



OFFICE OF THE UNDER SECRETARY OF DEFENSE
1100 DEFENSE PENTAGON
WASHINGTON, DC 20301-1100

COMPTROLLER

AUG 22 2008

MEMORANDUM FOR SEE DISTRIBUTION

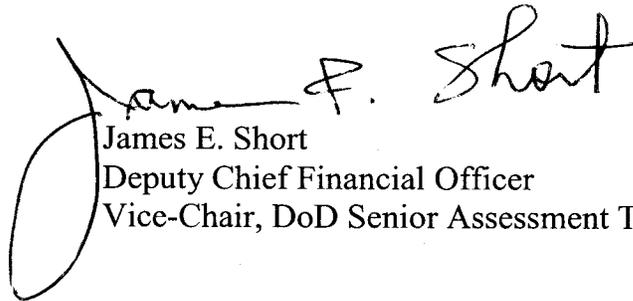
SUBJECT: Fiscal Year (FY) 2009 Guidance for Implementing Office of Management and Budget (OMB) Circular A-123, Appendix A: Internal Controls over Financial Reporting (ICOFR)

Each year specified Department of Defense (DoD) components must submit, as part of their annual Statement of Assurance (SOA), assertions on the effectiveness of their internal controls over financial reporting. To support their ICOR SOA, the components must perform Appendix A procedures in accordance with OMB and as prescribed by DoD.

Attached is the DoD FY 2009 annual guidance for implementing the Appendix A process. The guidance and interactive, standardized forms are also available on the Comptroller's public website:

http://www.defenselink.mil/comptroller/micp_OneProgram_TwoProcesses.html

For more information, contact Mrs. Kathy Hammer, DoD ICOFR Program Manager. Mrs. Hammer can be reached by email at Kathy.Hammer@osd.mil or commercial 703-602-0300 x 132, DSN 327-0300 x 132.

A handwritten signature in black ink that reads "James E. Short". The signature is written in a cursive style with a large, looped initial "J".

James E. Short
Deputy Chief Financial Officer
Vice-Chair, DoD Senior Assessment Team

Attachments:
As Stated

DISTRIBUTION: SECRETARIES OF MILITARY DEPARTMENTS
UNDER SECRETARY OF DEFENSE (ACQUISITION, TECHNOLOGY,
AND LOGISTICS)
UNDER SECRETARY OF DEFENSE (PERSONNEL AND READINESS)
ASSISTANT SECRETARY OF DEFENSE (HEALTH AFFAIRS)
COMMANDER, UNITED STATES ARMY CORPS OF ENGINEERS
COMMANDER, UNITED STATES SPECIAL OPERATIONS
COMMAND
DIRECTOR, NATIONAL SECURITY AGENCY
DIRECTOR, DEFENSE ADVANCED RESEARCH PROJECTS
AGENCY
DIRECTOR, DEFENSE THREAT REDUCTION AGENCY
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE INTELLIGENCE AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY
DIRECTOR, DEFENSE CONTRACT AUDIT AGENCY
DIRECTOR, DEFENSE SECURITY SERVICE
DIRECTOR, NATIONAL GEOSPATIAL INTELLIGENCE AGENCY
DIRECTOR, MISSILE DEFENSE AGENCY
DIRECTOR, DEFENSE COMMISSARY AGENCY
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, CHEMICAL AND BIOLOGICAL DEFENSE PROGRAM



GUIDANCE FOR THE INTERNAL CONTROLS OVER
FINANCIAL REPORTING AS REQUIRED BY THE
OFFICE OF MANAGEMENT AND BUDGET A-123,
APPENDIX A

FISCAL YEAR 2009

JULY 1, 2008 –JUNE 30, 2009

Table of Contents

1.0 PURPOSE	3
1.1 ROLES AND RESPONSIBILITIES	4
1.2 DEPENDENCIES	6
2.0 INTERNAL CONTROLS AND THE STATEMENT OF ASSURANCE	7
2.1 ICOFR Reporting Process	10
2.1.1 Establishing a Senior Assessment Team	11
2.1.2 Identifying Key Business and Financial Reporting Processes	12
2.1.3 Preparing Narratives and Process Flow Charts (Deliverable A)	13
2.1.4 Steps for Developing Process Flow Charts	13
2.1.5 Reporting Weakness Dependencies (Part of Deliverable B)	18
2.1.6 Reporting Material Weaknesses and Preparing Corrective Action Plans	19
2.2 Preparing the Statement of Assurance on Internal Controls over Financial Reporting – Part of Deliverable E	21
3. 0 RISK ASSESSMENT AND TESTING	25
3.1 Suggested Approach to Testing	40
3.2 Evidential Matter	47
3.3 Sufficient Appropriate Audit Evidence	48
3.4 Site Testing	52
4.0 DOCUMENTATION	54
5.0 MONITORING AND SUSTAINMENT	55
6.0 FOCUS AREAS AND DELIVERABLE SCHEDULE	55
ATTACHMENT 1 – Test Plan (Deliverable C)	59
ATTACHMENT 2 – Part of Deliverable B: Chart 1: Risk Analysis Form	61
ATTACHMENT 3 – Risk Analysis Drop Down List Selections	64
ATTACHMENT 4 – Part of Deliverable E – Control Assessment Form with Test Results, Example	69
ATTACHMENT 5 – OUSD(AT&L) Oversight Summary for OMB Circular A-123, Appendix A Deliverables	73
ATTACHMENT 6 - Acronyms	77
ATTACHMENT 7 - References	80

1.0 PURPOSE

This guidance, released by the Department of Defense (DoD) Senior Assessment Team (SAT), provides a framework for assuring proper planning and implementation of Office of Management and Budget (OMB) Circular A-123, Appendix A, and instructions on the preparation of the annual Statement of Assurance (SOA) for Internal Controls Over Financial Reporting (ICOFR).

In December, 2004, the Office of Management and Budget (OMB) issued a revised “Circular A-123, Management’s Responsibility for Internal Controls.” The revision included a new appendix, Appendix A: ICOFR. Appendix A prescribed a method for the Executive Departments to assess, document and report on their internal controls over financial reporting.

Financial reporting is not limited to financial statement reporting. In addition to the financial statements, Appendix A also includes within the definition of “financial reporting” other significant internal and external financial reports that could materially affect spending, budgetary or other financial decisions.

Appendix A prescribes a process for assessing internal controls over financial reporting. The process includes:

- Establishing a high-level governance body such as a SAT,
- Evaluating internal controls at the entity level by understanding management’s attitude, awareness and actions of internal control, to include:
 - Integrity and ethical standards
 - Commitment to competence
 - Management philosophy
 - Organizational structure
 - Assignment of authority and responsibility
- Evaluating internal controls at the process, transaction, or application levels and obtaining knowledge of the organization’s key processes by
 - Performing process risk assessments with regard to financial assertions of completeness, obligations and rights, valuation, existence and occurrence, reporting and presentation, compliance with laws and regulations, and safeguarding of assets from fraud, waste and abuse
 - Identifying existing key controls intended to mitigate identified risk
- Assessing and testing the design and operation of internal controls over financial reporting
- Documenting the entire assessment process from the establishment of a senior assessment team to the identification of deficiencies and development of corrective action plans
- Issuing a SOA on ICOFR as a subset of the Annual Federal Manager’s Financial Integrity Act Statement of Assurance.

1.1 ROLES AND RESPONSIBILITIES

Management is responsible and accountable to develop and maintain effective internal controls over the financial reporting as well as stewardship of Federal resources. The Financial Improvement and Audit Readiness (FIAR) Plan prioritizes the DoD improvement efforts using the following criteria, as decided by the Under Secretary of Defense Comptroller and Chief Financial Officer (USD(C)), the Deputy Chief Financial Officer (DCFO), and the FIAR Committee:

- Impact on DoD financial statements,
- Ability to resolve long-standing problems and material weaknesses,
- Need for focused DoD leadership attention to resolve very complex and potentially long-standing problems,
- Dependency on business transformation initiatives and system solutions, and
- Availability of resources.

The DoD SAT aligns ICOFR focus areas with DoD FIAR priorities. The FY 2009 ICOFR focus areas approved by the DoD SAT on July 22, 2008 are aligned with the top priorities identified.

Senior Assessment Team Responsibilities

DoD Components that prepare financial statements are required to establish a SAT or to use an existing senior-level governance group to monitor the **OMB Circular A-123, Appendix A** implementation process. SATs must be composed of senior leaders who have the responsibility to change policies or procedures when resolving financial reporting weaknesses. The DoD SAT responsibilities are to:

- Identify focus areas of special interest to the Secretary of Defense,
- Determine materiality levels to be used in performing assessments,
- Provide guidance to Defense Components to ensure timely and substantive reports,
- Document the results of assessments of risk and internal controls for each of the focus areas,
- Ensure that sufficient documentation is retained to describe the results of the assessments. This documentation must include at a minimum:
 - a. Organizational charts
 - b. Flow charts with narratives
 - c. Risk analyses
 - d. Control analyses, and
 - e. Report results
- Determine which identified weaknesses should be reported to OMB in the assurance statement, and
- Monitor the corrective action plans of the Components which identified the weakness(es).

To lead by example, the Deputy Secretary of Defense established a SAT composed of senior leaders as a governance body for OMB Circular A-123, Appendix A implementation. The team is chaired by the Principal Deputy Under Secretary of Defense (Comptroller) and the vice-chair is the Deputy Chief Financial Officer. Other members include:

- Principal Deputy Under Secretary of Defense (Acquisition, Technology and Logistics)
- Principal Deputy Under Secretary of Defense (Policy)
- Principal Deputy Under Secretary of Defense (Personnel and Readiness)
- Deputy Under Secretary of Defense (Intelligence)
- Principal Deputy Assistant Secretary of Defense (Health Affairs)
- Principal Deputy Assistant Secretary of Defense (Network Information and Integration)
- Director of Administration and Management
- Assistant Secretary of the Army for Financial Management
- Assistant Secretary of the Navy for Financial Management
- Assistant Secretary of the Air Force for Financial Management
- Deputy Inspector General, for advisory purposes

Financial Improvement and Audit Readiness Directorate (FIAR)

Established by OUSD(C), the FIAR Directorate program office manages the FIAR Plan and ensures that DoD-wide financial improvement efforts continue to mature and are integrated with transformation activities across the Department. The FIAR Directorate, which reports to the Deputy Chief Financial Officer, organizes and convenes cross-Component financial improvement planning workshops, manages the audit readiness process, semi-annually publishes the FIAR Plan and maintains the FIAR Planning Tool.

DoD Components

The Component management is responsible for:

- Implementing this guidance, to include completing all ICOFR deliverables on time,
- Tracking their progress and requirements in their Financial Improvement Plans (FIPs) within the FIAR Planning Tool (PT),
- Submitting A-123 deliverables and integrate across business areas to ensure consistency between A-123 deliverables, FIAR/FIPS and the Enterprise Transition Plan (ETP),
- Identifying FIPs associated with Material Weaknesses in the FIAR-PT for inclusion in the ICOFR SOA,
- Ensuring the FIPs associated with the Material Weakness in the FIAR-PT reconcile with the ICOFR Tabs of the SOA,
- Preparing the Statement of Assurance (SOA) as required by the DoD Instruction 5010.40, “Managers’ Internal Control Program Procedures” and the annual guidance entitled, “FY 2009 Guidance for the Preparation of the Statement of Assurance,” available on the web: http://www.defenselink.mil/comptroller/micp_guidance.html,
- Responding effectively and timely to auditor requests during audits or examinations of financial information by implementing corrective actions based on auditors findings and acting on recommendations. Response times for correcting deficiencies may vary depending on the complexity of the corrective action and the risk of inaction.
- Correcting root causes of the audit or control exceptions, not just treating the exceptions themselves.

Process and Control Owners

The DoD employees must ensure that DoD programs operate and DoD resources are used efficiently and effectively to achieve desired objectives. Programs must operate and resources must be consistent with the missions, in compliance with laws and regulations, and with minimal potential for waste, fraud and mismanagement. Process owners must self-assess the controls for which they are responsible and communicate results to management.

Independent Auditor

Independent Public Audit (IPA) firms may be contracted by a Component or DoD Inspector General (DoD IG) to perform a review of internal controls over financial reporting. As a rule, external auditors review the internal controls including general and application controls affecting the recording and safeguarding of assets and the integrity of controls over financial statement preparation and reporting. The extent of the external audit work, including work related to information systems will be clearly defined in the statement of work when contracting with an IPA and in an engagement letter.

Financial Improvement Plans

The FIAR Plan reflects integrated and interdependent financial improvement solutions using high level Key Milestone Plans (KMPs) supported by detailed project plans known as FIPs. The Component FIPs detail corrective actions to accomplish the key milestones reported in the FIAR Plan. Additionally, system solutions and modifications being managed under the ETP are linked interdependently to the FIAR key milestones.

The Components have developed FIPs, which are specific to their processes, business practices, limitations, and approach. Each KMP in the FIAR Plan has correlating and sequential tasks in the FIPs. Therefore, achieving KMP outcomes depends on the Components: 1) maintaining robust and all encompassing FIPs and 2) successfully completing every relevant task established in the FIPs. The FIPs include corrective action plans for correcting material weaknesses. The FIPs associated with corrective action plans are identified as ICOFR in the FIAR-PT and are used to populate the ICOFR tabs of the Annual SOA. The dates in the FIAR-PT should be consistent with the dates certified in the ICOFR SOA.

1.2 DEPENDENCIES

Systems. In cases where the resolution of financial and management deficiencies are dependent upon information technology solutions, specific tasks related to Enterprise Resource Planning (ERP) system implementations should be addressed in each Component's FIPs. Improving financial information, eliminating material weaknesses and successfully achieving clean opinions on financial statement audits for the Military Services and Agencies in many cases depends upon the successful implementation of the ERPs.

Service Providers. A service organization (provider) is an entity that provides services to another organization. Entities must develop a comprehensive inventory of their service providers and determine the impact on the entity's system of internal controls related to their

own financial reporting. Services provided by a service organization are considered part of the entity's financial information system if they affect any of the following:

- Classes of transactions in operations that are significant to the entity's financial reporting;
- Procedures, either automated or manual, by which the entity's transactions are initiated, recorded, processed and reported in the financial reports;
- Related accounting records, whether electronic or manual, supporting information, and specific accounts in the entity's financial reports involved in initiating, recording, processing and reporting the entity's transactions;
- The method by which an entity's information system captures other events and conditions that are significant to the financial reports; or
- Financial reporting process used to prepare the entity's financial reports, including significant accounting estimates and disclosures.

2.0 INTERNAL CONTROLS AND THE STATEMENT OF ASSURANCE

Who is required to prepare the Statement of Assurance?

The Heads of the DoD Components that prepare stand-alone financial statements, as shown in Table 1 on page 9, are required to prepare a SOA on ICOFR. The ICOFR SOA must be based on an assessment strictly following the requirements of Office of Management and Budget (OMB) Circular A-123, Appendix A; the Chief Financial Officers Council (CFOC) Implementation Guide; and this annual Guidance. The assessments of ICOFR processes may disclose material weaknesses identified in the reliability of financial reporting within the financial reporting process. For discussion on materiality concept please turn to page 29. For instructions on how to prepare the Statement of Assurance and the timelines, refer to the FY 2009 Guidance for the Preparation of the Statement of Assurance, available on the web at: <http://www.defenselink.mil/comptroller/micp/index.html>. The ICOFR Tabs of the SOA are due to the DoD SAT by June 29 and should be provided with deliverable E on table 8, page 59. The tabs should be consistent with the information loaded in the FIAR-PT.

What period of time is covered and when is it due?

The 2009 ICOFR SOA will cover the one year period from 1 July 2008 through 30 June 2009, and be effective as of June 30th of the fiscal year (FY) 2009. Any financial material weaknesses previously reported in the overall FMFIA SOA should not be automatically transferred to the ICOFR SOA. Subject weaknesses may be transferred when test results, performed according to ICOFR requirements and properly documented, disclose the weakness. If a material weakness is expected to be corrected within the 4th Quarter (Qtr) (July – September) of FY 2009 but all actions are not completed as of June 30th, the Component Head should report the material weakness as still ongoing. The Component SAT approved ICOFR tabs of the SOA are due to the DoD SAT by June 29, 2009 as indicated above.

What does each ICOFR SOA consist of?

The ICOFR SOA will be presented in separate paragraph(s) in the same document as the FMFIA Overall Process SOA. For a more comprehensive understanding of the requirements, refer to the FY 2009 Guidance for the Preparation of the Statement of Assurance, available on the web at: <http://www.defenselink.mil/comptroller/micp/index.html>. The Head of the Component will only be required to sign one statement regardless of the number of Financial Statement Reporting Entities (FSREs) for which the Component must provide financial reporting assurance.

A separate paragraph for each statement of assurance over financial reporting will provide the assessment by the Component's senior management as to whether the Component's internal controls over financial reporting are in place, operating effectively, and being used for the financial reporting of each FSRE in accordance with the OMB Circular A-123, "Management's Responsibility for Internal Control, Appendix A."

Component heads will use one of three levels of assurance as discussed below. In some cases, ICOFR assurance may not have the same level of assurance as the FMFIA Overall, e.g., the Component could have an unqualified assurance on the overall and a qualified assurance on the financial reporting for the FSRE. In another example, the Component could have a qualified assurance on the overall and an unqualified assurance for the financial reporting for FSRE #1, but then no assurance on the financial reporting for FSRE #2. Regardless of the number of FSREs, a separate paragraph should cover the assurance level for the financial reporting of each FSRE.

- An **Unqualified Statement of Assurance** (reasonable assurance that internal controls over financial reporting are effective, with no material weaknesses reported). Each unqualified statement shall provide a firm basis for that position, which the Head (or principal deputy) will summarize in the cover memorandum.
- A **Qualified Statement of Assurance** (reasonable assurance that Internal Controls over financial reporting is effective with exception of one or more material weakness(es) noted). The cover memorandum must cite the material weakness(es) in internal control that precludes an unqualified statement.
- A **Statement of No Assurance** (no reasonable assurance because no assessments conducted or the noted material weaknesses are pervasive or have material impact on financial reporting numbers). The Head (or principal deputy) shall provide an extensive rationale for this position. If a statement of no assurance is given, the SOA must still document the known material weaknesses in the required format. Providing "no assurance" does not preclude you from documenting and reporting your corrective action plans.

ICOFR TABs D-1, E-1, F-1, and so on: For each FSRE, provide a list of the titles of all uncorrected and corrected material weaknesses. The numbering of the tabs will begin with TAB D. If the Component has three FSREs and each has material weaknesses that are being reported, TAB D-1 can provide the material weakness information for FSRE #1, TAB E-1 is for FSRE #2, and TAB F-1 is for FSRE #3. Each tab must reflect the name of the FSRE for which it applies.

TABs D-2, E-2, F-2, and so on (Uncorrected Weaknesses): For each FSRE, provide detailed narrative descriptions of all uncorrected material weaknesses including the plans and schedules for the corrective actions.

TABs D-3, E-3, F-3, and so on (Corrected Weaknesses): For each FSRE, provide a brief narrative describing the material weaknesses corrected in the current year, including the most significant actions taken to correct the weakness.

Table 1 describes the FSREs who are to submit, as a subset of the FMFIA Overall Process Statements of Assurance to the Secretary of Defense, the FMFIA Internal Controls over Financial Reporting Statements of Assurance, based on assessments of Internal Controls over financial reporting performed by FSRE management.¹ Beginning in FY 2009, the Department of Defense Inspector General was added as a reporting entity at the request of the DoD SAT. Other Components providing support services for the FSREs may be required to provide ICOFR documents to the DoD SAT of their processes which materially contribute to a FSRE’s financial reporting process.²

Table 1- Financial Statement Reporting Entities

Component	Financial Statement Reporting Entity (FSRE) and Its Parent Component
1. Office of the Secretary of Defense (OSD) (Director of Administration and Management for OSD)	1. Under Secretary of Defense (Comptroller)
	2. Military Retirement Trust Fund (MRTF) General Fund (GF)/ Under Secretary of Defense (Personnel and Readiness (P&R))
	3. Medicare Eligible Retirement Health Care Fund (MERHCF) GF/ Assistant Secretary of Defense (Health Affairs)/ Under Secretary of Defense (P&R)
	4. Defense Health Program (DHP) GF/ Assistant Secretary of Defense (Health Affairs)/ Under Secretary of Defense (P&R) / Service Medical Activity (SMA)
	5. Defense Health Program (DHP) GF/ Assistant Secretary of Defense (Health Affairs)/ Under Secretary of Defense (P&R) / Tricare Management Activity (TMA))
	6. Chemical Biological and Defense Program (CBDP) GF// Under Secretary of Defense (AT&L)
2. Department (Dept.) of the Army	7. Army GF
	8. Army Working Capital Fund (WCF)
	19. United States Army Corps of Engineers (USACE)
3. Dept. of the Navy	10. Navy GF
	11. Navy WCF

¹ The Financial Statement Reporting Entities (FSREs) are the organizations required by either the Office of Management and Budget (OMB) or the Department of Defense to produce stand-alone financial statements for the DoD Components.

