3. FIAR METHODOLOGY

3.A METHODOLOGY – REPORTING ENTITY

The Methodology consists of a mandatory set of standardized phases and tasks that reporting entities must follow to achieve audit readiness. The Methodology, shown in **Figure 14**, is discussed in the pages that follow.

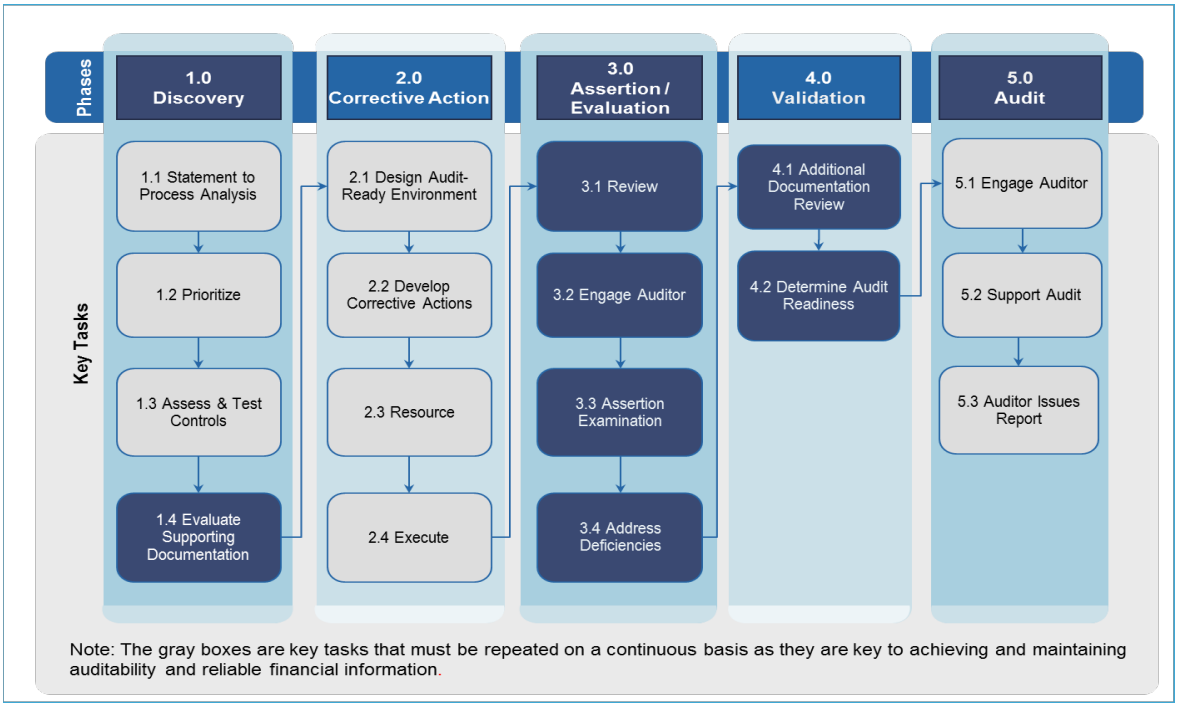

Figure 14. Phases and Key Tasks to Achieve Auditability and Reliable Financial Information

3.A.1 Phases and Key Tasks

The Financial Improvement and Audit Readiness (FIAR) Methodology consists of a series of phases, key tasks and underlying detailed activities that reporting entities must follow to improve financial information and achieve audit readiness. **Figure 14** graphically depicts the phases and the key tasks within each phase.

The phases and key tasks, which can be applied uniformly regardless of the size, materiality, or scope of an assessable unit, are as follows:

1. Discovery:
   a. Reporting entity documents business processes and its financial environment
   b. Reporting entity defines and prioritizes its processes into assessable units, and clearly defines the scope of its assertion and its strategy for achieving audit readiness
   c. Reporting entity identifies risks and financial reporting objectives and control activities, and tests the design and operational effectiveness of control activities
   d. Reporting entity evaluates the sufficiency and accuracy of documentation to support financial transactions, account balances and financial statement line items
   e. Reporting entity identifies and classifies any weaknesses and deficiencies in control activities and/or supporting documentation
   f. Reporting entity submits required work products to the FIAR Directorate for review in accordance with its Financial Improvement Plan (FIP) milestone dates; the FIAR Directorate reviews work

products to ensure all audit readiness dealbreakers have been addressed, and provides feedback and recommendations to the reporting entity on an ongoing basis

2. Corrective Action:
   a. Reporting entity defines and designs audit readiness environment, to include requirements for remediating deficiencies in internal controls and supporting documentation
   b. Reporting entity develops concrete corrective action plans (CAPs) to resolve each deficiency identified during the Discovery phase
   c. Reporting entity develops budget estimates of required resources (i.e., funding and staffing) to execute CAPs
   d. Reporting entity executes CAPs and performs procedures to verify that CAPs have successfully remediated the deficiencies
   e. Reporting entity notifies the FIAR Directorate that reporting entity is ready for an examination of its assessable unit
3. Assertion/Evaluation:
   a. FIAR Directorate evaluates documentation to determine audit readiness state
   b. FIAR Directorate provides feedback to the reporting entity on its status of audit readiness
   c. FIAR Directorate engages auditor to perform an examination of the reporting entity's audit readiness assertion; auditor identifies deficiencies, if any
   d. Reporting entity evaluates the nature and extent of deficiencies noted and implements corrective actions to remediate deficiencies
   e. Reporting entity performs procedures to verify that corrective actions successfully remediated auditor identified deficiencies
4. Validation:
   a. Reporting entity submits examination report and additional documentation demonstrating successful remediation of auditor-identified deficiencies to the FIAR Directorate and Department of Defense Office of Inspector General (DoD OIG)
   b. FIAR Directorate reviews examination report and additional documentation supporting successful remediation of deficiencies, and determines reporting entity's audit readiness state
5. Audit:
   a. Reporting entity engages an auditor
   b. Reporting entity supports specified elements audit (Wave 3) or full scope financial statement audits
   c. Auditor issues audit opinion

Reporting entities are responsible for executing the key tasks and activities in the *Discovery* and *Corrective Action* phases, including developing all required assertion work products to support their audit readiness assertion for their assessable units or financial statements. The OUSD(C) then engages an independent auditor to perform an examination on management's audit readiness assertion in the *Assertion/Evaluation Phase*. The reporting entity is responsible for implementing CAPs to remediate any auditor identified deficiencies, and must perform procedures to verify that the corrective actions successfully remediated the deficiencies. OUSD(C) reviews the independent auditor examination report and additional documentation supporting successful remediation of deficiencies to determine the reporting entity's audit readiness state. Once OUSD(C) validates that the reporting entity is audit ready, the reporting entity engages an independent auditor to perform the audit of the assessable unit or financial statement(s) in the *Audit Phase*.

Once the reporting entity asserts audit readiness for the entire SBR (overall Wave 2), the reporting entity will initially be subjected to a "Specified Elements Audit" in accordance with AU-C Section 805, *Special Considerations – Audits of Single Financial Statements and Specific Elements, Accounts, or Items of a Financial Statement*. In the first year under audit, the reporting entity will undergo an audit of schedules containing only current year appropriations and all related activity (i.e., obligations, outlays, etc.) against those appropriated funds. To undergo the first year audit, the reporting entity must prepare a Schedule of Current Year Budgetary Resources to include all information related to appropriations beginning with the current year, following the guidance in OMB Circular No. A-11, "Preparation, Submission, and Execution of the Budget" for preparation of the SF 133 (Report on Budget Execution and Budgetary Resources) and the related note disclosures, following the guidance in OMB Circular A-136 "Financial Reporting Requirements."

In subsequent years until an unqualified opinion is received, the reporting entity will commence audits of schedules of both current year and prior year audited appropriations and all related activity against those appropriated funds. Through each successive audit, the ending audited balances carry forward to the subsequent year's beginning balance, thereby reducing the percentage of unaudited beginning balances each year. The approach for auditing schedules of appropriation activity provides critical insight into whether a reporting entity's current business and financial practices, processes, controls, and systems support auditability. Reporting entities will commence a full scope financial statement audit of the entire SBR once they receive an unqualified opinion on their schedule(s) of budgetary activity.

Reporting entities are also required to annually prepare and submit a SOA over internal controls over financial reporting and internal control over financial systems. This is not a separate phase, but rather an annual requirement that must be performed regardless of the audit readiness status of the reporting entity. Requirements related to the submission of the annual statement of assurance including the summary CAP are described in Section 2.F. Please refer to the FIAR Guidance website to obtain the latest *Statement of Assurance Memorandum* Template and the *Corrective Action Plan* Template.

The terms "audit," "examination," and "specified elements audit," used throughout this document are defined as:

- Financial statement audit (Audit) – The primary purpose of a financial statement audit is to provide reasonable assurance through an opinion (or disclaimer of an opinion) about whether a reporting entity's financial statements are presented fairly in all material respects in conformity with United States (U.S.) generally accepted accounting principles (GAAP). These audits are performed in accordance with Generally Accepted Government Auditing Standards (GAGAS).
- Examination – Consists of obtaining sufficient, appropriate evidence to express an opinion, in accordance with GAGAS, on whether the subject matter is based on (or in conformity with) criteria[7] that are suitable (i.e., objective, measurable, complete and relevant) and available to users, in all material respects or the assertion is presented (or fairly stated), in all material respects, based on the criteria. See Section 2.D for an example management assertion template to be used when engaging an auditor for an *Assertion/Evaluation Phase* audit readiness examination.
- Specified elements audit[8] – Consists of an independent auditor conducting an audit in accordance with GAGAS and AU-C Section 805 to obtain sufficient, appropriate evidence to express an opinion in connection with specific elements, accounts or items of a financial statement.

[7] "Criteria" are the standards or benchmarks used to measure or present the subject matter and against which the practitioner evaluates the subject matter. Management may establish criteria for an examination; however, practitioners will evaluate management's criteria to ensure that it is suitable, that is, relevant, measurable, complete and objective. (http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-00101.pdf)

[8] The SBR audit will initially be limited to a "Specified Elements Audit" since the scope will be limited to audits of "schedules" containing only current year appropriations and all related activity against those appropriations. Audits of schedules containing only current year activity will provide the opportunity to assess progress and identify any issues in a way that a disclaimer on full financial statements would not.

3.A.2 Consideration of Service Providers

Embedded within the Methodology's phases are the reporting entity's considerations of its service providers and how their activities affect its financial processes and related audit readiness.

Reporting entities' management is responsible for the internal control over their financial information and, therefore, must ensure that they understand what financially significant activities are outsourced to service providers and the effectiveness of the service providers' related internal controls. In turn, service providers are responsible for providing a description of their controls that may affect their customer reporting entities' control environment, risk assessment, control activities, and information and communication systems. The description of controls should be detailed enough to provide the reporting entity auditors with sufficient information to assess the risks of material misstatement. For a detailed discussion of service providers' role in the Methodology, see Section 3.B.

3.A.3 Assessable Units

Reporting entities must follow the Methodology for each assessable unit. Assessable units can vary between line items, processes, systems, or classes of assets, depending on the wave and reporting entity preferences. These assessable units can be further separated into assessable sub-units at the reporting entity's discretion. **Reporting entities must establish assessable units for all processes, systems, or classes of assets that result in material transactions and balances in their financial statements.** As noted in Section 2.D, reporting entities must clearly define the beginning/initiation and end of the process for each assessable unit that is not a financial statement line item. Additionally, established assessable units should not be duplicative or overlap. To ensure completeness of assessable units, reporting entities should prepare quantitative drill downs depicting the dollar volume of activity flowing through each assessable unit consistent with the tasks in the *Discovery Phase* key activity 1.1.2. Wave-specific considerations when identifying assessable units are included in the following paragraphs.

Waves 1 & 2

The OUSD(C) has pre-defined one assessable unit for the SBR, Appropriations Received, which represents Wave 1. Due to its limited scope, the OUSD(C) has pre-defined this assessable unit for all reporting entities and directed them to prioritize this assessable unit to allow the Department to demonstrate immediate progress. Refer to **Appendix C** for a more detailed discussion of the scope of this wave.

