



United States Department of the Interior

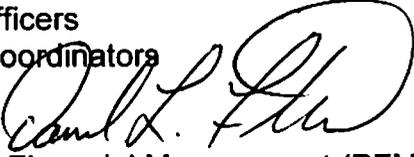
OFFICE OF THE SECRETARY
Washington, DC 20240



NOV 25 2009

FINANCIAL MANAGEMENT MEMORANDUM 2009-0095 (VI.A)

To: Assistant Secretaries
Bureau and Office Directors
Bureau Assistant Directors for Administration
Chief Financial Officers
Internal Control Coordinators

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

Subject: Guidance for Fiscal Year 2010 Integrated Internal Control Program

This memorandum transmits the Department of the Interior's (DOI) guidance for the FY 2010 Integrated Internal Control Program. The guidance includes activities and timeframes necessary to comply with the Federal Managers' Financial Integrity Act (FMFIA) and Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Controls*, including Appendix A, *Internal Control over Financial Reporting*. It also briefly addresses OMB A-123, Appendix B, *Improving the Management of Government Charge Card Programs*, and OMB A-123, 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.

An integrated, risk-based approach will be more efficient and contain less redundancy in business process assessments that, if properly performed, will satisfy a variety of the Department's review and reporting requirements. Bureaus and offices must assess risk in a consistent manner using the Integrated Risk Rating Tool (IRRT), considering inherent risk, control risk, and fraud risk. Internal control reviews will focus primarily where risk is high.

This year's program will focus on strategies and activities to ensure maximum efficiency and effectiveness of Interior's programs and make certain that the risk of fraud is minimized. Bureaus and offices must address Interior's core mission areas, core and support business service areas, and enterprise (technology) service domains (identified in the DOI Business Model), by doing the following:

- Operating efficiently – implementing streamlined processes to eliminate waste and reduce cost. Operational efficiency can be viewed as the ratio of resources expended by agencies to outputs.
- Operating effectively – achieving intended programmatic goals and objectives.
- Managing and protecting resources.

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

To implement the integrated, risk-based internal control program, bureau senior management 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 *Integrated Internal Control Program FY 2010 Annual Guidance* provides instructions and direction to facilitate compliance with FMFIA and OMB A-123 and to ensure that the Secretary's Annual Assurance Statement is accurate and adequately supported. Attachments 1 and 16 are the Schedules of Key Actions that outline key actions and deadlines for those actions. The guidance requires that bureaus and offices do the following:

- Planning
 - Verify component inventories and assessable units.
 - Identify and verify risks.
 - Integrate and coordinate internal control review activities.
- Evaluating Entity-Level Controls
 - Document and assess bureau/office-wide design of controls (including controls relating to financial reporting and information technology).
- Evaluating Process-Level Controls
 - Document key processes and controls.
 - Update the annual, risk-based Internal Control Review Plan, with a 3-year cycle.
- Testing Operating/Transaction-Level Controls
 - Perform control assessments and internal control reviews (ICRs.)
 - Document operating effectiveness of controls.
- Concluding, Correcting, and Reporting
 - Conclude on control effectiveness, suitability of compensating controls and whether any control gap is a material weakness.
 - Prepare and track 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 apply the Guidance for the Internal Control Program. PFM will encourage consistency in approach to assessing risk and use of PFM's templates for risk management and assessment of internal control. PFM will hold a lessons learned discussion at the end of the FY 2010 cycle.

We look forward to your cooperation and assistance as we fulfil the Department's Internal Control Program responsibilities this fiscal year. The guidance is Attachment A to this memo. If you have questions or want to discuss the requirements set forth in this memorandum, please contact Eric Eisenstein, Branch Chief, Internal Control and Audit Follow-up, at eric_eisenstein@ios.doi.gov or (202) 208-3417.

Attachments: As Stated

cc: Finance Officers Partnership
Assistant Inspector General for Audits
Department Audit Liaison Officers (ALOs)

Department of the Interior
Internal Control Program
Fiscal Year 2010 Annual Guidance

Table of Contents

Section	Page
I. The Internal Control Program	1
A. Governance Structure	2
B. Control Environment.....	2
II. The Internal Control Cycle	3
A. Verify Internal Control Components.....	5
1. Validate Component Inventory	5
2. Validate Assessable Units/Managers	5
B. Identify and Verify Risks	6
1. Integrated Risk Management Framework	6
2. Perform Risk Assessments	7
3. Assess Risk for Component/Assessable Unit.....	8
4. Update the Risk-Based Internal Control Review Plan with a Three-Year Cycle	10
C. Document Key Processes and Controls.....	12
1. Develop Narratives / Flowcharts.....	12
2. Controls	14
D. Assess Internal Controls.....	15
1. Complete Control Assessment	15
2. Conduct Reviews.....	15
1. Document Results	15
2. Implement Corrective Actions	16
3. Prepare Annual Assurance Statements.....	17
F. Monitor Corrective Actions and Document Lessons Learned	18
III. Appendix A, Assessment of Internal Control over Financial Reporting	19
A. Establish the Scope/Identify Significant Financial Reports	20
B. Determine Materiality	20
C. List Significant Financial Service Locations where Testing may Need to Occur.....	24
D. Confirm List of Third Party Providers and Ensure that SAS 70 Reviews Will be Completed When Required	24
E. Determine Key Processes Supporting Material Line Items	24
F. Financial Reporting Assertions	25
G. Complete Risk Assessment for Financial Reporting.....	26
H. Document Business Processes.....	27
I. Evaluate Entity-Level Controls	27
J. Document and Evaluate Process-level Controls.....	29
K. Evaluate Control Design.....	30
L. Evaluate Third-Party Service Providers	31
M. Understand the IT Infrastructure and Associated Risks	33
N. Test at the Transaction Level	34
O. Conclude, Report, and Correct	37
IV. Appendix B, Improving the Management of Government Charge Card Programs	40

V. Appendix C, Requirements for Effective Measurement and Remediation of Improper Payments.....40

Attachments:

OMB Circular A-123

- 1 Schedule of Key Actions
- 2 Template for Three-Year Component Inventory and Internal Control Review Plan
- 3 Template for Risk Analysis, Control Assessment, Test Plan
- 4 List of Inherent Risk Factors
- 5 Template for Corrective Action Plan
- 6 Template for Assurance Statement (Unqualified)
- 7 Template for Assurance Statement (Qualified)
- 8a Review Objectives Example
- 8b Process Narrative Example
- 8c Flowchart Instructions
- 8d Flowchart Example
- 8e Risk Analysis, Control Assessment, Test Plan Example

OMB Circular A-123, Appendix A

- 9 Significant Line Items by Bureau
- 10 Business Processes and Sub-processes
- 11 Crosswalk of Material Financial Statement Line Items to Business Processes
- 12 Template for Risk Assessment
- 13 Template for Control Assessment
- 14 Template for Type II SAS 70 Report Checklist
- 15 Template for Issue Log
- 16 Template for Status report on A-123, Appendix A Key Action Items by Bureau
- 17 Template for Assurance Statement (Unqualified)
- 18 Template for Assurance Statement (Qualified)
- 19 Standard Key Controls

List of Figures

- Figure 1: Internal Control Program Cycle4
- Figure 2: Integrated Risk Management Framework for the Bureau of Reclamation’s Hydro-Power Supply Management Function7
- Figure 3: Likelihood of Occurrence9
- Figure 4: Consequence of Impact9
- Figure 5: Depiction of the Risk Based on the Impact of the Likelihood of Occurrence9
- Figure 6: Items Included in RSI and RSSI23
- Figure 7: CFO Council’s Implementation Guide Sample Sizes36

I. The Internal Control Program

The Department's Integrated Internal Control Program comprises the plans, methods, and procedures used to support meeting the Department's missions, goals, and objectives, and it supports performance-based management. In addition to helping to fulfill the Department's mission functions, the Department's Integrated Internal Control Program contributes to complying with 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 fiscal year (FY) 2010, the Department will continue to employ the Integrated Risk Management Framework. The 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 (GAO) 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 helps the Department's program managers achieve desired results through effective stewardship of public resources. The goals for the FY 2010 Internal Control Program continue to be the following:

- 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; and,
- to improve the Department's Integrated Internal Control Program maturity level.

For the Department 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 the following:

- 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

In accordance with the Office of Management and Budget (OMB) Circular A-123 Interior has established a governance structure consisting of 1) a Senior Management Council, and 2) a Senior Assessment Team.