² Although AT&L is not a FSRE, they will have oversight of the ICOFR submissions received from the FSREs impacting the weaknesses they own, and will provide input on the ICOFR SOA tabs directly to the DoD SAT instead of through the Director of Administration and Management for OSD.

Component	Financial Statement Reporting Entity (FSRE) and Its Parent Component
	12. Marine Corps GF
4. Dept. of the Air Force	13. Air Force GF
	14. Air Force WCF
5. United States Special Operations Command	15. USSOCOM GF
6. Defense Advanced Research Projects Agency (DARPA)	16. DARPA GF
7. Defense Commissary Agency (DECA)	17. DECA GF
	18. DECA WCF
8. Defense Contract Audit Agency (DCAA)	19. DCAA GF
9. Defense Finance and Accounting Service (DFAS)	20. DFAS GF
	21. DFAS WCF
10. Defense Information Systems Agency (DISA)	22. DISA GF
	23. DISA WCF
11. Defense Intelligence Agency (DIA)	24. DIA
12. Defense Logistics Agency (DLA)	25. DLA GF
	26. DLA WCF
13. Defense Security Service (DSS)	27. DSS GF
14. Defense Threat Reduction Agency (DTRA)	28. DTRA
15. Missile Defense Agency (MDA)	29. MDA
16. National Geospatial-Intelligence Agency (NGA)	30. NGA
17. National Security Agency / Central Security Service (NSA/CSS)	31. NSA/CSS
18. Inspector General, Department of Defense	32. DoDIG

2.1 ICOFR Reporting Process

The process for supporting the SOA on ICOFR must follow strict rules directed by a TOP DOWN focus as described in the Appendix A of the OMB Circular A-123 and the CFOC Implementation Guide for OMB Circular A-123, Appendix A, ICOFR.

The process for preparing the SOA on ICOFR will be conducted in the following manner:

- Establish an Entity Senior Assessment Team (SAT) with appropriate membership and a defined charter of roles and responsibilities,

- Determine the “tone at the top” by identifying the Component’s environmental control document such as a Management Code of Conduct or Ethics Policy,
- For the assigned areas, identify key business processes and prepare process narratives, process flow charts, and organizational charts,
- Perform risk analyses. Obtain Federal Information Security Management Act (FISMA) Report (if applicable),
- Identify internal controls intended to mitigate identified risk, perform preliminary control assessment, and design the test plan to be used to test the control,
- Report Weakness Dependencies in the DoD FIAR web-based tool,
- Create detailed test plans for “Low Risk” controls, or corrective action plans for “High Risk” Controls,
- For Components correcting weaknesses for other Components, develop and enter corrective action plans in the FIP in the FIAR web-base tool,
- Test controls, reassess internal controls based on test results, and complete the control analyses (w/ test results),
- The items tested should be randomly selected (equal opportunity for all items in the universe to be selected) from a universe of transaction level data. This transaction level data should be reconciled to the balance on the financial statement or the balance of the segment being tested or asserted on,
- The testing should also be related to the specific financial statement assertion(s) for the transaction being tested,
- Update specific tasks and expand if necessary a corrective action plan when testing ascertains problems with internal controls,
- Components should demonstrate that they are able to provide specific evidential matter to the auditors in a reasonable amount of time such as 2 working days for most data,
- Enter material weakness corrective action plans into FIP in the DoD FIAR web-based tool,
- Components may enter corrective action plans into FIPs in the DoD FIAR web-based tool for reportable conditions that are not included in the FMFIA report,
- Issue Statement of Assurance on Internal Controls over Financial Reporting.

2.1.1 Establishing a Senior Assessment Team

Each of the FSREs shall establish and maintain a SAT to provide governance over their Appendix A program within the Component. The SAT membership and responsibilities are identified in section 1.1 of this Guidance. Any changes made to the SAT charter must be posted to the FIAR Tool. The SATs will be composed of senior leadership-level representatives, in decision-making capacities, from functional areas representing focus area processes and will be responsible for the preparation of the SOA on ICOFR within the prescribed process. The SATs shall be designated by the head of the Department/Agency and shall oversee the implementation

of Appendix A, OMB Circular A-123. One Component SAT may serve as the SAT for more than one FSRE. For example, one SAT may oversee the Navy General Fund and the Navy Working Capital Fund. It is recommended that at least one member of each SAT be a representative from the Core Business Mission (CBM).

The SAT shall document the results of the assessments of risk and internal controls for all material business processes related to areas where an “X” appears on Table 7 on page 56. The internal controls contained in any material financial or mixed information technology system(s) (e.g., the Defense Property Accountability System (DPAS)) that pertain to any implementation area must also be assessed. This will most likely require coordination with other organizations. Each SAT must ensure that sufficient documentation is retained to explain significant decisions made in identifying material business processes, assessment results, internal control test plans, and the determination of weaknesses to report outside of the entity. Documentation shall also include support for deliverables listed above. Documentation shall be maintained for 3 years and 6 months from the effective date of the ICOFR SOA which is June 30th of the fiscal year. (The document retention period may extend beyond 3 years and 6 months if assessments of material business processes have been delayed).

2.1.2 Identifying Key Business and Financial Reporting Processes

Assessments for the DoD implementation areas must contain a risk analysis of **all material business or process cycles** that affect the particular DoD focus area. To identify the business cycles that impact a focus area, determine what business transactions materially affect related account balances. Ask, “What significantly increases or decreases financial balances in this area?” If DFAS is the organization’s accounting service provider, DFAS may be able to provide assistance in identifying significant types of transactions which represent a material business cycle or segment. Components not having unqualified audit opinions must address material business processes in focus areas assigned in Table 7 on page 56.

Organizations with unqualified audit opinions must assess all **key** business processes for all **material** financial statement lines. The DoD has established its level of materiality as 0.99 percent of adjusted assets for proprietary accounts and 0.99 percent of total budgetary resources for budgetary accounts. Adjusted assets are calculated by subtracting the total intragovernmental assets (as indicated on the balance sheet) from total assets. All financial statement lines equal to or exceeding the organization’s level of materiality must be assessed.

Segments are elements of the financial environment that management will assert as audit ready and are:

- Separately identifiable and measurable (e.g. Civilian Pay, Military Pay, etc.),
- Significant either by dollar value or requires regulatory compliance (e.g. Military Equipment, Environmental Liabilities), and
- Substantially constant from year to year.

FSREs will identify process flows, key controls and related risks, events and transactions by segment and reconcile events and transactions to financial statement lines by segment. Once segments have been identified and corrective actions completed, management will support a

reasonable assurance of audit readiness by documenting the flow of events, transactions, and key internal controls (leverage the processes in OMB Circular A-123, Appendix A), assess risk, and test data integrity.

2.1.3 Preparing Narratives and Process Flow Charts (Deliverable A)

To begin the flowchart process, managers and process owners should describe, in narrative form, the steps in their processes which create or process a financial transaction from an operational event. Components must analyze the processes from the point of origin to the financial report and then from the financial report back to the point of origin in order to capture all transaction types, service providers and sub-allotees, and systems that are elements of the process. Process steps should be numbered.

It is recommended that processes be narrated and a walkthrough of processes be performed prior to being flowcharted. Interviews should be conducted with personnel who have knowledge of the relevant operations to validate that manuals, policies, forms and documents are accurate and being applied.

The narratives should be of sufficient depth to ensure that a reader familiar with ICOFR will understand the process. Transaction cycle flowcharts are not only an efficient way to document the key internal control points in a business process, but they also provide an effective way to confirm the accuracy of the transaction cycle narrative with the process owners, and identify where disparate processes could be standardized.

The following questions may help in preparing the narratives.

1. Does the process narrative have the preparer's name?
2. Are process owners' names evident on the process narrative?
3. Does the narrative clearly indicate the financial statement accounts, notes to the financial statements, and lines impacted by the process including budgetary and revenue accounts?
4. Is the process explained well in the narrative?
5. Does every process identified on the flowchart have an associated description in the narrative?
6. Are the steps in the narrative numbered to facilitate the flowcharting process?
7. Does the narrative indicate what systems are used?
8. Are the accounting entries clearly indicated?

2.1.4 Steps for Developing Process Flow Charts

The narrative and related flowchart must be at a transaction level of detail sufficient for clarification and instructional purposes and represent the types of documents the reporting organization might use for testing and monitoring purposes. Using the process narratives, create a flowchart or charts to depict the end-to-end business process under review. The flowcharts will become a vital part of an assertion package as a segment moves towards audit readiness. Prior to beginning the process for flow charts, it is recommended that the organization review the Business Enterprise Architecture (BEA) and Principal Staff Assistant (PSA) extensions (e.g. Human Resource Management Enterprise Architect) to reuse, as a baseline, any information

already in existence. Even though the BEA is the DoD's transformational "To-Be" architecture, the operational views, in many cases, remain the same, but the solution used to accomplish the mission will change. For example, Defense Integrated Military Human Resource System (DIMHRS) will replace legacy Military Personnel and Pay systems, but the business mission and financial touch point depicted in the architecture remain the same. It is also recommended that flow charts be developed using the current DoD development methodologies and notations when possible to ensure full interoperability with the current architectures used for compliance.

- Process steps should be numbered in the flowcharts and should agree with the numbers assigned in the narratives.
- Documenting the key internal control points in a business process will provide an effective way to confirm the accuracy of the transaction cycle narrative with the process owners, and identify where disparate processes could be standardized.
- The flowcharts of the processes must identify the key business processes. Flowchart descriptions should use verbs inside the symbols; e.g., **approve, support, or validate**. The financial reporting process from beginning to end belongs to the Component certifying its financial statements, whether or not sub-processes are performed by other organizations (which should be identified as a dependency).
- All sub-processes performed by other organizations must be incorporated into the reporting Component's documented processes as shown in the example Exhibit 1 – Process Flow Chart. Where material portions of key processes are performed by organizations other than the reporting Component (a secondary organization), it will be necessary for the reporting Component to obtain from the secondary organization either assertions, process narratives or flowcharts to complete the reporting Component's entire process flowchart.
- It is recommended that assertions be obtained from organizations external to the Department, and that flowcharts and related, subsequent deliverables assessing the flowcharted process controls be obtained from DoD.

The following questions may help in preparing flowcharts.

1. Is there a defined start symbol (or connector from another flowchart)?
2. Does the flowchart have a legend that describes the various shapes in the flowchart?
3. Is each shape in the flowchart appropriate (e.g., database reference shows a database shape)?
4. Where is the action being performed (could be externally, internally, systemic application, database, different dept, etc.)?
5. How is the action being performed? Does the symbol include an action description of what is being done at that step in the process?
6. Do the flowcharts indicate inputs and outputs for each activity/process?
7. Is the input and/or output specifically identified (i.e., exact name of query or name of report)?
8. Are control points identified and numbered between flowchart symbols?
9. Does the process end at the end of the flowchart? If yes, is there a defined end symbol? If no, is the next process connector on the flowchart instead of an end symbol?

10. If the process flowchart is linked to/from another, is the naming convention understandable and logical?

Flowchart deliverables shall include the name, phone number and email address of an operational point of contact. Flowcharts shall also include a legend for the flowchart symbols used. When the financial statement reporting entity identifies or becomes aware of significant discrepancies between the BEA their final flowcharts a financial improvement milestone should be included as to when the discrepancies will be corrected.

Exhibit 1 –Process Flow Chart Example

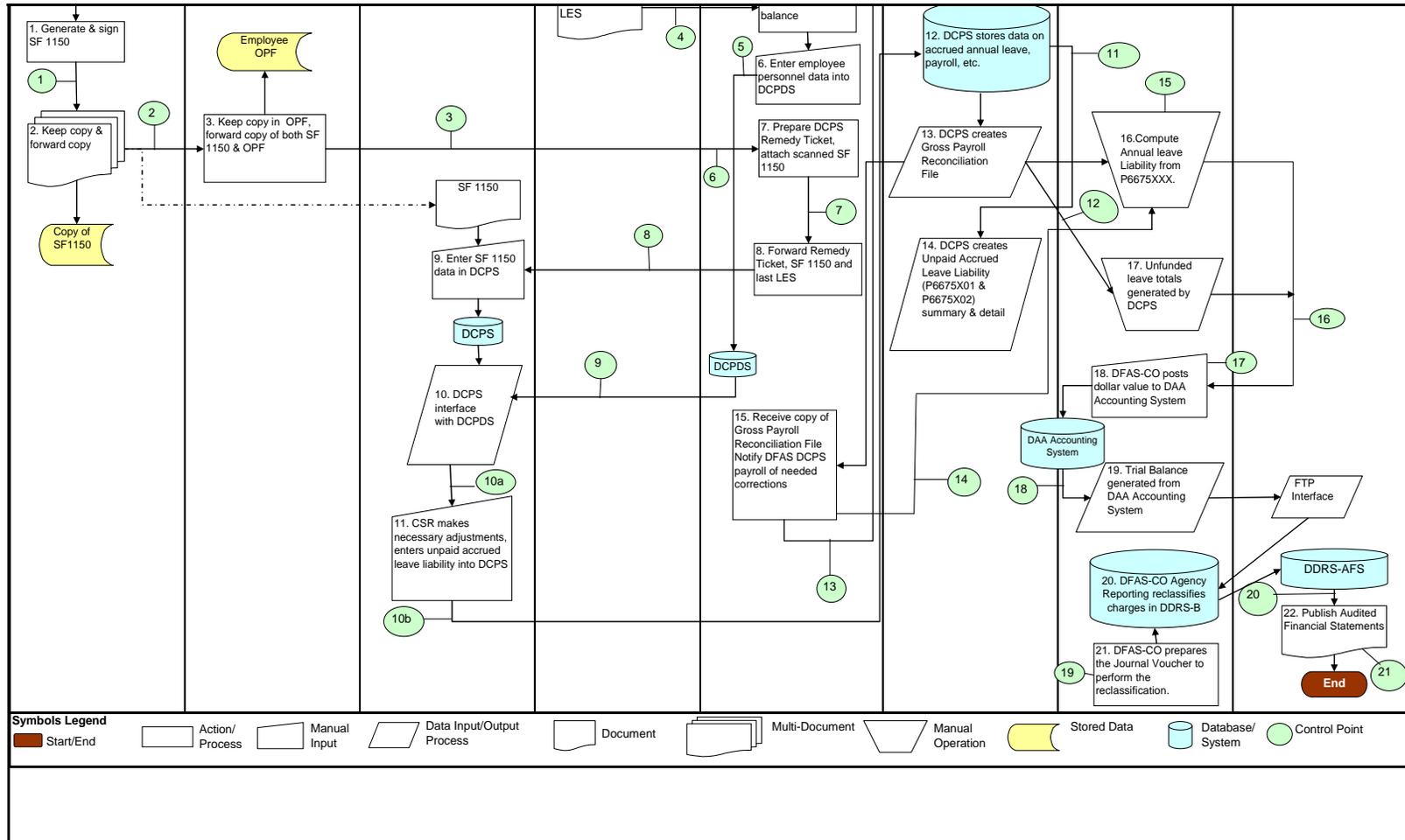
EXAMPLE - Flowchart: Transferring Accrued Annual Leave Liability for Employees Transferring In

DAA, Other Liabilities

POC: Name: Rudolf Flyer

Phone No.: 111-222-3333

E-mail: rudolf.flyer@osd.mil

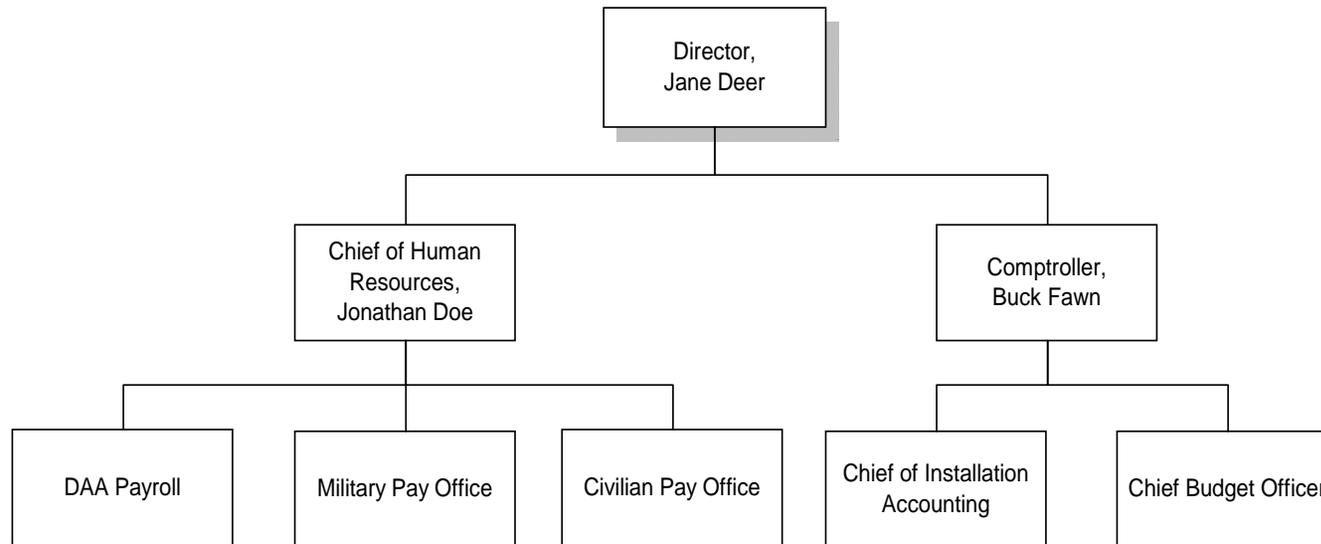


Organization charts must also be provided in support of Deliverable A and must reflect the chain of command for the department(s) described in the flowcharts. All organizational offices shown on the flowcharts should be shown on the organization chart. Each page of deliverables should include a footer or header with the name of the Component and contact information.

Exhibit 2–Organization Chart Example

Deliverable A (continued):

Defense Aircraft Agency Organization Chart



Note: The Payroll and Accounting Office functions for Defense Aircraft Agency are owned by the Defense Finance and Accounting Service. Defense Aircraft Agency is a fictitious organization used for example purposes.

The Department recognizes that some Components are in the process of developing and fielding systems solutions that are intended to remediate known, systemic, material internal control weaknesses. While each area is composed of more than one process and many sub-processes, where system solutions are identified within a Component’s process, the Component is to follow the decision tree below to determine at what point the various sub-processes are to implement the Appendix A process. The decision tree is based on the following assumptions: there is no one size that fits all for the DoD Appendix A approach; key processes are in a continuous state of discovery and correction; each process documentation initiative must identify the systems that either feed or are the recipient of the output generated from the processes; and full A-123 Appendix A process implementation is required prior to any transfer of data from existing process/sub-process/system, independent verification and validation, and any assertion and/or audit.

OMB Circular A-123, Appendix A, Decision Tree

1. Do you have an unqualified opinion?
 - a. Yes – Apply Appendix A requirements with DoD Guidance.
 - b. No – Proceed to question 2.

2. Are the business processes and Information Technology (IT) systems working as intended or in the validation/assertion phase?
 - a. Yes – Apply Appendix A requirements with DoD Guidance.
 - b. No – Proceed to question 3.

3. Are the business processes and/or systems deficient, but fixable, **without** system dependent solution?
 - a. Yes – Apply Appendix A requirements with DoD Guidance to measure corrective actions taken. Return to rule 2.
 - b. No – Proceed to question 4.

4. Are the business processes and/or systems deficient, but fixable, and require a change to an existing system as a solution (System Change Request (SCR))?
 - a. Yes:
 1. Apply DoD Guidance Appendix A requirements on business processes and systems that will continue without modification.
 2. For business processes and/or systems that will require corrective actions, apply Appendix A requirements to the changed business processes and/or systems when the system is at operational/production capability. Proceed to rule 1 upon completion of corrective actions.
 - b. No – Proceed to question 5.

5. Are the business processes and/or systems deficient, not fixable and requiring deployment of a “new” business process or system solution?
 - a. Yes:
 1. Apply DoD Appendix A Guidance requirements on business processes and systems that will continue without modification to assure full implementation upon system deployment.
 2. For business processes and/or systems that will require new system solutions to correct deficient controls, report the deficiency as a material weakness and the system solution as a corrective action plan. Proceed to rule 1 upon system deployment.
 - b. No – Proceed to question 1.

2.1.5 Reporting Weakness Dependencies (Part of Deliverable B)

At any time during a Component’s process analyses, a reporting FSRE Component may identify a weakness in its reporting process over which it has no control to correct because that part of the process is performed by another (a secondary) Component. If the primary Component determines the weakness to materially impact its financial reports, the primary Component should report the dependency relationship in the FIAR web-based tool Collaboration Site. For the 2009 ICOFR reporting year, the Collaboration Site will be available from October 1, 2008 until March 2, 2009 for

reporting Components to enter weaknesses which must be corrected by the secondary Components. The site requires the reporting Component to:

- Identify itself, the preparer of the report, and contact information;
- State the control weakness in specific and detailed terms;
- Explain how the weakness **materially** affects its financial reports or processes; and
- Identify who owns the weakness process (the secondary Component).