Beyond Wave 1, reporting entities have the flexibility to determine their appropriate assessable units for the remainder of the SBR (Wave 2). Assessable units for the SBR may be subaccounts that make up the obligations line item, classes of financial transactions or processing systems. For example, the "Obligations Incurred" line item on the SBR is comprised of many types of financial transactions that are processed through many systems. Assessable units within the "Obligations Incurred" line item may be comprised of classes of financial transactions, such as contractor payments, military pay, and civilian pay. An assessable unit may be a class of transactions or it may also be all financial transactions that are processed through a particular system. Determining assessable units is a key task of preparing for auditability because the assessable units provide the focus for financial improvement efforts.

Waves 3 & 4

For Waves 3 & 4, assessable units include classes, categories, or groupings of all General Property, Plant and Equipment (G-PP&E) and Inventory and Related Property. Asset-related assessable units may also be groups of data within an Accountable Property System of Record (APSR) or equivalent, such as the Reliability and Maintainability Information System (REMIS), which is used by the Air Force for aircraft accountability, and the Defense Property Accountability System (DPAS), which is used by the Marine Corps (and other reporting entities) to track certain general equipment categories. When the data in an APSR defines the assessable unit, the scope will include all mission critical assets within the system. Examples of assessable units for wave 3 include:

- Real property,
- Inventory,
- Operating Materiel and Supplies, and
- General Equipment

For Wave 4, assessable units also include other material financial statement line items on the Balance Sheet, Statement of Net Cost and Statement of Changes in Net Position (e.g., Environmental and Disposal Liabilities, Military Retirement and Other Federal Employment Benefits, Other Liabilities, Investments, Cash and Other Monetary Assets, Other Assets, etc.) as well as Internal Use Software, a component of the G-PP&E line item on the Balance Sheet. Wave 4 assessable units may include line items, accounts or balances that were addressed in an earlier wave. Reporting entities must determine whether sufficient testing was performed for both budgetary and proprietary accounts for those assessable units. It is important to note that additional testing may be required in Wave 4 to ensure complete coverage of all accounts (see discussion in section 2.C.4 for more information on Wave 4 assessable units).

3.A.4 Financial Systems Considerations

In addition to completing key tasks, activities and work products included in the FIAR Methodology, reporting entities are also responsible for fulfilling multiple financial systems requirements that have been established by separate regulations.

From a systems compliance standpoint, three of the major regulations that a reporting entity wants to concern itself with are the Federal Managers' Financial Integrity Act of 1982 (FMFIA), the Federal Financial Management Improvement Act of 1996 (FFMIA) and the Federal Information Security Management Act of 2002 (FISMA). Guidance has been developed to assist in the implementation of each regulation. The regulations and corresponding sources of implementation guidance have been presented in **Figure 15**.

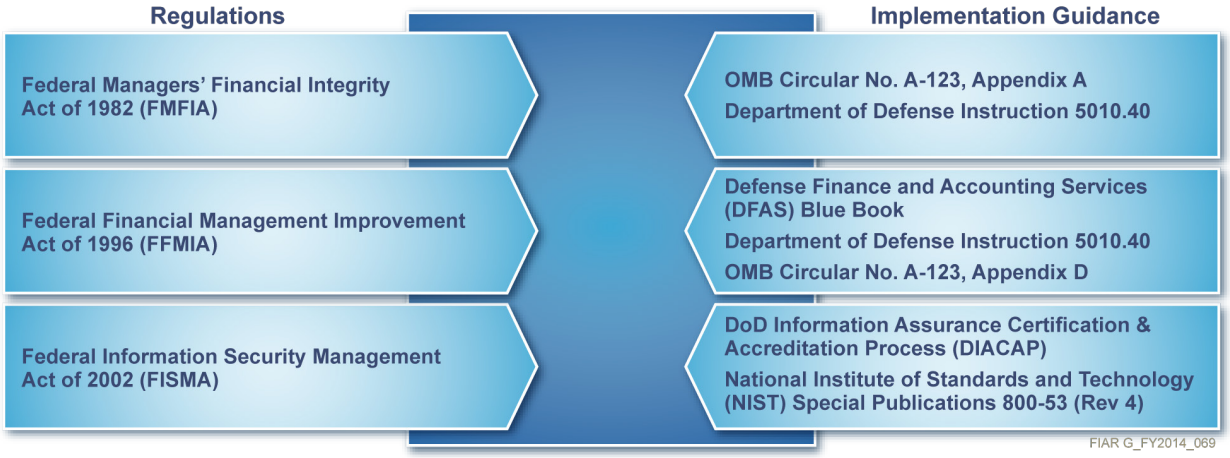

Figure 15. Regulations and Corresponding Implementation Guidance

Implementation guidance for systems compliance requirements varies significantly in terms of specificity. OMB Circular No. A-123 for example, focuses on general conditions that a reporting entity must comply with, whereas the DFAS Blue Book 7900.4-M maintains detailed requirements for specific components or modules of a financial system. Prior to executing the FIAR Methodology, each reporting entity's audit readiness team should ensure that it has a comprehensive understanding of systems compliance requirements. Summaries of FMFIA, FFMIA and FISMA are presented in **Figure 16**.

Regulation	Summary
Federal Managers' Financial Integrity Act of 1982 (FMFIA)	Focuses on operational, administrative, systems and financial controls. Amended the Accounting and Auditing Act of 1950 and directed agencies to complete ongoing self-assessments regarding the adequacy of these controls. Requires agencies to provide an annual Statement of Assurance to the President and Congress.
Federal Financial Management Improvement Act of 1996 (FFMIA)	Focuses on financial management systems and other systems that impact financial reporting. The statute contains a series of requirements aimed at improving federal financial management. Included in the Act is a requirement of agencies to incorporate applicable federal accounting standards into their financial management systems and a requirement for agencies to report on whether or not their financial systems routinely provide reliable financial information.
Federal Information Security Management Act of 2002 (FISMA)	Places an emphasis on cybersecurity. Requires federal agencies to develop, document and implement an agency-wide program to provide information security for the information and information systems that support its operations and assets.

Figure 16. Financial Systems Regulations

3.A.5 Federal Information System Controls Audit Manual (FISCAM)

Adopting an integrated audit readiness strategy that incorporates pertinent systems compliance requirements is paramount to ensuring that a reporting entity is able to achieve all of its financial system objectives in a timely and cost-effective fashion. In some instances, the performance of key tasks and activities for audit readiness purposes may be leveraged to help fulfill some of a reporting entity's systems compliance requirements. Conversely, in other situations, audit readiness may be a byproduct that arises from systems compliance undertakings. In both scenarios, by successfully aligning systems compliance objectives with FIAR initiatives, reporting entities will be able to gain efficiencies and avoid potentially duplicative efforts.

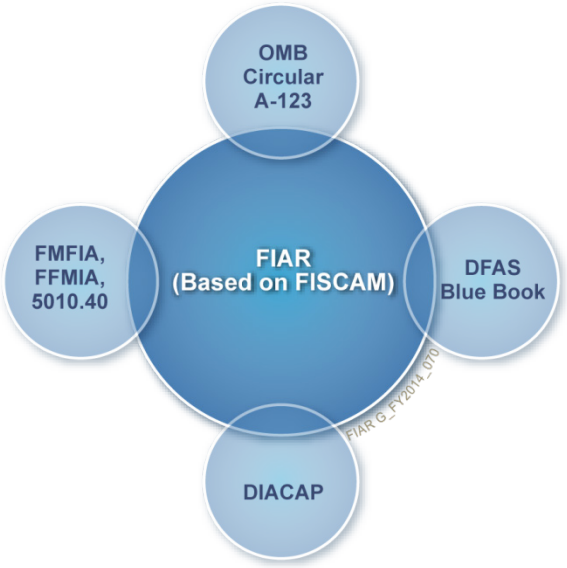

Figure 17. Integrated Audit Readiness Strategy

The GAO has developed and published its Federal Information System Controls Audit Manual (FISCAM) to describe (1) an audit methodology for assessing the effectiveness of IT controls, and (2) the information technology (IT) controls that auditors evaluate when assessing the confidentiality, integrity, and availability of information and information systems. FISCAM includes testing of IT controls necessary for financial statement audits including select requirements from FMFIA, FFMIA and FISMA. **Reporting entities must ensure that the requirements set forth in GAO's FISCAM are met for the systems that are necessary to achieve financial improvement and audit readiness.** The GAO's FISCAM is comprised of three sections for internal controls relevant to financial information systems:

- Entity Level Information Technology General Controls (ITGCs);
- Application Level ITGCs; and
- Automated Application Controls.

Entity Level ITGCs consist of: Security Management, Access Controls, Configuration Management, Segregation of Duties, and Contingency Planning. Entity Level ITGCs are pervasive across platforms and affect the entire organization.

Application Level ITGCs cover the same basic controls as Entity Level ITGCs (i.e., Security Management, Access Controls, Configuration Management, Segregation of Duties, and Contingency Planning), but are unique to individual business and/or financial systems and any feeder systems.

Automated Application Controls use a different set of control categories (Application Security, Business Process Controls, Interface and Conversion Controls and Data Management System Controls) and focus on a specific application (e.g., Defense Departmental Reporting System (DDRS), Defense Civilian Pay System (DCPS), etc.).

The FIAR Directorate has identified the FISCAM control activities and techniques needed to address the key internal controls over financial reporting risk areas most likely to impact financial reporting based on the Department's experience. The remaining FISCAM control activities (identified as "Other Control Techniques for Consideration in a Financial Statement Audit") should be considered by reporting entities when evaluating federal financial systems' compliance with laws and regulations (outside of audit readiness). A summary listing of ***FISCAM control activities and techniques*** can be found on the FIAR Guidance website.

As illustrated in the system view diagram included as **Figure 18**, in some cases, a reporting entity's financial systems may be owned and/or operated by executive agents and the transactions that flow through those systems may be processed by a service provider. In such situations, the reporting entity still has the ultimate responsibility for information technology controls over those systems through which its financial transactions flow, and will need to communicate and coordinate audit readiness efforts with the executive agent and service provider. Section 3.B provides a discussion of reporting entity and service provider roles and responsibilities in the execution of the FIAR Methodology and FIP reporting.

