United States Department of the Interior

OFFICE OF THE SECRETARY
WASHINGTON, D.C. 20240

TAKE PRIDE IN AMERICA

Memorandum

OCT 0 8 2008

To: Assistant Secretaries
Bureau and Office Directors
Chief Financial Officers

From: Daniel L. Fletcher, Director
Office of Financial Management (PFM)

Subject: Guidance for Fiscal Year 2009 Integrated Internal Control Program

This memorandum contains the Department of the Interior's (Department) guidance for the FY 2009 Internal Control Program. The guidance includes activities and timeframes necessary to comply with the Federal Managers' Financial Integrity Act (FMFIA); Office of Management and Budget (OMB) Circular A-123 (A-123), *Management's Responsibility for Internal Controls*; OMB A-123, Appendix A (Appendix A), *Internal Control over Financial Reporting;* OMB A-123, Appendix B, *Improving the Management of Government Charge Card Programs*, OMB A-123, and Appendix C, *Requirements for Effective Measurement and Remediation of Improper Payments.* Guidance related to the Department's Audit Follow-up Program and compliance with OMB Circular A-50 will be issued under separate cover.

The Department continues its efforts to move toward a comprehensive and risk based Integrated Internal Control Program in FY 2009. The Integrated Internal Control Program comprises the plans, methods, and procedures used to support meeting the Department's missions, goals, and objectives and, in doing so, supports performance-based management. In addition to supporting the Department's mission functions, the Department's Integrated Internal Control Program supports other legislative requirements such as the Government Performance Results Act (GPRA), the Chief Financial Officers Act (CFO Act), the Inspector General Act of 1978, as amended, the Federal Financial Management Improvement Act of 1996 (FFMIA), the Federal Information Security Management Act of 2002 (FISMA), the Improper Payments Information Act of 2002 (IPIA), the Single Audit Act, as amended, and the Clinger-Cohen Act of 1996. An integrated risk-based approach will be more efficient and contain less redundant business process assessments which, if properly performed, will satisfy many of the Department's review and report requirements.

During FY 2009, in addition to expanding the foundation for the Department's Integrated Internal Control Program established in FY 2008, the Program will focus on strategies and activities to ensure that bureaus and offices are:

- Operating efficiently and effectively,
- Managing and protecting resources,
- Complying with laws and regulations,

- Sustaining effective controls over financial reporting, and
- Using reliable program and financial information for day-to-day decision making.

To implement the Integrated Internal Control Program, bureau senior management leadership directs the planning, reviewing, and reporting for internal control over all programs and operations including financial reporting. Senior leadership coordinates among the various offices involved including programs, finance, budget, acquisition, and information technology to successfully meet the requirements for maintaining, testing, and reporting on internal controls. Bureaus are encouraged to leverage existing senior management teams to serve as Senior Management Council and Senior Assessment Teams for internal controls.

The attached Internal Control Program FY 2009 Annual Guidance provides instructions and direction to comply with FMFIA and OMB Circular A-123 to ensure that the Secretary's Annual Assurance Statement is accurate and adequately supported. Attachment 1 is the Schedule of Key Actions which outlines key actions and deadlines for those actions. The guidance requests bureaus and offices to:

- Verify component inventories and assessable units
- Identify and verify risks
- Document key processes and controls
- Update the 3-Year Internal Control Review Plan
- Perform control assessments and reviews (ICRs)
- Document results of assessments and reviews
- Prepare corrective action plans as necessary
- Prepare a Statement of Assurance on Internal Controls Over Financial Reporting
- Prepare an Annual FMFIA Assurance Statement

The Office of Financial Management will work with the bureaus to implement the Guidance for Fiscal Year 2009 Internal Control Program. PFM's efforts will focus on conducting internal control workshops, developing training on key concepts contained in the Guidance, and conducting lessons learned meeting at the end of the FY 2009 cycle. An implementation kick-off meeting for the FY 2009 internal control review cycle will be conducted in early December. Specific due dates for program reviews will be discussed at that time as well as questions on how to implement this guidance. In addition, PFM is preparing a user friendly program managers guide to internal controls and risk assessment that will be available on PFM's website. We look forward to your cooperation and assistance as we fulfill the Department's Internal Control Program responsibilities during FY 2009. If you have questions or want to discuss the requirements set forth in this memorandum, please contact Mary Braun, Branch Chief, Internal Control and Audit Follow-up and Financial Operations and Policy, at mary_c_braun@ios.doi.gov or (202) 208-4703

Attachments: as stated
cc: Assistant Inspector General for Audits
Department Internal Control Coordinators (ICCs)
Department Audit Liaison Officers (ALOs)

Department of the Interior

Internal Control Program

Fiscal Year 2009 Annual Guidance

Table of Contents

Attachments:

OMB Circular A-123

OMB Circular A-123, Appendix A

I. The Internal Control Program

The Department's Integrated Internal Control Program is a major part of managing the Department. The Integrated Internal Control Program comprises the plans, methods, and procedures used to support meeting the Department's missions, goals, and objectives and, in doing so, supports performance-based management. In addition to supporting the Department's mission functions, the Department's Integrated Internal Control Program encompasses other legislative requirements such as the Government Performance Results Act (GPRA), the Chief Financial Officers Act (CFO Act), the Inspector General Act of 1978, as amended, the Federal Financial Management Improvement Act of 1996 (FFMIA), the Federal Information Security Management Act of 2002 (FISMA), the Improper Payments Information Act of 2002 (IPIA), the Single Audit Act, as amended, and the Clinger-Cohen Act of 1996.

In FY 2009, the Department is employing an Integrated Risk Management Framework. The Department's Integrated Risk Management Framework considers the Department-wide objectives and relevant sources of risk from internal management factors and external sources and establishes control structure to address those risks. The Integrated Risk Management Framework is modeled after the Government Accountability Office's Risk Management Framework model. The Framework integrates the Department's Mission Areas and Outcome Goals, the Department's Strategic Plan, and the Department's Business Model.

Internal control also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. In short, internal control, which is synonymous with management control, helps the Department's program managers achieve desired results through effective stewardship of public resources. The goals for the FY 2009 Integrated Internal Control Program are:

- to ensure senior management oversight and coordination at Department and bureau level
- to develop and implement the Department's Integrated Risk Management Framework
- to provide senior management with risk assessments for significant Departmental components
- to implement a risk-based and cost-benefit based approach
- to improve consistency and comparability of bureau Internal Control Programs by continuing to refine the internal controls guidance, and providing tools, templates, and training
- to improve the Department's Integrated Internal Control Program maturity level.

For the Department of the Interior to have an effective internal control program, management and staff must have an understanding and commitment to controls. Although responsibility for controls lies with management, all employees have a role in the effective and efficient operation of controls established by management.

Management at all levels is responsible to reasonably assure that:

- programs achieve their intended results;
- the use of resources is consistent with agency mission;

- programs and resources are protected from waste, fraud and abuse;
- laws and regulations are followed; and,
- reliable and timely information is obtained, maintained, reported and used for decision making.

A. Governance Structure
OMB Circular A-123 requires that a governance structure consisting of a Senior Management Council and a Senior Assessment Team be established. At the Department, the Senior Management Council function is performed by the Management Excellence Council, which also serves as the Internal Control and Audit Follow-up Council. It is chaired by the Assistant Secretary - Policy, Management and Budget (PMB), and is comprised of all Assistant Secretaries, the Solicitor, the Deputy Assistant Secretary for Business Management and Wildland Fire, the Chief Information Officer, the Senior Procurement Executive, and the Inspector General (ex officio). The Council provides senior-level oversight of the Internal Control program, resolves issues related to the program, and decides reporting issues for the Department's Annual Performance and Accountability Report. The Council also ensures the Department's commitment to an appropriate internal control environment.

The duties of the Senior Assessment Team as defined in Circular A-123 are performed by the DOI Management Initiatives Team (MIT) which is chaired by the Assistant Secretary - PMB and comprised primarily of Deputy Assistant Secretaries and Bureau Deputy Directors. The duties of the MIT in implementing Circular A-123 are to ensure assessment objectives are clearly communicated throughout the agency and ensure assessments are planned, conducted, documented, and reported in a timely manner.

The Internal Control Work Group is comprised of bureau internal control coordinators, bureau finance representatives, as well as representatives from the CIO's office and the Office of Acquisition and Property Management. The Group meets regularly to discuss the status of the assessments of internal controls over both programs and financial reporting and related issues.