Upon approval by the ICOFR program manager, the program manager will notify the secondary Component of the reported weakness and inform the secondary Component that it has 90 days from the day the weakness was approved to provide to the reporting Component a satisfactory corrective action plan to remedy the weakness. After the reporting Component accepts the corrective action plan as a satisfactory remediation method, the corrective action plan must be entered in the secondary Component's FIP in the FIAR tool, complete with detailed corrective steps and realistic target dates for completion so that the reporting Component can copy the plan and paste it into its own corrective action plan to be included in its ICOFR SOA.

2.1.6 Reporting Material Weaknesses and Preparing Corrective Action Plans

The OMB Bulletin 07-04, "Audit Requirements for Federal Financial Statements," defines material weaknesses as a significant deficiency, or combination of significant deficiencies, that results in a more than remote likelihood that a material misstatement of the financial statements will not be prevented or detected. This definition of material weakness aligns with the definition of the same term to be used by management to prepare an agency's FMFIA assurance statement. The assessment process includes identifying material weaknesses and developing plans to correct them.

Corrective action plans should address the resolution of a specific identified control weakness and include the steps and associated timelines required to complete the corrective action. When developing and entering into the FIP a corrective action plan to resolve a material weakness which will be reported in the Component's ICOFR SOA follow these steps:

- State the as-is weakness conditions on the first line of the corrective action plan. The weakness should be clearly, yet briefly, stated.
- Following the stated weakness, list the tasks to be accomplished to correct weaknesses on subsequent lines in the FIP. All tasks must have a projected date that is giving quarter and fiscal year. No "to be determined" is allowed. Tasks should clearly describe what needs to be done in that step and should include a date (Quarter and Fiscal Year) by which the Component expects to complete the task. This will be a target date (Quarter and Fiscal Year) that will be reported on the Component's ICOFR SOA. It is recommended that the steps be a short duration from each other to reflect progress. If implementing new policy or process changes is a Component's solution to correcting a material weakness, the change should be reported to the responsible IRB to ensure the BEA and/or PSA extension(s) are updated, as necessary, to reflect the change(s).
- All tasks/lines within one plan to correct a weakness must have an A-123 identifier. To identify corrective action plans related to material weaknesses which will be reported in the

Component's ICOFR SOA, use the "A-123" data field in the FIP template and select ICOFR from the drop-down menu.

- Recognize corrective action plans related to significant deficiencies in the "A-123" field by selecting "Significant Deficiency." Recognize corrective action plans related to significant deficiencies or material weaknesses if the process is performance related, such as may be the case with DFAS. This will serve as notice that this corrective action will not be reported as a material weakness in the Component's ICOFR SOA and that the Component will manage the correction of the deficiency within the Component.
- Components (secondary Components) entering corrective action plans which they will perform within their own processes to correct a material weakness in another Component's process should enter the correction plan in their (the correcting Components') FIP. Enter the name of the Component for which the correction is being made in the "Resource Names" data field. These corrective actions must be in the web-based tool by June 1, 2009 so that the reporting Component will have time to copy the plans to their FIPs.
- Reporting Components receiving corrective action plans from weakness owner Components (secondary Components) must report the weakness in their ICOFR SOA as material because they justified the weakness as material to the financial reporting process when reporting the weakness dependency in the Collaboration Site of the FIAR tool.

Once reported, the same material weakness should never reappear as a new, re-titled weakness in a future ICOFR SOA. Instead, the original weakness should reflect that it was completed. The new instance should retain the same name as the original weakness but show a new date identified. For example, consider a material or systemic weakness that a Component originally identified in FY 2008 and corrected in FY 2009. Then in FY 2010, management assessments identify related problems and the Component wants to report it as a new material weakness in FY 2010. The material weakness should retain the same title as the original, but the "Year Identified" date would now appear as FY 2010, not FY 2008.

Weaknesses that slip year after year and do not meet the targeted correction dates reflect negatively on the Department's commitment to improve. Therefore, the Component's Senior Assessment Team should resolve material weaknesses as quickly as possible and ensure that the targeted correction dates are met.

Complete the Control Assessment Form (attachment 4) and add a copy to the Component's ICOFR TABs (material weaknesses related to Internal Controls over financial reporting) which will be included in the Component's overall FMFIA Annual Statement of Assurance. This will require that Components' SATs determine which weaknesses it will include in its ICOFR SOA as material before the Control Assessments and corrective action plans are submitted. The format for the Tabs is found on page 22.

2.2 Preparing the Statement of Assurance on Internal Controls over Financial Reporting – Part of Deliverable E

The statement will cover the one year period from 1 July – 30 June and be effective *as of June 30, 2009*. If a material weakness is expected to be corrected within the 4th Quarter (Qtr) of FY 2009 but all actions are not completed as of June 30th, the DoD Component Head should report the material weakness as still ongoing. Should an entity elect to contract for an audit opinion of its Internal Controls over financial reporting, the effective date may be adjusted to coincide with the audit opinion.

Statements of Assurance on Internal Controls over Financial Reporting constitute a paragraph or multiple paragraphs which follow the Overall Statement of Assurance in the Annual FMFIA Statement of Assurance.

EXAMPLE - Defense Aircraft Agency General Fund UNCORRECTED MATERIAL WEAKNESSES STATUS CORRECTIVE ACTIONS “Uncorrected Weaknesses Identified During the Period”

D-2-1

Title and Description of Issue: Leave liability for transferring employees is not captured and recorded correctly. The inability to reconcile gross payroll file and accrued liabilities may lead to misstatement of Accrued Leave Liability.

Functional Category: Financial Reporting, Accrued Leave Liability

Component: Defense Aircraft Agency (DAA) General Fund

Senior Official In Charge: Ms. Buck Fawn, Comptroller, Defense Aircraft Agency

Pace of Corrective Action:

Year Identified: FY 2007

Original Targeted Correction Date: 2nd Qtr, FY 2010

Targeted Correction Date in Last Year’s Report: 2nd Qtr, FY 2010

Current Target Date: 2nd Qtr, FY 2010

Reason for Change in Date: N/A

Validation Indicator: Leave liability for the transferring employees will be recorded correctly. Reconciliation of gross payroll files and accrued leave liability summary and detail reports will result in variance of less than 5 per cent.

Results Indicator: Accrued Leave Liability is correctly posted.

Source(s) Identifying Weakness: Control Test results, June 2007

Major Milestones to Include Progress to Date:

A. Completed Milestones:

Date:

Completed

Milestone:

Evaluated current accounting system capabilities for calculating leave liability.

Developed preliminary reconciliation process.

B. Planned Milestones for Fiscal Year 2009:

Date:

1st Qtr, FY 2009

Milestone:

Develop and issue reconciliation procedures.

Develop controls to ensure the correct data entry and to minimize the chances of error.

C. Planned Milestones Beyond Fiscal Year 2007:

Date:

2nd Qtr, FY 2010

Milestone:

Train employees on new procedures and implement.

2nd Qtr, FY 2010

Validate that the weakness is corrected by....

EXAMPLE - Defense Aircraft Agency General Fund

MATERIAL WEAKNESSES CORRECTED THIS PERIOD

D-3-1

Title and Description of Issue: All costs are not captured to appropriate orders. Customers are invoiced for incorrect amount of goods or services received. The inability to reconcile invoice with customer orders may lead to misstatement of Accounts Receivable.

Functional Category: Financial Reporting, Accounts Receivable

Component: Defense Aircraft Agency (DAA) General Fund

Senior Official in Charge: Mr. Buck Fawn, Comptroller, Defense Aircraft Agency

Pace of Corrective Action:

Year Identified: FY 2006

Original Targeted Correction Date: 2nd Qtr, FY 2010

Targeted Correction Date in Last Year's Report: 2nd Qtr, FY 2010

Current Target Date: N/A

Reason for Change in Date: Weakness corrected

Validation Indicator: Receivables/Payables balance, advances to and from balance, revenues and expenses are reflected accurately in correct period.

Results Indicator: A benchmark of at least 98% of instances where Requesting Component and Performing DoD Component reconcile receivables and payables, advances to and advances from, and revenue and expenses (or capitalized assets) in the same accounting period. Variances can be explained.

Source(s) Identifying Weakness: Control Tests, May 2007

Major Milestones to Include Progress to Date:

A. Completed Milestones:

<u>Date:</u>	<u>Milestone:</u>
Completed	Implemented process that required reconciliation between Requesting Component's and Performing DoD Component's receivables and payables, advances to and advances from, and revenue and expenses in the same accounting period.
Completed	Management represents that reconciliation results in financial reports which are properly classified, described, and disclosed.

Table 2 - ICOFR Deliverable A Checklist

Process Narratives, Flowcharts and Organizational Charts Checklist

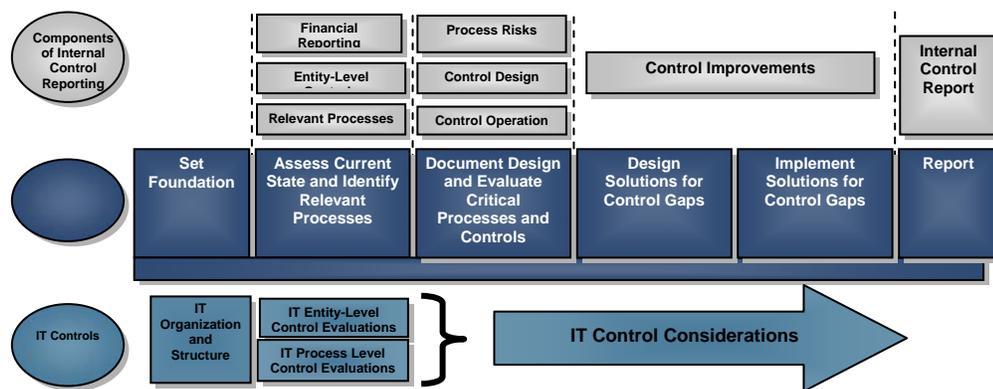
Component		Completed By		
Process		Date		
No.	Criteria or Requirement	YES	NO	Notes/ Action Required
General				
1	Does the deliverable include an info memorandum signed by the chair of the Component's Senior Assessment Team?			
2	Does the deliverable include flowcharts, process narratives and the entity's organizational chart?			
3	Does the deliverable include the name, phone number and e-mail address of an operational point of contact?			
4	Does every page of the deliverable have a footer with the name of the Component?			

5	Does the deliverable include the organization's code of conduct or ethics policy, a list of SAT members with titles, and the SAT Charter?			
Process Narratives				
6	Does the process narrative have the preparers name and is the process owner's name evident on the process narrative?			
7	Are the steps in the process narrative numbered? These numbers should also be included in the flowcharts (see step 9 below).			
8	Do narratives explain the steps in the process which cause an operational event to become a financial transaction?			
9	Does every process identified on the flowchart have an associated description in the narrative?			
Flowcharts				
10	Does the flowchart identify the format in which the model is being developed? (e.g. Word, PowerPoint, Excel, Visio)			
11	Are flowcharts presented in swim-lane format?			
12	Do flowchart swim-lane headers include the names of the organizations or offices performing the functions within the lane? Headers should <u>never</u> be functions.			
13	Do the steps in the flowchart include the numbers of the associated step in the process narrative?			
14	Do flowcharts include manual processes and system processes? Flowcharts should not be computer system flow diagrams. For clarification, identify the names of any systems and reports.			
15	Do the flowcharts capture processes from the point of origin to the financial statements and then back to the point of origin?			
16	Are the names of the systems (including the DoD Information Technology Portfolio Repository (DITPR) # if DoD business system required to be registered in the DITPR) and reports identified on the flowcharts?			
Organizational Charts				
17	Do organizational charts identify the chain of command for the departments explained in the flowcharts? All organizational offices shown in the flowcharts should be identified in the organizational chart.			
Control Environment Document				
18	Does the deliverable contain a Control Environment document?			
19	Does the Control Environment document have a date and signature?			

3.0 RISK ASSESSMENT AND TESTING

The assertion package process concentrates Components' efforts on areas of high risk by focusing on testing in the Discovery and Correction phase and obtaining results that will stand up to audit scrutiny. Testing validates the effectiveness of internal controls thus providing a reasonable comfort to management over its assessment of internal controls. An effective test will identify whether the breakdown in the control is due to the design of the control or whether the control simply is not operating as intended. Written policies and procedures, verified by tests of controls are validated during the assertion process and subsequent ICOFR reviews. At this stage of A-123 implementation, an overall strategy to internal controls should have been developed by the Components. One such approach is illustrated below.

Exhibit 3 – Approach to Internal Controls Example



Identifying Control Objectives for Testing Purposes

The purpose of testing is to evaluate internal controls designed to provide reasonable assurance that the following objectives are met:

- **Reliability of financial reporting** ("financial reporting controls") transactions are properly recorded, processed, and summarized to permit the preparation of the financial statements in accordance with generally accepted accounting principles (GAAP), and assets are safeguarded against loss from unauthorized acquisition, use, or disposition; (Financial Audit Manual (FAM) Section 310)
- **Compliance with applicable laws and regulations** ("compliance controls") transactions are executed in accordance with (a) laws governing the use of budget authority and other laws and regulations that could have a direct and material effect on the principal statements, and (b) any other laws, regulations, and DoD-wide policies (FAM Section 310).
- **Efficient and Effective use of operational resources**

More about Controls

- **Financial reporting controls:** Prevent or detect aggregate misstatements in significant financial statement assertions.
- **Safeguarding controls:** Safeguard assets against loss from unauthorized acquisition, use, or disposition.
- **Compliance controls:** Comply with significant provisions of applicable laws and regulations.
- **Budget controls:** Execute transactions in accordance with budget authority.
- **Operations controls:** For each relevant operations control, achieve the performance level desired by management for the planning, productivity, quality, economy, efficiency, or effectiveness of the entity's operations.
- **Safeguarding controls and Separation of duties:** often critical to the effectiveness of controls over liquid (easily sold or traded), readily marketable assets (such as cash, inventories, or property) that are highly susceptible to theft, loss, or misappropriation in material amounts.
- **Compensating controls:** exist to strengthen the primary control to a high level of operating effectiveness. An example of a primary control is an authorization control, such as approval of invoices by an e-payables manager before payment.
- **Frequency of the control's application:** generally, the more frequently a control is applied, the greater the likelihood that it will be effective.
- **Experience and skills of personnel performing the control:** the person applying a control has the necessary knowledge and expertise to properly apply it. There is direct correlation between the person's level of experience and skills with the controls, and the effectiveness of the controls.
- **Documentation of internal controls:** appropriate documentation of transactions and controls.

A deficiency in design exists when a) a control necessary to meet the control objective is missing or b) an existing control is not properly designed so that even if the control operates as designed, the control objective is not always met. Consider a control a key control if any of the following questions are answered in the affirmative:

- If the control failed, would it have an impact on financial reporting?
- If the control failed, would it jeopardize the applicable financial statement assertions?
- Is the control a preventive control that does not have a related detective control?
- Is the control a detective control that does not have a related preventive control?

Testing of controls is based on risk. Management should determine the approach and should use discretion when planning testing based on risk assessment. After all key controls have been tested

once, and a baseline established on the operating effectiveness of those controls, not all key controls will need to be tested every year. The risk-based approach generally requires that controls are stable, there are no known deficiencies, and that controls will be tested at least every three years. If the area being tested is material to a particular segment that has not been proven audit-ready or been successfully audited, the one-test baseline is not sufficient. At least three years of testing results should be used for a baseline before shifting to the 3-year rotation for low-risks controls for the areas deemed material. Further, for fully automated controls, management is required to verify that adequate change control procedures are in effect. Documentation of its risk-based testing plan and how the above circumstances are met must be maintained.

Evaluating Controls of Cross-Servicing Providers and Service Organizations

When evaluating the controls in place at cross-servicing providers or service organizations determine the extent of:

- Performing tests of controls over the activities of the cross-servicing organization or service organization (e.g., re-performance of selected items processed by the cross-servicing organization or service organization, or reconciling output reports with source documents); or
- Obtaining a service auditor's report on controls placed in operation and tests of operating effectiveness (e.g., Type II Statement of Auditing Standards (SAS) 70 report) or a report on the application;
- Agreed-upon procedures that describe the relevant tests of controls. A financial service provider's Type II SAS 70 report is reliable with no further testing required for their client agencies in those areas covered by the Type II SAS 70 report.

For the financial service provider, the Type II SAS 70 reporting process should be incorporated into management's assessment of Internal Controls over financial reporting.

Documentation should include copies of written policies and procedures, written memoranda, flowcharts of system configurations and significant processes, etc. The documentation should identify the control objectives and related control points designed to achieve those objectives. Documentation of the understanding of the entity and significant computer applications related to financial reporting should include:

- The significance and nature of the programs and functions supported by systems
- The nature of software utilities used and the ability to add, alter, or delete information stored in data files, database, and program libraries
- The nature of software used to restrict access to programs and data
- Significant interfaces
- Feeder systems
- Significant changes since the prior evaluation or expected in the near future.
- The general types and extent of significant software
- How (interactive or non-interactive) and where data is entered and reported
- The approximate number of transactions processed by each significant system
- The organization and staffing at the entity's data processing and software development sites, including key staff and organization changes since the prior evaluation

- The entity's reliance on service bureaus or other agencies for systems support
- Results of past internal and external reviews, including those conducted by the Office of the Inspector General and consultants specializing in security matters.

Determine Materiality

Accounting standards usually include a statement that the standard "need not be applied to immaterial items." As a result, "auditors should consider materiality and its relationship with audit risk when conducting an audit" [Statement of Auditing Standards (SAS) 220.1].

Management must determine if an item is immaterial in order to gauge what items will be important or unimportant to the auditors. As pointed out in SAS 220, "Materiality is not capable of general mathematical definition as it has both qualitative and quantitative aspects". This affects the approach used by auditors who will rely on their professional judgment. Concrete rules usually cannot be implemented to determine whether an item is material or not. Instead, we need to exercise judgment. However, some general rules should be considered.

To determine whether a particular item/transaction is material, consider the following:

- Evaluate its effect on an individual financial statement as well as the whole set of financial statements.

As a general audit rule, an error less than 5% would be regarded as immaterial. However, the DoD has established its level of materiality as 0.99 percent of adjusted assets for proprietary accounts and 0.99 percent of total budgetary resources for budgetary accounts. Adjusted assets are calculated by subtracting the total intragovernmental assets (as indicated on the balance sheet) from total assets. All financial statement accounts equal to or exceeding the organization's level of materiality must be assessed.

- Determine if it is a recurring or non-recurring error.
- Recurring errors must be investigated no matter how small the percentage is. Recurring errors imply that there is a problem with the accounting system, which should be investigated.

Some errors occur at the conceptual level, but not at the calculation/technical level. For example, an error in the treatment of fixed assets would have a significant effect on the accounts (if, for example, the purchase price of a piece of military equipment was not recorded but was expensed in its entirety in the year of purchase, rather than over the useful life of the asset, the reporting for that year would be seriously affected).

Determining materiality is not only a discrete measure, but is also a function of management's professional judgment and discretion. Therefore, management should consider key business areas and programs that impact financial statement results when determining materiality. Management must determine if errors or misstatements individually or in the aggregate could have a material effect on their financial statements. The different types of materiality amounts, defined below, are useful in this determination.

- **Reporting materiality** is the overall materiality that serves as the threshold of reporting weaknesses in internal controls that could result in a material misstatement of the financial statements. Using a lower level of materiality for testing controls will increase the likelihood that the financial statements are not materially misstated.²
- **Planning materiality** is used to determine significant accounts, elements, or disclosures in a financial report. Planning materiality is generally a percentage of reporting or overall materiality.
- **Design materiality** is the portion of planning materiality that has been allocated to line items, accounts, or classes of transactions (such as disbursements). This amount will be the same for all line items or accounts (except for certain intragovernmental or offsetting balances).
- **Testing materiality** is used to determine the extent of controls testing relative to each significant account, element, or disclosure. Testing materiality is generally a percentage of planning materiality.

Materiality determinations for planning, design and testing on the SAT's assessment of Internal Controls over financial reporting should be based on quantitative and qualitative considerations:

Quantitative considerations—For a balance sheet, the materiality base might be total assets reported. For a statement of net costs, the materiality base might be total income or total expenses. The materiality base would be used to determine the reporting or overall materiality, which in turn would be used to calculate planning and test materiality.

Qualitative considerations – Certain accounts or elements of a financial report may be significant due to the interest of OMB, the public or oversight committees.