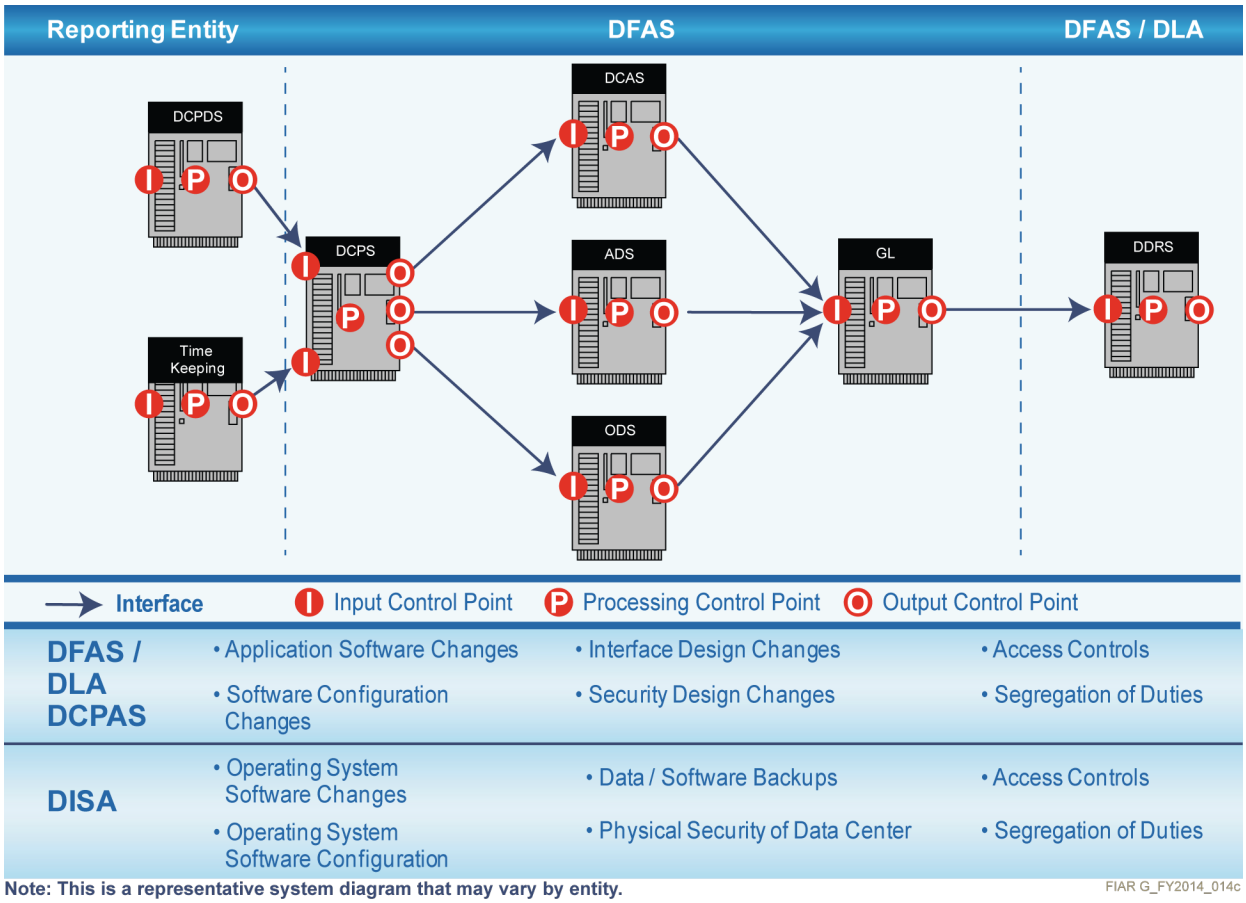

Figure 18. System View Diagram: Reporting entities must consider information technology input, process, output and general computer controls for all relevant reporting entity and service provider systems

Financial system controls are important to a reporting entity's audit readiness because system outputs (e.g., system reports) and electronic evidence (e.g., electronic invoices) may serve as KSDs for both the operating effectiveness of controls and transactions/balances. There are a variety of systems that must be considered in reporting entity audit readiness efforts, such as: general ledger systems, source/feeder systems, system interfaces, disbursing systems, reporting systems, and property management systems. **Therefore, reporting entities must ensure adequate entity-level and application-level ITGCs and automated application controls are in place or appropriate corrective actions are planned and implemented. The reporting entity must identify all key systems (including feeder systems and micro-applications) that affect the assessable unit being asserted as audit ready. These key systems should be evaluated and IT controls identified and tested if the reporting entity's:**

- **Controls within the system are identified as key controls in the internal controls assessment;**
- **Systems are used to generate or store original key supporting documentation;**
- **Reports generated by the system are utilized in the execution of key controls; or**
- **Systems are relied upon to perform material calculations (e.g., to compute payroll).**

In addition, if reporting entities are implementing an Enterprise Resource Planning (ERP) system, or engaging in other system modernization efforts, and the system is a solution for resolving audit impediments, the reporting entity should map known process and control weaknesses to the new system's requirements to ensure that the new system will adequately address the impediment. For example, reporting entities with environmental liability material weaknesses should reference the Deputy Under Secretary of Defense Installations and Environment (DUSD (I&E)) Environmental Liability business process reengineering requirements for mapping to their ERP system and control objectives provided as FROs.

It is important to note that financial systems may not be limited to traditional, large/complex legacy or ERP systems. There may be instances where end user computing tools such as spreadsheets, databases, or other software tools impact key controls or calculations that are relevant to financial reporting. These end user computing tools are sometimes referred to as "micro-applications". Micro-applications require control techniques that are aligned to the IT general and application control objectives. Reporting entities must evaluate the risk of micro-applications on the associated financial processing. For example, risk to the financial process can increase when the number of transactions and dollar value processed by the micro application increases. Implemented control techniques for these micro-applications should be commensurate with the relative sophistication of the software tool and its impact on internal controls over financial reporting. Examples of control techniques include restricted shared directories, password protection of files, locking cells and formulas, enabling edit macros, enforcing segregation of duties, and creating a change management process.

Supplemental guidance can be found on the FIAR Guidance website for assessing the relative impact and suggested levels of testing for ***micro-applications***.

When identifying information technology applications that are relevant to audit readiness assertions, reporting entities and service providers should also ensure they identify the specific "instances" of the application upon which their data resides, and ensure appropriate IT general and application control testing is performed on their specific instances. For example, the Department has four separate instances of its civilian personnel system, the Defense Civilian Personnel Data System (DCPDS). While the Defense Civilian Pay Advisory Service (DCPAS) is the system owner of DCPDS and is responsible for maintaining and updating the DCPDS application, the Army, Navy and Air Force each host an instance of DCPDS in their own data centers, in addition to the instance of DCPDS hosted by a DCPAS contractor. Therefore, reporting entities whose civilian personnel data resides on the Army's instance of DCPDS would need to coordinate with both the Army (for certain IT general controls) and DCPAS (for certain IT general and application controls), while a reporting entity whose civilian personnel data resides on the DCPAS instance of DCPDS would only need to coordinate with DCPAS.

3.A.6 Identify and Leverage Synergies

For each activity listed in the FIAR Methodology, a reporting entity should consider its associated responsibilities necessitated by relevant systems compliance guidance. When formulating a plan to carry out each FIAR activity, a reporting entity should strive to implement an integrated approach to execution that takes into account related requirements and that will allow for compliance with the systems regulations or FIAR standards that maintain the most stringent requirements and contain the greatest degree of specificity. In doing so, a reporting entity can ensure that it has met applicable standards efficiently and effectively.

If a reporting entity was planning to test payroll as part of activity *1.3.3: Execute Tests of Controls* from the FIAR Methodology for its civilian pay assessable unit, it could embed tests of systems compliance into its FIAR test plans to reduce the level of effort that would otherwise be needed to satisfy the related requirements separately.

For example, the reporting entity could include a test to be performed by the reporting entity and/or a service provider as part of its test plan that specifically addresses requirement 07.05.023 from the DFAS Blue Book 7900.4-M Vol. 7, which states, “To support pay processing, the payroll system must perform statutory limit and reasonableness tests on gross pay.” Rather than selecting a separate sample as part of an independent systems compliance testing initiative, the inclusion of an additional test for a FIAR test plan would result in a substantial savings of time and effort.

The crosswalk in **Figure 19** has been developed to help facilitate the design of an integrated strategy for DoD reporting entities pursuing a state of audit readiness.

The tasks that have been recorded on the vertical axis of the crosswalk have been identified as FIAR Methodology activities with systems compliance implications. The regulations and guidance to which these activities relate have been presented on the horizontal axis. Tasks from the FIAR Methodology that do not have systems compliance implications have not been included in the crosswalk. Within the crosswalk itself, a checkmark indicates that a FIAR activity can be performed in a manner that can also satisfy a corresponding systems compliance requirement. A “P” indicates that the completion of a FIAR activity will only partially satisfy a corresponding systems compliance requirement. In instances where a FIAR activity only partially satisfies a corresponding systems compliance requirement or vice versa, incremental documentation and testing may be required. The nature and extent of the incremental activity will be determined based upon the degree of the gap that exists between the FIAR workproducts and the systems compliance requirement. Reporting entities should refer to applicable sources of systems compliance guidance to identify the additional procedures that may be required to fully satisfy each systems compliance objective.

A representative approach for leveraging synergies and resolving gaps would be performed in the following sequence:

- Develop and execute an integrated FIAR and systems compliance testing strategy
- Evaluate FIAR and systems compliance work completed
- Identify gaps with FIAR or systems compliance requirements
- Design and perform incremental procedures to fully satisfy remaining requirements

A ***NIST 800-53 to FISCAM crosswalk*** can be found on the FIAR Guidance website. It can also be utilized by reporting entities to identify common requirements. However, documentation and testing must be performed in accordance with the FIAR Guidance where applicable.

FIAR Methodology Crosswalk to Systems Compliance Requirements								
FIAR Methodology				Systems Compliance Requirements				
Task No.[1]	Key Task	Detailed Activities	Resulting Work Product	OMB Circular No. A-123, Appendix A	FMFIA, FFMIA, and DoD MICP Procedures (DoD Instruction 5010.40)	DIACAP (NIST SP 800.53)	FISMA Self-Assessment (NIST SP 800.53)	DFAS Blue Book 7900.4-M
1.1	**Statement to Process Analysis**							
1.1.1	Overall Statement to Process Analysis	Develop process and system drill down analysis depicting asset/transaction classes, underlying processes, assessable units and sub-units and associated systems – including "as-is" and any planned "to-be" environments.	Statement to Process Analysis	✓	✓	P	P	✓
1.2	**Prioritize**							
1.2.3	Planned Systems and Process Replacements	Develop a systems inventory list to include all current and future systems.	Systems Inventory List	✓	✓	P	P	✓
1.2.4	Identify Financial Reporting Objectives	Identify and document entity level controls. Identify all relevant financial statement assertion risks and corresponding Financial Reporting Objectives.	Assessable Unit Prioritization and Audit Readiness Strategy Document	✓	P	P	P	P
1.2.5	Document Strategy and Prioritization	Prepare an assessable unit strategy document listing all assessable units prioritized by quantitative rank and adjusted for significant qualitative factors and scoping out legacy systems and processes that will not be part of the audit ready environment.	Assessable Unit Prioritization and Audit Readiness Strategy Document	✓	P	P	P	P
1.3	**Assess & Test Controls**							
1.3.1	Prepare Process & System Documentation	Prepare systems documentation to include narratives, risk assessments and internal control worksheets documenting processes, risk control activities, IT general computer controls for significant systems, applications or micro-applications, system certifications/accreditations, system and end user locations, systems documentation location and descriptions of hardware/software interfaces.	Process and System Documentation	✓	P	P	P	P

FIAR Methodology Crosswalk to Systems Compliance Requirements								
FIAR Methodology				Systems Compliance Requirements				
Task No.[1]	Key Task	Detailed Activities	Resulting Work Product	OMB Circular No. A-123, Appendix A	FMFIA, FFMIA, and DoD MICP Procedures (DoD Instruction 5010.40)	DIACAP (NIST SP 800.53)	FISMA Self-Assessment (NIST SP 800.53)	DFAS Blue Book 7900.4-M
1.3.2	Prepare Internal Controls Assessment	Prepare internal control assessment document for entity level controls and each assessable unit, summarizing control activities appropriately designed and in place.	Financial Reporting Objectives and Control Activities	✓	P	P	P	P
			Test Plans	✓	P	P	P	P
1.3.3	Execute Tests of Controls	Develop test plans and execute tests to assess the operating effectiveness of control activities for entity level controls and assessable unit level control activities.	Test Plans	✓	P	P	P	P
1.3.4	Summarize Test Results	Update control assessments with the results of tests of control activities.	Test Results	✓	P	P	P	P
1.3.5	Identify, Evaluate & Classify Deficiencies	Determine if exceptions should be considered deficiencies in the design or operating effectiveness of control activities. Evaluate and classify deficiencies in control activities as a control deficiency, significant deficiency or material weakness.	Updated Control Assessments	✓	P	P	P	P
1.3.6	Submit Annual ICOFR SOA & Material Weakness CAP Summary	Submit annual ICOFR SOA memorandum and material weakness summary corrective action plans.	Annual ICOFR SOA Memorandum and Material Weakness CAP Summary	✓	P	P	P	P
2.1	**Design Audit Ready Environment**							
2.1.1	Mitigate Deficiencies in Control Activities	Define requirements and design solutions to mitigate control activities, processes and/or systems and policies.	"To-Be" Process Flows and Narratives, CONOPS, Systems Requirements, and Policies and Procedures	✓	P	P	P	P
2.1.2	Mitigate Deficiencies in Supporting Documentation	Define requirements and design solutions to mitigate deficiencies in supporting documentation.	Solution Document That Summarizes How Documentation Deficiencies Will Be Resolved Or Overcome	✓	P	P	P	P