To promote the Integrated Internal Control Program at the bureaus, bureau senior management leadership directs the planning, reviewing, and reporting for internal control over all programs and operations including financial reporting. Senior leadership coordinates among the various offices involved including program offices, finance, budget, acquisition, and information technology to successfully meet the requirements for maintaining, testing, and reporting on internal controls. Bureaus are encouraged to use existing senior management teams to serve as Senior Management Council and Senior Assessment Teams for internal controls. Senior management review of bureau key internal control functions such as risk assessments, planned internal control reviews, and annual assurance statements should be documented.

B. Control Environment
In establishing the control environment, management must demonstrate its commitment to competence in the workplace. Management must clearly define areas of authority and responsibility, appropriately delegate the authority and responsibility throughout the agency, support human capital policies for hiring, training, evaluating and disciplining personnel, and

uphold the need for personnel to have and maintain the correct knowledge and skills to perform their assigned duties. Also, the organizational culture of an entity should be defined by management's leadership in establishing standards for ethical behavior and tone within the organization that should flow to all levels of the control environment.

Management is responsible for developing and maintaining internal control activities (controls) that comply with the following standards:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication, and
- Monitoring

II. The Internal Control Cycle

Internal control activities should be considered part of a continuing cycle of assessing the risks associated with each program component, identifying controls to mitigate that risk and testing those controls to ensure they are working effectively. Internal control should be an integral part of the cycle that occurs each year for planning, budgeting, and managing. The following sections of the Guidance provide an overview of the Internal Control Program cycle for program managers.

A. Verify Internal Control Components
B. Identify and Verify Risks
C. Document Key Processes and Controls
D. Assess Internal Controls
E. Document Results and Implement Corrective Actions
F. Monitor Corrective Actions and Document Lessons Learned

The following chart illustrates this cycle.

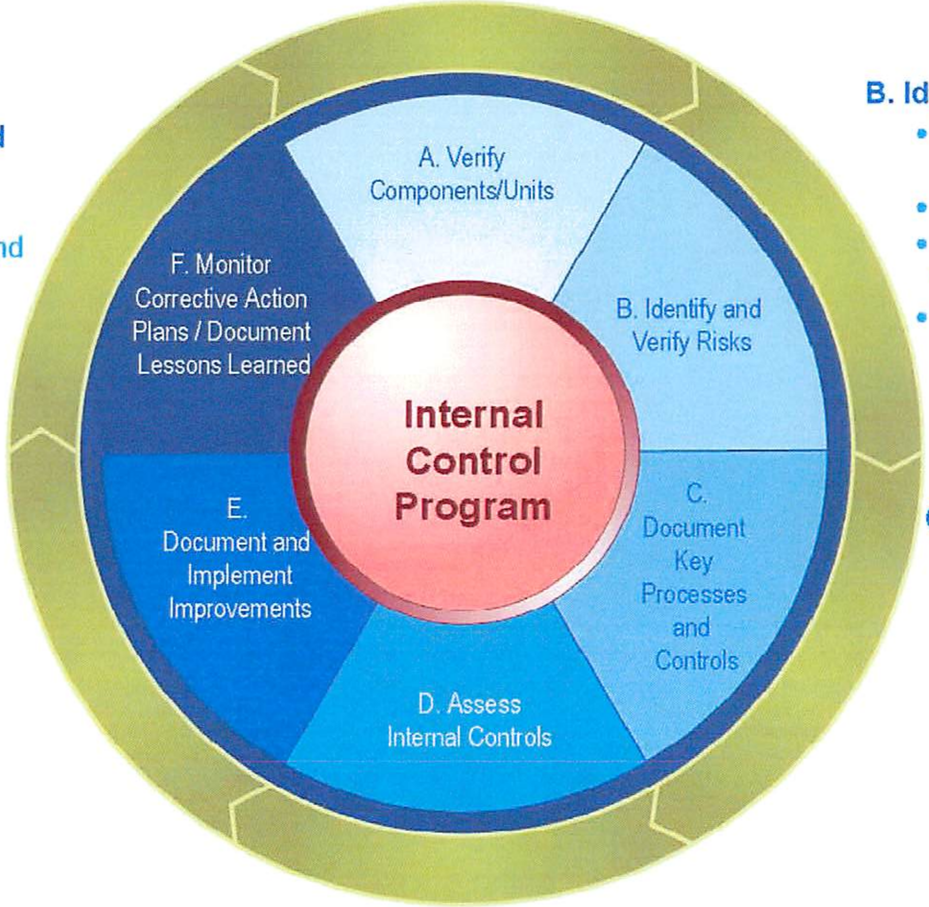
Internal Control Program Cycle

A. Verify Internal Control Components

- Validate Component Inventory
- Validate Assessable Units/Managers

F. Monitor Corrective Actions and Document Lessons Learned

- Monitor corrective actions
- Document lessons learned and revise the internal control program


A. Verify Components/Units
B. Identify and Verify Risks
C. Document Key Processes and Controls
D. Assess Internal Controls
E. Document and Implement Improvements
F. Monitor Corrective Action Plans / Document Lessons Learned
Internal Control Program

B. Identify and Verify Risks

- Integrated Risk Assessment Framework
- Perform Risk Assessments
- Assess Risk for Component/Assessable Unit
- Update 3-year Plan

C. Document Key Processes and Controls

- Narratives/Flowcharts
- Controls

E. Document Results and Implement Corrective Actions

- Document Results
- Implement Corrective Actions
- Prepare Annual Assurance Statements

D. Assess Internal Controls

- Complete Control Assessment
- Conduct Reviews

A. Verify Internal Control Components

This step includes: validating the Three-Year component inventory; validating the assessable units and assessable unit managers; coordinating stakeholder communication; and identifying the review team.

1. Validate Component Inventory

Beginning with FY 2007, PFM has asked each bureau to update and submit a component inventory. Bureaus have made significant progress in identifying their components over the past two fiscal years. However, it is important to review and validate existing components, identify new components, and refine the component structure to better support the bureau's mission or organization each year. Therefore, this guidance is once again asking for each bureau to review and update it's component inventory for the upcoming fiscal year.

A ***component*** is a bureau's significant programs, organizations, administrative activities, or functional subdivisions that flow from and are linked to the bureau's entity-wide objectives and strategic plans. A component has one or more sets of controls. Quantitative and qualitative factors should be considered to ensure that all of a bureau's significant programs are included. A ***component inventory*** is a list of all identified components. The component inventory should align with the bureau's mission and strategic plan. This can be accomplished by reviewing the bureau's organization chart as well as budget alignment, and structure used for Activity Based Costing (ABC). For example, most bureaus have the following components within their bureau:

1. Law Enforcement
2. Human Capital Management
3. Information Resources

2. Validate Assessable Units/Managers

Once a bureau component inventory has been identified, the sub-components, or assessable units, must be considered. An ***assessable unit*** is a subdivision of a component which is capable of being evaluated by risk and internal control assessments. Assessable units can be programs, program activities, or processes that are significant to a component's goals and objectives. Identification of components and subdivisions of components into *assessable units* ensures all significant processes within the bureau are identified and reviewed. An *assessable unit* should be large enough to allow managers to evaluate a significant portion of the activity being examined, but not so large that managers cannot perform a meaningful evaluation without extensive time and effort.[1] Assessable units usually exist below the organizational chart level. Each *assessable unit* should have a unit manager who will be responsible for ensuring appropriate risk assessments and control testing are performed and documented.

In FY 2007 the bureaus began the process of evaluating each component and determining what should be considered an assessable unit. As with the component inventory, the inventory of assessable units should be validated each fiscal year and adjusted if necessary. Each of these assessable units may have a manager designated as the lead person for that assessable unit.

[1] Genesco: Internal Controls; http://www.genesco.edu/CMS/

Continuing with the example given above, three components have been identified: Law Enforcement, Human Capital and Information Resources. Within one component, Human Capital, the following assessable units may exist:

1. Safety
2. Ethics
3. Training
4. Employee and Labor Relations

Update the component inventory using Attachment 2 and submit to PFM according to the Schedule of Key Actions.