Using a lower materiality threshold, managers would be more likely to discover deficiencies or weaknesses in the assessment phase that may not rise to the attention of the financial statement auditors. Managers would also be able to identify deficiencies or weaknesses that, although immaterial for the audit, are worthy of management's attention. Any unique management experience or direct knowledge of financial operations should be used in developing materiality thresholds. **The determination of materiality should be documented as the basis of assertion package internal controls testing.**

Example of Materiality Determination

The materiality levels for planning, design and testing of Agency A were developed using the guidance provided in the General Accounting Office (GAO)/Presidents Council on Integrity and

² Implementation Guide for OMB Circular A-123, Management's Responsibility for Internal Control Appendix A, Internal Controls over Financial Reporting, July 2005, http://www.cfoc.gov/documents/Implementation_Guide_for_OMB_Circular_A-123.pdf

Efficiency (PCIE) Financial Audit Manual,³ Section 200 – Planning, Chapter 230, Determine Planning, Design, and Test Materiality. The initial analysis was based upon the FY 2006 Consolidated Financial Statements. The materiality base was determined by taking the greater of total assets (\$11,936,307,000) and total expenses (\$9,044,876,000), with total assets being greater. The planning materiality was 3% of total assets, or \$358,089,000. Design materiality was determined to be 1/3 of the planning materiality, or \$119,362,000; and assessment materiality was determined to be 75% of design materiality, or \$89,521,000. In December 2007, Agency A updated the materiality level to reflect the data reported in the FY 2007 Consolidated Financial Statements. Total assets (\$12,730,176,000) exceeded total expenses (\$8,438,306,000), so assets were used as the materiality base. The planning materiality was 3% of total assets, or \$381,905,000. Design materiality was determined to be 1/3 of the planning materiality, or \$127,300,000; and assessment materiality was determined to be 75% of design materiality, or \$95,475,000. Agency A is using these materiality levels as a basis for determining which FSREs and financial statement line items are subject to test work.

Risk Assessment

Risk Assessment is the identification and analysis of risk. It helps to determine where material internal control weaknesses are most likely to exist, and forms a basis for determining how risk should be managed. Every entity faces a variety of risks from external and internal sources that must be assessed. Management has the best understanding of its agency, its associated risks, and the controls in place to mitigate risk. Therefore, management can and should use discretion when developing the testing approach. Management must use a reasonable approach to determine what, when, where and how to test the key controls, and properly document the tests and results. Risk assessment should be performed according to the Testing Comfort Matrix (TCM) at:

<https://fiar.bta.mil/sites/entry/FIAR%20Guidance%20Documents/Testing%20Comfort%20Matrix.xls>. Important areas within TCM are discussed below for further clarification.

Risk Description: The OMB Circular A-123 Implementation Guide states that management should identify internal and external risks that may prevent the organization from meeting its objectives. The intent of risk identification is to answer the question, “What can go wrong?” Identified risks should then be analyzed for their cause and potential effect or impact on the agency. The risk should explain how the process or system could create a financial reporting misstatement.

Steps for conducting the Risk Assessment – Testing Comfort Matrix

Please refer to Testing Comfort matrix at

<https://fiar.bta.mil/sites/entry/FIAR%20Guidance%20Documents/Testing%20Comfort%20Matrix.xls>

- Determine objectives. An organization must be able to clearly define its objectives as the starting point for evaluating risk. What do you want to happen before deciding what can go wrong?

⁴ GAO/PCIE Financial Audit Manual, July 2001, Section 230
<http://www.gao.gov/special.pubs/gaopcie/s200july2004.pdf>

- List all the risks related to achieving the objective to assess the likelihood and impact of what may go wrong. This analysis helps to develop the necessary controls to ensure the overall objective is met.
- Determine the **likelihood** of the risk occurring and the **impact** if it does occur. For example, there is a high likelihood that employees will take home office supplies, however the impact is probably minor. On the other hand, the likelihood of someone trying to steal a missile is very low, but the impact would be massive. Both the likelihood and impact of a risk could be considered, but the impact of a risk is almost always more important than its likelihood.

Inherent Risk: Inherent risk is the susceptibility of a material misstatement. Inherent risks can be assessed as low, moderate, or high. Inherent Risk is high where susceptibility for misstatement of financial information exists and could materially impact the Component's financial reports. Low risk will include testing on the first year of discovery, if sufficient documentation supports the compliant process and management's judgment of low risk, then it can go on a three year testing cycle, unless the process changes significantly. Inherent risk is moderate or low when the absence of controls will not necessarily result in a financial misstatement. An example of an inherent risk is that a cash business might have a higher risk of robbery than a business that only accepts credit cards. The business may have controls for safeguarding the cash, but has a higher inherent risk.

Control Risk: Control risk is the risk that a material financial misstatement could occur in an assertion and will not be prevented or detected and corrected on a timely basis by the entity's internal control. The use of management's professional judgment is essential in assessing inherent and control risk. The control risk is classified in three levels: low, moderate, or high.

- **Low Control Risk:** The preparer believes that the control, as designed and operating WILL prevent or detect any aggregate misstatements that could occur in the assertion in excess of design materiality (low risk of misstatement).
- **Moderate Control Risk:** The preparer believes that the control, as designed and operating, will MORE LIKELY THAN NOT prevent or detect any aggregate misstatements that could occur in the assertion in excess of design materiality.
- **High Control Risk:** The preparer believes that controls will PROBABLY NOT prevent or detect any aggregate misstatements that could occur in the assertion in excess of design materiality (high risk of misstatement).

Tests should only be performed for those controls which have been assessed as posing low or moderate control risk. **If control risk is high, there is no need to test the control.** A control risk that has been labelled high shows that the control is either not effective in design or operation or has not been implemented. For those controls identified as high risk or weak, develop corrective action plans to correct the weaknesses.

Relative Assertions: Examples of testing objectives and procedures for each management assertion are listed in the following table:

Table 3 - Categories of Assertions

Management Assertion	Transactions	Account Balances	Presentation and Disclosure	Examples of Testing Objective	Examples of Testing Procedures
Completeness	X	X	X	Sales revenue include all items shipped to customers.	Review the entity's periodic accounting for the numerical sequence of shipping documents and invoices.
Accuracy	X		X	Accounts receivable reflect sales transactions that are based on correct prices and quantities and are accurately computed.	Compare invoice prices with master price list and quantities with shipping records and customer's sales order; recalculate amounts on invoices.
Obligations		X	X	Real estate in the balance sheet is owned by the entity.	Inspect deeds, purchase contracts, settlement papers, insurance policies, minutes, and related correspondence.
Rights		X	X	Real estate in the balance sheet is owned by the entity.	Inspect deeds, purchase contracts, settlement papers, insurance policies, minutes, and related correspondence.
Valuation		X	X	Receivables are stated at net realizable value.	Review entity's aging of receivables to evaluate adequacy of allowance for uncollectible accounts.
Allocation		X		Receivables are stated at net realizable value.	Review entity's aging of receivables to evaluate adequacy of allowance for uncollectible accounts.
Cut-off	X			Sales transactions are reported in the proper period.	Compare shipping dates with dates of journal entries for sales recorded in the last several days of the old year and the first several days of the new year.
Existence		X		Inventories in the balance sheet physically exist	Observe physical inventory counts by entity personnel.
Occurrence	X		X	Inventories in the balance sheet physically exist	Observe physical inventory counts by entity personnel.
Classification	X		X		
Understandability			X		

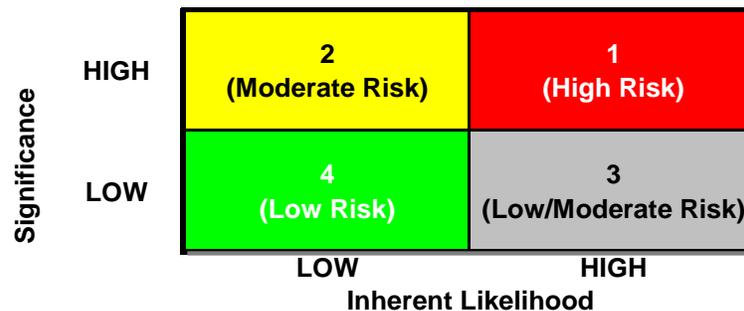
Table 3 “Categories of Assertions” above illustrates how to consider these broad categories of assertions in formulating testing objectives and designing testing procedures to obtain evidence supporting them. A combination of testing procedures generally will be necessary to achieve a single objective, and some testing procedures will relate to more than one objective. For example, observing physical inventory counts to obtain evidence that inventories included in the balance sheet physically exist. Observing inventory counts also provides evidence that the inventory quantities include all products, materials, and supplies on hand (completeness objective). In addition, it provides evidence about other accounts and objectives (such as the existence of plant) and about certain aspects of the entity's internal control (such as how management operates the business, restrictions on access to storage facilities, and the competence of employees).

Risk Mapping

The Risk Map⁴ prioritizes each risk according to significance and likelihood and maps the risks into four quadrants. The risk assessment map is a suggested tool. To map the risks into these quadrants, follow these steps:

For each risk, plot the significance on the vertical axis and the likelihood on the horizontal axis. Look at the quadrant where the risks are located. Position in the quadrant helps prioritize the risks and indicates the level of concern and attention which should be directed toward mitigating that risk.

Exhibit 4 – Risk Assessment Map



The Risk Map locates each risk in the following four quadrants:

1. “Prevent at Source” risks.

Risks in this quadrant are classified as Primary Risks and are rated “high” priority. They are the critical risks that threaten the achievement of company objectives. These risks are both significant in consequence and likely to occur. They should be reduced or eliminated with preventative controls and should be subject to control evaluation and testing.

2. “Detect and Monitor” risks.

Risks in this quadrant are significant, but they are less likely to occur. To ensure that the risks remain low likelihood and are managed by the company appropriately, they need to be monitored on a rotational basis. Detective controls should be put into place to ensure that these

⁴ <http://www.auditnet.org/docs/risk1.doc>, Risk Assessment Survey and Risk Mapping Tool. March 20, 2008.

high significance risks will be detected before they occur. These risks are second priority after Primary Risks.

3. “Monitor” risks.

Risks in this quadrant are less significant, but have a higher likelihood of occurring. These risks should be monitored to ensure that they are being appropriately managed and that their significance has not changed due to changing business conditions.

4. “Low Control” risks.

Risks in this quadrant are both unlikely to occur and not significant. They require minimal monitoring and control unless subsequent risk assessments show a substantial change, prompting a move to another risk category.

The completed Risk Map should give a basis for assessing risks and addressing each one in accordance with its potential impact on business strategy.

Where there are pervasive material weaknesses, management should focus on the remediation of those weaknesses rather than testing internal controls that are known to be ineffective. Risk tolerance is the amount of risk a Component is willing to accept in pursuit of financial integrity. Residual risk is the unmitigated risk that remains after controls are implemented. Management does not implement a system of absolute assurance, but implements controls to provide reasonable assurance. The risk that remains is the residual risk.

Review material weakness findings and recommendations reported in external audit reports to consider the existence of inherent risk and control problems. Perform the risk assessment using the business process flowcharts of key processes to identify risk. Indicate when high risk areas exist by referring to a control point indicator in the process flowcharts.

Automated and IT Dependent Controls

Management should consider the design and operation of the automated controls or IT dependent controls and the relevant general IT controls over the applications that provide the IT functionality. General IT controls ordinarily do not directly prevent or detect material misstatements in the financial statements. However, the effective operation of an automated or IT dependent control depends on effective general IT controls. Management would ordinarily consider and evaluate only the general IT controls that are necessary to adequately address financial reporting risks.

Inherent and Control Risk Determination

The following questions may be helpful in performing an inherent and control risk analysis and determining if a risk factor is significant:

1. Have all key financial controls been identified? (How do we prevent what could go wrong?)
2. Are the current controls designed to mitigate identified risk?
3. Are current controls documented in written procedures?
4. Does every control link to at least one risk? (There can be a one-(link) to-many (risks) relationship.)

5. What is the control designed to do?
6. Are there any risks/controls that apply to the whole process?
7. Does the control explain who performs, when in the process/cycle, and how the control is executed?
8. If a management review/monitoring control, does the control detail:
 - a. How often are reports/results reviewed?
 - b. What is the purpose of the review? (control objective: design and operation)
 - c. Who performs?
 - d. Follow-up procedures for discrepancies/unusual variances?
9. If there is a segregation of duties control, does the control detail:
 - a. Which responsibilities are segregated?
 - b. What is the control designed to do?
 - c. How are duties segregated? (one who orders does not receive)
 - d. Does the organization chart support the control?
10. If there is an approval or authorization control, does the control detail:
 - a. Whether it is manually documented or system driven?
 - b. Who approves? (what level of management?)
 - c. Existence of an established level of authorization?
11. If there is a reconciliation control, does the control detail:
 - a. Who prepares and performs the reconciliation? (control objective)
 - b. What is the purpose of the reconciliation?
 - c. Who reviews the reconciliation?
 - d. What reports are used and which systems generate the reports used?
 - e. How are differences investigated / resolved?
12. If there is a document control, does the control detail that:
 - a. Documents are pre-numbered and system generated (e.g., Military Interdepartment Purchase Requests (MIPRs), customer orders, invoices, etc)?
 - b. Documents are safeguarded (e.g., physical controls over checks, contracts, manual journal entry logs, receiving reports, etc.)?
13. If there is a physical asset control, does the control detail:
 - a. How is access to the asset and related record keeping appropriately restricted?
 - b. Is it reviewed periodically?
 - c. What procedures ensure the accuracy of the related record keeping (activity logs)?
14. If there is a system based control, does the control detail:
 - a. All key fields for data entry must contain valid information (e.g., current date, established dollar range) in order for a record to be accepted?
 - b. Information is validated against a master table (e.g., customer number, product number, vendor number, Purchase Order (PO) number, stock number)?
 - c. Master tables are reviewed and updated regularly to ensure accuracy and table data is safeguarded?
 - d. Duplicate postings/entries are not accepted?
 - e. Reporting period-end cut-off dates are enforced by the system?
 - f. System-based control overrides must be authorized?
15. Is the control frequency documented e.g., quarterly, monthly, weekly, daily, multiple times daily? (Control universe equals how many times control is performed/year)
16. Does the control description adequately explain how it mitigates the risk?
17. Is the control owner listed?
18. Are position titles (not names) used?

19. Is the control technique (Manual or Automated) listed? Is the control technique listed accurate?
20. Has the preparer assessed the design effectiveness? Does the control design address the risk identified?
21. Has the preparer documented any deficiencies (Control gaps) in the design effectiveness?
22. Is the control being performed as designed?
23. Have controls been documented where they occur? Note: controls that occur outside of the process (e.g., senior management operational review) should be documented.
24. Would a control weakness result in a conflict of interest?

Example Risk Analysis Worksheet

Examples	Event				
	Order Acceptance	Receiving	Vendor Maintenance	Invoice Processing	Performing Services (filling customer orders)
High Risk					
Complex Programs/ operations					
Complex transactions					
Use of accounting estimates					
Extensive manual processes / applications					
Decentralized accounting / reporting functions					
Changes in operating environment					
Significant personnel changes					
New / revamped information systems					
Moderate/High					
New technology					
Amended laws / regulations					
New accounting standards					
Moderate/ Low Risk					
Simple operations / accounting transactions					
Low transaction volume					
Centralized accounting functions					
Static operating environment					
Management Risk Analysis					

Testing Methodology

A major part of the testing strategy is based on a presumption about the assessment of control risk, before the documentation and tests of controls have been completed. In formulating the testing strategy before completing the documentation and testing of controls, the tester assumes that he or she already has an adequate understanding of the design (and its effectiveness) and the operation of the internal controls. The basis for that assumption generally is derived from knowledge (which may be limited in scope) obtained through inquiries, observation, and inspection of documents, records, and reports undertaken in the course of developing the understanding of internal control, from any tests of controls performed at that time, and from review of the results of previous testing work. The testing strategy as initially determined should be reviewed, and revised if necessary, as the testing phase progresses and new information becomes available.

Testing Strategy Memo (TSM)

The testing strategy memo which is found at the following link <https://fiar.bta.mil/sites/entry/FIAR%20Guidance%20Documents/Testing%20Strategy%20Memo.doc> should be prepared in the Planning phase and should be updated during the testing phase. Step by step explanation of the TSM is provided below. The guidelines should be considered minimum and are not all inclusive.

Overview of the TSM

- Internal Control testing should be performed in accordance with A-123 Appendix A and according to guidelines set forth by CFO council A-123, Appendix A implementation guide.
- The TSM incorporates the requirements of the FAM Entity Profile document (FAM section 220) and General Risk Analysis document (FAM section 290.04).

Understanding the Business

- Significant External and Internal Factors
- Accounting Policies and Issues
- Significant Provisions of Laws and Regulations
- Relevant Budget Restrictions

Internal Control Environment

- Risk Assessment
- Inherent Risks Arising from Information Systems (IS)
- Impact on Entity Level Controls
- Preliminary Assessment if IS Controls

Testing Scope Considerations

- Operational Controls to be Tested
- Related Party Transactions (If any)

Significant External and Internal Factors

- Identify significant external and internal factors that affect the entity's operation.

External factors might include:

- Sources of Funds
- Relevant legislation

Internal factors might include:

- Size of the entity
- Number of locations
- Complexity of operations
- Information system structure
- Qualifications and competence of key personnel

Significant Provisions of Laws and Regulations

Identify significant provisions of laws and regulations applicable to DoD. Consider the following:

- Compliance controls
- Whether DoD is likely to be in compliance with applicable provisions, including non-compliance due to budget restrictions
- Compliance findings noted in prior years

Relevant Budget Restrictions

- Identify significant budget restrictions, including limitations on spending as outlined in the appropriation law.

The following information should be reviewed and considered in identifying significant budget restrictions:

- Authorizing legislation
- Enabling legislation and amendments
- Appropriation legislation and supplemental appropriation legislation
- Apportionments and budget execution reports
- System of funds control document approved by OMB

Additionally, the SAT should consider any legally binding restrictions that the entity has established in its fund control regulations, such as lowering the legally binding level or compliance with the Anti-deficiency Act to the allotment level.

Confirming the Assessment of Control Risk by Performing Tests of Controls

In performing tests of controls, determine how activities are carried out, the consistency with which they are performed, and by whom they are carried out. Tests of controls may include inquiring of entity personnel who carry out activities, as well as others in a position to be aware of control breakdowns; observing how the activities are performed; examining records and documents for evidence that they have been carried out; and re-performing control activities by duplicating the actions of the entity's personnel.

After performing tests of controls, consider whether controls operated as previously understood. If they did not, but the assessment of control risk was nevertheless confirmed, amend the recorded understanding of internal control. If the control risk assessment was not confirmed by the tests of controls, amend the assessment and consider the implications for the audit strategy and the review

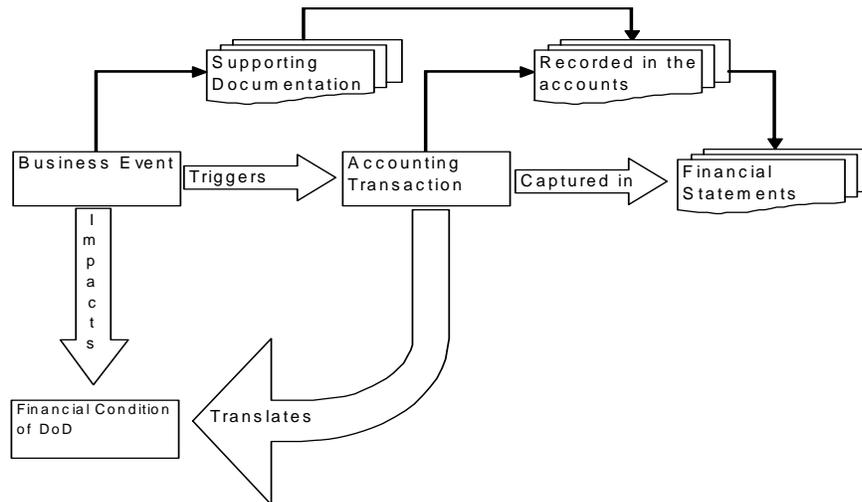
program, including how any deficiencies and breakdowns noted affect the risk that account balances could be materially misstated.

Example. Business events, such as opening a landfill, trigger accounting transactions. Transactions represent the impact the business event has on the financial condition of an entity and are recorded in system accounts, such as Estimated Cleanup Cost Liability (United States Standard General Ledger (USSGL) Account 2995). Double entry accounting, a proven method for capturing the financial impact of business events, records the transactions in the accounting system. Double entry accounting is based on the following accounting equation:

$$\text{Assets} - \text{Liabilities} = \text{Net Position}$$

When a liability is increased, either an asset needs to increase or the net position needs to decrease to keep the equation in balance. When the landfill is opened, creating an increase in the environmental liability, a corresponding entry is made to Future Funded Expenses (USSGL Account 6800), thus reducing the net position. The double entry captures the financial impact of this transaction by recording the liability (a future sacrifice of resources) and the expense (the cost of doing business during this accounting period). The accounts are summarized and categorized before being presented in the financial statements.

Exhibit 5 – Accounting Process Flow Example



3.1 Suggested Approach to Testing

Step 1 - Define the Segments in accordance with FIAR Plan Framework.