FIAR Methodology Crosswalk to Systems Compliance Requirements								
FIAR Methodology				Systems Compliance Requirements				
Task No.[1]	Key Task	Detailed Activities	Resulting Work Product	OMB Circular No. A-123, Appendix A	FMFIA, FFMIA, and DoD MICP Procedures (DoD Instruction 5010.40)	DIACAP (NIST SP 800.53)	FISMA Self-Assessment (NIST SP 800.53)	DFAS Blue Book 7900.4-M
2.2	**Develop Corrective Actions**							
2.2.1	Develop Plan and Update FIP	Develop corrective actions, or update existing corrective actions, in reporting entity FIPs that will execute the "to-be" solution.	Updated "Corrective Action" Section of FIP	✓	P	P	P	P
2.4	**Execute**	Execute systems, process, controls and documentation changes included in Corrective Action Plans.	Updated FIPs	✓	P	P	P	P
			Notification to FIAR Directorate of Corrective Action Plan Implementation	✓	P	P	P	P
3.4	**Address Deficiencies**	Evaluate deficiencies, implement corrective actions and verify implementation.	Updated FIPs	✓	P	P	P	P
4.1	**Additional Documenta-tion Review**	Submit additional documentation demonstrating that deficiencies have been successfully remediated.	Documentation Demonstrating Remediation of Deficiencies	✓	P	P	P	P

✓= FIAR Methodology Fully Satisfies Applicable Systems Compliance Requirements
P = FIAR Methodology Partially Satisfies Applicable Systems Compliance Requirements

[1] This crosswalk does not contain the complete listing of tasks from the FIAR Methodology. It only displays key tasks and detailed activities from the FIAR Methodology that have implications for systems compliance requirements.

Figure 19. FIAR Methodology Crosswalk to Systems Compliance Requirements

3.A.7 Detailed Activities

Key tasks are essential to accomplishing each of the five phases of the Methodology. The Methodology provides guidance to the reporting entities on the detailed activities that should be performed within key tasks that result in outcomes and work products that are essential to achieve audit readiness.

As the reporting entities prepare and execute their FIPs to accomplish the OUSD(C) priorities for budgetary and mission critical asset information, these detailed activities should be reflected in their FIPs as key tasks within the appropriate phase. See the Tools, Templates & Work Products section of the FIAR Guidance website for examples of required work products (described in **Figures 20 – 33 below**) necessary to achieving auditability and reliable financial information for the Department.

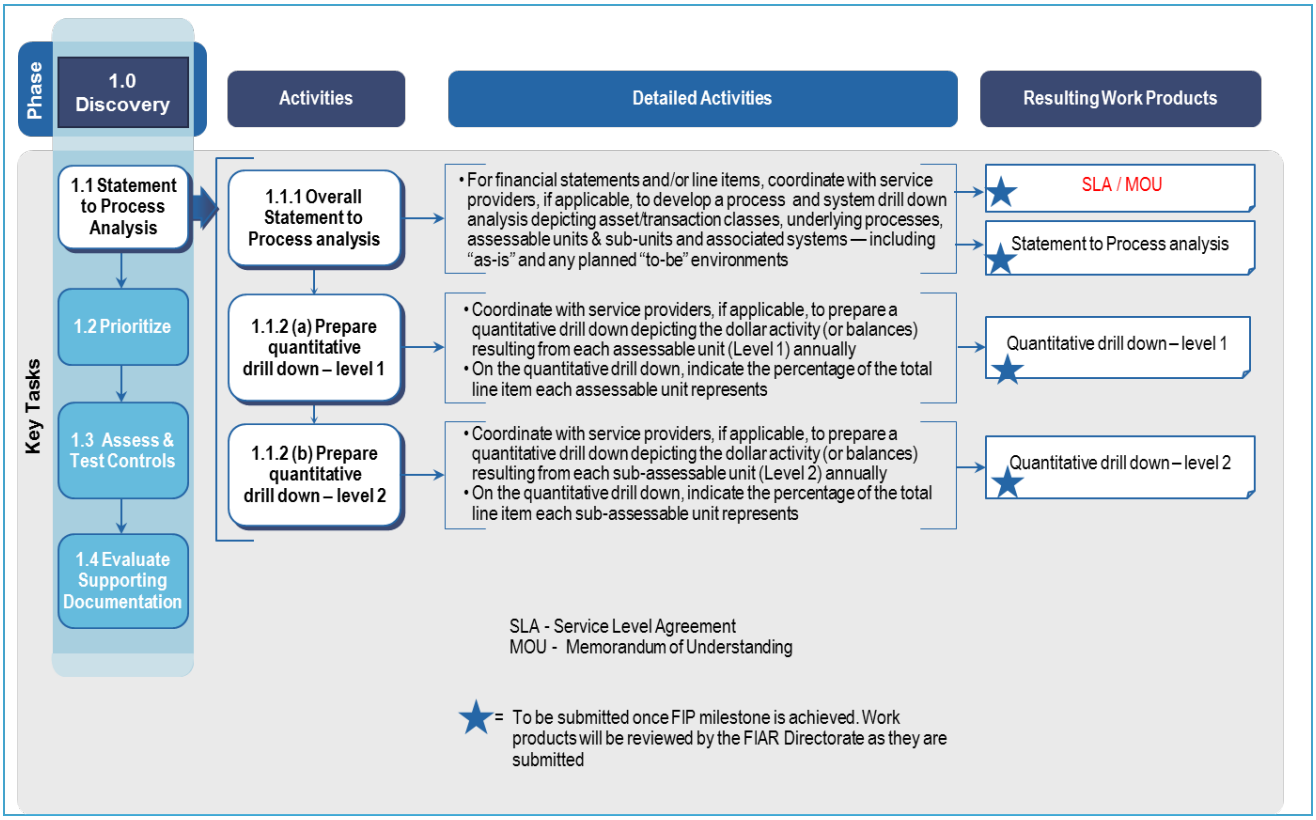

Figure 20. Discovery Phase – Statement to Process Analysis

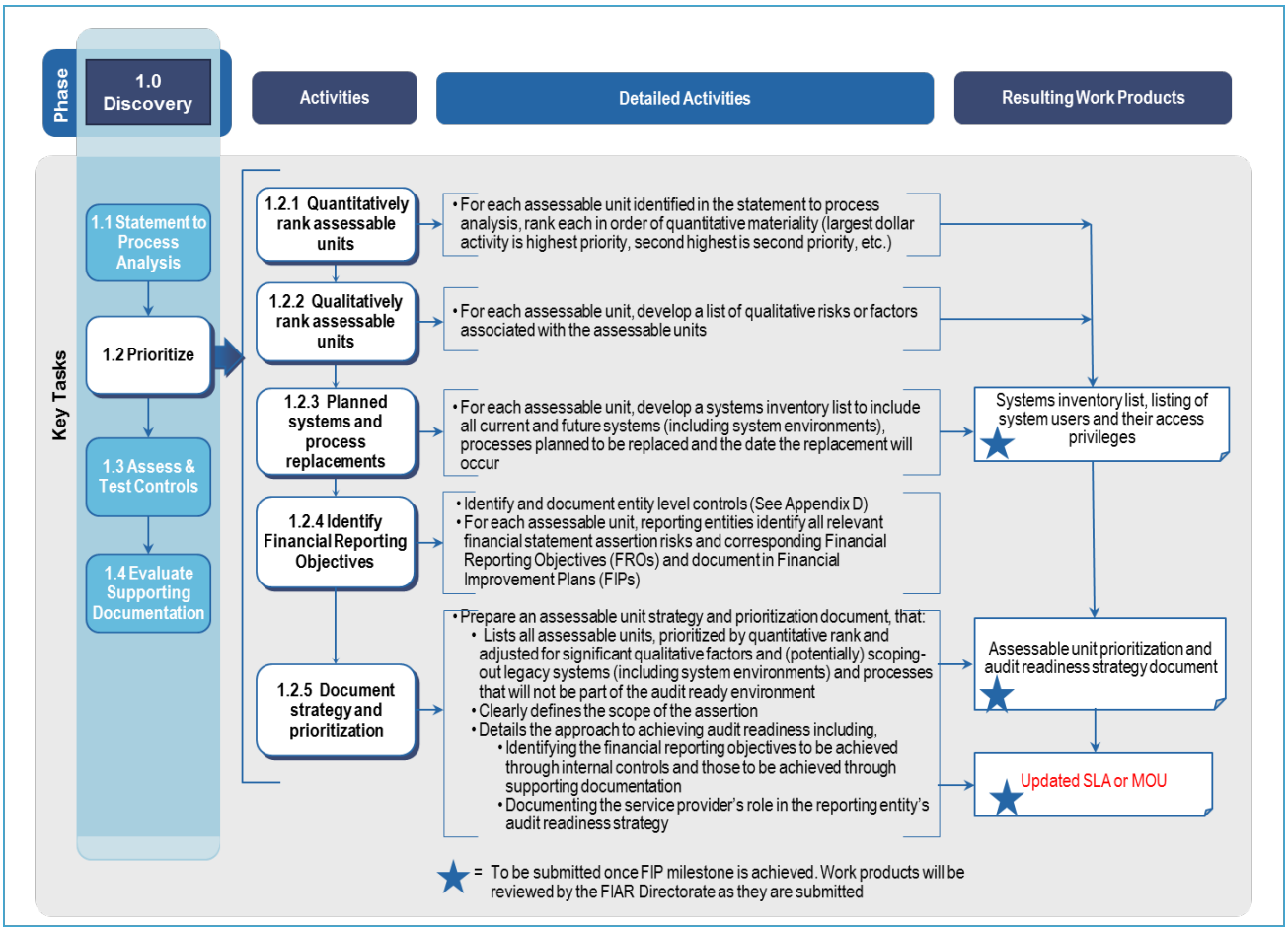

Figure 21. Discovery Phase – Prioritize

Reporting entities will be required to prepare and submit an assessable unit prioritization and audit readiness strategy document that clearly defines the scope of their audit readiness assertion.

When defining the scope, reporting entities must:

- Provide an overall summary of the assertion
- Identify the "in-scope" processes and manual controls
- Identify the "in-scope" IT Applications, Micro-Applications and associated IT General and Application controls
- Identify the key supporting documents (KSDs) included in the assertion
- Identify the role of the service providers (including discussion of relevant SSAE No. 16 reports and self-review efforts)
- Identify any exclusions (processes, controls, systems) from the scope of the assertion

By clearly defining the scope of the audit readiness assertions, reporting entities will help facilitate a more effective review of the assertion documentation by the FIAR Directorate.

