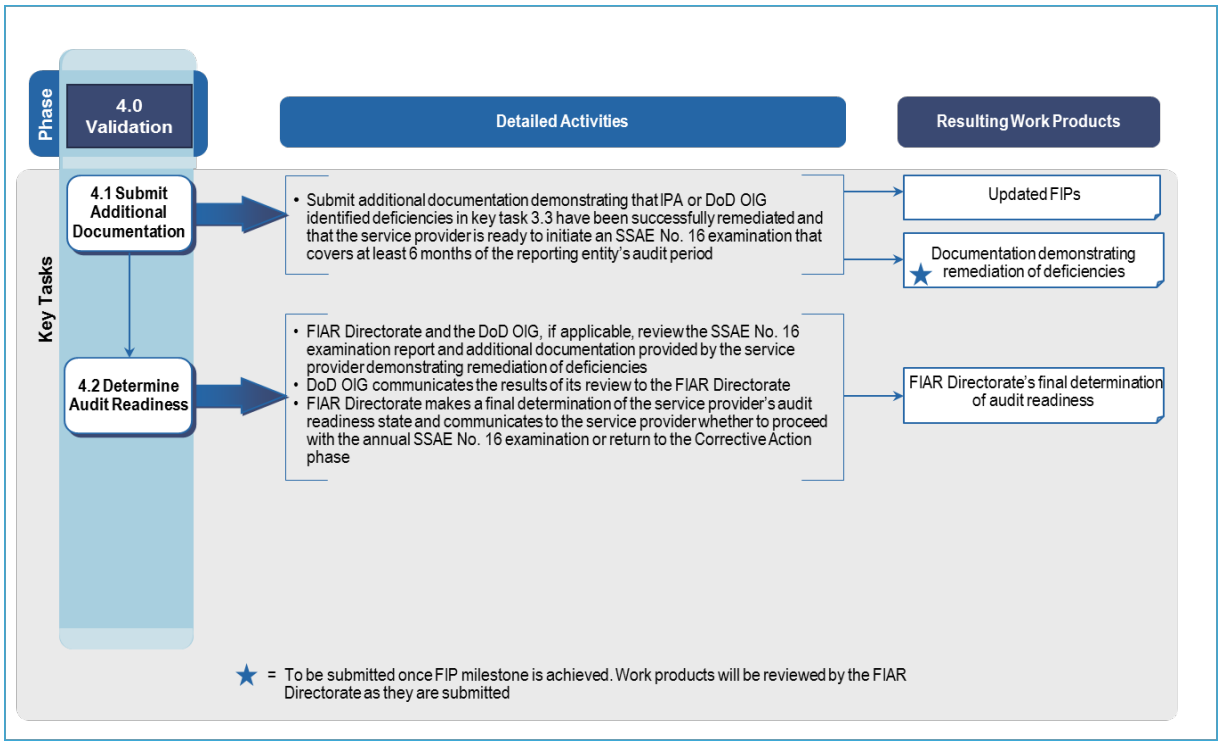

Figure 56. Validation Phase

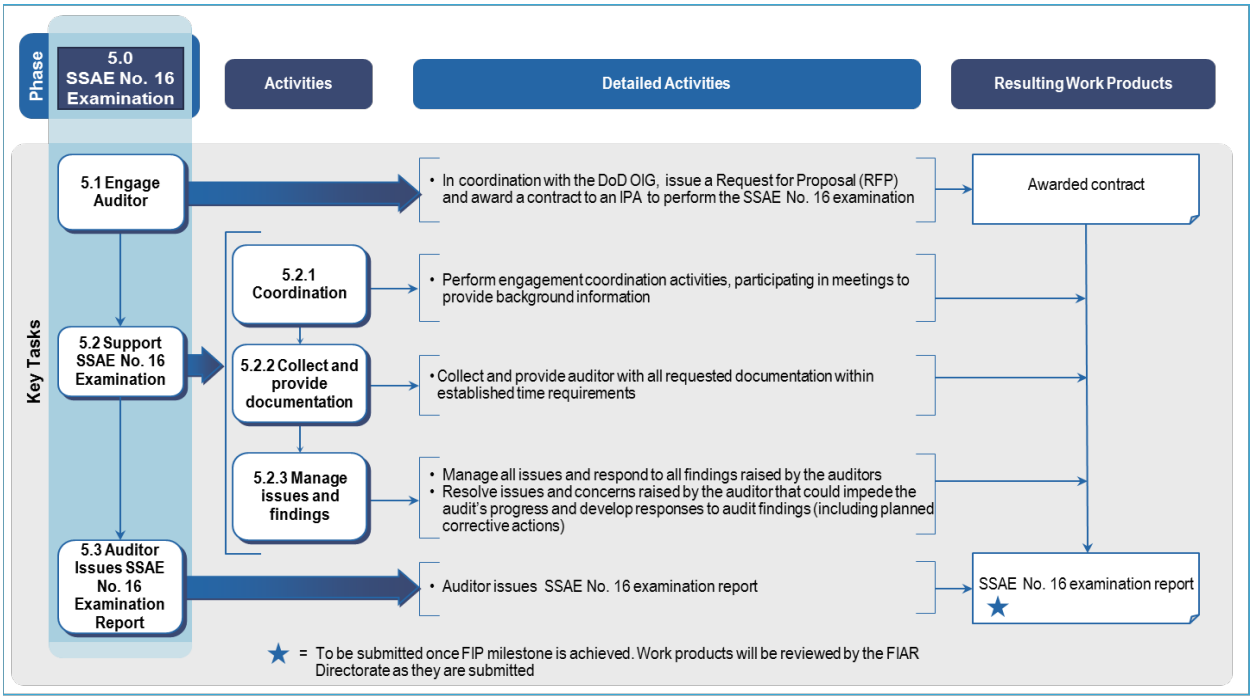

Figure 57. SSAE No. 16 Examination

3.B.6 Work Products

Service provider work products must follow the format of an SSAE No. 16 report and include the information that will be included in Section III and Section IV of the service auditor's report (even if the service provider is not pursuing an SSAE No. 16 examination). Section I of an SSAE No. 16 report contains the service auditor's report, which describes the scope of the SSAE No. 16 examination

and provides the service auditor's opinion. It is not required for the service provider's assertion documentation. Section II of an SSAE No. 16 report includes management's assertion, and Section III of an SSAE No. 16 report includes a description of the service organization's "system." Section IV of an SSAE No. 16 report includes a description of the control activities in place to achieve the control objectives, as well as the test plans and the test results (Type 2 report). Refer to the FIAR Guidance website for an example of a completed ***Section IV of the SSAE No. 16*** report and to download the ***SSAE No. 16 Section IV template***.

During the service provider's Discovery phase, the service provider should perform an audit impact assessment on service provider systems and processes, rather than the statement to process analysis and quantitative drill downs, to define the scope of the service auditor's report. **However, the service provider must coordinate with the reporting entity to prepare the overall Statement to Process Analysis, Quantitative Drill Down – Level 1 and Quantitative Drill Down - Level 2 for the reporting entity's assessable units.** The service provider will use these work products to determine the material processes, sub-processes, and systems the service provider is responsible for in supporting the reporting entity's audit readiness effort, either directly or by inclusion in the scope of the SSAE No. 16 report. (Note: the service provider does not need to submit the statement to process analysis and quantitative drill downs separately from the reporting entity.)

The graphic below illustrates the service provider work products outlined in accordance with the SSAE No. 16 report for Section II and Section III, and depicts how these service provider work products align to, and support reporting entity work products. The service provider's work products will be incorporated into the reporting entity's work products.