The Senior Management Council:

- is performed by Interior's Management Excellence Council, which also serves as the Internal Control and Audit Follow-up Council,
- is chaired by the Assistant Secretary - Policy, Management and Budget (PMB),
- is comprised of all Assistant Secretaries, the Solicitor, the Deputy Assistant Secretary for Budget and Business Management, the Chief Information Officer, the Senior Procurement Executive, and the Inspector General (ex officio),
- provides senior-level oversight of the Internal Control program, resolves issues related to the program, and decides reporting issues for the Department's Annual Financial Report, and,
- ensures the Department's commitment to an appropriate internal control environment.

The Senior Assessment Team:

- is performed by the DOI Management Initiatives Team (MIT),
- is chaired by the Assistant Secretary – PMB,
- is comprised of Deputy Assistant Secretaries and bureau Deputy Directors,
- is responsible for implementing OMB Circular A-123 and to ensure assessment objectives are clearly communicated throughout the agency, and,
- ensures assessments are planned, conducted, documented, and reported in a timely manner.

The Internal Control Workgroup is comprised of bureau internal control coordinators, bureau finance representatives, and 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 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 should be documented.

B. Control Environment

In establishing the control environment, management must demonstrate its commitment to competence in the workplace. As bureaus and offices address the core mission areas relating to

resource protection, resource use, serving communities, and recreation, as well as the business service areas (e.g., revenue collection, grants) and enterprise/technology service domains of the Department's Business Model, 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 performing activities that align with the following elements of the Committee of Sponsoring Organizations (COSO) framework:

- **Control Environment** – The Control Environment sets the tone of an organization influencing the control consciousness of its employees.
- **Risk Assessment** – Risk Assessment is the identification and analysis of risks to achievement of program objectives, helping to determine how the risks should be managed.
- **Control Activities** – Control activities are the policies and procedures that help ensure that necessary actions are taken to address risks related to the achievement of the program's objectives.
- **Information and Communication** – Information and communication encompasses the activities required to identify and communicate information in a timeframe that enables employees to carry out their responsibilities and take actions.
- **Monitoring** – Monitoring is the process to assess the quality of the internal control system's performance over time, including regular management and supervisory activities.

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. This section is exclusively dedicated to providing guidance for evaluating internal control over programs. For additional information on Interior's risk management approach and internal control review process, refer to the *Program Manager's Guide to Risk Management and Internal Control*. 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

Figure 1 on the following page illustrates this cycle.

Department of the Interior Internal Control Program Cycle

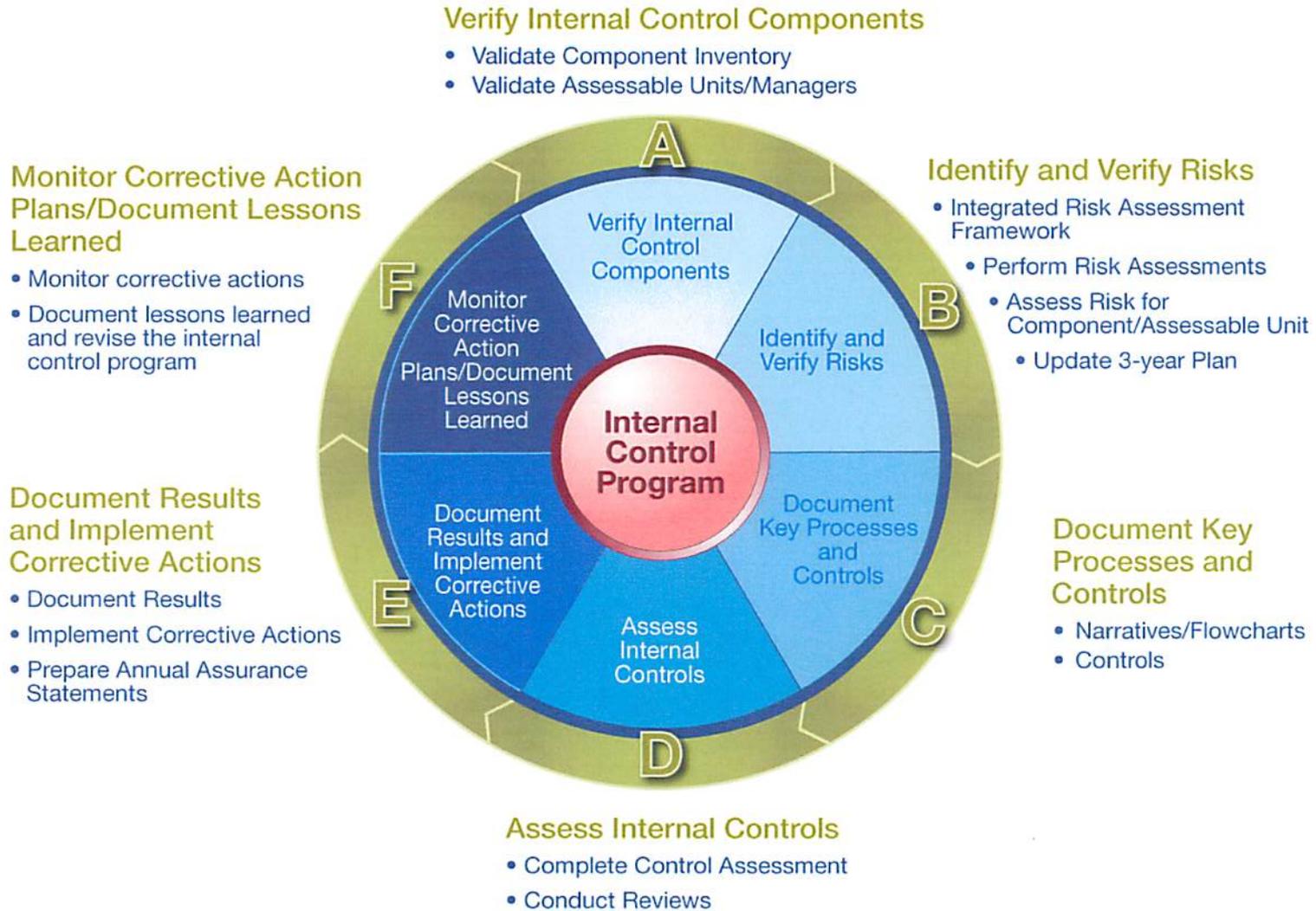


Figure 1: Internal Control Program Cycle

A. Verify Internal Control Components

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

1. Validate Component Inventory

Each bureau must validate, update, and submit a revised component inventory using the due dates contained in Attachment 1 (Note: Attachment 1 contains all deliverable due dates for the entire fiscal year.) 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. This guidance requires bureaus to review and update their component inventory for the upcoming fiscal year using Attachment 2 (columns A through E).

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 factors (those that have high dollar value) and qualitative factors (those that may be of particular interest to OMB, the public, or Congressional oversight committees, politically sensitive programs, or programs susceptible to fraud) 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, FWS has the following components within their bureau:

- National Wildlife Refuge System
- Law Enforcement
- Business Management and Operations

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 that 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. 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. As with the component inventory, the inventory of assessable units must be validated each fiscal year and adjusted if necessary.

Continuing with the example given above, three components have been identified: National Wildlife Refuge System, Law Enforcement, Business Management and Operations. Within one component, National Wildlife Refuge System, the following assessable units exist:

- Wildlife Resources
- Division of Natural Resources
- Fire Management
- Division of Visitor Services and Communication

B. Identify and Verify Risks

1. Integrated Risk Management Framework

In FY 2009, the Department implemented 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, **Figure 2** 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 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; and,
- Providing a process for managing risk when changes occur in the organization.