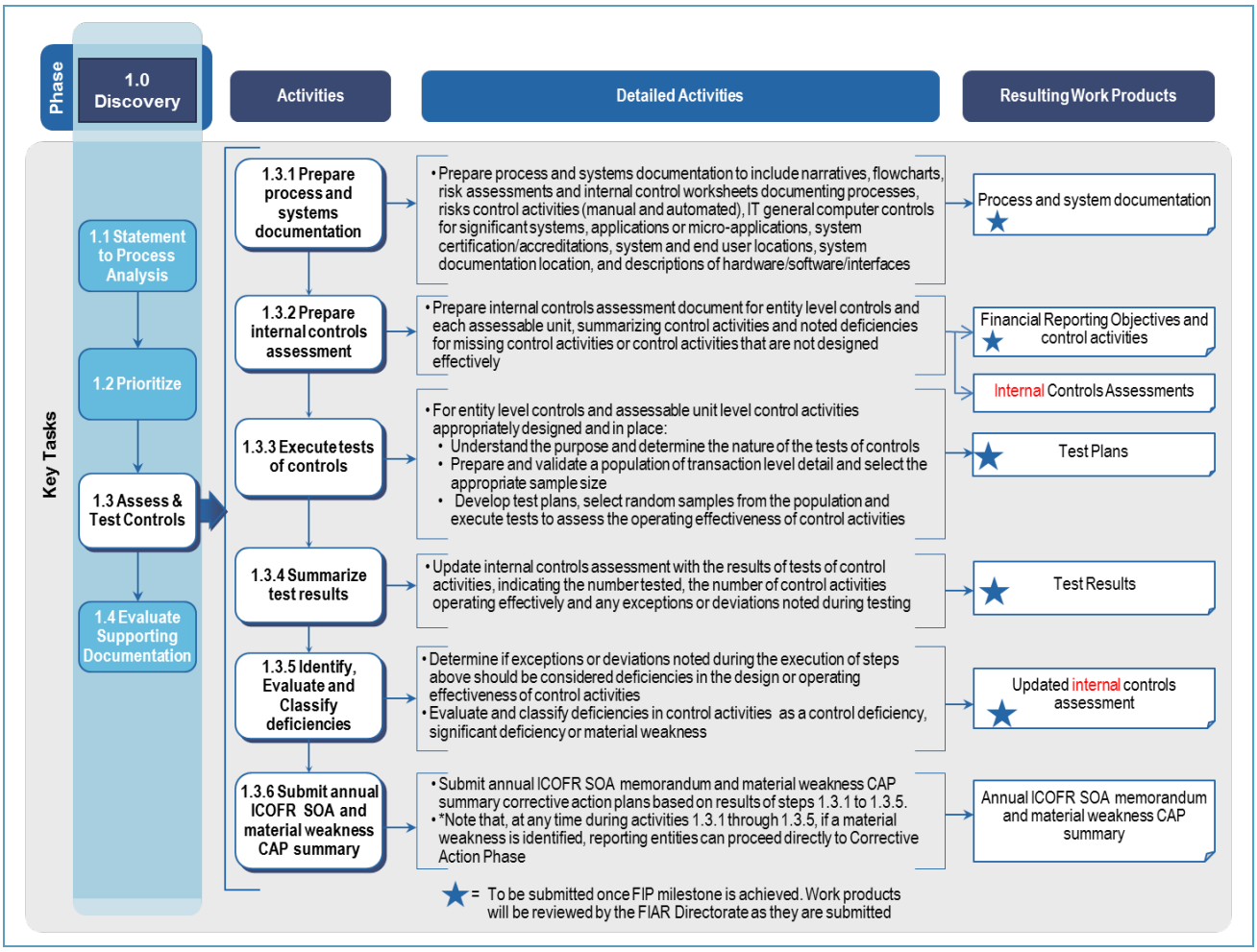

Figure 22. Discovery Phase – Test Controls and Develop ICOFR Statement of Assurance