B. Identify and Verify Risks

1. Integrated Risk Management Framework

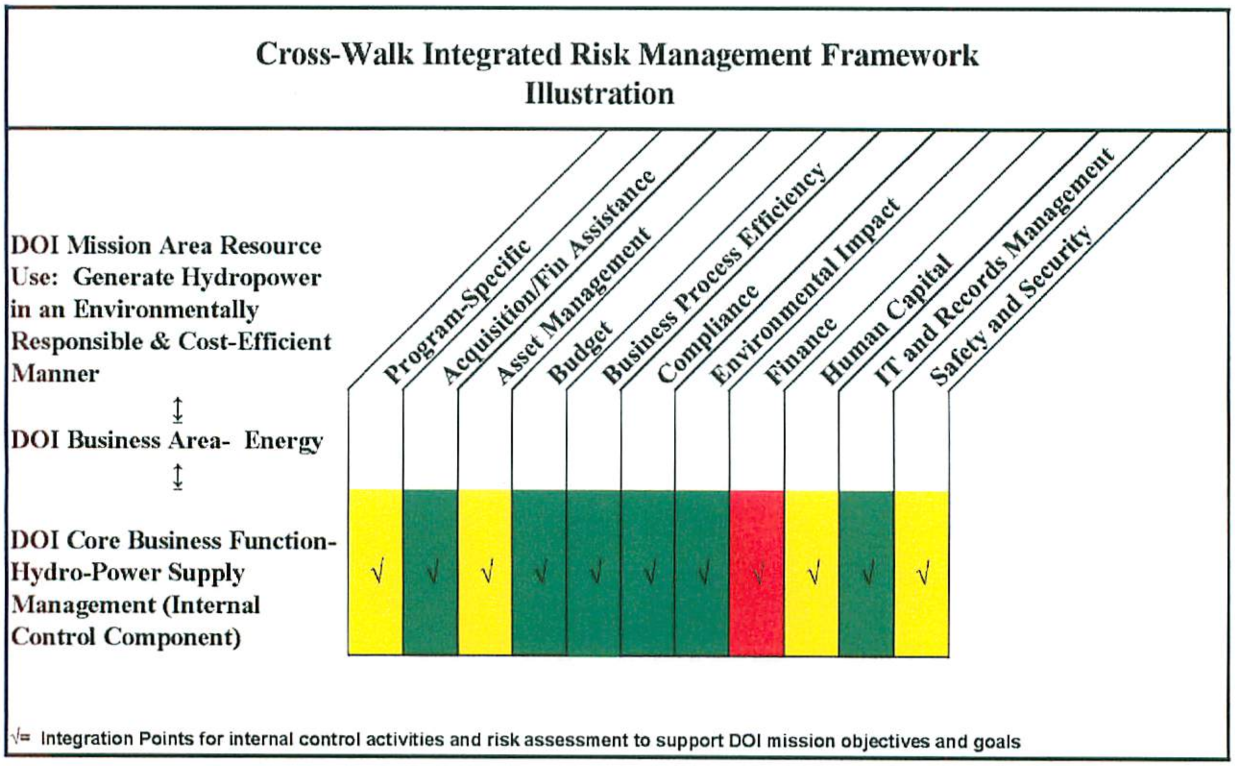
In FY 2009, the Department is implementing an Integrated Risk Management Framework. The Integrated Risk Management Framework is modeled after the Government Accountability Office's Risk Management Framework model. The Framework integrates the Department's Mission Areas and Outcome Goals, the Department's Strategic Plan, and the Department's Business Model. As an example, the chart on the next page illustrates the Integrated Risk Management Framework for the Bureau of Reclamation's Hydro-Power Supply Management Function. The Framework considers Department-wide objectives and relevant sources of risk from internal management factors and external sources and establishes a control structure to address those risks. The Framework "integrates" the Internal Control Program Component Inventory and Assessable Units, Key Business Processes, Risk Assessments, and Control Assessments.

The Integrated Risk Management Framework is designed to improve consistency and comparability of each bureau's risk assessments. The Framework is intended to be flexible and scalable. The process for determining risk ratings high (red), medium (yellow), or low (green) is provided in the following section on Performing Risk Assessments. The chart on the following page illustrates this process.

The Framework will be used for identifying and addressing major performance and accountability challenges and high-risk areas. Some of the anticipated benefits of the Framework include:

- Gaining the opportunity to examine potential risks that may not be otherwise formally reviewed for certain programs (i.e., human capital, budget, etc.)
- Leveraging existing reviews and receiving formal acknowledgement of strong internal control practices
- Gaining access to tools and templates that may not be currently used
- Conveying knowledge to other organizations that are less developed in the risk assessment process (i.e. sharing best practices)
- Following a structured, disciplined approach and detailed guidance for conducting risk assessments

- Gaining a comprehensive understanding of inherent risks in programs and the control activities in place to address these risks
- Assessing and improving effectiveness of control activities and, therefore, program performance
- Providing process for managing risk when changes occur in the organization



Cross-Walk Integrated Risk Management Framework Illustration

DOI Mission Area Resource Use: Generate Hydropower in an Environmentally Responsible & Cost-Efficient Manner

↕

DOI Business Area- Energy

↕

	Program-Specific	Acquisition/Fin Assistance	Asset Management	Budget	Business Process Efficiency	Compliance	Environmental Impact	Finance	Human Capital	IT and Records Management	Safety and Security
DOI Core Business Function- Hydro-Power Supply Management (Internal Control Component)	🟨 √	🟩 √	🟨 √	🟩 √	🟩 √	🟩 √	🟩 √	🟥 √	🟨 √	🟩 √	🟨 √

√= Integration Points for internal control activities and risk assessment to support DOI mission objectives and goals

2. Perform Risk Assessments

Risk assessment is an internal management process conducted to ensure that an organization:

- identifies, assesses, and considers the consequences of events that could prevent the achievement of its goals and objectives and/or could result in significant loss of resources;
- identifies, analyzes and manages risks relevant to achieving the objectives of safeguarding assets; and,
- is in compliance with relevant laws and regulations.

Simply stated, risk is the possibility that events could occur or might not occur and, as a consequence, result in adverse outcomes.

Once the process and related components and assessable units are identified and related goals and objectives defined, management must identify the risks that could impede the efficient and effective achievement of those objectives. Risk challenges include traditional, irregular, catastrophic, and disruptive risk. Management should also consider conditions described in auditor-identified findings, noncompliance with laws and regulations, as well as issues found during internal management reviews as well. The types of risks to be considered include:

- ***Inherent Risk*** – includes conditions or events that exist which could negatively impact achieving the mission or objectives assuming no controls are in place. Also includes the nature of the program (component/assessable unit) and whether the program had significant audit findings, or, the potential for waste, loss, unauthorized use, or misappropriation due solely to the nature of an activity itself.
- ***Control Risk*** – is the risk that controls may fail to prevent or detect identified inherent risks.
- ***Residual Risk*** – the risk that remains after management's response to risk (considering controls that are in place).
- ***Fraud Risk*** – the risk that there may be fraud or misuse of assets that causes appropriated funds to be wasted, preventing the program from achieving its mission. Fraud Risk should be considered for all risk categories.

Attachment 3 should be used to document the risk assessment, control assessment and test plan, and submitted to PFM when complete. To ensure an integrated approach, the Department's Integrated Risk Management Framework provides a list of risk categories and related risk factors that apply to most components/ assessable units (see Attachment 4). The list is a beginning point. It is not all-inclusive nor will every item apply to every agency or activity within the agency. Even though some functions and points are subjective in nature and require the use of judgment, they are important in performing a risk assessment. Management should consider these risk categories and factors, as applicable, when assessing risk for components/assessable units.

There are three factors that determine the significance of the risks you have identified:

1. The consequence of the risk.
2. The likelihood of occurrence.
3. Management's capacity in acceptance of risk.

3. Assess Risk for Component/Assessable Unit

After management has identified existing risks, the risks must then be assessed as to their likelihood of occurrence and consequence of impact. ***Likelihood*** is the probability that the event could occur. ***Consequence*** is the impact of the event should it occur.

Risks must then be assessed as high, medium, or low. High risk areas could have a significant impact on the component or assessable unit's operations, efficiencies, or compliance; low risk areas would not materially impact operations, efficiencies, or compliance. High impact risk areas must be assessed for effective mitigating internal controls. Risk assessment should be accomplished by a multi-disciplinary team.