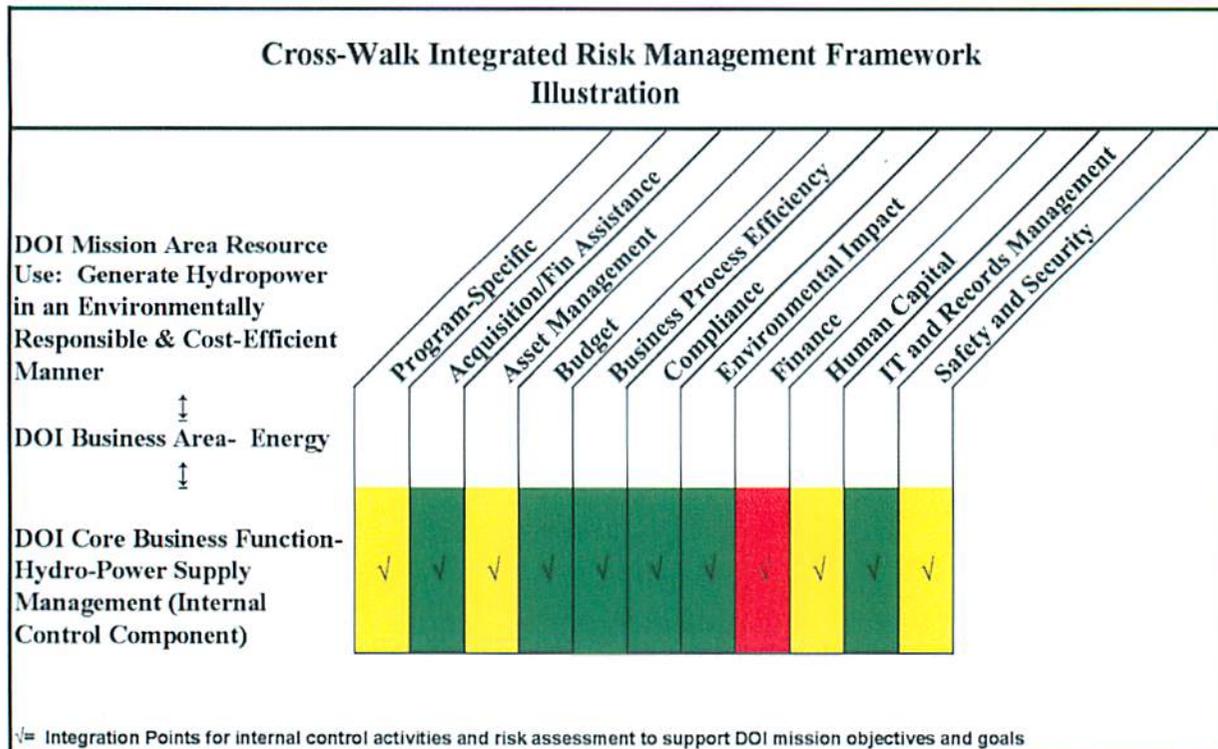


Figure 2: Integrated Risk Management Framework for the Bureau of Reclamation's Hydro-Power Supply Management Function

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.

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 control reviews. 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); and,
- **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.

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, and 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 to confirm effective mitigating internal controls are in place and operating as management intends. 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 following figures can be used to determine the level of risk. **Figure 5** uses a scale of 1 to 5 for likelihood of occurrence and consequence of impact to determine high, medium, or low risk.

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

Figure 3: Likelihood of Occurrence

1. Insignificant	<ul style="list-style-type: none"> No impact on the program Very low impact on financial information
2. Minor	<ul style="list-style-type: none"> Consequences can be absorbed under normal program operating conditions Potential impact on the program Low impact on financial information
3. Moderate	<ul style="list-style-type: none"> There is some impact on the program objectives Moderate impact on financial information
4. Major	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Failure to meet program objectives Loss of life, immediate danger to health or property Significant environmental/ecological damage Significant financial loss

Figure 4: Consequence of Impact

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

Figure 5: Depiction of the Risk Based on the Impact of the Likelihood of Occurrence (See Figure 3 for detail) vs. the Consequence of Impact (see Figure 4 for detail)

The Department introduced the Integrated Risk Rating Tool (IRRT) to each bureau/office during FY 2009 as a consistent means of assessing risk throughout the Department. This tool is an automated way to assess risk described in this section. In FY 2010, all bureaus/offices are required to use the tool to assess risk for each assessable unit in the component inventory and to document the results on Attachment 3. The IRRT contains tabs for each risk factor noted in Attachment 4 and asks questions that will determine the likelihood of occurrence and the consequence of the potential impact to determine the inherent risk. After noting what controls are in place to mitigate those risks, a residual risk is then determined. The bureaus/offices must use this tool, evaluate and summarize the results for each assessable unit, and transfer the risks onto the Risk Analysis page of Attachment 3. Transfer the resulting risk rating onto Attachment 2, Columns F through I.

It is important to note that risk assessments of information systems are prescribed by the National Institute of Standards and Technology (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 Risk-Based Internal Control Review Plan with a Three-Year Cycle

Validating each bureau's/office's annual comprehensive, risk-based internal control review plan under a three-year cycle is essential for effective implementation of A-123. 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.

Component materiality, most often considered in financial audits, can also be useful for risk assessment and internal control reviews. PFM plans to set component materiality levels for individual bureaus and offices within the Department's consolidated financial statements. Then, bureau/office management should use these materiality levels as they evaluate programs in the risk assessment process and determine which ones have monetary values that warrant current-year internal control reviews.

All assessable units with high inherent risk must be tested annually, if feasible. When all inherently high-risk assessable units are tested, managers will have documented support to enable them to accurately assess their controls. After a baseline has been established, and if there are no changes in key personnel, key systems, or key processes, rotational testing may be considered. If deficiencies are found, testing of that inherently high risk assessable unit should be conducted every year. The test schedule should be reflected on the three-year plan (Attachment 2, columns J through N). Some Information Technology (IT) controls must be tested annually as discussed in the FISMA.

Assessable units with medium risk ratings should be tested on a three-year cycle, while low risk assessable units should be incorporated into the testing schedule as resources permit but not less than once every five years.

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 that 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, including system security and restricted access, as well as FISMA- required testing of systems. Some of these requirements can be achieved in one assessment process. The Office of Acquisition and Property performs an entity-level review (*Conducting Acquisition Assessments under OMB Circular A123*, May, 2008) that provides support for the overall entity-level review being conducted by the Department. PFM, the OCIO and PAM are also focusing on a coordinated, risk-based approach to assessing internal controls related to the IT and acquisition programs to determine which program-related areas are of the highest risk and should be assessed.

As another example, if the Office of Inspector General (OIG) is conducting an audit of a certain area of a program and is reviewing the internal controls within that area, it would be redundant for the assessable unit manager to implement an internal control review in that same area of the program.

Two types of control reviews are: [Internal Control Review \(ICR\)](#) and [Alternative Internal Control Review \(AICR\)](#). The difference between an ICR and an AICR is who conducts the review. A review conducted by the assessable unit manager is considered an ICR. A review conducted by other outside sources, (such as the OIG or GAO), 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 the following:

- 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), 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 greatest extent possible.

Departmental Functional Reviews (DFRs) - To comply with statutory requirements, directives and risk-based analysis, the Department's Offices of the Chief Information Officer (OCIO), Acquisition and Facilities Management (PAM), and the Office of Occupational Health and Safety (OHS) may prescribe selected DFRs, 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 ICRs. Guidance for conducting and reporting the results of these reviews will be provided by the responsible offices.

Use Attachment 2 to provide the updated component inventory/assessable unit inventory, the risk associated with each component and assessable unit, and an updated three-year plan. 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.

come from the Senior Executive Service (SES) official responsible for signing that component's assurance statement and be submitted to PFM as soon as the need is identified.

It is important to note that, with the issuance of the American Recovery and Reinvestment Act of 2009 (ARRA), bureaus must take into account the increased risks associated with complying with ARRA and ensure that appropriate internal control reviews are planned and conducted so that controls are designed properly and operate effectively to mitigate those risks. These additional internal control reviews should be noted separately on the three-year plan as reviews being conducted for ARRA.

	Due to PFM / File Description	Due Date	Attachment Number
	Component Inventory of Assessable Units	1/29/10	2

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 programs' objectives and processes, perform assessable unit-level risk assessments, and identify risk areas that align with the entity-level high risks (as noted in the previous section). **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. Once management has decided that a key process requires review because it is aligned within a high risk area, management should plan for a review, document the process and controls, and conduct a control assessment. The control assessment is described further in the following section.

Prior to documenting narratives, flowcharts, and internal controls in a control matrix, it is often beneficial to document the goals of a program / assessable unit, and describe what risks management seeks to mitigate by examining the control activities. In other words, management should define why they want to examine a program / assessable unit and identify what controls are failing to help the organization meet its goals or objectives (see Attachment 8b for an example).

1. Develop 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. A narrative example has been provided in Attachment 8b.

Steps for Preparing a Narrative

- See Attachment 8b as a guide that can be used in conjunction with a flowchart and control matrix
- Identify the relevant laws, policies, procedures, and guidance that govern the process
- Identify Interior's relevant core mission area - resource protection, resource use, serving communities, and recreation – or other business or IT service area.
- Define the beginning and the end of the process
- Document the steps taken throughout the process including:
 - Individuals conducting the activity
 - Documents created/completed
 - Information Technology systems accessed/updated
 - Decision points
 - Potential internal controls (identified as controls in the assessment phase)
- Number the potential internal controls so that the activity can be traced from the narrative to the flowchart, to the control matrix

The narrative should describe important activities in as much detail as would be required for a person unfamiliar with the key business process to understand it. To the degree possible, the narrative should group and describe activities that follow a linear progression.