Step 2 – Document Processes

Step 3 – Flowchart Key Processes in accordance with section 2.1.4

Step 4 – Identify Key Controls

Process and control owners identify the controls for which they are responsible for each process and sub-process within a segment. Identify the control activities, self-assess and document how the

controls were designed to achieve the specific control objective. Control owners investigate and document control deficiencies and communicate the results to management. The discussion on controls includes:

- Agency access to records and files (paper and electronic).
- Accountability (what actually exists versus what was recorded and appropriate action taken with respect to differences).
- Activities that ensure physical security of assets or records, periodic counts, and reconciliations.
- Segregation of duties.
- Proper execution of transactions and events.
- Accurate and timely recording of transactions and events.
- Control techniques (for example performing walkthroughs) and follow-up.
- Documentation of controls and tests of controls.
- Ready availability of source documents underlying identified universe of transactions.

Step 5 – Evaluate Key Processes and Controls

Identify control objectives for each process and sub-process within a segment. Evaluate the design of the controls to determine if they adequately address the risk that a material misstatement in the financial statements would not be prevented or detected in a timely manner. Methods for evaluations include:

- Inspection is examining documents and records for the existence of control evidence, such as initials or signatures. Examples of inspections include using operations manuals and flowcharts of evidence to determine the propriety of tasks under examination.
- Observation is watching personnel perform control activities in the normal course of duties. Because observation in itself does not provide evidence that the control has been in place, it is supplemented with corroborating information.
- Inquiry is oral or written investigation into how personnel perform their duties.
- Re-performance is inputting the same information and activities from the beginning of a process to see if the subsequent outcome matches the original figure and expected results.

Evaluations include a full understanding of known risks:

- How the data is transmitted and received.
- Data could be compromised at the source.
- Data might not be current, correct, or complete.
- Inadequate staff training.

Step 6 – Assess Risk and Test Controls

Risk assessment is the identification and analysis of risk. Begin by identifying the risks to reliable financial reporting that could, individually or in combination, result in a material misstatement to the financial statements for each process and sub-process within a segment. Identify the likelihood of effective controls and assess risks. The identification process should vary according to the characteristics of the entity, such as its size, complexity, organizational structure, and its processes and financial-reporting environment. This process forms a basis for determining how risk should be managed.

- Prepare Test Plans and test controls (See Attachment 1)
- Assess test results and document
- Identify material weaknesses and/or significant deficiencies
- Confirm Agency monitoring activities
- The items tested should be randomly selected (equal opportunity for all items in the universe to be selected) from a universe of transaction level data. This transaction level data should be reconciled to the balance on the financial statement or the balance of the segment being asserted on. The testing should also be related to the specific financial statement assertion(s) for the transaction being tested.
- Ascertain the availability of subsidiary ledgers and the universe of transactions that reconcile to trail balance information used to prepare financial statement line items and notes.

The risks to be evaluated include the risk of fraudulent activity (including the improper override of internal controls), which should be evaluated under the assumption that all entities have fraud risk.

Management then evaluates whether it has controls in operation that are properly designed to address the identified risks. An effective testing approach carefully considers the information from key inputs, applies them in a reasonable, consistent test plan development methodology, executes with skilled professionals in order to provide validation of processes' operating effectiveness for key controls, or, to identify gaps and findings quickly in order to begin remediation efforts.

Step 7 – Design Solutions for Control Gaps

Design solutions for control gaps by implementing controls to protect assets and reduce the risk(s) associated with an asset activity to acceptable levels. A control may also be established to prevent any significant new problems from being introduced into ongoing work. Controls may be either preventative or detective in nature. Depending on the situation, both preventative and detective controls may be necessary to afford an adequate level of protection from the risk of errors. Examples of control activities that might be present include:

Preventative Controls:

- Limiting system access to only those needed to do the job.
- Reading and understanding the policy/procedure.

- Managing review and approval of certain key activities.
- Using asset identification tags on property.
- Physical controls over vulnerable assets.
- Segregation of duties.
- Access restrictions to and accountability for resources and records.

Detective Controls:

- Exception reports that list incorrect or invalid transactions.
- Manager review of cash transactions.
- Comparison of monthly bank deposits to financial statements.
- Top-level reviews of actual performance.
- Reviews by management at the functional or actual level.

Other Controls:

- Efficiency and Effectiveness.
- Consistency and Continuity.
- Management of human capital.
- Controls over information processing.
- Establishment and review of performance measures and indicators.
- Proper execution of transactions and events.
- Accurate and timely recording of transactions and events.
- Appropriate documentation of transactions and internal control.

FRSEs assigned General Property as a focus area for 2009 must ensure controls are in place to address areas of concern identified by Acquisition Technology and Logistics (AT&L) for General Property in 2008 as follows:

Table 4 - Risk Assessment – General Property – EXAMPLE

Risk	Assurance	Mitigation
DPAS users may not have documentation (i.e. DD 250, lease agreements) to support transactions* entered into DPAS.	External - User	User activities are responsible for source (input) documentation used to populate DPAS, such documentation is to be maintained in accordance with the National Archives and Record Administration (NARA) approved record schedule of respective DPAS user's agency.
Data from DD 250 or equivalent receiving document may be manually entered into DPAS incorrectly causing assets, depreciation, amortization, etc to be valued inaccurately.	External - User	Utilize the automated interface between Wide Area Work Flow (WAWF) and DPAS
DPAS users may not manually enter or accept pending WAWF transactions into DPAS in a timely manner resulting in an understatement of assets.	External - User	Standard Operating Procedure (SOP) requires DPAS operators to monitor the pending transaction on a daily basis

Risk	Assurance	Mitigation
DPAS may receive inaccurate data via interface with WAWF. WAWF provides receiving data electronically.	External - WAWF	WAWF Issue
DPAS may receive inaccurate data via interface with Defense Logistics Information System (DLIS). DLIS provides National Stock Number (NSN) and unit prices.	External - DLIS	DLIS Issue
DPAS users may not enter a placed-in-service (PIS) date in DPAS in a timely manner to begin depreciation.	External - User	SOP is to monitor quality assurance metrics on a monthly basis which identifies capital assets not placed in service
User organizations may request incorrect accesses for users.	External - User	SOP is to work with the DPAS support team in developing user security profiles to limit access to only the role the user has been trained for and assigned to
User organizations may circumvent capitalization threshold by expensing asset Components (i.e. expensing a truck and chassis separately).	External - User	SOP is to review DPAS provided reports on a regular basis which identify assets valued above the capitalization threshold not being depreciated and those valued below the threshold which are activated, and take appropriate action.
User organizations may capitalize items that do not individually meet the capitalization threshold but is above the threshold in aggregate (i.e. motor pools).	External - User	SOP is to review DPAS provided reports on a regular basis which identify assets valued above the capitalization threshold not being depreciated and those valued below the threshold which are activated, and take appropriate action.
DPAS users may not capitalize ancillary costs with assets to capture full cost.	External - User	SOP is for appropriate users to be trained in DPAS Asset Receiving before they are permitted to gain access. Training includes discussions on ancillary costs and how to use the drop down menu procedure to add them in.
User organization may not capitalize assets for which it has preponderant use.	External - User	Preponderant use is not applicable for General Purpose Equipment (GPE)
DPAS user may misclassify GPE as another asset class or vice versa.	External - User	SOP is to review DPAS online help for assistance in determine asset class and to call the DPAS support desk for further assistance if confusion remains. Management review of quarterly reports may identify misclassified items.
Physical access to DPAS system may not be properly protected at user organizations.	External - User	Access to DPAS refresh is Public Key Infrastructure (PKI)/Common Access Card (CAC) enabled and a physical security SOP is in place

FRSEs reviewing General Property should ensure they have the proper controls to address the risks identified above. In addition, risks associated with Military Equipment were identified by AT&L. These areas should be reviewed to ensure proper controls are in place:

Table 5 – Military Equipment Summary of Issues EXAMPLE

Summary	Description of Issue	Materiality of the Issue
Component Program Managers are not updating their military equipment assets timely in Capital Assets Management System (CAMS)-Military Equipment (ME).	The P&E Policy Office has no assurance that Component PMs are updating their military equipment acquisitions and disposal timely in CAMS-ME.	If assets are not updated for quarterly and year-end financial reporting, the Component is misstating its military equipment financial value.
Component Financial Managers are not providing complete and/or correct Financial Account Codes (FACs) related to their Military Equipment programs.	The P&E Policy Office has no assurance that Component PMs are providing complete and accurate Financial Account Codes (FACs) for each program.	FACs are used to pull valuation data from the Core Accounting Systems. If the FACs are incomplete or inaccurate the military equipment financial statements will be misstated.
Inaccurate Useful Life Estimate	ME depreciation may be inaccurate due to incorrect UL estimate provided by program manager.	Inaccurate useful life estimates in CAMS-ME.
Incomplete Asset Update	ME valuation may be inaccurate due to Component Program Managers not completing asset updates by the end of each quarter.	Asset updates not completed in CAMS-ME by quarter-end.
Manual Updates Entered Incorrectly	Manual updates (asset placed in service or disposal date) may be entered incorrectly by the Component PM.	Misstated assets in CAMS-ME.
Unsupported Manual Adjustment	Manual adjustments to program data may be made without adequate supporting documentation.	No supporting documentation.
Inaccurate Attestation Changes	Component Program Manager (PM)/Financial Manager (FM) may communicate inaccurate changes on end of year attestation reports.	PM/FM attest to inaccurate changes.
Unverified Quarterly Attestation	ME valuation may be inaccurate due to Component not verifying quarterly attestation reports to financial data.	PM/FM did not compare quarterly reports to financial data.
Incorrect or Missing Business Enterprise Information Services (BEIS) Financial Account Code (FACS)	Expenditures may be inaccurate due to incorrect or missing FACs provided by Component FM.	Misstated expenditures.
Core Acct System Deficiencies	ME valuation may be inaccurate due to deficiencies in Component core accounting systems. CAMS-ME picks up expenditure data from BEIS, which interfaces directly with each Component's core accounting system.	Info BEIS received from Component accounting system is inaccurate.
Misrepresented General Property Plant and Equipment (PPE) as ME	Other assets such as General PPE may be misrepresented as ME.	Assets recorded in an inaccurate category.

Summary	Description of Issue	Materiality of the Issue
ME May Not Exist	ME reported on the financial statements may not exist as of the financial statement reporting date.	ME assets do not exist on the reporting data.
Unsupported Transactions	CAMS-ME users may not have documentation (i.e. DD 250, lease agreements) to support transactions* entered into CAMS-ME.	Asset may be unsupported.
Preponderant use is not compliant with Generally Accepted Accounting Principles.	The DoD FMR requires financial reporting of real property by the Preponderant User. However, the Preponderant User methodology is not compliant with Generally Accepted Accounting Principles and does not adequately disclose the full cost of operations. The Office of the Under Secretary of Defense (Comptroller) had stated that they recognize the policy is non-compliant and are working on an alternative compliant policy. <u>This is an example of a Policy update needed. The DoD FMR is being adjusted to mitigate the risk.</u>	.

All FRSE with military equipment should ensure proper controls are documented to reduce these risks.

Step 8 – Re-test Effectiveness of Solutions

New and revised policies, processes and procedures should be evaluated to ensure that the intended result is occurring. Ensure that new control solutions produce the desired effect.

- Prepare Test Plans and test controls
- Assess controls
- Identify material weaknesses and/or significant deficiencies
- Create corrective action plans
- Re-test controls
- Document results
- Confirm Agency monitoring activities

Step 9 - Approaching Financial Improvement

Prepare and manage FIPs and corrective action plans and enter into the FIAR Tool.

Step 10 – Monitoring or Sustainment

Each process is regularly monitored for sustained effectiveness of controls and situational changes.

3.2 Evidential Matter

During the testing, obtain evidential matter to support all management's assertions, statements, findings, and recommendations. Types of evidence include: 1) analytical evidence, which includes computations or the reviewing of relationships; 2) testimonial evidence, which includes both internal and external responses to inquiries or interviews; 3) documentary evidence, which is any permanent evidence that has been created; and 4) physical evidence, which is obtained through observation or direct inspection.

The third auditing standard of fieldwork states:

The auditor must obtain sufficient appropriate audit evidence by performing audit procedures to afford a reasonable basis for an opinion regarding the financial statements under audit. (AU Section 326.01)

Just as there are different forms of evidence, evidences can be obtained in different ways. General procedures to obtain evidence include:

- **Analytical** – use techniques that highlight relationships. For example, compare the environmental liabilities reported in FY 2004 for a specific program to the environmental liability reported in FY 2005 for that same program. Look for large increases or decreases and support for the fluctuation.
- **Tracing** – start with a source document and follow it through the process to the financial statements. This verifies the “completion assertion” by ensuring the source document was captured in the financial statements.
- **Vouching** – start with an amount in the financial statements and work back through the process to the source document. This procedure verifies the “existence or occurrence assertion,” ensuring that the amount recorded in the financial statements has supporting documentation justifying its inclusion.
- **Computation** – check the mathematical accuracy.
- **Inquiry** – question or interview individuals to obtain testimonial evidence.
- **External Confirmation** – request information from third parties to corroborate evidence.
- **Inspection** – obtain documentation from examining material such as records or documents. For example, examine the property record for an environmental liability site to verify the assumptions used when developing the estimate.
- **Observation** – directly observe actions performed by the staff.
- **Re-performance** - re-performance involves repeating, either in whole or in part, the same procedures performed by employees, particularly recalculations to ensure mathematical accuracy. Re-performance may involve some of the other techniques previously mentioned, such as comparing or counting. For example, comparing a vendor's invoice with the corresponding purchase order and receiving report, where there is evidence in the form of initials on a document that an employee previously made that comparison, is re-performance.

Relating the evidence obtained from testing procedures to the test objectives is an iterative process of accumulating, analyzing, and interpreting information in light of the tester's expectations, past experience with the entity's management, generally accepted accounting principles, good

management practices, and common sense. Procedures performed to meet one testing objective for one account frequently generate information that requires further action by the tester to achieve that particular test objective or other testing objectives related to that particular account or other accounts. Evidence that raises questions, for example, about recorded revenues also may raise questions about the adequacy of the allowance for inventory obsolescence, which in turn will require the tester to accumulate and analyze additional evidence.

3.3 Sufficient Appropriate Audit Evidence

Sufficiency is the measure of the quantity of audit evidence. Appropriateness is the measure of the quality of audit evidence, that is, its relevance and its reliability in providing support for, or detecting misstatements in, the classes of transactions, account balances, and disclosures and related assertions. The auditor should consider the sufficiency and appropriateness of audit evidence to be obtained when assessing risks and designing further audit procedures. The quantity of audit evidence needed is affected by the risk of misstatement (the greater the risk, the more audit evidence is likely to be required) and also by the quality of such audit evidence (the higher the quality, the less the audit evidence that may be required). Accordingly, the sufficiency and appropriateness of audit evidence are interrelated. However, merely obtaining more audit evidence may not compensate if it is of a lower quality.

The evidence obtained should be both competent and sufficient. To be competent, evidence must be both relevant and reliable.

To be relevant, evidence must affect the testers' ability to accept or reject a specific financial statement assertion. The tester reaches a conclusion on the financial statements taken as a whole through a series of judgments made throughout the testing about specific financial statement assertions. Each piece of evidence obtained is evaluated in terms of its usefulness in corroborating or contradicting an assertion by management. Evidence is relevant to the extent that it serves either of the purposes.

Confirmations do not provide evidence about collectability, completeness, or rights and obligations. A confirmed account may not be collectible because the debtor does not intend or is unable to pay; receivables may exist that have not been recorded and therefore cannot possibly be selected for confirmation. Similarly, physically inspecting and counting inventory gives evidence about its existence, but not about its valuation or about the entity's title to it.

Evidence also must be reliable if it is to be useful in an audit. The Financial Accounting Standards Board definition of reliability is also appropriate in the context of testing evidence. Reliability is "the quality of information that assures that information is reasonably free from error and bias and faithfully represents what it purports to represent." The reliability of testing evidence is influenced by several factors.

- **Independence of the source.** Evidential matter obtained by the tester from independent sources outside the entity being audited is usually more reliable than that from within the entity. Examples of evidence from independent sources include a confirmation from a state agency of the number of shares of common stock authorized to be issued, and a confirmation from a bank of a cash balance, a loan balance, or securities held as collateral. (The higher level of reliability that such evidence provides does not mean that errors in confirmations of

this nature never occur.) In contrast, evidence arising from inquiries of entity personnel or from inspecting documents provided by management is usually considered less reliable from the tester's viewpoint.

- **Qualifications of the source.** For evidence to be reliable, it must be obtained from people who are competent and have the qualifications to make the information free from error. (The independence-of-the-source criterion addresses the possibility of deliberate errors in the evidence; the qualifications-of-the-source criterion addresses the possibility of unintentional errors in the evidence.) Answers to inquiries about pending litigation from the entity's lawyers are usually more reliable than answers from persons not working in the legal department. The accounts payable clerk probably knows the true routine in the accounts payable section of the accounting department better than the controller does. Furthermore, testers should challenge their own qualifications when evaluating evidence they have gathered.
- **Internal control.** Underlying accounting data developed under satisfactory internal control is more reliable than similar data developed under less effective internal control.
- **Nature of the evidence.** Evidence varies in the extent to which it is fact-based versus opinion-based. Evidence obtained by a tester's direct, personal knowledge through counting, observing, calculating, or examining documents may be thought of as fact-based. Evidence based on the opinions of others, such as the opinion of an appraiser about the value of an asset acquired by the entity in a non-monetary transaction, the opinion of a lawyer about the outcome of pending litigation, or the credit manager's opinion about the collectability of outstanding receivables, may be thought of as opinion-based. Evidence that is opinion-based often requires more judgment by both the preparer (i.e., the appraiser, the lawyer, or the credit manager) and the tester than does evidence that is fact-based and, therefore, may be less reliable than fact-based evidence. Sometimes, however, only opinion-based evidence is available to the tester for evaluating a particular financial statement assertion.

Test Sampling and Sample Size

Test sampling is the application of a test procedure to less than 100 percent of the items within an account balance or class of transactions for the purpose of evaluating some characteristic of the balance or class. There are two general approaches to test sampling: **non-statistical and statistical**. Both approaches require professional judgment in planning, performing, and evaluating a sample and in relating the test evidence produced by the sample to other test evidence when forming a conclusion about the related account balance or class of transactions.

The sufficiency of test evidence is related to the design and size of a test sample, among other factors. The size of a sample necessary to provide sufficient test evidence depends on both the objectives and the efficiency of the sample. For a given objective, the efficiency of the sample relates to its design; one sample is more efficient than another if it can achieve the same objectives with a smaller sample size. In general, careful design can produce more efficient samples. Evaluating the appropriateness of test evidence is solely a matter of judgment and is not determined by the design and evaluation of a test sample. The choice of non-statistical or statistical sampling does not affect auditing procedures to be applied, the appropriateness of the test evidence obtained with respect to individual items in the sample, or the actions that might be taken in light of the nature

and cause of particular misstatements. Sample items should be selected in such a way that the sample can be expected to be representative of the population. Therefore, all items in the population should have an opportunity to be selected. For example, haphazard and random-based selection of items represents two means of obtaining such samples.

Due to time and resource constraints, it would be impractical to test every item for each control. Sampling should be used to limit the number of transactions and other items tested, yet ensure the testing is adequate for conclusions to be drawn. For Appendix A, the selection of sample size is based on the professional judgment, expert knowledge of the reviewer, and CFO Council guidance.

Attribute sampling includes selecting a sample of transactions from the total population and verifying the presence or absence of certain qualities. The result of each test is mutually exclusive (i.e., the control passes or fails the test).

The items tested should support the preliminary assessment of control risk as low and thus test effectiveness of these controls. Management should consider the frequency and complexity of the transaction type when determining sample size. Below is a guideline for determining an adequate sample size:

Transaction Occurrence	Sample Size
Annually	1
Quarterly	2
Monthly	3
Weekly	10
Daily	30
Recurring	45

Note that the above table only provides guidance in relation to sample size and that management should use judgment and consider additional factors, such as the significance of the control and whether the control is manual or automated, when developing sample size. Management should also use judgment when designing procedures to ensure that specific control objectives and assertions are sufficiently supported by the internal control.

Performance and Evaluation

Auditing procedures that are appropriate for the particular test objective should be applied to each sample item. Consideration of unexamined items to be misstated could lead to a conclusion that the balance or class contains material misstatement; consider alternative procedures that would provide sufficient evidence to form a conclusion. There are several acceptable ways to project misstatements from a sample. For example, select a sample of every twentieth item (50 items) from a population containing one thousand items. If discovered overstatements of \$3,000 in that sample, project a \$60,000 overstatement by dividing the amount of misstatement in the sample by the fraction of total items from the population included in the sample. Add that projection to the misstatements discovered in any items examined 100 percent. This total projected misstatement should be compared with the tolerable misstatement for the account balance or class of transactions, and appropriate consideration should be given to sampling risk. If the total projected misstatement is less

than tolerable misstatement for the account balance or class of transactions, consider the risk that such a result might be obtained even though the true monetary misstatement for the population exceeds tolerable misstatement.

Example. If the tolerable misstatement in an account balances of \$1 million is \$50,000 and the total projected misstatement based on an appropriate sample is \$10,000, reasonable assurance may exist that there is an acceptably low sampling risk that the true monetary misstatement for the population exceeds tolerable misstatement. On the other hand, if the total projected misstatement is close to the tolerable misstatement, conclude that there is an unacceptably high risk that the actual misstatements in the population exceed the tolerable misstatement. Using professional judgment in making such evaluations is recommended.