Planning internal control reviews to be performed in the coming fiscal year should be a result of the risk assessment and control testing.

The matrix can be used to determine high, medium, or low levels of risk. The matrix uses a scale of 1 to 5 for likelihood of occurrence and consequence of impact to determine high, medium, or low risk.

Likelihood of occurrence:

1. Rare/Remote	Event may only occur in exceptional circumstances
2. Unlikely	Event could occur in rare circumstances
3. Possible	Event could occur at some time
4. Likely	Event will probably occur in most circumstances
5. Almost Certain	Event is expected to occur in most circumstances

Consequence of impact:

1. Insignificant	• No impact on the program • Very low impact on financial information
2. Minor	• Consequences can be absorbed under normal program operating conditions • Potential impact on the program • Low impact on financial information
3. Moderate	• There is some impact on the program objectives • Moderate impact on financial information
4. Major	• Severe injury • Significant property or resource damage • High level risk that impact ability to meet program objectives • Program goals or objectives are impacted • Major impact on financial reports
5. Catastrophic	• Failure to meet program objectives • Loss of life, immediate danger to health or property • Significant environmental/ecological damage • Significant financial loss

Likelihood of Occurrence

Almost Certain	Medium	Medium	High	High	High
Likely	Medium	Medium	Medium	High	High
Possible	Low	Medium	Medium	High	High
Unlikely	Low	Low	Medium	Medium	High
Rare/Remote	Low	Low	Low	Medium	Medium
	Insignificant	Minor	Moderate	Major	Catastrophic

Consequence of Impact

Below are suggested steps to determine component and/or assessable unit risk:

1. For the process that is being evaluated in terms of risk, assemble employees who work in the process and who are impacted by the process, including both managers and line employees, to obtain diverse viewpoints. This group should also include financial, IT, and other business functions support staff as necessary, that are significant to the component/assessable unit.
2. Make a list of <u>all the possible things</u> (Attachment 4 provides risk categories/factors for consideration) that could go wrong with the program by answering the following questions:
   a) What are the major objectives or initiatives for this program?
   b) Within those objectives/initiatives what are some of the factors potentially affecting:
      i) Accomplishment of the program (e.g. lack of funding, personnel retirements, the bridge collapses, the animal becomes extinct, etc.)?
      ii) Efficiency of program expenditures (e.g. what could cause your unit costs to be high, does rework exist as an integral part of a process, does equipment break down regularly)?
      iii) Compliance with legal and regulatory requirements?
      iv) Fraud, waste and abuse in the program?
      v) Data integrity and security?
      vi) What other risk factors may affect my program? (refer to the list of risk factors)
3. For each item listed in #2, using professional judgment, determine the likelihood or probability of this occurring during the next twelve months?
4. For each item listed in #2, using professional judgment, determine the severity of impact on the program if the event occurred.

5. Plot the risks using the chart above to determine the risk rating for each potential event or risk.
6. Based on all the various risks that have been identified, identify the overall component and/or assessable unit risk rating as High, Medium or Low risk.
7. Document the rationale for the overall risk rating.

It is important to note that risk assessments of information systems are prescribed by NIST Special Publication (NIST SP) 800-30, *Risk Management Guide for Information Technology Systems*. The process for conducting a risk assessment stated in NIST SP 800-30 is similar to the process in A-123, enhancing the concept of integration.

4. Update the Three-Year Plan

After managers have assessed program vulnerabilities through risk assessment, they must develop a schedule for testing assessable units' controls which are used to mitigate those risks. Annually validating each bureau/office's comprehensive three-year risk-based internal control review plan to evaluate internal controls over programs and operations is essential for effective implementation of A-123.

All assessable units with high-risk must be tested at least once within a three-year rotation. Once high-risk assessable units are tested, managers will have documented support to enable them to accurately assess their controls. If there are no changes in key personnel, key systems, or key processes, the control testing may remain on a 3-year cycle. The test schedule should be reflected on the three-year plan. Some IT controls must be tested annually as discussed in the Federal Information Security Management Act (FISMA).

Bureau personnel should look for opportunities to integrate, coordinate activities, and leverage internal reviews already being conducted elsewhere in the bureau. For instance, business processes and related IT systems which are key to each business process in accomplishing mission objectives must be assessed for effective internal control. FISMA requires comprehensive reviews of systems to ensure the effectiveness of information security controls that support operations and assets and certification and accreditation. OMB Circular A-123 requires testing of systems which includes system security and restricted access, and FISMA-required testing of systems as well. Some of these requirements can be achieved in one assessment process. The Office of Acquisition and Property Management also has been issued guidelines by OMB to conduct A-123 entity level internal control reviews (issued May 2008), which can support the overall entity level review being done by the bureau.

As another example, if the OIG is conducting an audit of a certain area of a program and is looking at the internal controls within that area, it would seem redundant if the assessable unit manager implemented an internal control review in the same area in addition to the OIG audit.

Two types of control reviews are: *Internal Control Review (ICR)* and *Alternative Internal Control Review (AICR)*. The differences between an ICR and an AICR is merely who is conducting the review. A review conducted by the assessable unit manager is considered an ICR. A review conducted by other outside sources is considered an AICR.

Management may use other sources of information for planning purposes and to avoid duplication of conducting reviews. Sources of information may include:

- Management knowledge gained from daily operation of programs and systems (ICR),
- OIG and GAO reports, including audits, inspections, reviews, investigations or other products (AICR),
- Annual evaluation and reports pursuant to FISMA and OMB Circular A-130, *Management of Federal Information Resources,* or any other system reviews (ICR),
- Current year PART assessments (AICR), and
- Single Audit reports for grant-making bureaus (AICR).

However, the sources of information listed above should take into consideration whether the process included an evaluation of internal controls. Bureaus should avoid duplicating reviews which assess internal controls and should coordinate efforts with other evaluations to the extent possible.

Departmental Functional Reviews (DFR's) - To comply with statutory requirements and OMB directives, the Department's Offices of the Chief Information Officer (OCIO) and Acquisition and Facilities Management (PAM) will prescribe selected DFR's for IT systems, property, financial assistance (i.e., grants and cooperative agreements), acquisition management, and other functional areas deemed necessary. These DFRs should be treated as Internal Control Reviews (ICRs). Guidance for conducting and reporting the results of these reviews will be provided by the responsible offices.

In updating the three-year plan, bureaus and offices must use the template provided by PFM (Attachment 2). The schedule of key milestone dates (Attachment 1) has the due date for this submission. The three-year plan must identify test plan schedules for all components in a Bureau's inventory regardless of when that component will be reviewed.

If bureaus need to defer, delay, or cancel any reviews from the priorities plan, they must justify in writing to PFM the reason for these changes and explain how these changes do not weaken support for the assurance statement. **Requests must come from the SES official responsible for signing that component's assurance statement and be submitted to PFM as soon as the need is identified.**

C. Document Key Processes and Controls

Once entity-level management has identified its high-risk areas, component and assessable unit managers must consider whether their processes are included within the entity-level high risk parameters. If so, assessable unit managers should then identify their key program's processes, perform assessable unit-level risk assessments, and identify risk areas that align with the entity-level high risks. ***Key Processes*** are those processes that are integral to the successful achievement of the program's mission, consist of an entire end-to-end process, and may be cross-cutting; that is, a key process may involve several assessable units when documenting the entire end-to-end process.

1. Narratives/Flowcharts

Once key processes are identified, the program manager should describe, in narrative form, the steps that are taken to perform the particular process. This should include all applicable laws, regulations and policies that determine how an assessable unit operates, as well as any automated systems involved in the process. Program processes are generally contained in bureau policy memoranda, handbooks, directives and standards, etc. Ideally, a program has a current manual or handbook for each assessable unit. Flowcharting is a good way to assist in analyzing a program process for risks and key controls. Flowcharts should identify each risk and key control point that is mentioned in the business process narrative.

2. Controls

Controls are all the methods by which a component/assessable unit governs its activities to accomplish its mission. Simply put, controls are all the things a program does to ensure what is supposed to happen does happen, and what should not happen does not. These include policies, procedures and mechanisms in place to mitigate risk so that the program's mission is met. The qualities of the controls are more important than the number of controls.