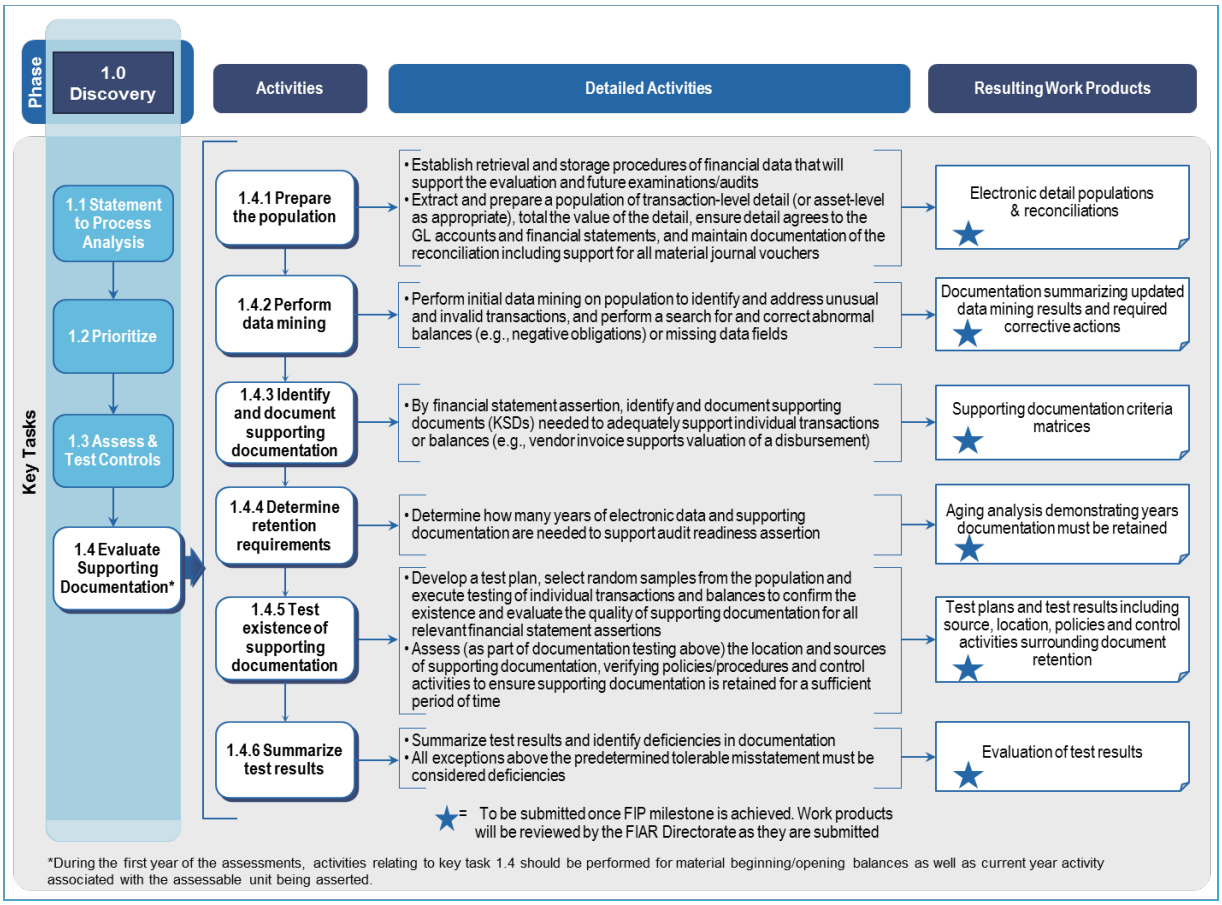

Figure 23. Discovery Phase – Evaluate Supporting Documentation

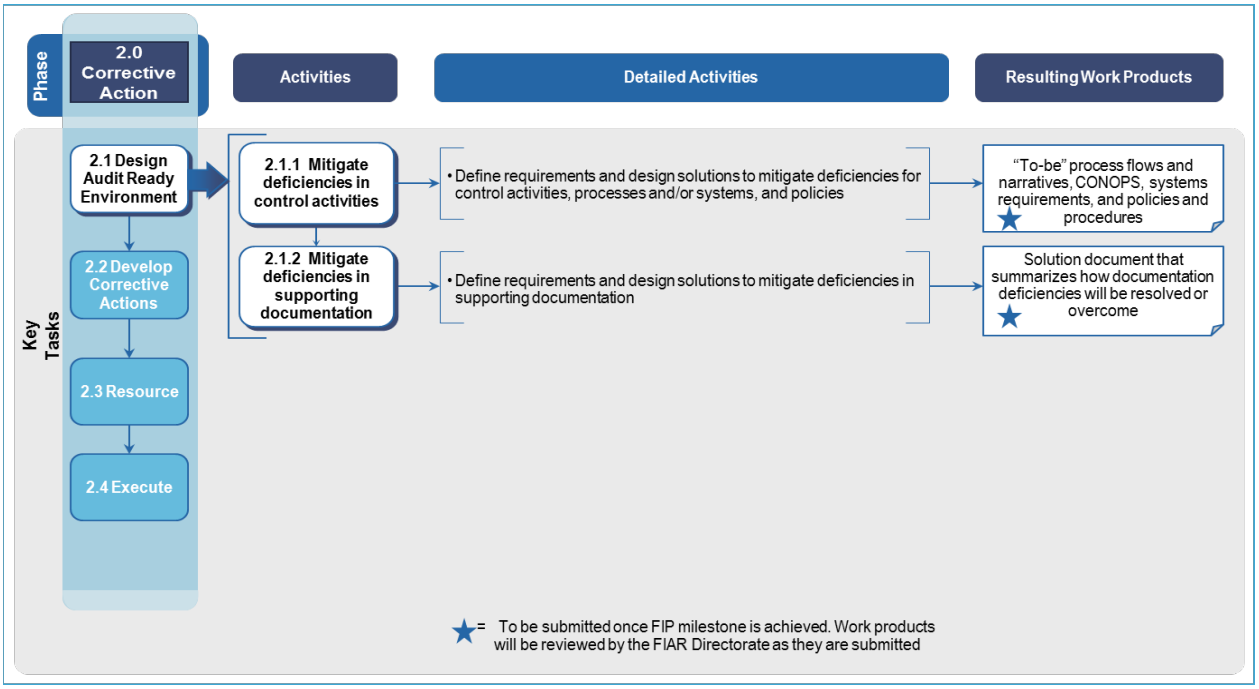

Figure 24. Corrective Action Phase – Design Audit Ready Environment

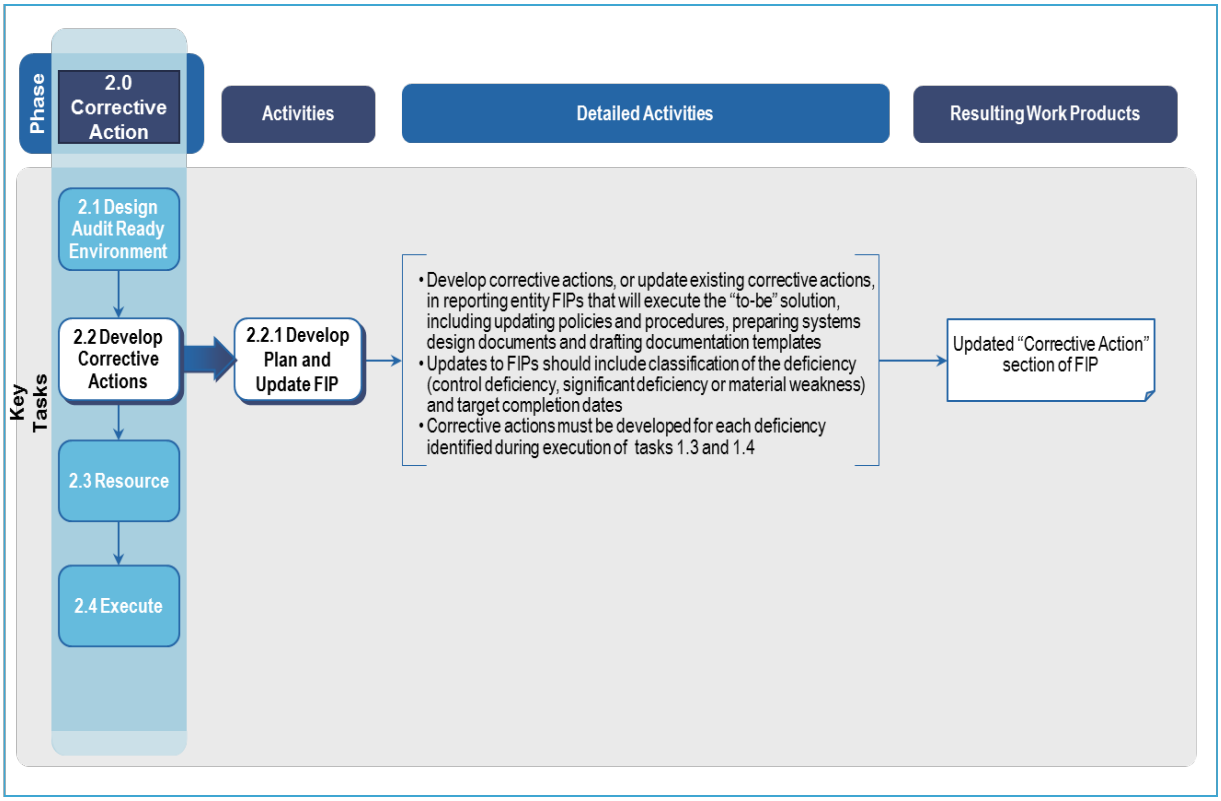

Figure 25. Corrective Action Phase – Develop Corrective Actions

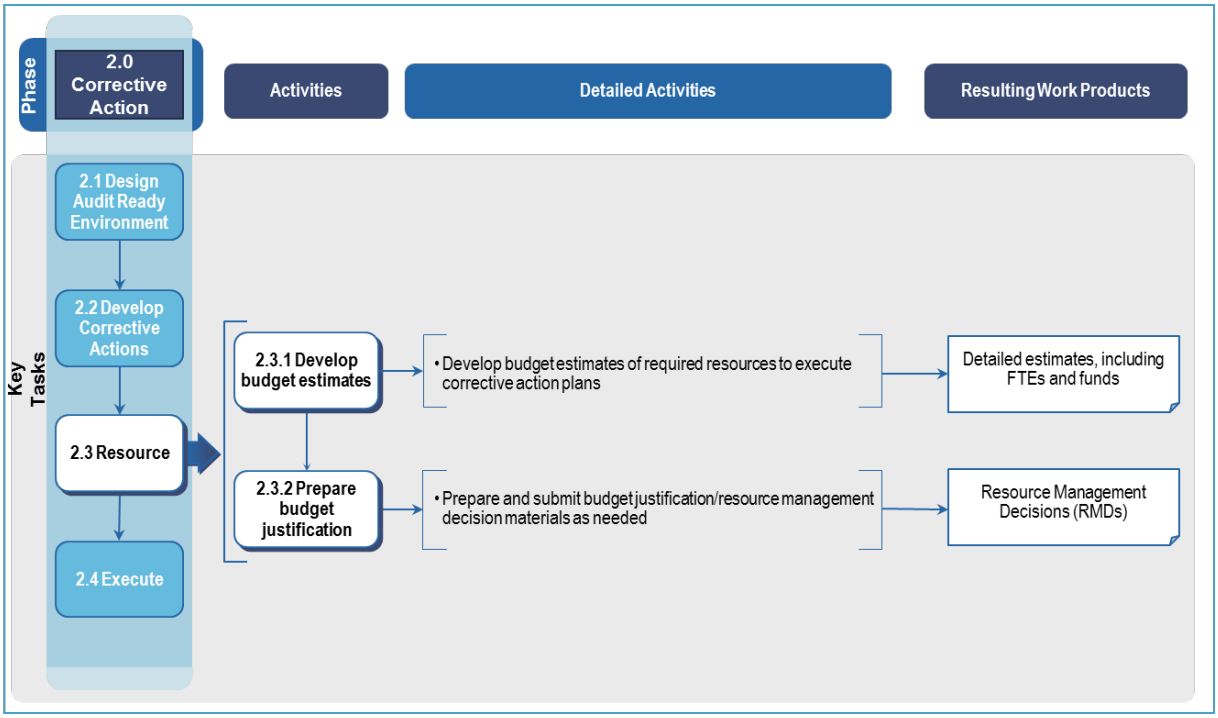

Figure 26. Corrective Action Phase – Resource

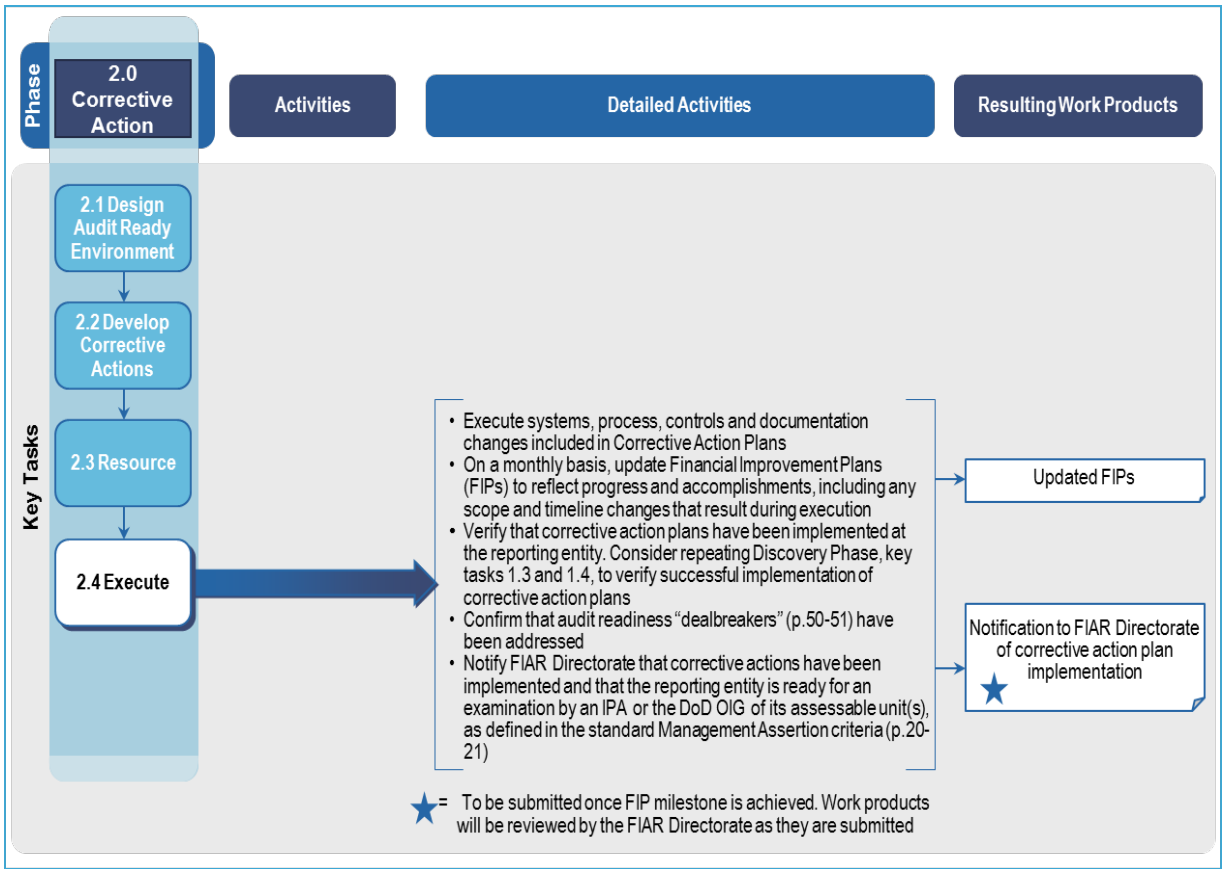

Figure 27. Corrective Action Phase – Execute

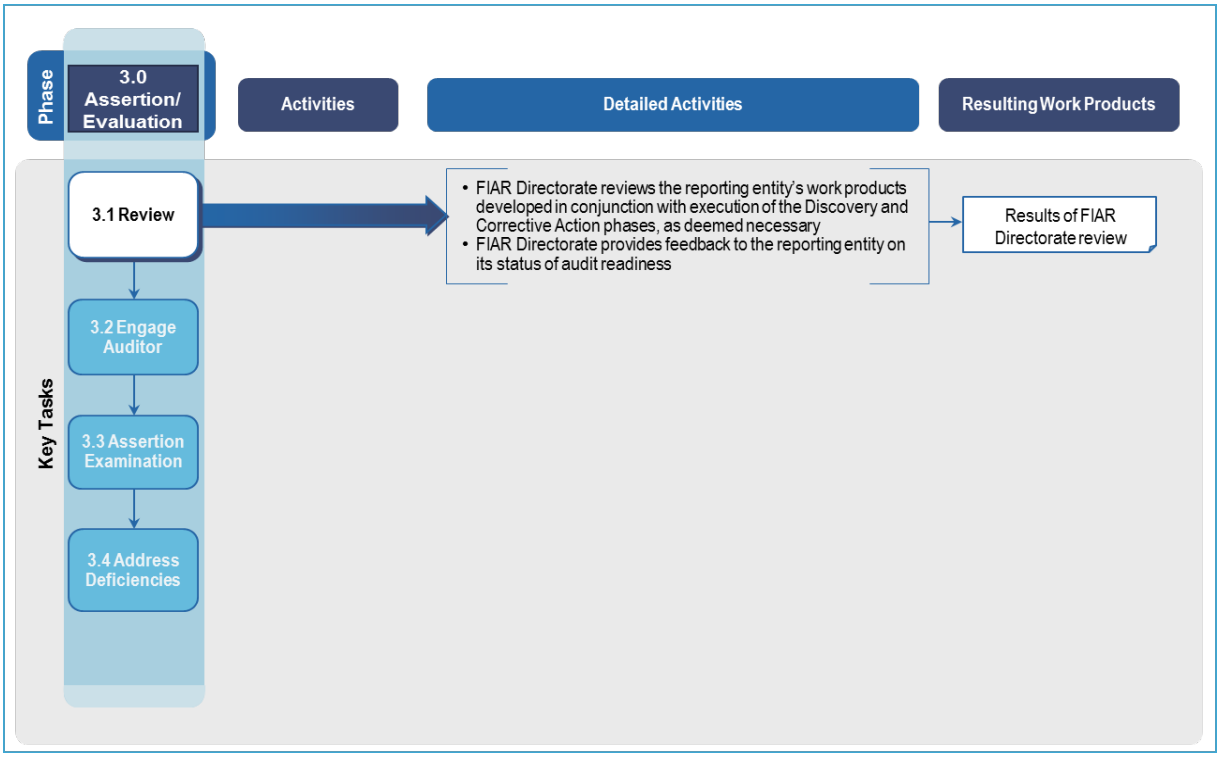

Figure 28. Assertion/Evaluation Phase – Review and Concurrence

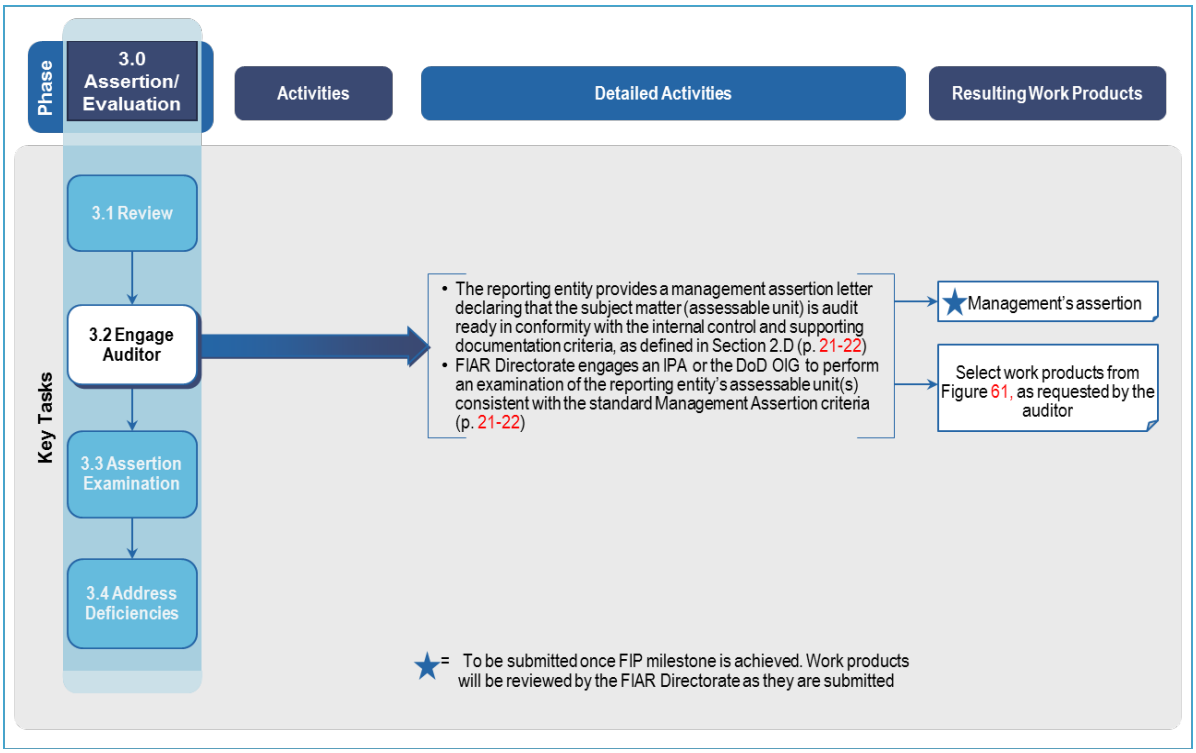

Figure 29. Assertion/Evaluation Phase – Engage Auditor

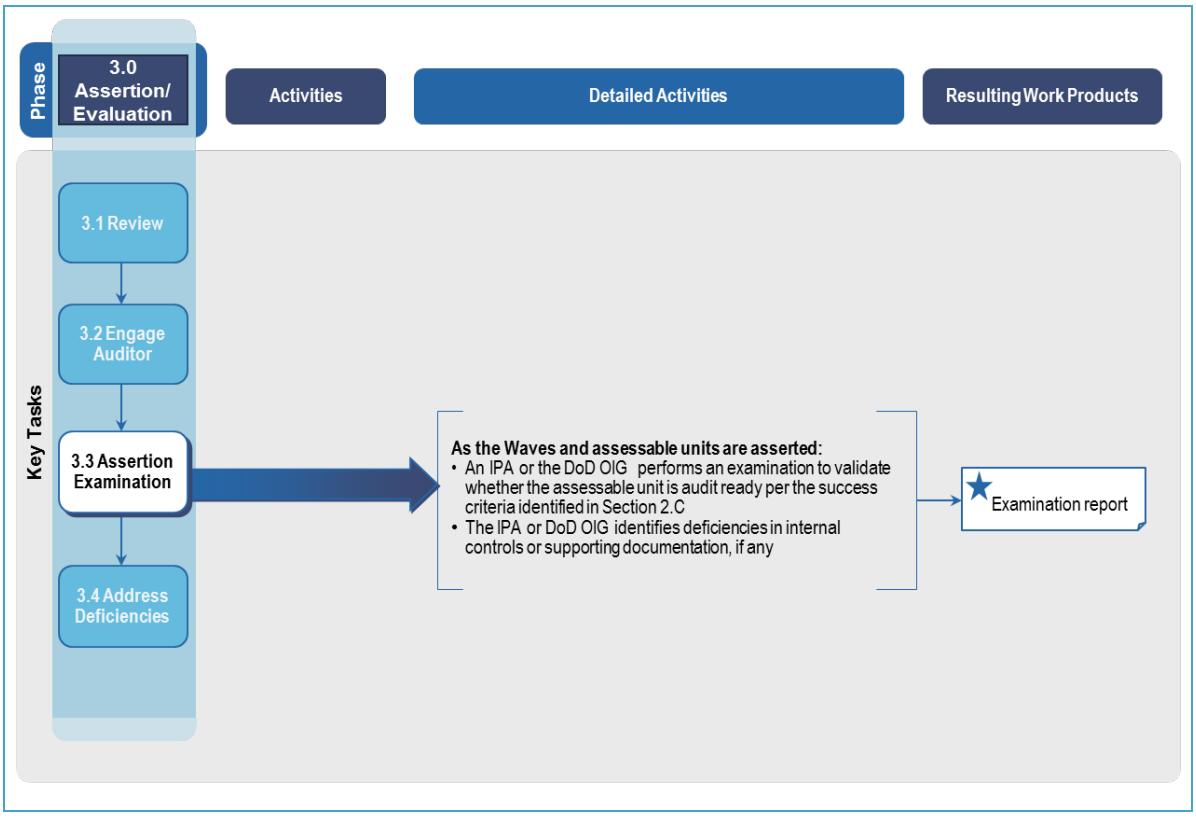

Figure 30. Assertion/Evaluation Phase – Assertion Examination

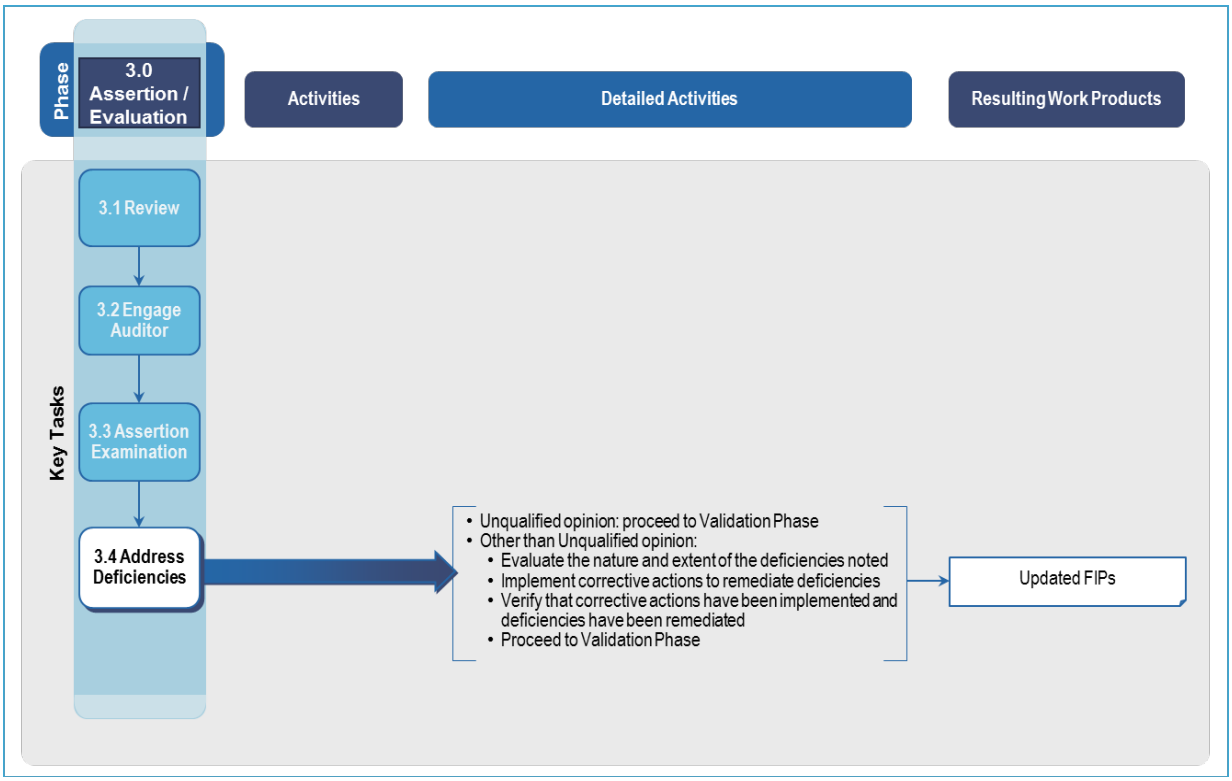

Figure 31. Assertion/Evaluation Phase – Address Deficiencies

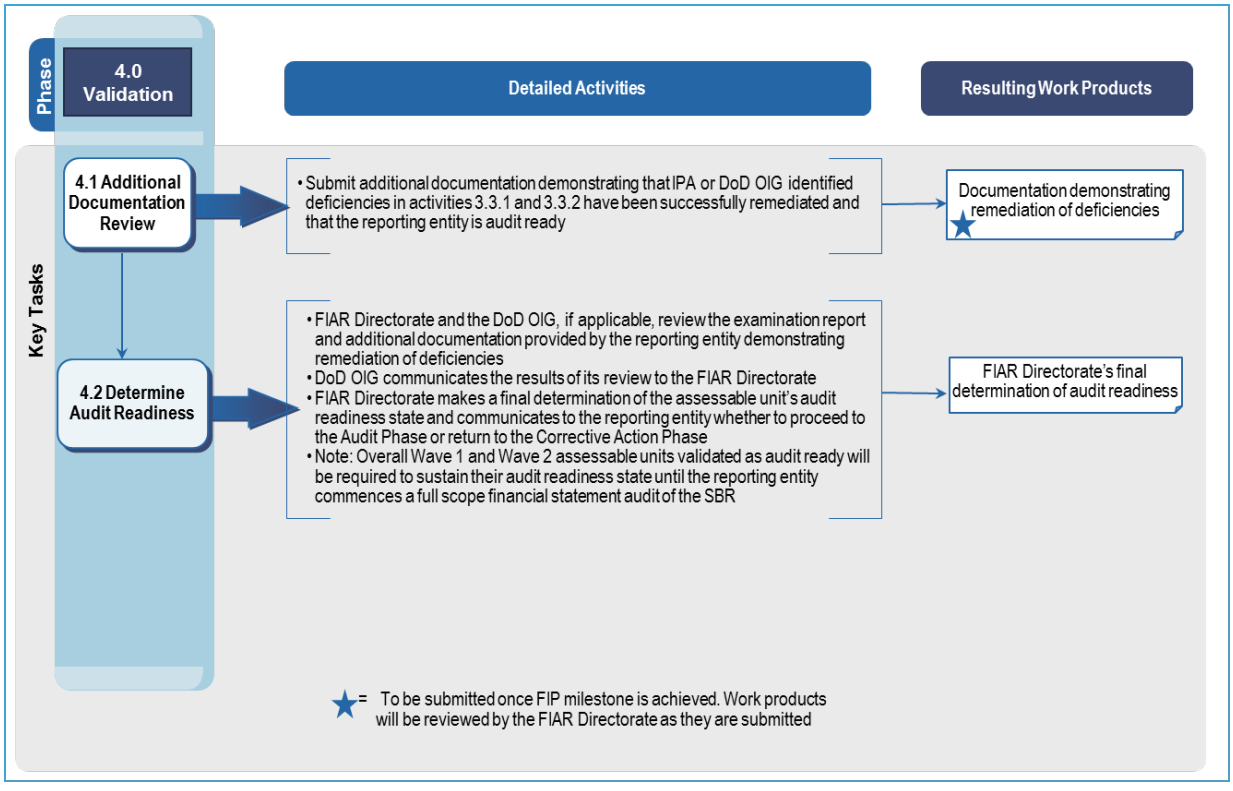

Figure 32. Validation Phase

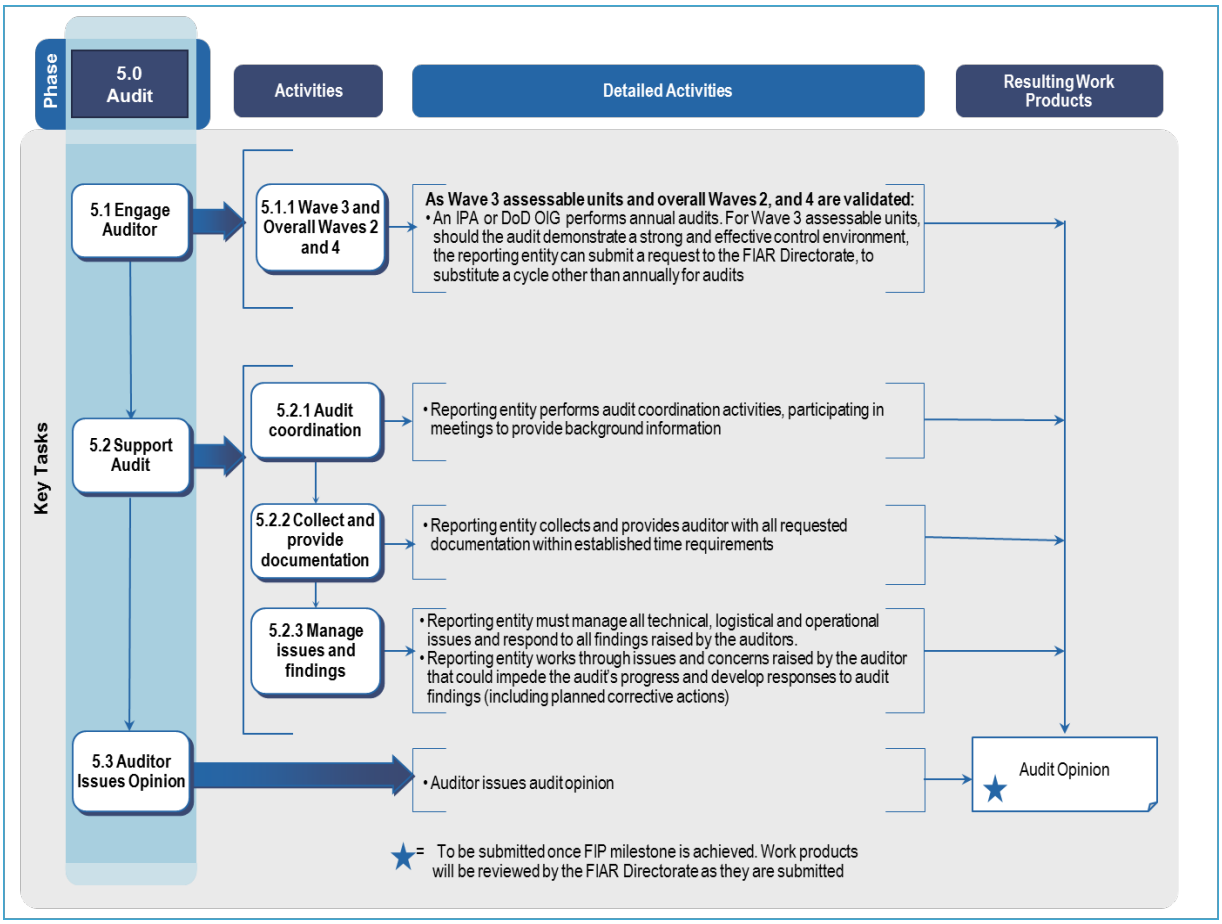

Figure 33. Audit Phase

3.A.8 Capabilities

Generally Accepted Government Auditing Standards (GAGAS) require auditors to collect evidence supporting the fair presentation of financial statement amounts by focusing on two primary areas: internal controls and supporting documentation. Therefore, to achieve audit readiness reporting entities must:

- **Limit the risk of material misstatements by identifying and implementing a combination of control activities and supporting documentation to demonstrate that the FROs, relevant to the subject matter, assertion or process, have been achieved; and**
- **Be able to support account transactions and balances with sufficient, relevant and accurate audit evidence, defined as KSDs in Appendix C, supplemented by the reporting entity's own documentation requirements.**

To maximize the efficiency and effectiveness of audit readiness efforts, the Department has identified relevant financial statement risks, FROs and KSDs required to substantiate financial transactions and balances for each of the four prioritized waves. For a full discussion of these requirements, see **Appendix C**.

Financial Reporting Objectives

FROs are the outcomes needed to achieve proper financial reporting and serve as a point of reference to evaluate the effectiveness of control activities, and the accuracy and sufficiency of documentation supporting transactions and account balances. Reporting entities and service providers must include and address all FROs in their FIPs by focusing on:

INTERNAL CONTROLS

Effective internal controls mitigate risks and provide assurance that financial information is properly and accurately recorded and reported. They are critical to successful financial statement audits. Effective internal controls ensure that:

- Key risks are mitigated; and
- Financial statement assertions are achieved.

During the *Discovery Phase*, identifying and assessing the design and operational effectiveness of internal controls is necessary to understand and evaluate the effectiveness of operational business processes. Internal controls must be documented and the documentation must be readily available to evidence execution of the control activity. The documentation should be properly managed and maintained. The *Discovery Phase* includes assessments to identify inherent risks[9] and testing control activities to identify weaknesses. CAPs are developed and implemented to remediate noted weaknesses, and additional procedures are performed (i.e., repetition of key tasks 1.3 and 1.4) to verify successful implementation of corrective actions.

Reporting entities must indicate whether they have assessed control activities that meet FROs, and whether the control activities are effective. If they are not effective, then specific corrective action and validation tasks must be included in the reporting entity's FIP and linked to the appropriate FRO. By embedding the FROs in the FIPs and linking corrective actions to them, the Department is better assured that financial reporting deficiencies will be identified and resolved. Additionally, progress toward achieving reliable financial information and auditability can be better monitored, managed, and measured.