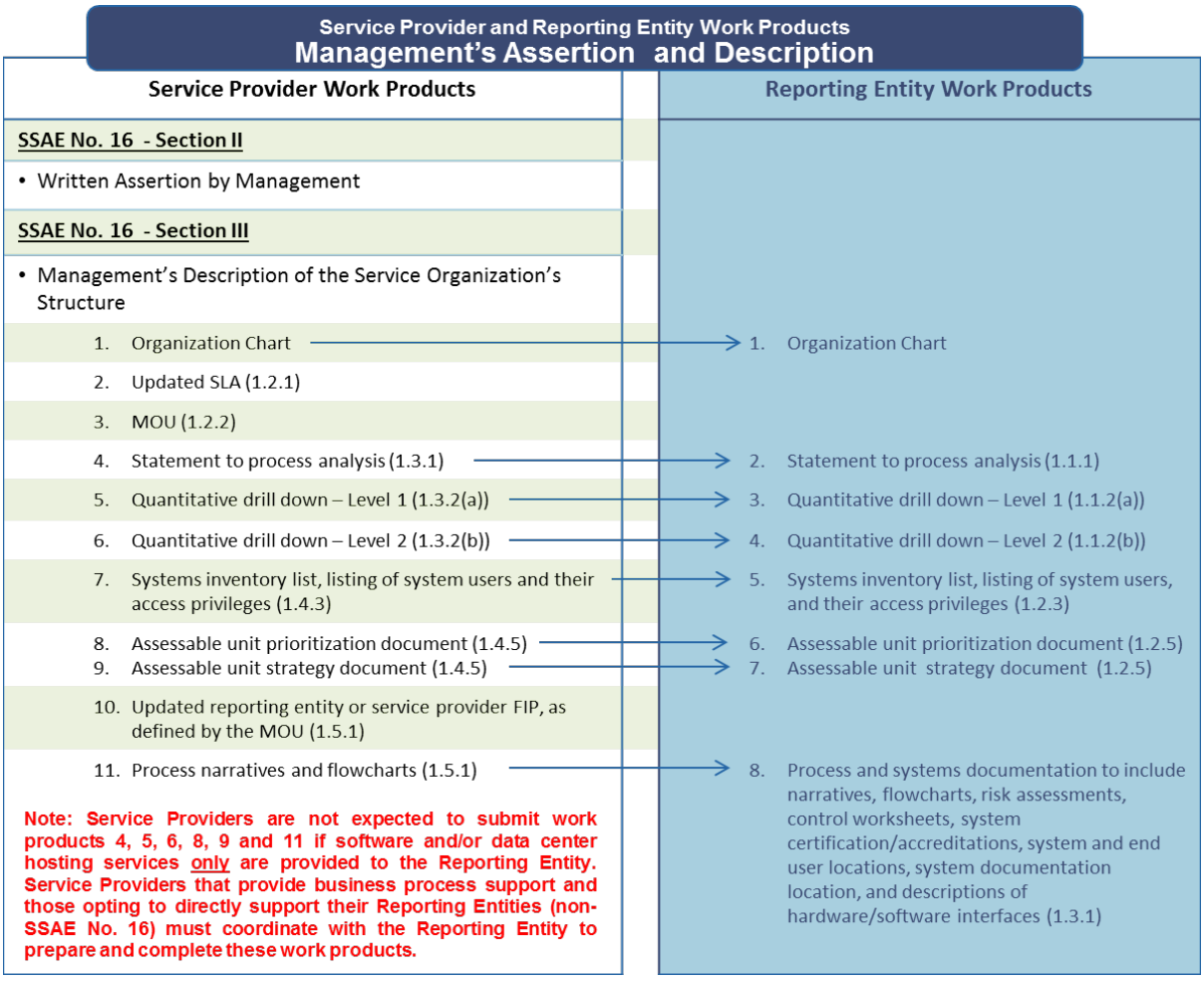

Figure 58. Service Provider and Reporting Entity Work Products – SSAE No. 16 Section III

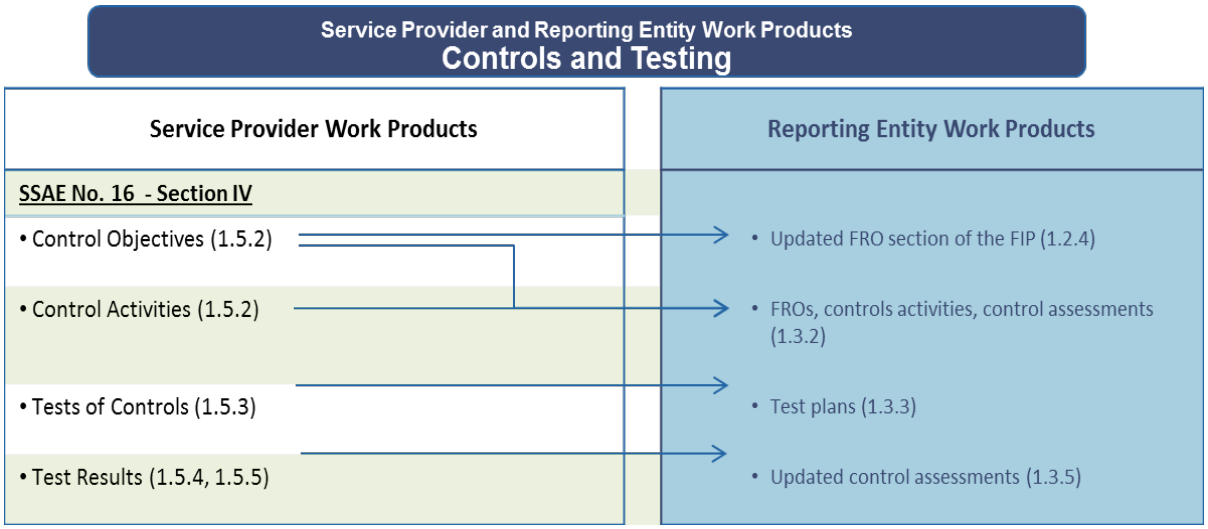

Figure 59. Service Provider and Reporting Entity Work Products – SSAE No. 16 Section IV

If the service provider is not prepared to assert audit readiness and undergo an SSAE No. 16 examination, the service provider is still required to support its customers by discussing an SSAE No. 16 examination timeline and working with customer auditors so as not to impede customer audit readiness progress.