Control Activities help ensure management directives are carried out. Examples include: documentation (written procedure for handling receipt of incorrect shipments of supplies), segregation of duties (using different personnel to purchase and receive goods), recording (comparison of inventory against inventory log), security (safes or locks), approvals, and authorizations. Controls over information systems also need to be in place. During times of change, controls must adjust to remain effective.

Key Controls are those critical controls which, if not executed, put the program objective at risk of failing. Key controls should be those controls that reduce risk to a low rating. Management relies upon these key controls to provide reasonable assurance of effective and efficient operations and compliance with applicable laws and regulations.

D. Assess Internal Controls

1. Complete Control Assessment

When assessing key controls, management should determine if the control is working properly. The next step is to prepare test plans for those key controls. Use the template at Attachment 3 to do this. For key controls that were assumed ineffective or non-existent resulting in high residual risk, bureaus should develop and implement mitigating corrective action plans to remediate the control weakness. For example, if an assessable unit does not have a policies and procedures manual outlining how the unit should operate, testing becomes a moot point. A corrective action plan should be put in place immediately to ensure that a policies and procedures manual is written.

2. Conduct Reviews

Controls in place that management believes to be effective must be tested and documented to support management's belief. Test methods include interviews, document analysis, observation, physical examination, questionnaires, and transaction testing. More than one method can be used when testing key controls.

As noted earlier, perform the tests using the test plan as prepared and report the results of the test on the Test Plan Form and on the Control Assessment Form (Attachment 3).

E. Document Results and Implement Corrective Actions

1. Document Results

Management must evaluate the results of control testing. As a result of the assessment of key controls, management will conclude whether:

- There are control gaps;
- The operating effectiveness of the control is effective, partially effective or not effective.

Results will identify when a deficiency exists. Judgment needs to be applied to decide whether the consequences of ineffective controls are significant enough to report as control deficiencies or material weaknesses. Internal control reporting is subject to cost-benefit constraints, and no system is designed to provide absolute assurance that undesirable conditions will not occur.

Bureaus must document the testing of internal controls and maintain documentation of the review for possible review by PFM and the OIG. Bureau managers and employees should identify control deficiencies from the results of the testing. A control deficiency should be reported to the next level of management; this allows the chain of command structure to determine the relative importance of each deficiency.

A *control deficiency* exists when the testing of a control has failed. A *reportable condition* is a control deficiency or combination of control deficiencies that are considered by management to be of significance and could adversely affect the program's ability to meet its mission. A *material weakness* is a reportable condition that the bureau head determines to be significant enough to be reported outside the agency and is included in the annual FMFIA assurance statement and reported in the bureau's PAR. Determining the level of deficiency requires a judgment by bureau managers as to the relative risk and significance of the deficiency.

It is important to note that OMB guidance on reporting deficiencies for Information Technology systems is prescribed by FISMA and the definitions differ from those in A-123 and A-123, Appendix A. FISMA requires bureaus and agencies to report a significant deficiency as: "1) a material weakness under FMFIA, and 2) an instance of a lack of substantial compliance under FFMIA, if related to financial management systems. In this case, significant deficiency is defined as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken."

OMB Circular A-123 considers a material weakness to be a "reportable condition in which the agency head determines to be significant enough to report outside of the agency".
Bureaus must notify PFM of material internal control weaknesses in a timely manner. A Corrective Action Plan (CAP) that addresses the weakness must be developed and submitted to PFM for tracking purposes.

2. Implement Corrective Actions
As stated above, the assessments of internal controls within key processes may uncover weaknesses or deficiencies in internal control. To correct a deficiency, the assessable unit manager, together with Senior Management, should create a CAP. A CAP will most likely consist of revising or enhancing an already existing control, or implementing a new control. Use the CAP template provided in Attachment 5.

CAPs should address the resolution of a specific identified control weakness and include the steps and associated timelines required to complete the corrective action. An entry of "TBD" is not an acceptable target date for a corrective action plan. When developing a CAP to resolve a material weakness or noncompliance, use the standard CAP template and:

- State the as-is weakness/noncompliance condition in the Description of Finding/ Recommendation column. The weakness should be briefly detailed and clearly stated.
- List the tasks to be accomplished to correct weaknesses on Corrective Action Tasks column. Tasks should clearly describe what needs to be done in that step and should include a date the bureau/office/component expects to complete the task. It is recommended that the steps be a short duration from each other.

If system development and deployment is a bureau/office/component's solution to correcting a material weakness or noncompliance issue, the corrective action plan must include the following:

- A schedule for development and fielding to the point where the component believes the weakness will be corrected, and internal controls will be effective;
- Tasks within the schedule demonstrating attention to internal controls which include addressing the five financial management assertions and the four system control assertions discussed in the Appendix A portion of this guidance; and
- Compliance with the Department Business Enterprise Architecture.

Weaknesses that slip year after year and do not meet target correction dates reflect negatively on the Department's commitment to improve. Therefore, the Bureau's Senior Assessment Team should resolve material weaknesses and noncompliance issues as quickly as possible and ensure that the targeted correction dates are met. CAPs for material weakness and noncompliance issues must be provided to PFM with the related assurance statements.

3. Prepare Annual Assurance Statements
The Department uses an integrated organizational structure to implement its internal control program. To ensure support for the Secretary's annual assurance statement, the chain of accountability begins with program managers, ascends to bureau and office directors, then to

program assistant secretaries, and ultimately to the Secretary. Bureau and office directors should provide assurance statements to their assistant secretaries. **Bureaus and offices are required to obtain assurances from SES managers one level below the Deputy Director. Bureau and office Chief Information Officers must submit a separate assurance statement (template prescribed in the OCIO's guidance) to their director and provide a copy to PFM and the OCIO.**

Bureaus and offices are required to prepare an annual assurance statement that includes:

- Management's assertion about the effectiveness of internal control over operations, financial reporting and compliance with laws and regulations. All reviews, evaluations, and audits should be coordinated and evaluated to support the assurance. The due date for this submission can be found Attachment 1, *Schedule of Key Actions.*
- Assurance for Section 2, evaluating and reporting on the controls that protect the integrity of Federal programs, should be based on the results of internal control assessments that were completed in the current fiscal year.
- Assurance for Section 4 of FMFIA concerns the evaluation and reporting on financial systems that protect the integrity of Federal programs.
- Assurance for internal controls over financial reporting and any related material weakness and corrective actions must be identified separately.

Assurance should consider any FFMIA material weakness and non-compliance issues identified to date by financial statement audits for bureaus and offices. Bureaus and offices are required to provide reasonable assurance as to substantial compliance with FFMIA and to identify any non-compliance in the three components of the FFMIA: financial system requirements, Federal accounting standards, and the U.S. Standard General Ledger at the transaction level. Also, a statement must be included regarding the bureau or office's general compliance with the FISMA requirements and Appendix III of OMB Circular A-130, *Management of Federal Information Resources.*

Bureau and office directors are required to submit their annual assurance statements through their assistant secretaries, and should ensure adequate time for assistant secretary review and approval so that each signed statement can be delivered on or before the date on which it is due. Templates that must be used for the September 30 annual assurance statements are provided in Attachments 6 and 7.

F. Monitor Corrective Actions/ Document Lessons Learned

Monitoring the effectiveness of internal control should occur in the normal course of business. Periodic assessments should be integrated as part of management's continuous monitoring of internal control and be reflected on the three-year control test schedule. Results of testing should

Reports from internal control reviews must be sent electronically to PFM; however, documentation to support the review should be maintained in the bureau/office. Documentation must comply with current OMB, GAO, and Department standards and should be accessible so that PFM and the OIG can perform compliance reviews. Status of corrective actions for any

FMFIA material weaknesses identified by the bureau must be reported to PFM on a monthly basis.

Site Visits
PFM will conduct comprehensive site visits at each bureau throughout the year to review progress in implementing ICRs and AICRs; to provide oversight and coordination in the assessment of internal controls; to review the adequacy and validity of assessable unit identification and risk assessments; to assess the documentation and testing of key controls over financial reporting; and the implementation of corrective actions to close out open audit recommendations.

Example
An example of the process or evaluating, testing, and documenting programmatic controls using the Department's Attachment 3 has been provided (Attachments 8a-c) as a reference.