Flowcharts are a good way to assist the bureaus in analyzing a program process for risks and key controls. Flowcharts should identify each key control point that is mentioned in the business process narrative.

Flowchart Template Description

A flowchart is a graphical representation of the steps described in the narrative. Flowcharts are useful because they: (1) show relationships between steps that are not easily described in a written format, (2) highlight control activities, and (3) allow users to potentially identify redundant activities. Flowcharts are an efficient way to document the key internal control points in a business process, they also. The flowcharts 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. Use consistent numbering in the narrative, flowchart, and control matrix to aid the reader in connecting the documents. For example, a control numbered "COOP 8.3.2" in the narrative should be reflected with the same title in the flowchart and control matrix. A flowchart template is provided in Attachment 8d. Details on how to prepare a flowchart are provided below.

Flowchart Template Instructions

The Assessable Unit Manager is responsible for preparing or delegating responsibility for preparing the flowchart. In some assessable units, staff responsible for daily operations may be of assistance with flowchart preparation as they are typically familiar with the process and internal controls within the assessable unit.

While preparing the narrative should generally precede that of the flowchart, in some cases, a narrative may not exist or be finalized at the time of flowchart preparation. In instances where a narrative does not exist, the following steps should be followed to prepare the flowchart:

- Identify process owner(s), and collect information regarding the key business process, via interviews, prior to flowcharting;
- Define the beginning and end of the process; and
- Understand which organizations, in addition to the assessable unit, are involved in the key business process.

The flowchart should be completed early enough to allow sufficient time to complete remaining internal control review items such as the control matrix. Assessable Unit Managers should consider the time requirements for preparing flowcharts, if they did not already exist, when preparing their internal control review timelines.

Steps for Preparing to Draft a Flowchart

- Identify key individuals/groups within the process
- Define the beginning and the end of the process
- Document the steps taken throughout the process including:
 - Documents created/completed
 - Information Technology systems accessed/updated
 - Key decision points
- Identify controls within the process

Interior is making a concerted effort to demonstrate the successes of its programs, activities, and functions, toward its mission goals, through the Internal Control Program. Assessable Unit Managers should submit draft or final narratives to their bureaus' Internal Control Coordinator.

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 can be realized. 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. An example is provided in Attachment 8e. Identify **key controls** in the Control Assessment Form tab of Attachment 3.

D. Assess Internal Controls

1. Complete Control Assessment

When assessing **key controls**, management should plan the assessment, and then determine if the control is designed properly before testing is conducted to determine if a control is working properly. A test plan should be prepared by management (Control Assessment Form tab within Attachment 3) to test only the **key controls** for each process. For **key controls** that were designed inappropriately, assumed ineffective, or that are 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 are designed properly, and that management believes to be effective, must be tested and documented to support management's assertions. Test methods include interviews, document analysis, observation, physical examination, questionnaires, and transaction testing. More than one method can be used when testing key controls.

Conducting the control assessment and planning the control testing should be documented using the Control Assessment Form and the Test Plan form in Attachment 3.

E. Document Results and Implement Corrective Actions

1. Document Results

Management must evaluate the results of control testing, using the Control Assessment form in Attachment 3, and document planned corrective actions using the Template for Corrective Action Plans in attachment 5. As a result of the assessment of key controls, management will conclude whether:

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

The results of testing will identify when a deficiency exists. Judgment needs to be applied by the bureaus to decide whether the consequences of ineffective controls are significant enough to report as control deficiencies or material weaknesses. Internal control reporting efforts are 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, as well as by bureau staff in a subsequent year.

A **control deficiency** exists when the testing of a control has failed. A control deficiency identified by the bureau 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

significant deficiency (previously known as a reportable condition) is a control deficiency, or combination of control deficiencies, that in management’s judgment, should be communicated because they represent significant weaknesses in the design or operation of internal control that could adversely affect the organization’s ability to meet its internal control objectives. A **material weakness** is significant deficiencies in which the agency head determines to be significant enough to report outside of the agency. Material weaknesses are communicated by the bureau in their annual FMFIA assurance statement and reported by the Department in the Annual Financial Report (AFR).

Determining the level of deficiency requires judgment by bureau managers as to the relative risk and significance of the deficiency. Component materiality should be considered in distinguishing material weaknesses from significant deficiencies and other deficiencies. A component that has a control deficiency or significant deficiency might rise to the level of material weakness if the component is material to the bureau/office’s budget.

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.”

Bureaus must notify PFM of material internal control weaknesses or noncompliance in a timely manner. A Corrective Action Plan (CAP) that addresses the weakness must be developed and submitted to PFM monthly for tracking purposes as discussed further below.

Due to PFM / File Description	Due Date	Attachment Number
Risk Analysis, Control Assessment, and Test Plan (all tabs)	09/15/10	3

2. Implement Corrective Actions

As stated above, the assessments of internal controls within key processes may identify 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. A template for the CAP is included in Attachment 5.

CAPs should address the resolution of a specific identified control deficiency 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 any deficiency, use the standard CAP template and:

- State the as-is deficiency condition in the *Description of Finding / Recommendation* column. The deficiency should be briefly detailed and clearly stated.

- List the tasks to be accomplished to correct the deficiency in the *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 deficiency, the corrective action plan must include the following:

- A schedule for development and fielding to the point where the component believes the deficiency 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.

Deficiencies 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 deficiencies identified as 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.

	Due to PFM / File Description	Due Date	Attachment Number
	Template for Corrective Action Plans	09/15/10	5

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 the following:

- 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.
- 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. Please note that the templates may be updated, as necessary, during FY 2010 to include reasonable assurance over controls around ARRA activities.

	Due to PFM / File Description	Due Date	Attachment Number
Assurance Statement		09/30/10	6 or 7

F. Monitor Corrective Actions and Document Lessons Learned

Monitoring the effectiveness of internal control should be incorporated into 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 must be documented and corrections to deficiencies found as a result of an internal control review must be tracked by the bureau until implemented.

Summary reports on the results of the testing (i.e. a completed Attachment 3) 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 with 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 of documenting the business process, developing a flow chart, and evaluating, testing, and documenting programmatic controls using the Department's Attachment 3 has been provided (Attachments 8a-e) as a reference.

The table below summarizes the instruction in Section II of this guidance and lists the key steps required to complete program reviews:

Action	Relevant Attachment	Due Date
Identify risk categories and related risk factors by using the List of Inherent Risk Factors	4	--
Update the "Risk Analysis Form" of the Template for Risk Analysis, Control Assessment, and Test Plan	3	Second Quarter
Update the Three-Year Component Inventory and Internal Control Review Plan and submit attachment	2	01/15/10
Identify key controls in the "Control Assessment Form" tab of the Template for Risk Analysis, Control Assessment, and Test Plan	3	Second Quarter
Prepare test plans, identify key controls, and document test results in the "Control Assessment Form" and the "Test Plan Form" tabs of the Template for Risk Analysis, Control Assessment, and Test Plan	3	Third Quarter
Document control assessment results in the Template for Risk Analysis, Control Assessment, and Test Plan for each review conducted and submit attachment	3	09/15/10
Document planned corrective actions in the Template for Corrective Action and submit attachment	5	09/15/10
Provide the Assurance Statement (attachment 6 or 7)	6 or 7	09/30/10

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. Appendix A 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 Appendix A is a subset of the assurance statement required under FMFIA on the overall internal control of the agency.

The Department uses a top-down approach focusing on the assurance at the Department-wide level. This approach begins with the Department’s significant consolidated financial reports and works back to material line items, key processes, key controls, and supporting documentation. This approach also focuses resources on the items most material and most at risk to Interior’s financial reporting.

A. Establish the Scope/Identify Significant Financial Reports

The scope of significant financial reports to be considered under Appendix A determines both the breadth and depth of financial reporting. 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 financial reports may be 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

Steps to be Completed

- Determine what financial reports are significant. Please note that items a and b from the previous list will most likely apply to all bureaus/offices.
- If any financial reports are identified that are not on the previous list, the bureau should document the process used to select the report and why it is significant to the bureau
- Provide list and analysis to PFM

Due to PFM / File Description	Due Date	Attachment Number
Listing of Significant Financial Reports	1/8/10	N/A

B. Determine Materiality

Determining materiality for financial reporting takes into consideration 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.”

As defined in Financial Accounting Standards Board (FASB) Statement of Financial Concepts No. 2, 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. Materiality is based on the concept that items of little importance, which do not affect the judgment or conduct of a reasonable user, do not require investigation. Materiality has both quantitative and qualitative aspects. Even though quantitatively immaterial, certain types of misstatements could have a material impact on or warrant disclosure in the financial statements for qualitative reasons.