[9] The GAO/PCIE *Financial Audit Manual*, Section 260: Identify Risk Factors, Paragraph .02, defines inherent risk as "the susceptibility of a relevant assertion to a misstatement that could be material, either individually or when aggregated with other misstatements, assuming that there are no related controls."

SUPPORTING DOCUMENTATION

Reporting entities must identify and retain sufficient and accurate documentation to support individual financial transactions and accounting events prior to asserting audit readiness for each of the four waves (i.e., Appropriations Received, SBR Audit, Mission Critical Asset Existence and Completeness (E&C) and Full Financial Statement Audit) of the FIAR strategy. Assessing the sufficiency and accuracy of supporting documentation is an essential FIP task and is a critical audit requirement for SBR and E&C audit readiness assertions. In fact, the Government Accountability Office/President's Council on Integrity and Sufficiency Financial Audit Manual (GAO/PCIE FAM) states that organizations must retain documentation to support:

1. **Balances reported in the financial statements;**
2. **Systems of internal control;**
3. **Substantial compliance of the financial management systems with FFMIA requirements;**
4. **Substantial compliance of internal controls with FMFIA requirements;**
5. **Compliance with laws and regulations; and**
6. **Required supplementary information (RSI) including any stewardship information (RSSI).**

The GAO/PCIE FAM also states that auditors performing financial statement audits must obtain sufficient evidential matter to form an opinion on an organization's financial statements.[10]

Auditors must adhere to professional standards, which have been codified as the Clarified Auditing Standards (AU-C). AU-C Section 500, *Audit Evidence*, discusses the auditor's responsibility to obtain sufficient, appropriate evidential matter from management and other sources. **Appendix C** provides the KSD requirements for each prioritized wave of the FIAR Strategy.

Audit Readiness "Dealbreakers"

Drawing on lessons learned from past audit readiness efforts, the FIAR Directorate has compiled a list of dealbreakers that have prevented reporting entities from demonstrating audit readiness or succeeding in audits. **Figure 34** lists the most common dealbreakers and links each back to the detailed activities within the phases of the FIAR Methodology. During the Assertion/Evaluation phase, the FIAR Directorate will provide feedback to the reporting entity as to whether they have successfully addressed the dealbreakers and recommend additional procedures to make improvements prior to an examination.

Dealbreakers	FIAR Guidance Reference
1. The general ledger does not reconcile to transaction detail, including support for all material journal vouchers related to the assessable unit.	**Figure 23**, Discovery Phase, Task 1.4 Evaluate Supporting Documentation, Activity 1.4.1 Prepare the population
2. Testing of transaction samples back to source documents that:	**Figure 23**, Discovery Phase, Task 1.4 Evaluate Supporting Documentation, Activity 1.4.5 Test existence of supporting documentation
a. Do not cover all material transaction types, sub-processes, and locations; b. Are not extensive enough to draw conclusions consistent with the effectiveness of controls. Specifically, if controls are ineffective, sufficient substantive testing (i.e., test of details performed through statistical or valid non-statistical sampling, or substantive analytical procedures) must be performed that would reduce the risk of material misstatements to an acceptable level, resulting in evidence that the balances are fairly stated.	**Appendix D**, Section D.3, Test Existence of Supporting Documentation Section 3.C. Preparing for an Audit Sub-section 3.C.1 Assertion Documentation

[10] Government Auditing Standards (Yellow Book) are the requirements for those performing Federal financial statement audits. The GAO/PCIE FAM is subordinate to the Yellow Book requirements in the event conflicts arise.

Dealbreakers	FIAR Guidance Reference