In addition to the evaluation of the frequency and amounts of monetary misstatements, consideration should be given to the qualitative aspects of the misstatements. These include (a) the nature and cause of misstatements, such as whether they are differences in principle or in application; errors or caused by fraud; or due to misunderstanding of instructions or to carelessness, and (b) the possible relationship of the misstatements to other phases of the audit.

If the sample results suggest that planning assumptions were incorrect, take appropriate action. For example, if monetary misstatements are discovered in a substantive test of details in amounts or frequency that is greater than is consistent with the assessed levels of inherent and control risk, alter risk assessments. Also consider whether to modify the other tests that were designed based upon the inherent and control risk assessments. For example, a large number of misstatements discovered in confirmation of receivables may indicate the need to reconsider the control risk assessment related to the assertions that impacted the design of substantive tests of sales or cash receipts.

Projected misstatement results for all test sampling applications and all known misstatements from non-sampling applications should be considered in the aggregate along with other relevant test evidence when evaluating whether the financial statements taken as a whole may be materially misstated. Either a non-statistical or statistical approach to test sampling, when properly applied, can provide sufficient test evidence.

Statistical sampling helps (a) to design an efficient sample, (b) to measure the sufficiency of the test evidence obtained, and (c) to evaluate the sample results. By using statistical theory, quantify sampling risk to assist in limiting it to an acceptable level. However, statistical sampling involves additional costs of training of testers, designing individual samples to meet the statistical requirements, and selecting the items to be examined. Because either non-statistical or statistical sampling can provide sufficient test evidence, considering their relative cost and effectiveness in each circumstances.

Table 6 - Factors Influencing Sample Sizes for a Substantive Test of Details in Sample Planning

Factor	Smaller sample size	Larger sample size	Related factor for substantive sample planning
a. Assessment of inherent risk.	Low assessed level of inherent risk.	High assessed level of inherent risk.	Allowable risk of incorrect acceptance.
b. Assessment of control risk.	Low assessed level of control risk.	High assessed level of control risk.	Allowable risk of incorrect acceptance.
c. Assessment of risk for other substantive tests related to the same assertion (including analytical procedures and other relevant substantive tests).	Low assessment of risk associated with other relevant substantive tests.	High assessment of risk associated with other relevant substantive tests.	Allowable risk of incorrect acceptance.
d. Measure of tolerable misstatement for a specific account.	Larger measure of tolerable misstatement.	Smaller measure of tolerable misstatement.	Tolerable misstatement.
e. Expected size and frequency of misstatements.	Smaller misstatements or lower frequency.	Larger misstatements or higher frequency.	Assessment of population characteristics.
f. Number of items in the population.	Virtually no effect on sample size unless population is very small.		

3.4 SITE TESTING

Per the CFO Council Implementation Guide, functional or process managers must consider the agency's structure when planning an assessment of internal controls within the agency. If an agency has multiple locations, the management team must develop, document and communicate an appropriate testing approach, to achieve economies of testing while maintaining the ability to provide reasonable assurance on the effectiveness of controls. A testing approach should include, but is not limited to how the sites and/or sample(s) will be selected and how a rotation schedule will impact the locations.

Site Selection

Site selection is largely driven by materiality considerations. As defined in Financial Accounting Standards Board (FASB) Statement of Financial Concepts No. 2, *Qualitative Characteristics of Accounting Information*, materiality represents the magnitude of an omission or misstatement of an item in a financial report that in 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.

Using financial data generated from the reporting system of record, management and/or designated staff should generate a materiality matrix as follows:

1. Examine the Component's financial statements and determine the material segments or business events, based on the DoD threshold for financial statement materiality;
2. Examine the financial statements at the organization level (i.e. NAVAIR, NAVSEA, NAVFAC, etc.) and identify the relevant account balances for each material segment or business event, and for any "immaterial" segments also targeted by the DoD for inclusion;
3. Identify organizations with material transaction amounts. Organizational-level materiality should be designated by the Component's Senior Assessment Team;
4. Identify sub-units with material transaction amounts for the organizations identified in number three (3) above, if necessary;
5. For each material organization and segment combination identified in numbers three (3) or four (4) above, specify the types of records (source documents) retained, location(s) of the records, and a point of contact for each organization.

Having identified the material organizations and business events or segments within the Component, the internal control unit should validate the materiality determinations through consultation with the organizations and sub-units identified. These entities will then identify the specific locations to be visited during the testing phase of the internal control assessment process. The selection of locations may be driven purely by materiality considerations, but is usually also influenced by other qualitative and quantitative factors. Some factors to be considered are:

- Significance of the location to the organization or overall Component. Locations that house significant information technology centers, business cycles or accounting applications should be selected for testing even if the associated line item balances for that location are quantitatively immaterial.
- Results of prior internal and external audits. Problems noted in prior audit exercises could indicate ongoing areas of concern for the current evaluation period, with more recent audit results having a higher degree of relevance to the current planning efforts.
- Results of previous control testing exercises. The results of previous control testing exercises may indicate a need to maintain a focus on certain locations, segments or transactions.
- Management's preliminary assessment of inherent and control risk. Locations at which the inherent and/or control risks are high generally require more extensive testing than locations at which those risks are expected to be low.
- Centralization of accounting. A high degree of centralization will influence the selection of the central location for the bulk of testing activities, with limited tests performed at other locations.

- Uniformity of systems. Where there is greater uniformity of significant systems across locations, reasonable assurance over the operating effectiveness of those systems may be gained from testing in fewer locations. Where systems vary widely across locations, or where users have the opportunity to customize applications, reasonable assurance can only be obtained by testing all versions of the system – thereby increasing the number of sites selected. The planning team should then consider the significance and impact of each system on financial reporting and select sites to reflect an appropriate cross-section of all locations.
- Three-year cycle of testing. The DoD has adopted the rotation plan recommended in SAS No. 110.42, which suggests that key controls (which have already demonstrated operating effectiveness through the results of testing) may be tested just once in each three-year period. Therefore all controls need not be tested each year, and depending on the distribution of key controls throughout various locations, site selection may be adjusted accordingly on a rotating basis.

Where controls are performed in multiple locations, process managers should also consider: the consistency with which control procedures are conducted at the various locations; the portion of activity flowing through each location; and the risk of misstatement associated with the controls to aid in targeting the locations that will ultimately be included in test work.

Once site selection has been completed, the organizations will prepare and submit to management's internal control lead a schedule for on-site testing by segment, to include site locations, personnel involved, anticipated human resource, reporting or systems impact(s), if relevant, and start and end dates. The Component's internal control lead will consolidate testing schedules across the Component by segment, and submit the consolidated schedule in the FIAR Tool at or before the end of the first quarter of the fiscal year.

4.0 DOCUMENTATION

Management should ensure that documentation is prepared in sufficient detail to provide a clear understanding of the work performed (including the nature, extent, and timing and results of audit procedures performed), the evidence obtained and its source, and the conclusions reached. The Components are encouraged to reference the Financial Audit Manual (FAM) for further guidance that describes detailed audit documentation requirements. Documentation is a key part for achieving audit readiness, and due diligence may allow the information to be used in future tests of controls.

Documentation Retention. All DoD Components **are required** to retain evidential material collected in testing process that supports the assessments made and conclusions reached. Testers are strongly encouraged to save all documents. All test results should be documented in PSSC format i.e. Purpose, Source, Scope and Conclusion. References should also be made in the Testing Comfort Matrix (TCM). All documentation should be established and retained in such a way that if another tester tries to re-perform the testing work, s/he reaches the same conclusion. All efforts should be made in developing common share drive with limited access. Where necessary, hard copies should be retained as well. Senior assessment team should decide during the planning phase as to where to keep such documentation. Refer to section 4.1.1 for further notes on documentation retention policies.

5.0 MONITORING AND SUSTAINMENT

It is imperative that the Department be able to continually confirm that progress, once made, is being sustained. Failure to do so is a material risk to the Department's ability to attain an annual unqualified audit opinion on its financial statements. To sustain improvements, management must continue the financial policies, procedures, and internal controls that supported management's initial audit-readiness assertions, and maintain momentum toward overall improvement.

Phase 4 of the business rules, Audit Readiness Sustainment, calls for continually monitoring progress already made and annually verifying that audit-ready segments remain audit ready while discovery and correction is being completed on other segments. Four fundamentals of the financial environment are reviewed during the Sustainment phase:

- Internal control policies and procedures
- Business processes
- Automated systems
- Compliance with laws and regulations

Monitoring and Reporting Sustained Progress

Segments that have been validated as audit ready are continually reviewed, monitored, and reported on by management and the entity's audit committee or senior assessment team. Any material changes to the segment's dependencies or newly identified deficiencies are reported to the OUSD(C). When material changes have been made that effect the segment's audit readiness status, then the segment, or the changes to the segment, is revalidated as audit ready. Additionally, any material weaknesses that are identified during the sustainment phase are reported in the entity's annual Statement of Assurance and corrective actions are taken. Once material weaknesses are corrected, the segment is revalidated as audit ready.

Annual Evaluations Using Appendix A as Guidance

Annual evaluations of each audit-ready segment are being completed using OMB Circular A-123, "Management's Responsibility for Internal Control," Appendix A "Internal Controls over Financial Reporting" as guidance. A-123 Appendix A, which is also applied during the Discovery and Correction phase, incorporates continual monitoring necessary to assure that corrective actions remain effective. The evaluation is performed by a Service Audit Agency, if available. Otherwise, management may choose to use either the Office of the Inspector General (OIG) or an Independent Public Accountant, depending on the risk and materiality of the segment.

6.0 FOCUS AREAS AND DELIVERABLE SCHEDULE

The segments and focus areas for the September 2009 FIAR Plan and the ICOFR focus areas are identified in table 7 as follows:

Table 7 - 2009 ICOFR Focus Areas

**End-to-End Business Process and FIAR Segment
2009 ICOFR Focus Areas**

End-to-End Business Processes and FIAR Segments	Audit Readiness Validation											% Assets % Liabilities
	Army			Navy			Air Force		DLA		ODOs and Other FRSEs	
	GF	WCF	USACE	GF	WCF	USMC	GF	WCF	GF	WCF		
Acquire to Retire (A2R)												
Military Equipment	X	NA	NA	X	NA	X	X	NA	N/A		MDA USSOCOM	23%
Real Property	X	X	X	X	X	X	X	X	X	X	DECA GF WCF DFAS WCF* DIA DISA GF* WCF DTRA MDA NGA NSA USSOCOM	7%
General Property & Equipment	X	X	X	X	X	X	X	X	X	X	CBDP DCAA DECA GF WCF DFAS WCF TMA DIA DISA GF* WCF DSS DTRA MDA NGA NSA USSOCOM	1%
Internal Use Software	X	X	X	X	X	X	X	X	X	X	DODIG* DFAS GF WCF DISA GF* DIA NGA NSA	0%
* Hire to Retire (H2R)												
Military Pay	X			X		X	X		N/A		N/A	
Civilian Pay	X			X			X		X	X	ALL	
Federal Employment Compensation Act (FECA) Liabilities - Applicable if material to DoD statements	X	X	X	X	X	X	X	X	X	X	ALL	
Procure to Pay (P2P)												
Services	X	X	X	X	X	X	X	X	X	X	ALL	
Order to Cash (O2C)												
Supply, Depots, and Other Working Capital Fund Activities		X			X			X		X		
Reimbursable Authority	X		X	X		X	X		X	X	ALL	
Foreign Military Sales (FMS)	X			X			X		X	X		
Plan to Stock (P2S)												
Operating Material & Supplies	X	X		X	X	X	X	X		X	SMA DTRA MDA USOCOM	9%
Inventory		X			X			X		X	DECA WCF* DTRA	6%
Environmental Liabilities (EL)												4%
Defense Environmental Restoration Program (DERP)	X		X	X		X	X			X		
Non-DERP	X		X	X			X			X		
Base Realignment And Closure (BRAC)	X		X	X			X			X		
Weapon Systems	X			X		X	X			N/A		
Chemical Weapons Disposal	X			N/A		N/A	N/A			N/A		

Budget to Report (B2R)											
Budgeting - Authorizations Received										X	
Record Warrants	X		X	X		X	X				If Applicable
Record Apportionments	X		X	X		X	X				If Applicable
Allocate and Allot Funds	X	X	X	X	X	X	X	X	X	X	All
Financial Reporting – Compilation	X	X	X	X	X	X	X	X	X	X	All
Funds Balance With Treasury (FBWT)	X	X	X	X	X	X	X	X	X	X	
Reconciliation	X										All
Cash & Other Monetary Assets (If material to statements)	X		X	X		X	X		X	X	All
Medicare Eligible Retiree Health Care Fund											MERHCF
Other Health Care											TMA, SMA
Military Retirement Trust Fund											MRTF
Investments	X		X	X			X				MERHCF MRTF
Accounts Payable/Other Liabilities											All - DFAS (lead)
Accounts Receivable/Other Assets											All - DFAS (lead)
Financial Statement Audit											

* Hire to Retire includes point of authorization through point of delivery. This includes pays, allowances, deductions, allotments, and disbursements.

Previous Focus New Focus Area for 2009

In addition to the assigned focused areas above, the FSREs with Unqualified Opinions, Qualified Opinions and those undergoing audit must apply the ICOFR process to all material lines on the financial statements undergoing audit. This also applies to TMA Components (Contract Resource Management and the Uniformed Services University of the Health Sciences) who are undergoing validation through examination prior to audit.

Components shall submit the ICOFR SOA based on their management reviews of Internal Controls over financial reporting. Components responsible for submitting more than one SOA, i.e., General Fund and Working Capital Fund, are to submit deliverables supporting each SOA under separate cover – one set of deliverables for General Fund, and one set for Working Capital Fund. The FSREs are to submit via their respective Entity Senior Assessment Team, to the Office of the Under Secretary of Defense (Comptroller)’s FIAR Directorate, Attention: ICOFR Project Manager. Item F, the ICOFR SOA, will be incorporated into the overall FMFIA SOA and submitted to the Secretary of Defense as described in the Annual FMFIA Overall Statement of Assurance Guidance. A copy of the ICOFR tabs is due by June 29, 2009 to the FIAR Directorate via the FIAR Tool.

A list of SAT members, their titles, and the Component’s SAT Charter is due to the ICOFR Program Manager with the first deliverable on December 20, 2008 if changes have been made to the copy on the FIAR portal. The FSRE Appendix A point of contact (POC) for each SAT shall post the deliverables on the FIAR portal. In addition, a memorandum signed by the chair of the FRSE SAT certifying the accuracy of the information posted to the portal must also be uploaded to the FIAR portal.

Each deliverable posted to the FIAR portal must be followed with a cover transmittal memorandum signed by the chair of the Component SAT stating that the deliverable has been prepared in accordance with DoD implementation guidance as stated above. This memorandum is to be posted to the FIAR portal.

Table 8 - Schedule of Deliverables

Due Date for Submission to FIAR Directorate / ICOFR Manager	Deliverable
Assessing and Documenting	
A December 19, 2008	A. Memo from Component SAT Chair – Process Narratives, Flow Charts, and Organizational Charts for Assigned Areas, Component-level Control Environment Document such as a Management Code of Conduct or Ethics Policy, SAT membership and Charter (if changed from previous submission).
B March 2, 2009	A. Memo from Component SAT Chair – Completed Risk Analysis Form, FISMA Report (if applicable), List of Auditor-Identified Material Weaknesses Related to Financial Reporting. B. Weakness Dependencies Reports submitted in FIAR Tool Collaboration Site
C May 1, 2009	A. Memo from Component SAT Chair – Completed Detailed Test Plans (without results) in electronic format only.
D June 2, 2009	A. Corrective action plans in FIAR Tool for Weaknesses Reported in Collaboration Site
E June 29, 2009	A. Memo from Component SAT Chair – SAT approved ICOFR tabs of Annual FMFIA SOA. Control Assessment Form with test results). Milestone information must be completed with the ICOFR tabs. B. All corrective action plans must be entered into DoD Financial Improvement Tool * List of accomplishments related to material weaknesses. * Those without direct access must provide all corrective action plans in the FIP format to the program office by June 20 th . The Intel community must provide all corrective action plans in the FIP format to the program office by June 20 th .
Reporting	
F September 1, 2009	A. Statement of Assurance as required by FY 2009 Guidance for the Preparation of the Statement of Assurance

ATTACHMENT 1 – Test Plan (Deliverable C)

Test Plan	
Entity	
Preparer	Name of person who is completing the test plan
Acct Line	Implementation area or business cycle
Control #	
Risk	
Internal Control Currently in Place	
Control Type	Identify whether the control is Manual or Automated
Control Frequency	How often the control is performed (e.g. Continuous, Daily, Weekly, Bi-weekly, Monthly, Quarterly, Annually)
Testing Period	The timeframe when the test samples are being reviewed (1 year’s worth, 1 week’s worth, 1 day’s worth/ 4 th work day, 2 nd quarter).
Test Method	Identify the basic control test that is performed on the key control. The four basic types of tests include Inquiry/Interview, Inspection, Observation, and Re-performing a given control procedure. External Assurance is also acceptable for internal controls performed by external sources.
Documentation Location	If applicable to the testing, cite the location of the documents to be sampled and the office responsible for maintaining the documentation.
Population and Sample Size	A population is the total number of times the control is performed within the given time period, from which you wish to describe or draw conclusions. A sample is a group of units selected from the population. By studying the sample it is hoped to draw valid conclusions about the larger group. The sample size is the number of items selected for review.

Criteria for Effectiveness/ Tolerance Rate	State the tolerance rate: How many exceptions are acceptable for the test to still be successful? Provide the decision basis for establishing your tolerance rate. The tolerance rate is the maximum allowable number of deviations from the prescribed control. Give sample size and number of allowable exceptions.
Test Description	Describe how the test plan will be performed, where it will be performed and who will be performing the testing.
Test Strategy	Describe how the test is intended to validate that the control effectively mitigates identified risk as designed and operated.
Test Results	How many samples passed/failed testing?

See the Comptroller website for blank test plan forms and additional instructions.

Once the test plan is developed, the criteria should be integrated into a testing document. The testing document tracks the test work performed to ensure all control objectives are tested for effectiveness for each sample selected and serves as a worksheet for the tester.

ATTACHMENT 2 – Part of Deliverable B: Chart 1: Risk Analysis Form

RISK ANALYSIS

1 Entity	Defense Aircraft Agency	2 Account Line		Other Liabilities	4 Preparer	First N. Last
		3 Business Cycle/ Segment, Accounting Application		(+/-) Accrued Leave Liability	5 Preparer's Phone #	(123) 456-7890
6 Control #	7 Risk	8 Assertion	9 Inherent Risk	10 Internal Control Currently In Place	11 Preliminary Control Risk	12 Internal Control Test Method to Be Used
1	SF 1150 is generated with errors	Presentation and Disclosure	Moderate	DAA HRO meets with transferred in employee and obtains leave balance from last LES for determination of interim leave balance	Low	Inspection
2	SF 1150 may not be timely received by losing HRO resulting in incomplete OPF	Completeness	Low	NO FURTHER ACTION NECESSARY		
3	Delay in submission of SF 1150 and OPF to gaining HRO resulting in understated liability	Rights and Obligations	Moderate	Losing HRO pursues SF 1150 from losing payroll office	Low	Inspection
4	Employee takes leave prior to receipt of SF 1150 at gaining payroll office and leave is not captured	Completeness	Moderate	DCPDS interfaces with DCPS; Gaining payroll office makes adjustments in DCPS once SF 1150 is received	Low	Inspection
5	Manual Data entry to DCPDS increases the chances of erroneous or incorrect Data input. Wrong account codes can be assigned or wrong amount can be input. The codes in the uploading might not be current or updated.	Accuracy	Moderate	None identified	High	Corrective Action Plan
6	Output by DCPDS system is based on the manual entry which could have erroneous/incorrect data. Output could be incorrect or the the output could be corrupt as well.	Accuracy	Moderate	None identified	Moderate	Management will monitor
7	DCPS Remedy Ticket is incorrectly prepared	Rights and Obligations	Moderate	None identified	Moderate	Management will monitor

RISK ANALYSIS

1 Entity	Defense Aircraft Agency	2 Account Line		Other Liabilities	4 Preparer	First N. Last
		3 Business Cycle/ Segment, Accounting Application		(+/-) Accrued Leave Liability	5 Preparer's Phone #	(123) 456-7890
6 Control #	7 Risk	8 Assertion	9 Inherent Risk	10 Internal Control Currently In Place	11 Preliminary Control Risk	12 Internal Control Test Method to Be Used
8	Funded leave liability is not posted/captured when employee transfers from another agency	Rights and Obligations	Moderate	DAA HRO receives leave liability report.	Low	Inspection
9	Data is incorrectly entered into DCPS resulting in DCPS producing inaccurate data	Accuracy	High	DCPS is reconciled to DCPDS data (system edits), CSR makes necessary adjustments to DCPS data	Low	SAS 70 for DCPS
10a	CSR would make incorrect adjustments	Completeness	High	DCPS is reconciled to DCPDS data (system edits), corrections input into system	Low	Inspection of reconciliation; SAS 70 for DCPS
10b	DCPS produces inaccurate data	Accuracy	High	DCPS is reconciled to DCPDS data (system edits), corrections input into system	Low	Inspection of reconciliation; SAS 70 for DCPS
11	Data in Gross Payroll Reconciliation File does not agree to Unpaid Accrued Leave Liability summary and detail reports	Accuracy	High	DAA HRO validates that corrections have been made to the Gross Payroll Reconciliation File and timekeeping records; System edits	Low	Inspection
12	Unpaid Accrued Leave Liability does not agree to unfunded leave totals in DCPS	Accuracy	High	System edits	Low	SAS 70 for DCPS
13	Gross Payroll Reconciliation File is not reconciled with the rejects, therefore, the computed liability may be misstated	Completeness	High	DAA HRO validates that corrections have been made to the Gross Payroll Reconciliation File and timekeeping records; separation of duties	Low	Inspection

RISK ANALYSIS

1 Entity	Defense Aircraft Agency	2 Account Line		Other Liabilities	4 Preparer	First N. Last
		3 Business Cycle/ Segment, Accounting Application		(+/-) Accrued Leave Liability	5 Preparer's Phone #	(123) 456-7890
6 Control #	7 Risk	8 Assertion	9 Inherent Risk	10 Internal Control Currently In Place	11 Preliminary Control Risk	12 Internal Control Test Method to Be Used
14	Since the corrections are to be requested from DFAS by DAA HRO, some of the errors might go undetected or not identified in time. This could cause the reconciliation file to be out of balance.	Existence	Low	DAA HRO validates that corrections have been made to the Gross Payroll Reconciliation File	Low	Inspection
15	Computation is manually prepared for annual leave liability and may be incorrectly calculated	Reporting	High	Supervisory validation of computation	Low	Inquiry/Interview for computation validation
16	Computation of unfunded leave totals is incorrectly calculated	Accuracy	Moderate	Annual review of computation algorithm; system edits	Low	SAS 70
17	Liability may be under/over stated due to manual input errors	Reporting	High	Supervisory validation of DAA Accounting System entries	Low	Inspection
18	Values might be mapped to the wrong trial balance line	Accuracy	Moderate	System programmers assigned responsibility for ensuring current requirements for mapping be programmed into the system	Low	SAS 70 for DCPS Reperform
19	Liability may be under/over stated due to manual reclassification of GLAC 2210	Reporting	High	Supervisory validation of DAA Accounting System entries	Low	Inspection
20	Controls might not provide reasonable assurance that DDRS produces financial statements that are supported by audit trails that are adequate for the financial management entity and external auditors to trace amounts reported in the financial statement	Validity	High	System mapping edits	Low	Inspection
21	Certification of liabilities may occur without all liabilities having been properly classified or included in the financial statements	Completeness	High	Senior management review of statements for reasonableness and soundness using comparative accounting periods	Low	Inspection

ATTACHMENT 3 – Risk Analysis Drop Down List Selections for Column 2

Drop Down List Selections for Column 2 of Risk Analysis and Control Assessment Forms	
Implementation Area Assessed	Business Cycle/Segment, Accounting Application
FBWT	(+) Receipt of Treasury Warrant
	(+) Advances from Customers
	(+) Collections from Earnings/ Order to Cash
	(+) Purchase Returns
	(+) Sales / Revenues
	(-) Procure to Pay
	(-) Appropriation Rescissions
	(-) Payments of Payables
	(-) Payroll/ Hire to Retire
	(-) Appropriations Used
	(+/-) Cash Transfers
	(+/-) Clearing uncleared/undistributed transactions
	(+/-) Other
Investments	(+) Accounts Receivable, Intragovernmental
	(+) Accounts Receivable, Public
	(+) Amortization of Discount
	(+) Appropriation Used
	(+) Interest Received
	(+) Purchase of Investment
	(+) Unliquidated Obligations
	(-) Amortization of Premium
	(-) Appropriation Unexpended
	(-) Sale of Investment
	(+/-) Transfer of Investment
	(+/-) Year-end Close-out
	(+/-) Other
Accounts Receivable (Intragovernmental)	(+) Intragovernmental Revenues/Sales/Order to Cash
	(+) Public Costs
	(+) Duplicate Payments
	(+) Intragovernmental Costs
	(+) Filled Orders
	(+/-) Obligations
	(-) Collections
	(+) Cancelled year Receivables
	(+/-) Elimination Entries
Accounts Receivable (Public)	(+) Revenues from Public/Order to Cash
	(+) Filled Orders
	(+) Public Debt/Hire to Retire
	(+) Duplicate Payments
	(+) Public Costs
	(+) Filled Orders
	(-) Collections

Drop Down List Selections for Column 2 of Risk Analysis and Control Assessment Forms	
Implementation Area Assessed	Business Cycle/Segment, Accounting Application
Accounts Receivable (Public)	(-) Allowance for Loss on Accounts Receivable
	(+/-) Balances Brought Forward
	(+) Cancelled year Receivables
Inventory	(+) Purchases/ Procure to Pay/ Acquisition
	(-) Purchase Returns
	(+) Undelivered Orders
	(+) Unliquidated Obligations
	(-) Appropriation Unexpended
	(+) Appropriation Used
	(-) Intragovernmental Revenues /Order to Cash
	(-) Public Revenues /Sales /Order to Cash
	(+) Purchased for Resale
	(+) Held in Reserve for Future Sale
	(-) Held for Repair
	(-) Excess, Obsolete, and Unserviceable
	(+/-) Raw Materials
	(+/-) Work-in-Process
	(-) Allowance
	(+/-) Finished Goods
	(+/-) Reporting/ Materiel Mgmt
(+/-) Valuation	
Operating Materiel and Supplies (OM&S)	(+) Procurement of OM&S/ Procure to Pay
	(+) Undelivered Orders
	(-) Consumption of OM&S
	(-) Unliquidated Obligations
	(+) Held for Use
	(+) Held in Reserve for Future Use
	(-) Excess, Obsolete, Disposed & Unserviceable
	(-) Held for Repair
	(-) Allowance
	(+/-) OM&S Reporting/ Materiel Mgmt
(+/-) OM&S Valuation	
Real Property	(+) Appropriation Used
	(+) Capital Lease
	(+) Contract for Construction (Obligation)
	(+) Leasehold Improvements
	(+) Procurement of Real Property/Procure to Pay
	(+) Transfer In of Real Property/Property Management
	(-) Capital Lease Amortization
	(-) Contract for Destruction/Property Management
	(+/-) Construction in Progress (CIP) to Real Property
(-) Depreciation	

Drop Down List Selections for Column 2 of Risk Analysis and Control Assessment Forms	
Implementation Area Assessed	Business Cycle/Segment, Accounting Application
Real Property	(-) Destruction of Real Property/Property Management
	(-) Sale of Real Property
	(-) Transfer Out of Real Property
	(+/-) Unliquidated Obligations
	(+/-) Real Property Valuation
	(+/-) Real Property Reporting/Property Management
	(+/-) Preponderant Use Adjustment/ Reporting
	(+/-) Other
Military Equipment	(+) Appropriation Used
	(+) Contract for Construction (Obligation)
	(+) Military Equipment Found on Installation
	(+) Purchases/ Procurement of Mil. Equipment
	(+) Transfer In of Military Equipment
	(+) Work in Progress (WIP) Military Equipment
	(+) WIP to Military Equipment
	(-) Appropriation Unexpended
	(-) Depreciation of Military Equipment
	(-) Disposal of Military Equipment
	(-) Lost Military Equipment
	(-) Sale of Military Equipment
	(-) Transfer Out of Military Equipment
	(+/-) Undelivered Orders
	(+/-) Unliquidated Obligations
	(+/-) Year-end Close-out
	(+/-) Reporting/ Property Mgmt
	(+/-) Valuation
General Property	(+) Appropriation Used
	(+) Capital Lease
	(+) Contract for Construction (Obligation)
	(+) Leasehold Improvements
	(+) Procurement of General Property/Procure to Pay
	(+) Transfer In of General Property/Property Management
	(-) Capital Lease Amortization
	(-) Contract for Destruction
	(+/-) Construction in Progress (CIP) to General Property
	(-) Depreciation
	(-) Destruction of General Property
	(-) Sale of General Property/Property Management
	(-) Transfer Out of General Property
	(+/-) Unliquidated Obligations
	(+/-) General Property Valuation
(+/-) General Property Reporting	

Drop Down List Selections for Column 2 of Risk Analysis and Control Assessment Forms	
Implementation Area Assessed	Business Cycle/Segment, Accounting Application
Internal Use Software (IUS)	(+) Appropriation Used
	(+) Contract for Development (Obligation)
	(+) Procurement of IUS/Procure to Pay
	(+) Transfer In of IUS/Asset Management
	(-) Internal Use Software Amortization/Depreciation
	(+/-) Work in Progress (WIP) to Internal Use Software
	(-) Sale of Internal Use Software/Asset Management
	(-) Transfer Out of IUS/Asset Management
	(+/-) Unliquidated Obligations
	(+/-) Internal Use Software Valuation
	(+/-) Internal Use Software Reporting
	(+/-) Other
Other Assets	(+) Appropriation Used
	(+) Contract for Construction (Obligation)
	(+) Procurement of Other Assets/Procure to Pay
	(+) Transfer In of Other Assets/Asset Management
	(+/-) Work in Progress (WIP) to Other Assets
	(-) Transfer Out of Other Assets/Asset Management
	(+/-) Unliquidated Obligations
	(+/-) Other
Accounts Payable (Intragovernmental)	(+) Acquisition/Procure to Pay
	(+) Order to Cash
	(+) Receipt of Goods / Services
	(+/-) Unliquidated Obligations / Liquidated Obligations
	(+/-) Elimination Entries
	(+/-) Estimated Payables
	(+) Accounts Payable From Cancelled Appropriations
Accounts Payable (Public)	(+) Acquisition/Procure to Pay
	(+) Order to Cash
	(+) Receipt of Goods & Services
	(+) Undelivered Orders
	(-) Unliquidated Obligations
	(+) Accounts Payable From Cancelled Appropriations
	(+) Contractor Withholds
	(+) Interest
	(+/-) Elimination Entries
	(+/-) Balance Brought Forward
	(+) Appropriation Used
FECA Liabilities	(+) Receive Bill from Department of Labor
	(-) Appropriation Unexpended
	(-) Pay Bill from Department of Labor
	(+/-) Unliquidated Obligations

Drop Down List Selections for Column 2 of Risk Analysis and Control Assessment Forms	
Implementation Area Assessed	Business Cycle/Segment, Accounting Application
Environmental Liabilities	(+) Mission Operations
	(-) Clean-up
	(-) Pay Bill
	(+/-) Environmental Protection Agency (EPA) Decisions
	(+/-) Other
Other Liabilities	(+/-) Accrued Leave Liability
	(+) Incur Liability
	(-) Pay Liability
	(+/-) Capital Leases
	(+/-) Insurance
	(+/-) Advances and Prepayments
	(+/-) Deposits Held in Escrow
	(+/-) Transfer In/Out Other Liabilities
	(+) Claims or Other Contingencies
	Health Care
(+/-) Cost of Contracted Care	
(+/-) Funding for Health Care	
(+/-) Code Patient Care Correctly	
(+/-) Valuing Pharmaceutical Costs	
(+/-) 3 rd Party Insurance Billings and Revenue	
(+/-) Other	
Appropriations Received	(+) Receive Appropriation
	(-) Rescind Appropriation
	(+/-) Other
	(+) Unexpended Appropriations – Cumulative
	(+) Unexpended Appropriations – Appropriations Received
	(+) Unexpended Appropriations – Transfers-In
	(-) Unexpended Appropriations – Transfers-Out
	(+) Unexpended Appropriations – Adjustments
	(-) Unexpended Appropriations – Used
	(-) Unexpended Appropriations – Prior-Period Adjustments Due to Corrections of Errors
	(-) Unexpended Appropriations – Prior-Period Adjustments Due to Changes in Accounting Principles

ATTACHMENT 4 – Part of Deliverable E – Control Assessment Form with Test Results, Example

CONTROL ASSESSMENT

1 Entity	Defense Aircraft Agency			2 Account Line	Other Liabilities		4 Preparer		First N. Last	
			3 Business Cycle/Segment, Accounting Application	(+/-) Accrued Leave Liability		5 Preparer's Phone #		(123) 456-7890		
6 Control #	7 Risk	8 Internal Control Currently In Place	9 Control Objective	10 Description of Control Design and Test	11 Was Control Design Effective?	12 Description of Control Application Test	13 Was Control Application Effective?	14 New Control Risk Level	15 Test Results	16 Material Weakness
1	SF 1150 is generated with errors	DAA HRO meets with transferred in employee and obtains leave balance from last LES for determination of interim leave balance	Ensure that there is additional support aside from the SF 1150 to determine interim leave balance	Receipt of both the SF 1150 and LES records should identify errors. Test: Logical Judgement Evaluation	Yes	DAA HRO receives both SF 1150 and LES records before preparation of DCPS Remedy Ticket	Yes	Low	Sample size 2; No exceptions	No
2	SF 1150 may not be timely received by losing HRO resulting in incomplete OPF	NO FURTHER ACTION NECESSARY								No
3	Delay in submission of SF 1150 and OPF to gaining HRO resulting in understated liability	Losing HRO pursues SF 1150 from losing payroll office	HRO pursues SF 1150	Requests by gaining HRO results in receipt of missing SF 1150. Test: Logical Judgement Evaluation	Yes	Gaining HRO makes request to losing HRO	Yes	Low	Sample size 2; No exceptions	No
4	Employee takes leave prior to receipt of SF 1150 at gaining payroll office and leave is not captured	DCPDS interfaces with DCPS; Gaining payroll office makes adjustments in DCPS once SF 1150 is received	Ensure that information in DCPS accurately reflects leave balance	DCPS interfaces with DCPDS and gaining payroll office will capture leave and make any necessary adjustments in DCPS. Test: Logical Judgement Evaluation	Yes	CSR reviews information in DCPS to identify and makes needed corrections	No	Low	Sample size 2; No exceptions	No
5	Manual Data entry to DCPDS increases the chances of erroneous or incorrect Data input. Wrong account codes can be assigned or wrong amount can be input. The codes in the uploading might not be current or updated.	None identified	To test that correct and complete information is entered in the system.	Employee personal data is entered into DCPDS. Test: Logical Judgement Evaluation	Yes	DAA HRO reviews the file before the upload and reviews the data actually uploaded.	No	High	Corrective Action Plan	No
6	Output by DCPDS system is based on the manual entry which could have erroneous/incorrect data. Output could be incorrect or the the output could be corrupt as well.	None identified	Ensure all leave liability is captured	DCPS interfaces with DCPDS and gaining payroll office will capture leave and make any necessary adjustments in DCPS. Test: Logical Judgement Evaluation	Yes	CSR reviews information in DCPS to identify and makes needed corrections	Yes	Low	Sample size 2; No exceptions	No

CONTROL ASSESSMENT

1 Entity	Defense Aircraft Agency		2 Account Line	Other Liabilities		4 Preparer		First N. Last		
			3 Business Cycle/Segment, Accounting Application	(+/-) Accrued Leave Liability		5 Preparer's Phone #		(123) 456-7890		
6 Control #	7 Risk	8 Internal Control Currently In Place	9 Control Objective	10 Description of Control Design and Test	11 Was Control Design Effective?	12 Description of Control Application Test	13 Was Control Application Effective?	14 New Control Risk Level	15 Test Results	16 Material Weakness
7	DCPS Remedy Ticket is incorrectly prepared	None identified	Ensure that data in DCPS agrees to data in DCPDS	DCPS interfaces with DCPDS nightly and DCPDS updates DCPS. Test: Logical Judgement Evaluation	Yes	DAA HRO receives copy of Gross Payroll Reconciliation File from DCPS, reconciles, and notifies DFAS payroll for necessary adjustments	Yes	Low	Sample size 10; No exceptions	No
8	Funded leave liability is not posted/captured when employee transfers from another agency	DAA HRO receives leave liability report.	Ensure that accrued leave liability data in DCPS is correct	Reconciliation identifies discrepancies in DCPS and necessary adjustments. Test: Logical Judgement Evaluation	Yes	DAA HRO receives copy of Gross Payroll Reconciliation File from DCPS, reconciles, and notifies DFAS payroll for necessary adjustments	Yes	Low	Sample size 10; No exceptions	No
9	Data is incorrectly entered into DCPS resulting in DCPS producing inaccurate data	DCPS is reconciled to DCPDS data (system edits), CSR makes necessary adjustments to DCPS data	Ensure Gross Payroll Reconciliation File agrees to unpaid accrued leave liability	Validation process should ensure that corrections have been made. Test: Logical Judgement Evaluation	Yes	DAA HRO receives copy of Gross Payroll Reconciliation File from DCPS, reconciles, and notifies DFAS payroll for necessary adjustments	Yes	Low	Sample size 10; No exceptions	No
10a	CSR would make incorrect adjustments	DCPS is reconciled to DCPDS data (system edits), corrections input into system	Ensure Gross Payroll Reconciliation File agrees to the Unpaid Accrued Leave Liability prior to generation of unfunded leave totals by DCPS	DCPS system edits reconcile Gross Payroll Reconciliation File to Unpaid Accrued Leave Liability summary and detail reports prior to computation of unfunded leave liability , noting errors. Test: Logical Judgement Evaluation	Yes	DCPS generates unfunded leave totals after reconciliation of Gross Payroll Reconciliation File to the Unpaid Accrued Leave Liability summary and detail reports	Yes	Low	Sample size 10; No exceptions	No
10b	DCPS produces inaccurate data	DCPS is reconciled to DCPDS data (system edits), corrections input into system	Ensure Gross Payroll Reconciliation File is validated prior to posting to trial balance	Copy of Gross Payroll Reconciliation File is forwarded to DAA HRO for validation prior to computation of Annual Leave Liability. Test: Logical Judgement Evaluation	Yes	DAA HRO receives copy of Gross Payroll Reconciliation File from DCPS, reconciles, and notifies DFAS payroll for necessary adjustments	Yes	Low	Sample size 10; No exceptions	No

CONTROL ASSESSMENT

1 Entity	Defense Aircraft Agency		2 Account Line	Other Liabilities		4 Preparer		First N. Last		
			3 Business Cycle/Segment, Accounting Application	(+/-) Accrued Leave Liability		5 Preparer's Phone #		(123) 456-7890		
6 Control #	7 Risk	8 Internal Control Currently in Place	9 Control Objective	10 Description of Control Design and Test	11 Was Control Design Effective?	12 Description of Control Application Test	13 Was Control Application Effective?	14 New Control Risk Level	15 Test Results	16 Material Weakness
11	Data in Gross Payroll Reconciliation File does not agree to Unpaid Accrued Leave Liability summary and detail reports	DAA HRO validates that corrections have been made to the Gross Payroll Reconciliation File and timekeeping records; System edits	Ensure that DFAS Accounting staff correctly compute annual leave liability	Validation of computation should identify errors. Test: Logical Judgement Evaluation	Yes	Documentation of supervisory validation is kept	Yes	Low	Sample size 5; No exceptions	No
12	Unpaid Accrued Leave Liability does not agree to unfunded leave totals in DCPS	System edits	Ensure that unfunded leave liability computation algorithm is reviewed annually.	Periodic system reviews and SAS 70 for DCPS. Test: Logical Judgement Evaluation	Yes	DCPS system owner keeps track and documents annual reviews of computation algorithms and related system reviews, including SAS 70 reviews	Yes	Low	Sample size 2; No exceptions	No
13	Gross Payroll Reconciliation File is not reconciled with the rejects, therefore, the computed liability may be misstated	DAA HRO validates that corrections have been made to the Gross Payroll Reconciliation File and timekeeping records; separation of duties	Ensure correct input of liability amounts	Supervisory validation of DAA Accounting System entries should identify errors. Test: Logical Judgement Evaluation	Yes	Supervisor validates DAA Accounting System entries prior to generation of trial balance	Yes	Low	Sample size 2; No exceptions	No
14	Since the corrections are to be requested from DFAS by DAA HRO, some of the errors might go undetected or not identified in time. This could cause the reconciliation file to be out of balance	DAA HRO validates that corrections have been made to the Gross Payroll Reconciliation File	Ensure that values are mapped to the correct trial balance lines	Document programming changes. Test: Logical Judgement Evaluation	Yes	Supervisor validates that values are mapped to the correct trial balance lines prior to generation of trial balance	Yes	Low	Sample size 2; No exceptions	No
15	Computation is manually prepared for annual leave liability and may be incorrectly calculated	Supervisory validation of computation	Ensure GLAC reclassification accuracy	Supervisory review will identify errors. Test: Logical Judgement Evaluation	Yes	Supervisor performs review	No	High	Sample size 10; 4 exceptions	Yes
16	Computation of unfunded leave totals is incorrectly calculated	Annual review of computation algorithm; system edits	Ensure controls provide reasonable assurance that DDRS-DCM produces financial statements that are supported by adequate audit trails for financial management and external auditing purposes.	Review of mapping edits and documentation of audit trails to ensure that program mapping produces financial statements that are in accordance with Treasury requirements. Test: Logical Judgement Evaluation	Yes	System user determines if records of system mapping edits are kept and updated periodically, including system and re-performing testing	Yes	Low	Sample size 2; No exceptions	No