III. Appendix A, Assessment of Internal Control over Financial Reporting

FMFIA and OMB Circular A-123 apply to each of the three objectives of internal control: effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. While the standards of internal control are applied consistently toward each of the objectives, Appendix A requires the Department to specifically document the process and methodology for applying the standards when assessing internal control over financial reporting. This Appendix also requires management to use a separate materiality level when assessing internal control over financial reporting. The Secretary's annual assurance statement on the effectiveness of internal control over financial reporting required by this Appendix is a subset of the assurance statement required under FMFIA on the overall internal control of the agency.

A. Scope

The scope of significant financial reports to be considered under Appendix A includes both the *breadth* and *depth* of financial reporting. OMB A-123, Appendix A provides management the flexibility to determine which financial reports are significant. At a minimum, the basic quarterly and year-end consolidated financial statements are considered significant financial reports to be included in the assessment of internal control over financial reporting. The financial reporting process also includes processes and controls that could materially affect financial statement or note disclosure balances.

The following principal financial reports are subject to Appendix A requirements:

a) Annual/Quarterly Financial Statements
b) Year-end Financial Statement information supporting financial report of the U.S. Government
c) SF-133, Report on Budget Execution and Budgetary Resources
d) SF-132, Apportionment and Reapportionment Schedule
e) SF-224, Statement of Transactions
f) FMS Form 2108, Year-end Closing Statement

Specific Steps:

a) Determine if other financial reports are significant.
b) Document process used to determine reports other than standard Financial Statements.
c) Determine process used to develop supporting information for establishing compliance with Generally Accepted Accounting Principles.
d) Provide list and analysis to PFM.

B. Materiality

Materiality for financial reporting is the risk of error or misstatement that could occur in a financial report that would impact management's or a user's decisions or conclusions based on such a report. Materiality may be based on quantitative factors as well as qualitative factors. Management must consider how an error would affect management or operations that rely on the key financial reports within the assessment scope. An error that would materially affect the day-to-day decisions based on these key reports would be considered a material error.

As the CFO Council's Implementation Guide states, "Materiality is a function of management's professional judgment and discretion. Therefore, management should consider key business areas and programs that impact financial statement results and include these considerations when determining materiality. Management must determine if there is more than a remote likelihood that errors or misstatements in a financial report individually or in the aggregate could have a material effect on the financial report."

1. **Quantitative factors** for materiality were calculated after a comparative analysis of financial statement line item balances for all bureaus as of September 30, 2007. PFM will perform an analysis of FY 2008 consolidated financial statements when they are available and update the bureau quantitative materiality if necessary. The Department has defined the materiality base as Net Outlays in the Combined Statement of Budgetary Resources. Report materiality is defined as 3 percent of the materiality base and planning materiality is one-third of the report materiality to allow for the precision of audit procedures for FY 2009. Report materiality is calculated as $303 million and planning materiality as $101 million as shown below. See Attachment 9, List of Significant Line Items by Bureau.

Line Item (as of 9/30/07)	**Amount**	**Report Materiality (*3%)**	**Planning Materiality (*1/3)**
Net Outlays	$10,106,117,000,	$303,183,510	$101,061,170

RSI and RSSI Materiality The scope of financial reporting subject to Appendix A requirements covers required supplementary information (RSI) and required supplementary stewardship information (RSSI) as well as the principal financial statements and accompanying notes. A materiality threshold of $101 million has been defined for the Department's financial statement line items, but that definition does not apply to items presented in the RSI and RSSI Sections. The quantitative data in the following items do not have a direct relationship to the information in the financial statements, but all are measured in dollars.

Item	Units of Measure
Deferred Maintenance: • Roads, bridges, and trails • Irrigation, dams, and other water structures • Buildings • Other structures	Dollars
Investment in Research and Development	Dollars
Investment in Human Capital	Dollars
Investment in non-Federal Physical Property	Dollars

Specific Steps

a) Use the chart above to set quantitative materiality for RSI and RSSI data at the Bureau level.
b) Identify any additional significant line items or accounts based on quantitative materiality, and document the rationale.
c) Identify significant line items or accounts based on qualitative materiality. Documentation of the rationale for identifying significant accounts which should be completed, include Attachment 12 and a narrative explanation.
d) Provide analysis to PFM.

2. Qualitative Materiality includes an evaluation of factors that may make certain line items, footnotes or accounts of a financial report significant due to the interest of OMB, the public or Congressional oversight committees. A list of audit findings as reported in the FY 2007 PAR and the spreadsheet with significant financial reporting line items are available upon request. Notices of Findings and Recommendations received by the Bureaus to-date for the FY 2008 audit should also be considered. Although a finding may not be material to the account balance, it may indicate an underlying problem that should be of concern as management determines the materiality of each line item. Changes in business process, accounting standards and/or in format reporting standards are considered qualitative factors that should be considered when determining material items, lines, or processes to be tested.

C. Determining Key Processes Supporting Material Line Items

Business processes are the foundation of the internal control assessment and support significant material balances on the financial reports. Key processes that support material financial statement line items should generally be the same processes that have been identified as processes key to the component. When defining key business processes, management should review financial statements and related disclosures, including emerging GAAP standards that will become effective in the current year and may need to be reviewed and tested, as well as cycle memoranda, flowcharts, and any other analyses that are available to management.

A business process is a sequence of events, consisting of the methods and records used to establish, identify, assemble, analyze, classify, and record (in the general ledger) a particular type of transaction. A line item relies on account-related processes and account-related applications to establish records for all transactions. These processes and applications consist of methods to report transactions and demonstrate accountability for all assets and liabilities. Examples include:

- Reconciling Fund Balance with Treasury with Treasury,
- Accepting Reimbursable Orders,
- Maintaining Inventory Control,
- Managing Property and Equipment, and
- Establishing Accruals and Accounts Payable.

Specific Steps:
See Attachment 10 for a list of business processes and sub-processes applicable to the Department's operations. Bureaus and offices should use this standard nomenclature, if possible; all are expected to do so by FY 2009 or the date of conversion to FBMS, whichever is later.

a) Review list of business processes and determine if list includes all potential business processes within the bureau.
b) Use Attachment 11 to prepare crosswalk between key business processes and significant line items or accounts. Review business process documentation, including flowcharts, to ensure that all appropriate financial processes are included.
c) Provide feedback to PFM.

D. Identifying Key Financial Reporting Assertions
Internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reports. Reliability of financial reporting means that management can reasonably make the following financial assertions:

- All reported transactions actually occurred during the reporting period and all assets and liabilities exist as of the reporting date--**existence and occurrence**;
- All assets, liabilities, and transactions that should be reported have been included and no unauthorized transactions or balances are included--**completeness;**
- All assets are legally owned by the agency and all liabilities are legal obligations of the agency--**rights and obligations;**
- All assets and liabilities have been properly valued, and where applicable, all costs have been properly allocated--**valuation;**
- The financial report is presented in the proper form and any required disclosures are present--**presentation and disclosure;**
- The transactions are in compliance with applicable laws and regulations-- **compliance;**
- All assets have been **safeguarded** against fraud and abuse; and
- **Documentation** for internal control, all transactions, and other significant events is readily available for examination.

Reliability of financial reporting means that management can also rely on the following IT objectives:

- **Completeness:** fatal edits exist for mandatory data fields; batch totals are reconciled; sequence edits exists and work; system will not accept numbers outside of a certain range;
- **Accuracy**: Key data elements for transactions (including standing data) recorded and input to the computer are reasonably correct. Changes to standing data are accurately input. Programmed algorithms are accurately calculated within the system.
- **Validity**: Transactions, including changes to standing data, are authorized. Tables are current and accurate. Report mapping is accurately programmed.
- **Restricted Access**: Systems are protected against unauthorized amendments and manipulation of data and ensure confidentiality of data. Physical assets are secure and segregation of duties exists.

These IT objectives must also be assessed for inherent risk and effective controls.

Specific Steps:

a) Use Attachment 11 to prepare a crosswalk between significant line items or accounts and financial reporting assertions.
b) Document the rationale for assigning each assertion to each significant line item.
c) Provide analysis to PFM.

E. Document Understanding of Processes and Control Design

Once key business processes are identified, they must be described in detail in order to perform an in-depth control analysis. One vehicle most suited to process analysis is a detailed business process flowchart. To begin the flowchart process, managers and process owners should describe, in narrative form, the steps in their processes in sequential terms. Components must analyze the processes from the point of origin to the financial reports and then from the financial report back to the point of origin (the point of initiation of the transaction) in order to capture all operational functions, transaction types, service providers, and systems that are elements of the process. Process steps should be numbered.