3. All financial statement assertions and relevant risks are not addressed either through control or substantive testing.	**Figure 21**, Discovery Phase, Task 1.2 Prioritize, Activity 1.2.4 Identify Financial Reporting Objectives **Figure 22**, Discovery Phase, Task 1.3 Assess & Test Controls, Activity 1.3.3 Execute tests of Controls **Figure 23**, Discovery Phase, Task 1.4 Evaluate Supporting Documentation, Activity 1.4.5 Test existence of supporting documentation
4. Reconciliations, transaction populations, and supporting documentation cannot be provided in a timely manner.	Section 3.C. Preparing for an Audit Sub-section 3.C.1 Assertion Documentation
5. Control activities for high transaction volume areas (e.g., supply, contracts, FBWT, Inventory, OM&S, GE, etc.) are not designed and/or operating effectively.	Section 3.C. Preparing for an Audit Sub-section 3.C.1 Assertion Documentation
6. IT general and application controls are not deemed effective and tested for management to rely on automated application controls or system generated reports (i.e., KSDs) from IT systems and/or micro-applications.	Section 3.C. Preparing for an Audit Sub-section 3.C.1 Assertion Documentation
7. Supporting documentation testing (i.e., substantive testing) cannot overcome ineffective or missing ITGC and application controls when transaction evidence is electronic and only maintained within a system or the key supporting evidence is system generated reports.	Section 3.C. Preparing for an Audit Sub-section 3.C.1 Assertion Documentation
8. Service provider processes, risks, and controls are not integrated within the scope of testing if those processes are material to the assessable unit.	Section 3.B FIAR Methodology – Service Provider Sub-section 3.B.4 Methodology - Service Provider
9. Management has not established retrieval and storage procedures for financial data that will support management evaluation and future examinations/audits.	**Figure 23**, Discovery Phase, Task 1.4 Evaluate Supporting Documentation, Activity 1.4.1 Prepare the Population
10. Material Beginning Balances/Opening Balances are not evaluated through appropriate testing.	**Figure 23**, Discovery Phase, Task 1.4 Evaluate Supporting Documentation

Figure 34. Most Common Audit Readiness Dealbreakers

3.A.9 Standard FIP Framework

Recognizing the benefits from a standard FIP framework and content, the FIAR Directorate, working collaboratively with reporting entities, developed a standard framework and template for the FIPs. The framework incorporates the Methodology Phases and FROs, and is compatible with the Department's FIAR Planning Tool (FIAR-PT), which is a web-based software tool that provides DoD-wide access and visibility to the plans in a controlled environment.

Reporting entities and service providers (as necessary) are required by the standard FIP framework to include information that will improve their ability to manage their FIPs and the Department's ability to monitor progress indicators; examples include:

- Task start, finish, and baseline dates;
- Percent complete;
- Primary and secondary financial statement assertions;

- FIAR milestone designations;[11]
- Responsible persons;
- End-to-end process indicators;
- Lead and support organization designations; and
- Resource requirements to include level of effort to complete and level of effort committed.

Reporting entities and service providers must use the standard FIP framework, regardless of their audit ready status (i.e., under audit or preparing for audit). The FIPs are living documents and must be maintained and updated as reporting entities progress through the phases/tasks/activities of the Methodology. Although the sequence of the information included in the standard FIP template may be altered, all required information must be included. FIP dates will be used to update the FIAR Plan Status Report, which serves as the Department's annual Financial Management Improvement Plan, required by Section 1008(a) of the NDAA for FY 2002, to address the issues preventing the reliability of Department financial statements. See FIAR Guidance website for the ***standard FIP template*** and ***FIP Preparation and Submission Instructions*** document.

[11] It should be noted that reporting entities will also be meeting OMB Circular A-123, Appendix A milestones as part of their efforts for meeting the FIAR methodology milestone dates.