CONTROL ASSESSMENT

1 Entity	Defense Aircraft Agency		2 Account Line	Other Liabilities		4 Preparer		First N. Last		
			3 Business Cycle/Segment, Accounting Application	(+/-) Accrued Leave Liability		5 Preparer's Phone #		(123) 456-7890		
6	7	8	9	10	11	12	13	14	15	16
Control #	Risk	Internal Control Currently In Place	Control Objective	Description of Control Design and Test	Was Control Design Effective?	Description of Control Application Test	Was Control Application Effective?	New Control Risk Level	Test Results	Material Weakness
17	Liability may be under/over stated due to manual input errors	Supervisory validation of DAA Accounting System entries	Senior management reviews statements for reasonableness and soundness using comparative accounting periods prior to certification of liabilities should ensure completeness	Comparative analysis ensures completeness and that all liabilities are accurately represented. Test: Logical Judgement Evaluation	Yes	Determine if records of documentation are kept to show senior management review	Yes	Low	Sample size 2; No exceptions	No
18	Values might be mapped to the wrong trial balance line	System programmers assigned responsibility for ensuring current requirements for mapping be programmed into the system	To ensure that all the mappings are current and correct.	Updated and current mappings in the system ensure the accuracy and validity of the data being input. Test: Logical Judgement Evaluation	Yes	Reperform the process with the recent mapping changes to test if the control is working	Yes	Low	Sample size 2; No exceptions	No
19	Liability may be under/over stated due to manual reclassification of GLAC 2210	Supervisory validation of DAA Accounting System entries	Supervisory validation of entries help in timely catching of any reporting errors.	Supervisory validation ensures completeness and that all liabilities are accurately represented. Test: Logical Judgement Evaluation	Yes	Observe and review documentation to test if Supervisors validate the entries	Yes	Low	Sample size 2; No exceptions	No
20	Controls might not provide reasonable assurance that DDRS produces financial statements that are supported by audit trails that are adequate for the financial management entity and external auditors to trace amounts reported in the financial statement	System mapping edits	To provide reasonable assurance that DDRS produces financial statements that are supported by audit trails that are adequate for the financial management entity and external auditors.	System mapping edits allow to track the changes and locate the source of data generated. Test: Logical Judgement Evaluation	Yes	Inspect the system records to test if it tracks and records the edits	Yes	Low	Sample size 2; No exceptions	No
21	Certification of liabilities may occur without all liabilities having been properly classified or included in the financial statements	Senior management review of statements for reasonableness and soundness using comparative accounting periods	To ensure the certification of liabilities occurs only after all liabilities having been properly classified or included in the financial statements	Review of statements by the the senior management by using comparative accounting periods. Test: Logical Judgement Evaluation	Yes	Inspect and review the documentation	Yes	Low	Sample size 2; No exceptions	No

ATTACHMENT 5 – OUSD(AT&L) Oversight Summary for OMB Circular A-123, Appendix A Deliverables

Focus Areas: Military Equipment, General Purpose Equipment

Oversight Mission: The Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), through the Director, Acquisition Resources and Analysis, operates the Property and Equipment (P&E) Policy Office, which leads the Department-wide effort to value military and general purpose equipment in accordance with Federal accounting standards, and to resolve the associated material weaknesses. The P&E Policy Office, with contractor support from a public accounting firm, works closely with the DoD Components in implementing a centralized approach for valuation and audit readiness; manages the Capital Asset Management System – Military Equipment (CAMS-ME), which provides a central repository for military equipment asset valuations (excluding Air Force assets beginning in FY 2009) until the Component Enterprise Resource Planning (ERP) systems are deployed; and manages the Defense Property Accountability System (DPAS) for general purpose equipment (again, until ERPs are deployed). The office also addresses property management and accountability policy and procedures to help the Components resolve issues related to their existence assertions.

Oversight Activities:

- **Policy Guidance.** DoD Instruction 5000.64, “Accountability and Management of DoD-Owned Equipment and Other Accountable Property,” provides the framework to ensure that assets are accounted for and managed in a manner necessary to meet changing operational requirements and are consistent with Federal Accounting Standards. The Instruction outlines Components’ responsibilities to establish implementing regulations and procedures; develop and maintain effective and meaningful performance measures; and perform periodic internal reviews and audits necessary to assess property accountability and management system effectiveness.
- **Business Rules and Position Papers.** In coordination with Office of the Under Secretary of Defense (Comptroller) (OUSD(C)), the Services, and the DoD Office of the Inspector General (DoD IG), the P&E Policy Office publishes business rules based on Statements of Federal Financial Accounting Standards, position papers, and other policy memoranda to guide valuations of military equipment and address property management and accountability of equipment. The P&E Policy Office represents DoD before the Federal Accounting Standards Advisory Board (FASAB) (when asked) to address implementation of Federal accounting standards for military equipment, in policy-making discussions with the Accounting and Auditing Policy Committee (AAPC), and with the DoD IG on audit readiness.
- **Executive Steering Group.** The Executive Steering Group (ESG) provides stakeholder planning and oversight to facilitate the implementation of the steps needed to achieve military equipment audit readiness by making recommendations to improve management processes and practices and setting program strategy and critical success factors. The ESG members include Army, Navy, Air Force and US Special Operations Command (USSOCOM) senior officers and executives responsible for acquisition, logistics, and

property and financial management; as well as representatives from OUSD(AT&L), OUSD(C), and the DoD IG.

- **Valuation Methodology for Military Equipment.** The P&E Policy Office undertook an effort to develop a standardized, consistent methodology for implementing Federal Accounting Standards that could leverage existing business infrastructure and integrate future improvements in order to progress towards a clean audit opinion and better management information for senior decision makers. This methodology takes advantage of current accounting, accountability, and logistics systems to gather and compile the data required for these valuations.
- **Audit Support.** The P&E Policy Office is the "point organization" for requesting the DoD IG's review of military equipment valuations and responding to IG audit findings. This office engages the DoD IG to ask for reviews of internal controls and agreed upon procedures for the military equipment valuation. Much valuable information is gleaned through engagements and the office continues to work with the DoD IG and FASAB in an effort to improve the valuation effort.
- **Training and Support Tools.** The P&E Policy Office maintains a number of training courses that address valuation and property accountability to include Proper Financial Accounting Treatment for Military Equipment, Foundations of Government Property, and Physical Inventories. They also maintain decision support tools to help business/financial management analysts determine the proper financial accounting treatments for purchase requests.

Focus Areas: Real Property, Environmental Liabilities

Oversight Mission: The USD(AT&L), through the Deputy Under Secretary of Defense for Installations and Environment (DUSD(I&E)) has oversight responsibility for delivering installation assets and services necessary to support our military forces in a cost effective, safe, sustainable and environmentally sound manner. This includes oversight for improved reporting of environmental liabilities, which is one of the remaining material weaknesses of the DoD financial statements identified by the DoD IG. In its oversight role, ODUSD(I&E) reviews financial statement information submitted by the Components to the OUSD(C) through their Financial Management offices. OUSD(AT&L) does not create environmental liability financial transactions nor maintain financial feeder systems. However, ODUSD(I&E)'s program management responsibilities and initiatives include oversight activities that serve as management controls for environmental liability reporting and correction of weaknesses.

Oversight Activities:

- **Policy Guidance.** ODUSD(I&E)'s Environmental Management Office publishes the Defense Environmental Restoration Program (DERP) Management Guidance to provide guidance on the implementation of DERP cleanup actions at active installations, base realignment and closure (BRAC) installations, and formerly used defense sites (FUDS). Within the DERP, the Installation Restoration Program (IRP) addresses sites impacted by hazardous substances, while the Military Munitions Response Program (MMRP) responds to unexploded ordnance and military munitions waste at areas other than operational ranges.

The management guidance provides instruction on developing cleanup cost estimates to support the budget process, program management, and financial reporting. Environmental liability requirements associated with cleanup activities outside the DERP are provided in the document, “Guidance for Recognizing, Measuring, and Reporting Environmental Liabilities Not Eligible for Defense Environmental Restoration Program Funding.”

- **Environmental Liabilities Implementation Plan.** ODUSD(I&E)’s Business Enterprise Integration (BEI) Office is responsible for leading I&E transformation by conducting Business Process Reengineering (BPR) efforts, including the Environmental Liabilities Recognition, Valuation, and Reporting (ELRV&R) Requirements and the Real Property Inventory Requirements (RPIR). These requirements include standardized business processes, data elements, and business rules to support environmental liability valuation and recognition for financial reporting. Together with the appropriate environmental liabilities guidance, the requirements provide the methodology and blueprint to correctly and appropriately identify, value, and report environmental liabilities. Once the transformation requirements are implemented by the Components, environmental liabilities estimates will be auditable and readily accessible for financial reporting.
- **Real Property and Installation Lifecycle Management Investment Review Board / Domain Governance Board.** The ODUSD(I&E) Domain Governance Board (DGB) defines the business transformation priorities and oversees the business transformation initiatives for the Real Property & Installation Lifecycle Management (RP&ILM) core business mission area (CBMA). The ODUSD(I&E) Investment Review Board is responsible for the review and approval of investments to modernize defense business systems for RP&ILM CBMA capabilities.
- **Environmental Liabilities Working Group (ELWG).** The joint service ELWG, co-chaired by ODUSD(I&E) and OUSD(C), provides a forum for DoD Components to discuss environmental liability policy implementation. The ELWG discussions and products assist the Components in identifying, estimating, and reporting environmental liabilities in a manner that contributes to a clean audit opinion of the Department’s financial statements.
- **Internal Control Deliverables Review.** ODUSD(I&E) is conducting a review of the Component OMB Circular A-123, Appendix A, deliverables on internal controls, including process flow diagrams, correction action test plans, and resulting actions. This review will support standardization of efforts across the Department and compliance with DoD policy and procedures.
- **Environmental Program Management Reviews (PMRs).** Environmental PMRs allow ODUSD(I&E) to perform oversight over environmental program performance and execution by the DoD Components at least annually.
- **Defense Installation Strategic Plan.** The Defense Installation Strategic Plan provides goals, objectives, and metrics for managing the DoD’s installation and environment program. The Strategic Plan is updated annually.

- **Defense Environmental Program Annual Report to Congress (DEPARC).** To meet the legislative reporting requirements of the DEPARC, the ODUSD(I&E)'s Environmental Management office collects and analyzes environmental management information that covers the Environmental Restoration, Compliance, Conservation, and Pollution Prevention program areas and provides input used in conducting PMRs.
- **Department Audit Reports.** Numerous DoD and government-wide methods, mechanisms, and techniques are employed to ensure compliance and conformance in the execution of I&E programs, including:
 - Inspector General or Audit Service findings
 - DoD IG reports and reviews
 - Government Accountability Office (GAO) reports and reviews
 - Congressional reviews and hearing

Focus Areas: Inventory, Operating Materials and Supplies

Oversight Mission: The USD(AT&L), through the Deputy Under Secretary of Defense for Logistics and Materiel Readiness (DUSD(L&MR)) serves as the Defense Logistics Executive with overall responsibility for improving and maintaining the Defense Logistics and Global Supply Chain Management System. The DoD supply chain contains over 5.2 million items that support individuals and weapon systems, 20 maintenance depots and shipyards, receives more than 35.5 million requisitions annually, processes nearly 8,200 contracts, and conducts business with over 100,000 active suppliers.

Oversight Activities:

- **Policy Guidance.** DoD Directive 4140.1, "Supply Chain Material Management Policy," DoD Directive 4151.18, "Maintenance of Military Materiel," and DoD Directive 4500.9E, "Transportation and Traffic Management," along with other DoD publications, establish requirements and standards for the logistics and materiel readiness.
- **Defense Logistics Board.** The Defense Logistics Board is an advisory council of logistics officials who advise the DUSD(LM&R) and the USD(AT&L) on managing DoD's logistics program.

ATTACHMENT 6 - Acronyms

Acronym	Definition
AAPC	Accounting and Auditing Policy Committee
AT&L	Acquisition, Technology and Logistics
B2R	Budget to Report
BEA	Business Enterprise Architecture
BEI	Business Enterprise Integration
BEIS	Business Enterprise Information Services
BPR	Business Process Reengineering
BRAC	Base Realignment and Closure Commission
BTA	Business Transformation Agency
CAC	Common Access Card
CAMS-ME	Capital Asset Management System - Military Equipment
CBDP	Chemical Biological and Defense Program
CBM	Core Business Mission
CBMA	Core Business Mission Area
CFO	Chief Financial Officer
CFOC	Chief Financial Officers Council
CIP	Construction in Progress
CSS	Central Security Service
DAA	Defense Aircraft Agency
DARPA	Defense Advanced Research Projects Agency
DCAA	Defense Contract Audit Agency
DCFO	Deputy Chief Financial Officer
DCPDS	Defense Civilian Personnel Data System
DCPS	Defense Civilian Personnel System
DDRS	Defense Departmental Reporting System
DECA	Defense Commissary Agency

Acronym	Definition
DEPARC	Defense Environmental Program Annual Report to Congress
DERP	Defense Environmental Restoration Program
DFAS	Defense Finance and Accounting Service
DGB	Domain Governance Board
DHP	Defense Health Program
DIA	Defense Intelligence Agency
DIMHRS	Defense Integrated Military Human Resources System
DISA	Defense Information Systems Agency
DITPR	DoD Information Technology Portfolio Repository
DLA	Defense Logistics Agency
DLIS	Defense Logistics Information System
DoD	Department of Defense
DoDIG	Department of Defense Inspector General
DPAS	Defense Property Accountability System
DSS	Defense Security Service
DTRA	Defense Threat Reduction Agency
DUSD(I&E)	Deputy Under Secretary of Defense for Installations and Environment
DUSD(L&MR)	Deputy Under Secretary of Defense for Logistics and Materiel Readiness
EL	Environmental Liabilities
ELRV&R	Environmental Liabilities Recognition, Valuation, and Reporting
ELWG	Environmental Liabilities Working Group
EPA	Environmental Protection Agency
ERP	Enterprise Resource Planning

Acronym	Definition
ESG	Executive Steering Group
ETP	Enterprise Transition Plan
FAC	Financial Account Code
FAM	Financial Audit Manual
FASAB	Federal Accounting Standards Advisory Board
FASB	Financial Accounting Standards Board
FBWT	Funds Balance With Treasury
FECA	Federal Employees Compensation Act
FIAR	Financial Improvement and Audit Readiness
FIPs	Financial Improvement Plans
FISMA	Federal Information Security Management Act
FM	Financial Manager
FMFIA	Federal Management Financial Integrity Act
FMR	Financial Management Regulation
FMS	Foreign Military Sales
FSRE	Financial Statement Reporting Entity
FUDS	Formerly Used Defense Sites
FY	Fiscal Year
GAAP	Generally Accepted Accounting Principles
GAO	Government Accounting Office
GF	General Fund
GLAC	General Ledger Accounting Classification
GPE	General Purpose Equipment
H2R	Hire to Retire
HRM	Human Resource Management
HRM EA	Human Resource Management Enterprise Architecture
HRO	Human Resource Office pg 62
ICOFR	Internal Controls Over Financial Reporting

Acronym	Definition
IRP	Installation Restoration Program
IS	Information Systems
IT	Information Technology
IUS	Internal Use Software
KMP	Key Milestone Plan
LES	Leave and Earnings Statement (pg 62)
MDA	Missile Defense Agency
ME	Military Equipment
MERHCF	Medicare Eligible Retirement Health Care Fund
MIC	Managers' Internal Control
MIPRs	Military Interdepartmental Purchase Request
MMRP	Military Munitions Response Program
MRTF	Military Retirement Trust Fund
NARA	National Archives and Record Administration
NAVAIR	Naval Air Systems Command
NAVFAC	Naval Facilities Engineering Command
NAVSEA	Naval Sea Systems Command
NGA	National Geospatial-Intelligence Agency
NSA	National Security Agency
O2C	Order to Cash
ODO	Other Defense Organizations
ODUSD(I&E)	Office of the Deputy Under Secretary of Defense for Installations and Environment
OIG	Office of the Inspector General
OM&S	Operating Materiels and Supplies
OMB	Office of Management and Budget
OPF	Official Personnel Folder
OSD	Office of the Secretary of Defense
OUSD(AT&L)	Principal Deputy Under Secretary of Defense

Acronym	Definition
	(Acquisition, Technology and Logistics)
OUSD(AT&L)	Office of the Under Secretary of Defense for Acquisition, Technology and Logistics
OUSD(C)	Office of the Under Secretary of Defense (Comptroller)
P&E	Property and Equipment
P&R	Personnel and Readiness
P2P	Procure to Pay
P2S	Plan to Stock
PCIE	President's Council on Integrity and Efficiency
PIS	Place in Service
PKI	Public Key Infrastructure
PM	Program Manager
PMR	Program Management Review
PO	Purchase Order
PPE	Plant Property and Equipment
PSA	Principal Staff Assistant
PSSC	Purpose, Source, Scope, and Conclusion
RP&ILM	Real Property & Installation Lifecycle Management
RPIR	Real Property Inventory Requirements
SAS	Statement of Auditing Standards
SAT	Senior Assessment Team
SCR	Systems Change Request
SMA	Service Medical Activity
SOA	Statement of Assurance
SOP	Standard Operating Procedure
TCM	Testing Comfort Matrix
TMA	Tricare Management Activity
TSM	Testing Strategy Memo

Acronym	Definition
USACE	US Army Corps of Engineers
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USD(C)	Under Secretary of Defense (Comptroller)
USSGL	US Standard General Ledger
USSOCOM	US Special Operations Command
WAWF	Wide Area Work Flow
WCF	Working Capital Fund
WIP	Work in Progress

ATTACHMENT 7 - References

American Institute of Certified Public Accountants, *Statements on Auditing Standards 31: Evidential Matter* (August 1980)

Department of Defense, *Financial Management Regulation Vol. 1, General Financial Management Information, Systems and Requirements*, Chapter 2: *Conceptual Framework* (Washington, D.C., December 1998).

Department of Defense, *Financial Management Regulation Vol. 4, Accounting policy and Procedures*, Chapter 13: *Environmental and Nonenvironmental Liabilities* (Washington, D.C., October 2005).

Department of Defense Instruction (DoD 5010.40), *Managers' Internal Control (MIC) Program Procedures* (Washington, D.C., January, 4, 2006)

Department of Defense, *Financial Management Regulation Vol. 6B, Form and Content of the Department of Defense Audited Financial Statements*, Chapter 10: *Notes to the Financial Statements* (Washington, D.C., February 2006).

Federal Accounting Standards Advisory Board, *Statement of Federal Financial Accounting Concepts No. 4: Intended Audience and Qualitative Characteristics for the Consolidated Financial Report of the United States Government* (Washington D.C., March 2003).

Federal Accounting Standards Advisory Board, *Statement of Federal Financial Accounting Standards No. 5: Accounting for Liabilities of the Federal Government* (Washington D.C., December 1995).

Federal Accounting Standards Advisory Board, *Statement of Federal Financial Accounting Standards No. 6: Accounting for Property, Plant, and Equipment* (Washington D.C., November 1995).

Federal Accounting Standards Advisory Board, *Federal Financial Accounting And Auditing Technical Release No. 2: Determining Probable and Reasonably Estimable for Environmental Liabilities in the Federal Government as a reasonable effort to identify contamination* (Washington D.C., March 1998).

Financial Accounting Standards Board, *Statement of Financial Accounting Concepts No. 2: Qualitative Characteristics of Accounting Information* (Norwalk, Connecticut, May, 1980).

Financial Accounting Standards Board, *Statement of Financial Accounting Standards No. 143: Accounting for Asset Retirement Obligations* (Washington D.C., June 2001).

General Accounting Office, *Government Auditing Standards 2003 Revision*, Chapter 3: *General Standards* (Washington D.C., June 2003)

National Archives and Records Administration, *General Records Schedules: Transmittal NO. 8* (Washington, D.C., December 1998)

Office of the Management and Budget, (OMB) Circular A-123, "Management's Responsibility for Internal Control." (Washington, D.C., month, year)

Office of the Under Secretary of Defense, *Memorandum: Financial Improvement Initiative Assertion Package Criteria and Organization* (Washington, D.C., November 2004)

Office of the Deputy Under Secretary of Defense (Installations and Environment), *Management Guidance for the Defense Environmental Restoration Program* (Washington, D.C., September 2001)

Office of the Deputy Under Secretary of Defense (Installations and Environment), *Guidance for Recognizing, Measuring, and Reporting Environmental Liabilities not Eligible for Defense Environmental Restoration Program Funding* (Washington, D.C., November 15, 2005)

Statement on Auditing Standards (SAS) No. 31, Evidential Matter, as amended by SAS No. 80 (AU Section 326), (Washington, D.C., Month, Year)