Quantitative materiality factors

- **Planning materiality**

The Department estimates materiality as defined above in relation to the element of the financial statements that is most significant to the primary users of the statements. Although a computation may determine planning materiality, judgment is needed to evaluate whether the computed level should be adjusted for such items as unrecorded liabilities, contingencies, and other items that are not incorporated in the financial statements (and not reflected in the materiality base) but that may be important to the financial statement user. The planning materiality threshold for the set of financial statements and accompanying notes and the thresholds for other reports are considered when determining extent of testing. Materiality and therefore extent of work may differ from report to report ensuring that items required to be reported will be detected.¹ Materiality should be reconsidered at least immediately prior to concluding on the assessment and determining what control weaknesses must be reported.²

Interior’s planning materiality for financial statement line items, based on net cost to the government (appropriations), is specified as 1% of Net Outlays for the prior fiscal year’s Combined Statement of Budgetary Resources (the materiality base). Quantitative factors for planning materiality are calculated after a comparative analysis by PFM of financial statement line item balances for all bureaus as of September 30 of the previous fiscal year.

Component materiality is a materiality level which is set for individual components within the overall consolidated financial statements. There are many approaches to setting component materiality which include aggregate component materiality, where the sum of each component equals the consolidated materiality, and maximum aggregate component materiality, where the aggregate component materiality can be expressed as a multiple of consolidated materiality. The multiple is then applied to each component. As a result, the component materiality level is not a mathematical portion of the consolidated materiality level.

¹ Revised Circular A-123, Appendix A, Section II.C.

² Page 17 in CFO Council’s *Implementation Guide for OMB Circular A-123, Management’s Responsibility for Internal Control, Appendix A*

- **Testing materiality**

Interior's testing materiality is the same as planning materiality. Management's materiality is well below the financial statement auditor's materiality defined by GAO as 1% of the larger of Assets or Expenditures.

- **Reporting materiality**

Reporting materiality is a function of management judgment, and it serves as a threshold of reporting control weakness as reportable or material, impacting whether an unqualified statement of assurance can be issued. In the reporting phase, the Department considers whether misstatements are quantitatively or qualitatively material. If considered to be material, the Department is precluded from issuing an unqualified statement of assurance over financial reporting. Report materiality generally should be 3% of the materiality base.

Qualitative materiality factors

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 previous fiscal year AFR and the spreadsheet with significant financial reporting line items are available upon request. Notices of Findings and Recommendations issued by the auditors 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 reporting format standards are considered qualitative factors that should be considered when determining material items, lines, or processes to be tested.

Qualitative characteristics to consider include:

- Changes in business process;
- Changes in accounting standards and/or in format reporting;
- Importance of a balance or amount to oversight agencies and their reliance on such balance or amount;
- Knowledge of past errors;
- Susceptibility to loss due to errors or fraud (e.g., intentional manipulation of estimates used in the financial reports or material misappropriation of assets);
- Accounting and reporting complexities associated with the account (e.g., environmental liabilities, actuarial liabilities, accruals);
- Likelihood of significant contingent liabilities arising from the underlying activities;
- Changes in account characteristics;
- Notices of Findings and Recommendations issued by the auditors should be considered. Regardless of the quantitative materiality, these may indicate underlying problems that should be considered for qualitative analysis; and,
- Political sensitivity of a program or balance.

Notes, 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 is defined by the Department’s consolidated financial statement line items, but that definition does not apply to items presented in some of the Notes, RSI and RSSI sections. The quantitative data in the following items (**Figure 6**) 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: <ul style="list-style-type: none"> • 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

Figure 6: Items Included in RSI and RSSI

In addition to the above, Notes containing information regarding the number within land management categories of Stewardship Lands, Heritage Assets, and Collectible Heritage Assets must also be considered and assessed for inclusion/exclusion from the testing process.

Steps to be Completed

- PFM will provide the quantitative materiality by financial statement line item and bureau/office.
- Bureaus must identify, based on qualitative materiality, any additional financial statement line items and notes which should be added to assigned line items
- Bureaus must document the rationale for their qualitative analysis, showing how each qualitative factor bulleted above (in the “Qualitative materiality factors section”) affects/does not affect their bureau. Specifically, Bureaus should document the following: (1) the qualitative factors used for scoping and planning; and (2) the impact these factors have on documenting and testing as they relate to line items and processes selected for documentation and testing.
- Prepare a narrative summary of the qualitative analysis and rationale for adding significant accounts and provide to PFM

Due to PFM / File Description	Due Date	Attachment Number
Narrative Rationale of Qualitative Analysis	1/8/10	N/A

C. List Significant Financial Service Locations where Testing may Need to Occur

Bureaus/offices should develop a listing of significant financial service locations and **submit the list to PFM**. If the list is the same as the previous year, bureau/offices should notify PFM that there were no changes.

Due to PFM / File Description	Due Date	Attachment Number
Listing of Significant Financial Service Locations for Testing	1/8/10	N/A

D. Confirm List of Third Party Providers and Ensure that SAS 70 Reviews Will be Completed When Required

Third parties that provide significant financial services to the bureaus/offices are considered part of its internal control environment. As such, their activities should be considered in making the assessment of internal controls over financial reporting. Specifically, those third party service providers that have a role in handling significant financial transactions may have SAS 70, Type II reviews (see Section 2.4 for definitions) performed of their operations to provide bureaus assurance that controls over their operations are effective.

PFM, with the assistance of the bureaus, will identify those third parties that provide significant financial transactions to a majority of bureaus/offices. PFM will then contact these service providers and request copies of SAS 70 reports. PFM will inform bureaus/offices of these actions so that multiple requests for the same report are not made to the service provider.

Bureaus/Offices will identify those third parties that provide significant financial transactions to that specific bureau/office and provide a listing to PFM. The bureau/office will be responsible for requesting copies of SAS 70 reports from those service providers.

Due to PFM / File Description	Due Date	Attachment Number
Listing of Significant Service Providers	1/22/10	N/A

E. Determine 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. Examples include:

- Financial Reporting
- Funds Management
- Acquisition and Payables

A business sub-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. Examples of sub-processes of Fund Balance and Investments Management process include:

- Fund Balance with Treasury Reconciliation

- Investments
- Cash Receipts and Disbursements

When defining key business processes, management should review financial statements and related disclosures, as well as revisiting their process memos, flowcharts, and any other analyses that are available.

PFM developed a standard list of business processes and sub-processes for financial reporting at DOI. This listing was based on the Financial and Business Management System nomenclature. See Attachment 10 for the business process listing.

Steps to be Completed

- Review list of identified business processes and sub-processes in Attachment 10 and determine if the list includes all potential business processes for financial reporting within your bureau/office
- Provide to PFM a listing of business processes and sub-processes and a brief explanation on the processes that differ from Interior standard processes
- Prepare a crosswalk between significant line items and business processes and sub-processes. See Attachment 11 for the required Business Process crosswalk format

	Due to PFM / File Description	Due Date	Attachment Number
	Rationale for Business Processes and Sub-processes	1/8/10	N/A

F. Financial Reporting Assertions

Internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reports. The July 2008 GAO Financial Audit Manual classifies the financial reporting assertions in the following five broad categories:

- **Existence or occurrence:** Recorded transactions and events occurred during the given period, are properly classified, and pertain to the entity. An entity’s assets, liabilities, and net position exist at a given date.
- **Completeness:** All transactions and events that should have been recorded are recorded in the proper period. All assets, liabilities, and net position that should have been recorded have been recorded in the proper period and properly included in the financial statements.
- **Rights and Obligations:** The entity holds or controls the rights to assets, and liabilities are the obligations of the entity at a given date.
- **Accuracy/valuation or allocation:** Amounts and other data relating to recorded transactions and events have been recorded appropriately. Assets, liabilities, and net position are included in the financial statements at appropriate amounts, and any resulting valuation or allocation adjustments are properly recorded. Financial and other information is disclosed fairly and at appropriate amounts.
- **Presentation and disclosure:** The financial and other information in the financial statements is appropriately presented and described and disclosures are clearly expressed. All disclosures that should have been included in the financial statements have been included. Disclosed events and transactions have occurred and pertain to the entity.

Risks are associated with each type of assertion. The bureaus should review each significant account and determine the type of material error or misstatement that may occur for each assertion. The results of the evaluation of these assertions and identification of risks will help determine the types of controls that should be assessed and the tests that will likely need to be performed during the control documentation and the evaluation of design and operating effectiveness phases.