It is recommended that processes be narrated prior to being flowcharted. Interviews should be conducted with personnel who have knowledge of the relevant operations to validate the processes as they exist.

The narratives should be of sufficient clarity to ensure that a reader will understand the detailed 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.

Based on process narratives, processes must be flowcharted to assess risk and identify control gaps. If flowcharts already exist, they should be reviewed to ensure they reflect the current process and are adequately detailed to describe financial processes. Flowchart deliverables should identify financial transaction detail within the business process, such as posting obligations and receiving customer orders. The narrative and related flowchart must be at a 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.

F. Risk Assessment for Financial Reporting

Risk assessment is an internal management process for identifying, analyzing and managing risks relevant to achieving the objectives of reliable financial reporting, safeguarding of assets and compliance with relevant laws and regulations. The types of risks include the following:

- ***Inherent Risk*** – the susceptibility of an assertion to misstatement, assuming there are no related specific control activities. *Inherent risk* factors include: the nature of the agency's programs, transactions and accounts and whether the agency had significant audit findings.

- ***Control Risk*** – the risk that misstatements will not be prevented or detected by the agency's internal control (assessed separately for each significant financial statement assertion in each significant cycle or accounting application).
- ***Combined Risk*** – the likelihood that a material misstatement would occur (inherent risk) and not be prevented or detected on a timely basis by the agency's internal control (*control risk*).
- ***Fraud Risk*** – the risk that there may be fraudulent financial reporting or misappropriation of assets that causes a material misstatement of the financial statements.

Specific Steps:

a) Considering Appendix 11 Crosswalk, use Appendix 12 to document the risks identified to each material line item in the Department's financial statements
b) Provide analysis to PFM.

Entity-level controls and control gaps may indicate additional risk. The reviewers must identify and test the design and operation of key controls.

G. Evaluating Entity Level Controls

Evaluating internal control at the entity-wide level is generally accomplished through observation, inquiry, and inspection, rather than the detailed testing that lends itself to the transaction or process level internal controls. In general, questionnaires and checklists are most useful at the entity-wide level.

Specific Steps:

a) Use the GAO Entity Level Control Evaluation Tool (Attachment 19), which may be modified as appropriate, to document this process.
b) Prepare and submit summary report to PFM.

H. Evaluating Process Level Controls

The material line items on the significant financial reports were identified during the Planning step of the assessment process. Those material line items may be categorized as "material" either through quantitative (e.g., percentage of line item balance) or qualitative (e.g., amount of risk associated with the line item) criteria. Once the material line items are identified, managers must understand the key business processes that support those line items and the related internal controls over those processes.

Understand key financial reporting processes.

The crosswalk analysis ties key business processes to material financial report line items or accounts. This process was documented, primarily with the Attachment 11 format. Once existing documentation has been obtained, the managers will ensure documentation is current and contains enough detail to support the assessment. Outdated documentation poses the risk that the current control environment is not sufficiently understood. To ensure documentation is up to date, managers should maintain retention policies and procedures to account for changes in processes as they relate to changes in control environments.

Identify *key controls.*

A *key control* is a control, or set of controls, that address the relevant assertions for a material financial statement line item or significant risk.

Describe the key controls for each control activity and document supporting work paper reference for each line item.

Complete the documentation of the processes and controls that affect the material line items on the financial statements. Once key financial reporting processes have been documented, document the design of controls that are relevant to financial reporting. The understanding of control design should relate the impact on the line item or account where the potential misstatement could occur, the control objective, and the control technique.

Answer the following questions:

a) How could potential misstatements in significant financial reporting processes affect the related line item or account at a financial reporting assertion level?
b) How does the related control objective prevent or detect the potential misstatement?
c) Are identified control techniques likely to achieve the control objectives?

To determine the control technique's design effectiveness, consider:

a) Whether the control technique directly relates to the financial reporting assertion;
b) Frequency of the control's application;
c) Experience and skills of personnel performing the control;
d) Separation of duties; and
e) Procedures followed when a control identifies an exception condition.

For each key business process:

a) Identify relevant procedures and directives for that process.
b) Identify organizational element that performs the functions in this process.
c) Conducting walkthroughs of the process to determine actual process that is followed.
d) Conduct group interviews of personnel involved in the process to obtain explanation of procedures followed.
e) Validate process flowcharts and narratives prepared by program managers.
f) Identify gaps in business process procedures.
g) Identify recommendations for corrective actions for gaps.

For each material line item or account, using Attachment 13:

a) Document your understanding of how potential deficiencies in key business processes could adversely impact financial reporting.
b) Identify control objectives (e.g., personnel should be prevented from having uncontrolled access to both assets and records). Document this understanding.
c) Identify relevant control techniques (e.g., segregation of asset custody from record keeping function) to achieve control objectives. Document this understanding.

Control Deficiencies

If a control over a significant account or group of accounts is missing or its design is determined to be not effective considering the associated risk of error, a report of deficiencies and suggestions for improvement will be prepared and submitted to PFM. The deficiencies are defined as:

> A ***control deficiency*** exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.
>
> A ***design deficiency*** exists when a control necessary to meet the control objective is missing or an existing control is not properly designed, so that even if the control operates as designed the control objective is not always met.
>
> An ***operation deficiency*** exists when a properly designed control does not operate as designed or when the person performing the control is not qualified or properly skilled to perform the control effectively.

Prepare a summary report based on the evaluation of controls at the process level. Identify gaps in controls and categorize as control deficiency, design deficiency or operation deficiency. For each deficiency, identify recommendations to correct the deficiency.

I. Testing Transaction-Level Controls

Although management has evaluated the design of the controls, for controls to be effective, they must operate as designed. To ensure key controls are operating as designed requires testing of the operation of these controls that were identified in the transaction cycle narratives, flowcharts, and control matrices and determined to be effective during the assessment of the design of controls. Controls that were determined to not be effective do not have to be tested but should be redesigned to become effective. The purpose of the test would be to determine the extent to which the controls were applied, the consistency of their application, and who applied them. To ensure that all key controls are tested, a testing approach should be determined. The testing approach should define the nature, timing, and extent of testing necessary to provide sufficient evidence to support management's assertion. This would require that the transaction cycle narratives, flowcharts, and control matrices be reviewed; the controls that will be tested be listed in a test program; the nature, timing, and extent of testing for each control be defined in the test program; and the controls in the test program be cross-referenced back to the narratives, flowcharts, and control matrices to ensure that all key controls will be subject to testing.

The testing should address both manual and information technology controls. For any given transaction cycle, and assuming an effective information technology control environment, the senior assessment team may place greater reliance with less testing on automated controls than on manual controls.

Nature of testing. In developing the test program, the senior assessment team should define a testing procedure for each key control. The following would be considered acceptable tests:

- Inquiries of appropriate agency personnel
- Inspection of documents, reports, or electronic files indicating performance of the control
- Observation of the application of a specific controls
- Reperformance of the application of the control by the senior assessment team.

Inquiry and observation are less persuasive forms of evidence than inspection and reperformance.

Timing of testing. The senior assessment team should schedule the testing to occur throughout the year; although for some controls, more or less rigorous testing may be appropriate.

Develop a risk-based testing plan, considering the CFO Council's Implementation Guide suggested sample size:

Annually - 1
Quarterly – 2
Monthly – 3
Weekly – 10
Daily – 30
Recurring - 45

J. Reviewing Type II SAS 70 Reports

Bureaus/offices should consider controls in place at each cross-servicing provider or service organization as part of the Department's assessment of internal control over financial reporting. Services provided by a service provider organization are considered part of the bureau's/office's information system if they affect the following: classes of transactions in the bureau/office that are significant to financial reporting, procedures by which the bureau/office initiates, processes, or reports transactions and related, supporting accounting records, and bureau/office financial reporting processes. If they are considered part of the bureau's/office's information system, the bureau/office considers the activities and reliability of internal controls of the service provider in the assessment of internal control over financial reporting.