Steps to be Completed

- Prepare a crosswalk between business processes and sub-processes and the related financial statement assertions in Attachment 11

Due to PFM / File Description	Due Date	Attachment Number
Crosswalk for Business Processes and Sub-processes to Assertions	1/22/10	11

G. Complete 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 in place. 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.

DOI has developed an Integrated Risk Rating Tool (IRRT) which provides a consistent methodology to assess risk across all bureaus/offices. The IRRT is an excel spreadsheet and includes one tab to identify risk for Appendix A. Bureaus may use the Appendix A tab of the IRRT or Attachment 12 to assess risk. The results of the risk assessment will be used in the development of the bureau/office testing plan.

Steps to be Completed

- Obtain a copy of the Appendix A tab from the IRRT or a copy of Attachment 12 from PFM.
- Use the IRRT risk tabs to document the risks identified for each of their material line items or complete Attachment 12 and prepare a summary of the results to PFM.

- Submit a summary of the results to PFM.

	Due to PFM / File Description	Due Date	Attachment Number
Risk Assessment		1/22/10	12
Narrative Summary of the risks identified		1/22/10	N/A

H. Document Business Processes

Once the key business processes are identified, they must be described in detail in order to perform an in-depth control analysis. These processes should be documented through a process narrative, flowchart and control matrix.

Business process narratives provide a written summary describing each process's starting point, processing, and completion point. The narratives should be of sufficient clarity to ensure that a reader will understand the detailed process. The process narrative should identify and number the controls.

Flowcharts of the business process should be developed based on these process narratives. The controls should also be identified and numbered on the flowchart to correspond with the process narrative numbering. Use consistent numbering in the narrative, flowchart, and control matrix to aid the reader in connecting the documents. Refer to the previous section, Section II, for more information concerning flowcharts.

	Due to PFM / File Description	Due Date	Attachment Number
Preliminary Process Narratives including process owner concurrence		1/22/10	N/A
Final Process Narratives including process owner concurrence		3/31/10	N/A
Preliminary Process Flowcharts including process owner concurrence		1/22/10	N/A
Final Process Flowcharts including process owner concurrence		3/31/10	N/A

I. Evaluate Entity-Level Controls

The control environment is the organization structure and culture created by management and employees to provide internal control. The control environment is the foundation for all other components of internal control and influences the control consciousness of those working in the organization.

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

- **Control Environment** – Management and employees have a positive and supportive attitude toward internal control and are conscientious. Management conveys the message that

integrity and ethical values must not be compromised. Interior demonstrates a commitment to the competence of its personnel and employs good human capital policies and practices. Management has a philosophy and operating style that is appropriate to the development and maintenance of effective internal control. Interior's organizational structure and the way in which it assigns authority and responsibility contribute to effective internal control. The agency has a good working relationship with Congress and oversight groups.

- **Risk Assessment** – Interior has established clear and consistent entity-wide objectives and supporting activity-level objectives. Management has made a thorough identification of risks, from both internal and external sources, which may affect the ability of the agency to meet those objectives. An analysis of those risks has been performed, and Interior has developed an appropriate approach for risk management. In addition, mechanisms are in place to identify changes that may affect the agency's ability to achieve its financial reporting objectives.
- **Information and Communication** – Information systems are in place to identify and record pertinent operational and financial information relating to internal and external events. That information is communicated to management and others within Interior who need it and in a form that enables them to carry out their duties and responsibilities efficiently and effectively. Management ensures that effective external communications occur with groups that can affect the achievement of the agency's missions, goals, and objectives. The agency employs various forms of communications appropriate to its needs and manages, develops, and revises its information systems in a continual effort to improve communications.
- **Control Activities** – Appropriate policies, procedures, techniques, and control mechanisms have been developed and are in place to ensure adherence to established directives. Proper control activities have been developed for each of Interior's activities. The control activities identified as necessary are actually applied properly.
- **Monitoring** – Interior internal control monitoring assesses the quality of performance over time. This is done by implementing procedures to monitor internal control on a continuous basis as a part of the process of carrying out its regular activities. This includes ensuring that managers know their responsibilities for internal control and control monitoring. In addition, separate evaluations of internal control are periodically performed and the deficiencies found are investigated. Procedures are in place to ensure that the findings of all audits and other reviews are promptly evaluated, decisions are made about the appropriate response, and actions are taken to correct or otherwise resolve the issues promptly.

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. The IRRT contains a tab within the Excel workbook that encompasses questions pertaining to the Entity-level review.

Steps to be Completed

- PFM will provide to each bureau/office the IRRT.
- Bureaus/Offices will use the IRRT entity level and efficiency evaluation tabs to document the entity level and efficiency evaluation review and provide a narrative summary of the results to

PFM.

Due to PFM / File Description	Due Date	Attachment Number
Entity Level Assessment and Efficiency Evaluation Review (IRRT)	3/1/10	N/A
Narrative Summary of the Results	3/1/10	N/A

J. Document and Evaluate Process-level Controls

Controls are all the methods by which a component/assessable unit governs its activities to accomplish its mission. Simply put, the controls within a program 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.

Document Controls and Identify Key Controls

Documenting controls entails documenting the activities and processes for initiating, recording, and reporting transactions for significant accounts and disclosures in order to identify the controls within each process; assessing the effectiveness of the design of the controls to determine whether the controls, as designed, would prevent or detect a material error or misstatement related to an account or groups of accounts; and document the assessment process.

A key control is a control whose failure could result in a potential for a material misstatement of the financials. Bureaus/Offices are responsible for identifying key controls in each of the key business process. The key controls should be documented on the business process control matrix.

Additionally, business process narratives should clearly identify key manual controls and workarounds. Key manual controls identified in the business process narratives should be traceable from the business process narratives through the flowcharts and control matrices. In other words, control matrices should identify key manual controls in a manner identical to the way they are identified in business process narratives and flowcharts.

Key manual controls, which mitigate known IT control gaps or failures, should be clearly marked as a workaround. Also, the specific system should be indicated (e.g., FBMS or other system) if the workaround is mitigating. If there is an IT control failure and there is a mitigating manual control for that failure, the manual control must be linked to that specific IT control failure.

Control Matrices are developed to ensure that risks in the key business process have been identified and controls developed to mitigate the risk. The bureau/office should identify and document risks in each sub-process and then identify control objectives and activities necessary to mitigate those risks.

During FY 2009, the Finance Officers Partnership designated a sub-team, led by the Fish and Wildlife Service, to review three business processes and determine a standard set of key controls for each business process. The business processes that were reviewed are Fund Balance with Treasury, Financial Reporting, and Acquisition and Payables. The results of the team's work can be seen in Attachment 19. Each bureau must identify these same key controls shown in the

attachment in their business process narratives and control matrix. Additional business processes will be reviewed during FY 2010 to identify common key controls used by all the bureaus.

Steps to be Completed

- Bureaus/Offices should develop or update business process narratives, flowcharts, and control matrices for each of the key business processes and provide to PFM. See Attachment 13 for the control matrix format.

Obtain the process owner’s concurrence on the documentation of controls

Process narratives, flowcharts, and control matrices should be reviewed and approved by personnel responsible for the respective business processes. Process owners should sign and date the documentation to show that management has accepted the documentation as a correct representation of the process and controls (electronic concurrence of the business process memo and controls by the process owner is adequate).

	Due to PFM / File Description	Due Date	Attachment Number
	Process Control Matrices including process owner concurrence	3/31/10	13

K. Evaluate Control Design

Evaluate the key controls and determine if they are designed to prevent or detect material errors or misstatements related to an account or group of accounts. It may not be necessary to evaluate control design every year if a business process and the key controls have not changed from the subsequent year and the previous test indicated the control design was satisfactory. In those cases, the bureau/office should document no changes were made in process and provide a reference to the previous test of design work completed.

The design of key controls may be evaluated through interview, inquiry, inspection, re-performance and/or observation of the controls. Select transactions subject to the control and evaluate whether the design of the control would detect any errors or misstatements, assuming the control was properly executed. Key questions for management to consider include the following:

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

It is important to consider the following during the review of the control design’s effectiveness:

- Directness of the control technique in relation to the financial reporting assertion
- Frequency of the control’s application (e.g., daily, weekly, monthly)
- Experience and skills of personnel performing the control
- Separation of duties
- Procedures followed when a control identifies an exception condition.

Specifically, it is recommended that bureaus/offices complete the following for each key business process:

- Conduct walkthroughs of the process to determine the actual process that is followed.
- Conduct group interviews of personnel involved in the process to obtain explanation of procedures followed.
- Validate process flowcharts and narratives prepared by program managers.
- Analyze controls design and identify any gaps.
- Identify recommendations for corrective actions for gaps.

The bureau/office should document the results of the evaluation of control design. The documentation should include the following:

- Names of any persons interviewed
- Specific items selected for evaluation
- Results of the evaluation that include a conclusion on the effectiveness the control design.
- Corrective action plans if the control design is not effective.

Testing is not needed if a control over a significant account or group of accounts is missing or the design is not suitable to the associated risk. Instead, absent or unsuitable controls should be noted in the issue log and corrective actions should be planned and implemented. Conducting testing of controls helps determine if any actual loss, fraud, error, improper payment, or noncompliance occurred.

Due to PFM / File Description	Due Date	Attachment Number
Results of Evaluation of Control Design (if applicable)	6/30/10	N/A

L. Evaluate Third-Party Service Providers

The Department uses internal and external service organizations to process some financial data. The external service providers were identified during the Planning phase. These external service organizations should be evaluated to determine whether the functions performed are significant. If the functions are significant, evaluate evidence describing the operating effectiveness of the provider’s controls. Third-party service providers are considered part of DOI’s information system when they affect the following:

- The classes of transactions in operations significant to financial reporting.
- The procedures, by which transactions are initiated, recorded, processed, and reported from the occurrence to their inclusion in the financial reports.
- The related accounting records, whether electronic or manual, supporting information, and specific accounts in the financial reports involved in initiating, recording, processing and reporting transactions.
- How the Department’s information system captures other events and conditions that are significant to the financial reports.

- The financial reporting process used to prepare the Department's financial reports, including significant accounting estimates and disclosures.

A service provider may contract with its auditors to issue a report, based on Statement of Auditing Standards No. 70 (SAS 70), Service Organizations. There are two types of reports, as follows:

- **Type I Report:** Covers the design of a service provider's controls.
- **Type II Report:** Covers both the design and the operating effectiveness of the service provider's controls.

If only a Type I report for the service provider is available, tests of the provider's controls must be performed to assess operating effectiveness of the internal controls over financial reporting related to the functions performed by the service provider. A Type II report for the service provider represents additional evidence about the effectiveness of the controls at the service provider as long as the following matters are addressed to satisfaction.

In reviewing and evaluating the SAS 70 report, bureaus/offices have several primary responsibilities, which are to be documented in Attachment 14 and submitted to PFM. The bureau/office must review the following:

- The type of opinion provided by the auditor. If the opinion is not unqualified, obtain an understanding of the nature of the auditor's findings and how these findings may affect the operating effectiveness of Interior's internal controls over financial reporting.
- The time period covered by the report. The report should cover a sufficient portion of the assessment period to provide evidence of the operating effectiveness for the entire assessment period. If a significant period of time has passed between the end of the time period covered by the service auditor's test of controls and the date of assessment, perform procedures to determine any information in the SAS 70 Type II report in need of update to reflect significant changes in the service organization's controls.

In addition, bureau/office must complete the following in accordance with OMB Bulletin No. 07-04, sections 6.15 through 6.18:

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

In addition, roll forward memos from the service provider for the period July 1 to September 30 (or the gap between the end of the period in the SAS 70 report and the end of the fiscal year)

should also be obtained and reviewed by the bureau/office. Documentation of the review should be maintained.

The SAS 70 reports will have a disclaimer for those controls that should exist at the bureau/office. Each bureau/office must examine these disclaimed controls and, for those considered key controls, appropriately test the controls. The bureau/office must also ensure that those disclaimed controls not considered key are a part of its documentation of controls.

Steps to be Completed

- PFM has provided bureaus/offices with a SAS 70 Review Checklist (see Attachment 14 for review and use). PFM will obtain and send out SAS 70 reports for those providers that are used by all Interior bureaus/offices. Bureaus/offices must obtain all other SAS 70 reports deemed necessary to review for their bureau/office.
- Bureaus/Offices will review SAS 70 reports, document the review on the checklist and submit to PFM.

Not all third party service providers have SAS 70 reviews conducted or will share the review results with the bureau/office. In that case, the bureau/office must document its attempts to obtain the reviews.

	Due to PFM / File Description	Due Date	Attachment Number
	Type II SAS 70 Report Checklist	9/1//10	14

M. Understand the IT Infrastructure and Associated Risks

The IT infrastructure and related controls are critical to achieving the Department’s missions and manage processes. Strong IT controls are necessary for good internal control over financial reporting. It is critical that technology based controls are assessed. The bureau/office staff should work closely with their respective Chief Information Office when assessing the IT controls over financial reporting.

Evidence that IT system components are operating effectively supports the assessment of internal controls over financial reporting. Applicable system components (e.g. calculations, accumulations, interfaces, and reports) are those affecting significant accounts or disclosures and other relevant financial assertions. Evaluate the following elements of IT controls:

General IT policies and procedures

- General IT policies and procedures are controls relating to key areas like IT strategic planning, budgeting, roles and responsibilities, segregation of duties, resource management, and third-party providers. The Department is integrating the assessment of IT controls as part of the evaluation of internal controls over financial reporting. Compliance with FFMIA and FISMA serve as a foundation for documenting and evaluating the IT controls over financial reporting.

IT general controls

- **Systems development and change management:** Ensure that IT systems perform their intended functions in an unimpaired manner, free from unauthorized or inadvertent manipulation, and are able to achieve data completeness, accuracy, and timeliness.
- **Availability:** Key financial systems subject to outage would adversely affect internal controls because the capability to process, retrieve, and protect data is vital to the Department's ability to accomplish its mission. Key elements related to data availability that need to be considered are business continuity, contingency plans, and environmental and hardware maintenance controls.
- **Information security:** The Department-wide IT security program develops policies, assigns responsibilities, monitors security-related controls, and otherwise manages security risks. Access controls for general support systems and applications should provide reasonable assurance that computer resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized alteration, disclosure, loss, or impairment.

IT automated controls

- Include the identification and evaluation of key automated controls during the evaluation of the design and operating effectiveness of key controls. Computerized operations may be assessed further by considering the following factors:
 - Uniform processing of transactions
 - Automatic processing
 - Data validated in real-time or after the transaction was processed
 - Increased potential for undetected misstatements
 - Existence, completeness, and volume of the audit trail
 - Nature of the hardware and software used
 - Unusual or non-routine transactions

N. Test at the Transaction Level

Define and document the testing approach

The purpose of testing is 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 business process memos narratives, flowcharts, and control matrixes 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 memos, flowcharts, and control matrixes to ensure that all key controls will be subject to testing.

Testing documentation should be prepared in sufficient detail to provide a clear understanding of the test's purpose, source, and conclusion, as well as evidence of secondary review. The documentation should be sufficient enough so that an independent party would understand the nature, timing, extent,

and results of the procedures performed. In effect, an independent party should be able to re-perform the test described in the working papers and reach the same conclusions.

Risk-Based Approach

Bureaus/Offices must take a risk-based approach in determining when to test key controls. Once a baseline is established on the operating effectiveness of key controls, not all key controls must 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. Specifically, risk-based testing is permitted under the following circumstances:

In instances where more than one key control is in place to accomplish a particular control objective, not all complementary controls have to be tested each year, provided that for those controls not tested:

- There are no known weaknesses in the function of the control;
- The control has been tested within the past 3 years and no deficiencies were found; and,
- There have been no changes in the design or operation since it was last tested (e.g., change in personnel responsible for implementing the control).

In instances where similar key controls are employed across multiple systems (e.g., computer access controls), not all systems have to be tested each year, provided that for those systems not tested:

- There are no known significant weaknesses of such control;
- The control has been tested within the past 3 years and no deficiencies were found;
- There have been no changes in the design or operation of the control since it was last tested; and,
- The system is not individually significant to the financial report.

In instances where key controls are fully automated (including automated general, application, and security controls), not all controls must be tested each year, provided that, for those controls not tested:

- The control is fully automated as opposed to a manual control or partially automated;
- The control is not dependent on some manual intervention to be effective;
- Management has verified that adequate change controls exist over the automated control;
- No changes in the design or operation of the control have occurred since the control was last tested;
- There are no known significant weaknesses of such control; and,
- The control has been tested in the past three years and no deficiencies have been found.

Steps to be Completed

- Management must document its risk based testing plan in narrative form and address how it complies with the above requirements.
- The analysis must be submitted to PFM for review and approval.

Nature of testing

In developing the test program, the bureaus/offices should define a testing procedure for each key control. The following are the four basic types of tests:

- **Inquiry** – Asking people if certain controls are in place and properly functioning (e.g., do you reconcile your activity or do you review a certain report each month).
- **Inspection** – Looking at evidence of a given control procedure (e.g., looking for signatures of a reviewing official or reviewing past reconciliations).
- **Observation** – Observing actual controls in operation (e.g., observing a physical inventory or watching a reconciliation occur).
- **Re-performance** – Re-performing a given control procedure (e.g., recalculating an estimate or re-performing a reconciliation).

Inquiry and observation are less persuasive forms of evidence than inspection and re-performance.

Timing of testing

The bureau/office should schedule testing to occur throughout the year or quarterly for those controls that coincide with preparation of quarterly financial statements to OMB. Certain financial reporting controls traditionally only operate at year-end, so there is only one opportunity to test and no opportunity to remedy failure. Consider implementing them during the quarterly financial reporting process, so time is available for remediation and verification.

Location and extent of testing

The selection of locations for testing should consider the risks of error and materiality. The locations and extent of testing should be documented in the test plan.

Figure 7 shows suggested sample sizes from the CFO Council's Implementation Guide:

Occurrence	Sample Size	Example
Ongoing	45	Approval of requisitions
Daily	30	Daily downloads of charge card transactions
Weekly	10	Weekly receipt of invoices
Monthly	3	Month end journal entry approval
Quarterly	2	Reconciliations
Semi-annually	1	Reconciliations
Annually	1	Approval of budgetary documents

Figure 7: CFO Council's Implementation Guide Sample Sizes

To generate the selection, a random number generator should be used. In the case of less frequent occurrences, a representative selection could also be used. If a random number generator is not available there are alternate methods that can be employed. One method is to obtain a listing of the transactions for the section currently being tested (this can be electronic or hard copy). Pick an arbitrary number (n) and using the listing select every nth number. An example of this procedure would flow like this: There are 10,000 transactions in the population and the sample

selection size was determined to be 45. The arbitrary number picked is 150. The first selection would be transaction number 150. The subsequent transactions selected would be number 300, 450, 600, and so on until the sample selection size of 45 is reached. This method can be altered to accommodate most populations. If selections over a certain dollar amount or certain time periods are desired for testing, then the listing of transactions needs to be altered to fit the constraints of the test.

Steps to be Completed

- The analysis of risk based testing and an overarching test plan documenting the bureau's overall approach to testing, including sample selection and sample size must be submitted to PFM for review and approval.

Due to PFM / File Description	Due Date	Attachment Number
Narrative description of the risk-based testing plan approach	7/30/10	N/A

O. Conclude, Report, and Correct

Concluding on effectiveness

Test results will support management’s judgment whether a control is functioning adequately or not. Beyond just dollar amounts, consider whether a control that is not executed properly or consistently would allow a material error or misstatement to occur. Process owners should review and validate detected errors and determine if compensating controls may mitigate the problem. A compensating control is a technique or other effort(s) designed to mitigate the absence of a control or to mitigate a deficiency in control design or operating effectiveness. The sampling plan should allow for the expansion of the sample to determine if the initial error rate is correct when it appears the original smaller sample was not representative of the function of the controls. If, after additional testing, the control is still considered to be not functioning, it should be documented as deficient (i.e., a control that is not functioning nor is mitigated by other controls).

As a final step, process owners should also review the likely impact of the control gaps on financial reporting. A control gap exists when a control for a given financial statement assertion does not exist, does not adequately address a relevant assertion, or is not operating effectively. List the gaps in the list of deficiencies and document suggestions for repairing controls and processes. This provides management the opportunity to remedy the deficient controls prior to the Department’s assessment date.

SAS 115 included the following definitions of deficiencies:

- **Deficiency in Internal Control** – 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 and correct misstatements on timely basis.
- **Deficiency in Design** – 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 would not be met.

- **Deficiency in Operation** – exists when a properly designed control does not operate as designed or the person performing the control does not possess the necessary authority or competence to perform the control effectively.
- **Material Weakness** – a deficiency or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity’s financial statements will not be prevented, or detected and corrected on a timely basis.
- **Significant Deficiency** – a deficiency, or a combination of deficiencies, in internal control, that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Reporting

The bureau/office must consider the likelihood and degree of potential for misstatement in order to assign the level of deficiency to be reported. When all results have been reported, management can then make the determination if the consolidation of deficiencies is incidental, consolidate to create a significant deficiency, or rise to the level of material weakness for reporting in the assurance statement.

The bureau/office should determine if a deficiency is mitigated by a compensating control. If a compensating control exists and found to be operating effectively, the bureau can decide not to report the deficiency.

- **Issue Log**

Material weaknesses, significant deficiencies, and non-compliance issues identified during testing should be noted on the Issue Log. Deficiencies that were not determined to be material weaknesses, significant deficiencies, or non-compliance issues should be tracked by the bureau/office.

Steps to be Completed

- PFM will provide each bureau/office an issue log (see attachment 15).
- Bureaus/Offices will complete the issue log (with all issues identified) and provide to PFM at the same time as the June 30 assurance statement, but not as an attachment to the assurance statement.

- **Reporting required as of June 30 (including material weaknesses)**

DOI is required to provide a statement of assurance over the effectiveness of internal controls over financial reporting as of June 30 of the fiscal year in the AFR. The AFR is published after September 30 because it includes the agency’s audited financial statements that are prepared using balances as of September 30.

- **Reporting required as of September 30 (including material weaknesses)**

As discussed above, the assessment of internal control over financial reporting is as of June 30. If an agency receives an audit opinion on the internal controls over financial reporting, the “as of” date can be changed to September 30 to better align with the audit opinion.

- **Changes in Status between June 30 and September 30**

Review the Department’s plan for correcting deficiencies to ensure that sufficient time is available to both complete the remediation and retest the controls prior to either the assessment date (June 30) or the fiscal year-end (September 30). Attempting to correct

control deficiencies as they are identified benefits the Department by improving the controls in the current fiscal year and allowing for preparation of the assurance statement without including control deficiencies corrected prior to June 30, or at least reporting they were corrected prior to the end of the fiscal year.

If adequate time is available, test the remedied controls to determine whether the design and operation of the controls are effective as of June 30 or September 30. The testing should be tracked to ensure that it covers transactions in the proper period. Any additional testing that cannot be completed for the applicable period in time for the results to be reported in management's September 30 assurance statement should not be performed since there is no benefit for the year to which the report pertains.

Use the following process to identify changes in the internal control environment that may impact management's assessed effectiveness of internal controls over financial reporting after June 30:

- Survey departmental and bureau management to identify any potential changes in the internal control environment that require assessment, such as:
 - Major changes in the Department's mission or programs;
 - Reorganizations or other changes to the Department's organizational structure;
 - Significant increases or decreases in staffing levels; and,
 - Turnover of key management or personnel who perform key control activities.
- Communicate with persons leading other Departmental assessments, reviews, and audits to determine if any potential material weaknesses were identified that were not detected during the earlier assessment;
- Review the results of follow-up testing used to validate the effectiveness of CAPs if material weaknesses were reported as resolved;
- Review results of the financial statement audit;
- Review results of any program audits performed by the OIG or GAO; and,
- Review results of any bureau review or evaluation.

Interior is required to provide a statement of assurance over any weaknesses significant enough to report outside Interior and must be included in Interior's assurance statement that is in the AFR. Significant deficiencies identified under FISMA are also considered material weaknesses and must be included in the assurance statement if they might cause a material misstatement to the Department's financial reports.

Develop a CAP using the standard template (Attachment 15) for all deficiencies. Provide quarterly updates on material weakness and significant deficiency CAPs to PFM. PFM will monitor the status of the corrective action plan implementation.

Steps to be Completed

- PFM will provide each bureau/office a sample CAP (see attachments 15).
- Bureaus/Offices will develop a CAP for each deficiency.
- Bureaus/Offices will provide PFM CAPs for material weaknesses, significant deficiencies, and non compliance issues on a quarterly basis.

Due to PFM / File Description	Due Date	Attachment Number
Conclude on Control Effectiveness	7/30/10	N/A
Prepare Report on Control Deficiencies and Determine the impact on Financial Reporting	7/30/10	N/A
Issues Log	Quarterly and 8/16/10	15
Assurance Statement	8/16/10	17 or 18
Verify Key Controls have no Reportable Changes from 6/30/10 to 9/30/10	9/30/10	N/A
Updated Assurance Statement	9/30/10	17 or 18

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. §§ 3561-3567), 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. A risk assessment was conducted during FY 2009 and separate guidance will be distributed to the appropriate financial areas if a risk assessment for improper payments is necessary for FY 2010.