In reviewing and evaluating the SAS 70 report, bureaus and offices have several primary responsibilities, which are to be documented in Attachement 14. In accordance with OMB Bulletin No. 07-04, sections 6.15 through 6.18, reviewers should:

1. Determine the extent to which a particular service provider's activities and processes are significant to the bureau/office in assessing internal control over financial reporting;
2. Determine whether the report is sufficient in scope;
3. Obtain an understanding of controls at the service provider that are relevant to the bureau's/office's portion of the assessment;
4. Obtain an understanding of controls that the bureau/office has over activities of the service provider;
5. Obtain evidence that relevant controls at the service provider operate effectively, and if that is the case, no further testing of those controls is required; and

6. Address *agency control considerations* identified in the SAS 70 report.

If exceptions exist, additional procedures are to be considered (e.g., test reconciliation of output with source documents).

Review and analysis of the SAS 70 report should be well-documented in the internal control assessment workpapers. A checklist has been developed for bureau use and can be found in Attachment 14.

K. Concluding, Correcting, and Reporting

Test results will support management's judgment whether a control is functioning adequately or not. Exceptions noted in test-work over properly designed internal controls would indicate ineffectiveness. Management must consider the extent of a deficiency in such cases.

Deficiencies can range from a *simple deficiency* (e.g., missing initials indicating a supervisor's review on 1 of 26 reconciliations sampled) to a *significant deficiency* (e.g., only 8 monthly reconciliations were performed for the year) to a *material weakness* (e.g., reconciliation of several key accounts were not performed throughout the year, only at year-end). A significant deficiency in FISMA would result in a material weakness in internal control over financial reporting. A *simple deficiency* is an internal control deficiency that creates minimal exposure for management and is generally an anomaly. A *significant deficiency* usually indicates a history of internal control deficiencies that when consolidated equate to a reportable condition.

Material weaknesses and significant deficiencies should be listed on the issue log. Prepare a corrective action plan (CAP), including targeted milestones and completion dates. Provide report to PFM on a quarterly basis; if material or significant, provide a CAP monthly. PFM will monitor the status of the corrective action plan implementation.

Issues found during testing of internal controls over financial reporting should be noted on the issue log (see Attachment 15).

- This is part of PFM's and the Bureau's means of monitoring the assessments performed to satisfy compliance with OMB A-123, Appendix A.
- The issue log should contain all the results of testing that indicate deficiencies with key controls. A deficient key control is one that has been determined as ineffective and that it would not prevent, detect, and/or correct a significant misstatement in financial reporting. Bureaus will document all testing results within their testing documentation which can be made available upon request.
- Financial statement findings should be added to the issue log after the issuance of the auditor's report. At this point, there will no longer be a requirement to maintain the CAP on the issue log; however, reference the CFO's audit tracking database for the status of the CAP.
- Once IT findings are final, they should be added to the issue log but referenced to the POAM for tracking purposes.
- The status of issue log items should be provided to PFM on a quarterly basis.

- Once all issues on the issue log are implemented, maintain the log for documentation purposes. Once PFM has been provided with your final issue log showing all actions as being corrected, it is no longer necessary to keep sending quarterly updates. If management added an issue to the log which it considers insignificant, the results column can be noted with why it is insignificant and then considered closed.
- On October 1 or in the new fiscal year (when a new cycle begins) just carry forward on the issue log remaining open issues. All issues considered by management to be insignificant or closed need not be carried forward.
- Management has some discretion on what items belong on the issue log.

Reporting

The process for supporting the Statement of Assurance on Internal Control over Financial Reporting (ICFR) 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, ICFR.

The process for preparing the Statement of Assurance for ICFR will be conducted in the following manner:

- The established Entity Senior Assessment Team (SAT) will fulfill its roles and responsibilities.
- Consider results of the risk assessment.
- Consider impact of tests of design and tests of operations, as well as implications of conclusions about the "tone at the top"
- Consider evaluations of applicable SAS 70 Reports and additional testing performed.
- Consider Federal Information Security Management Act (FISMA) Report (if applicable).
- Consider internal controls intended to mitigate identified risk, preliminary control assessment, and tests of controls.
- Consider weakness interdependencies identified.
- Create corrective action plans, as appropriate.
- Complete issue log.
- Issue Statement of Assurance on Internal Controls over Financial Reporting using the templates provided in Attachments 17 and18.

A monthly status report reporting on the progress of each phase of the process is required to be sent to PFM using the template in Attachment 16.

IV. Appendix B, Improving the Management of Government Charge Card Programs

In August 2005, OMB issued Appendix B to OMB Circular A-123. This appendix requires agencies to maintain internal controls in government charge card programs. A significant requirement of this appendix is that agencies perform credit checks on all new purchase and travel card applicants. Each agency is required to maintain a charge card management plan. The required elements of the Department's charge card management plan are listed in Appendix B, but a significant requirement concerns performing credit checks on all new purchase and travel card applicants. The Office of Acquisition and Property Management (PAM) has issued a charge card management plan and it is located on its web site (www.doi.gov/pam) for reference. This establishment and testing of internal controls is dictated in the management plan and each bureau procurement office is responsible for maintaining and testing internal controls in this area. The testing of other charge card-related controls should be performed where the controls are applied.

V. Appendix C, Requirements for Effective Measurement and Remediation of Improper Payments

OMB issued Appendix C to OMB Circular A-123 in August 2006. This appendix aims to improve the integrity of the government's payments and the efficiency of its programs and activities. It incorporates the Improper Payments Information Act of 2002 (IPIA) (Pub. L. No. 107-300) and section 831 Defense Authorization Act for Fiscal Year 2002 (Pub. L. No. 107-107, codified at 31 U.S.C. §§ 3561-3657), also known as the Recovery Auditing Act.

To implement IPIA and Appendix C, the Department has conducted annual risk assessments of programs exceeding $100 million in annual outlays. The results of the risk assessments show that DOI is at low risk for improper payments. Therefore, the Department issued a Financial Administration Memorandum in April 2007 converting the annual risk assessment requirement to a 3-year risk assessment plan. The next Departmental risk assessment will be conducted in FY 2009 and, assuming the results show the Department continues to be at low risk for improper payments, every three years thereafter.

OMB prescribed a four step process to assess the risk of making improper payments and estimating the amounts involved to determine their significance. The steps incorporate modifications of the FY 2006 assessment process to accommodate our FY 2009 assessment process.

Step 1: Review programs exceeding $100 million in annual outlays to determine if there have been any significant changes in legislation and /or significant increases in funding levels affecting these programs. These changes would precipitate a risk assessment of those programs for improper payments. NOTE: do not include programs already identified and base-lined in FY 2006.

Step 2: For programs determined to be susceptible to significant improper payments, perform a statistically valid estimate of the annual amount of improper payments in programs and activities.

Step 3: For programs determined to be susceptible to significant improper payments, prepare and implement a plan to reduce improper payments.

Step 4: For the programs determined to be susceptible to significant improper payments, agencies shall report through its Performance and Accountability Reports, to the President and Congress, estimates of the annual amount of improper payments in these programs and the progress in reducing them.

The Office of Financial Management (PFM) requires a copy of the Risk Rating Worksheet – Improper Payments (see next page) for any program rated as a "high risk" of being susceptible of making improper payments. Agencies shall complete their annual risk assessment by February 27, 2009 and shall report the estimates not later than November 13, 2009 in the annual PARs to OMB as set forth in OMB Circular A-136, Financial Reporting Requirements, for IPIA and Recovery Auditing Act reporting. Additional guidance will be sent to the bureaus during the first quarter of FY 2009.

Risk Rating Worksheet - Improper Payments

PROGRAM TITLE____

ANNUAL PROGRAM OUTLAYS $ __________

ESTIMATED ANNUAL NUMBER OF PROGRAM PAYMENTS ______________

ANNUAL ESTIMATED AMOUNT OF IMPROPER PAYMENTS $_____________

% OF ANNUAL NUMBER OF PAYMENTS MADE IMPROPERLY ___________

RISK RATING: High______ Medium_______ Low ________

Use separate sheets of paper as necessary to respond to each of the following:

1) PROVIDE THE CRITERIA USED TO DETERMINE THE RISK RATING.

2) LIST SIGNIFICANT WEAKNESSES.

3) SUMMARIZE THE RATIONALE/DECISIONS SUPPORTING THIS ASSESSMENT.

4) PROVIDE THE NAMES AND TITLES OF THE PRIMARY CONTRIBUTORS PREPARING THIS RISK ASSESSMENT.

5) BUREAU PROGRAM/ACTIVITY CONTACT: ______________________________

Phone Number: