Description of document:	Department of the Interior (DOI) Office of Financial Management Internal Control and Audit Follow-up Handbook, 2015
Requested date:	14-March-2017
Released date:	20-March-2017
Posted date:	31-July-2017
Source of document:	FOIA Request Department of the Interior Office of the Secretary (OS) Clarice Julka; MS-7328 MIB 1849 C Street, NW Washington, DC 20240 Fax: (202) 219-2374 E-Mail: Contact Us Online FOIA request form

United States Department of the Interior
OFFICE OF THE SECRETARY
Washington, DC 20240

IN REPLY REFER TO:
7202.4-OS-2017-00339

March 20, 2017

Via Email

On March 14, 2017, you filed a Freedom of Information Act (FOIA) request seeking the following:

> A digital/electronic copy of the DOI Internal Control and Audit Follow-Up ICAF Handbook.

Your request was received in the Office of the Secretary FOIA office on March 14, 2017, and assigned control number **OS-2017-00339**. Please cite this number in any future correspondence or communications with the Office of the Secretary regarding your request.

We are writing today to respond to your request on behalf of the Office of the Secretary. Please find attached one file, consisting of 151 pages, which are being released to you in their entirety. This completes our response to your request.

Because your entitlements as an "other-use requester" (See 43 C.F.R. § 2.39) were sufficient to cover all applicable FOIA charges, there is no billable fee for the processing of this request.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. 552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

The 2007 FOIA amendments created the Office of Government Information Services (OGIS) to offer mediation services to resolve disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. Using OGIS services does not affect your right to pursue litigation. You may contact OGIS in any of the following ways:

Office of Government Information Services (OGIS)
National Archives and Records Administration
8601 Adelphi Road
College Park, MD 20740-6001
E-mail: ogis@nara.gov
Web: https://ogis.archives.gov
Telephone: 202-741-5770
Fax: 202-741-5769
Toll-free: 1-877-684-6448

Please note that using OGIS does not affect the timing of filing an appeal with the Department's FOIA & Privacy Act Appeals Officer.

If you have any questions about our response to your request, you may contact Karmen Young by phone at 202-513-0765, by fax at 202-219-2374, by email at os_foia@ios.doi.gov, or by mail at U.S. Department of the Interior, 1849 C Street, NW, MS-7328, Washington, D.C. 20240.

You also may seek dispute resolution services from our FOIA Public Liaison, Clarice Julka.

Sincerely,

Clarice Julka
Digitally signed by CLARICE JULKA
Date: 2017.03.20 13:11:59 -04'00'

Clarice Julka
Office of the Secretary
FOIA Officer

Electronic Enclosure

U.S. DEPARTMENT OF THE INTERIOR
MARCH 3, 1849

Department of the Interior

Office of Financial Management

Internal Control and Audit Follow-up Handbook

As Revised March 27, 2015

Table of Contents

EXECUTIVE SUMMARY

This handbook is a reference tool to assist Department Managers, Internal Control Coordinators, and Audit Liaison Officers who are responsible for carrying out responsibilities in the Internal Control Program and/or Audit Followup Program. These responsibilities include implementing recommendations contained in audit reports issued by the Office of Inspector General (OIG) and the Government Accountability Office (GAO) and for carrying out the requirements of the Federal Managers' Financial Integrity Act (FMFIA), which requires agencies to annually provide a statement of assurance regarding the effectiveness of internal controls, administrative and accounting controls, and financial management systems.

This handbook provides:

- an overview of the Departmental Internal Control and Audit Followup Programs;
- pertinent references to the Office of Management and Budget and GAO guidance; and,
- detailed guidance and instruction to implement the provisions and requirements of the Department's Internal Control and Audit Followup Programs.

Interior believes that maintaining integrity and accountability in all programs and operations: (1) is critical for good government; (2) demonstrates responsible stewardship over assets and resources in Interior's care; (3) ensures high quality, responsible leadership; (4) ensures the sound delivery of services to customers; and, (5) maximizes desired program outcomes. Management, administrative, and financial system controls have been developed and implemented to reasonably ensure that:

- programs and operations achieve their intended results efficiently and effectively;
- resources are used in accordance with the Department's mission;
- programs and resources are protected from waste, fraud, and mismanagement;
- laws and regulations are followed; and
- reliable, complete, and timely data is maintained and used for decision making at all levels.

Interior firmly believes that correction of identified material weaknesses and the timely implementation of OIG and GAO audit recommendations is essential to improving the efficiency and effectiveness of its programs and operations as well as achieving integrity and accountability goals.

The Assistant Secretary – Policy, Management and Budget is the Interior’s Chief Financial Officer, Chair of the Internal Control and Audit Followup Council, and Audit Followup Official. The Audit Followup Official is responsible for ensuring that systems and procedures are in place to respond to, resolve, and track the Interior’s progress in implementing recommendations contained in audit reports and that actions are taken to correct identified program and administrative material weaknesses. The Assistant Secretary has delegated day-to-day responsibility for the Internal Control and Audit Followup Programs to the Office of Financial Management (PFM).

The staff of the Internal Control and Audit Followup (ICAF) Branch within PFM carries out the day-to-day responsibilities of the Internal Control and Audit Followup Programs. Department Managers, Internal Control Coordinators, and Audit Liaison Officers are encouraged to contact the ICAF staff for assistance as they carry out the requirements of the Internal Control and Audit Followup Programs.

SECTION 1
INTERNAL CONTROL PROGRAM

TABLE OF CONTENTS

1. INTRODUCTION

1.1. PURPOSE

The purpose of this chapter is to provide practical guidance and suggestions for planning and conducting an internal control review that meets the Department of the Interior's (Interior's, DOI's, the Department's) Internal Control Program (ICP, the Program) requirements. This document is intended to be used by Interior's personnel as a "how to" reference when completing internal control reviews of programs, activities, and functions. This document is closely aligned with the requirements for the Office of Management and Budget's (OMB) Circular A-123 (A-123), *Management's Responsibility for Internal Control*; Departmental requirements; and Interior's goals for having efficient, effective, and accountable programs.

1.2. BACKGROUND

The following information provides a brief overview of Interior's Internal Control Program.

1.2.1. Definition of an Internal Control

An internal control is an activity, process, or procedure used to mitigate risk and to help organizations achieve its mission-related objectives. Controls are the activities used to accomplish organizational objectives, safeguard assets, and comply with laws and regulations in an effective, efficient manner. Controls may include critical processes for accomplishing organizational goals, program reviews, facility inspections, corrective action plans, or program monitoring activities.

For example, the Continuity of Operations Planning (COOP) Programs throughout DOI coordinate the development of emergency action plans and training of emergency responders. The development of emergency action plans is considered an internal control because the plans mitigate the risk of loss of operations and further loss or damage in the wake of an unplanned failure or catastrophe. Without development of these plans, the COOP Program could not achieve its annual goals. This program will be used as an example throughout this chapter.

1.2.2. Federal Internal Control Compliance Requirements

Legislative and regulatory requirements for federal agencies to establish and maintain adequate internal control programs are not new; they date back more than fifty years. The historical evolution of the internal control program is characterized by a number of key events that have a significant influence on the current program as it operates today. In December 2004, the OMB revised A-123 to state that Government agencies and management have a fundamental responsibility to develop, establish, and maintain effective internal controls as a primary method of improving accountability, effectiveness, and efficiency, and for preventing fraud, waste, and mismanagement to achieve desired objectives. Program, Information Security, and Financial managers must operate and use resources consistent with an agency's mission and in compliance with laws and regulations. The Congress, the OMB, and the Government Accountability Office (GAO) have reinforced this need.

It further requires, in Appendix A, that management submit an assurance statement over financial reporting through June 30 each year, to be updated in the annual assurance statement due September

30 each year. The A-123 requires submitting the Agency-wide Annual Assurance Statement (Program and Finance) by September 30.

Specifically, A-123 requires managers to "take systematic and proactive measures to (i) develop and implement appropriate, cost-effective internal control for results-oriented management; (ii) assess the adequacy of internal control in Federal programs and operations; (iii) separately assess and document internal control over financial reporting consistent with the process defined in Appendix A; (iv) identify needed improvements; (v) take corresponding corrective action; and (vi) report annually on internal control through management assurance statements."

Additionally, A-123 states, “Instead of considering internal control as an isolated management tool, agencies should integrate their efforts to meet the requirements…to improve effectiveness and accountability. Thus, internal control should be an integral part of the entire cycle of planning, budgeting, management, accounting, and auditing. It should support the effectiveness and the integrity of every step of the process and provide continual feedback to management."

To comply with OMB Circular A-123 agency-wide Annual Assurance Statement requirements, agency managers should continuously monitor and improve the effectiveness of internal controls associated with their programs. This continuous monitoring, and other periodic assessments, should provide the basis for the bureau Directors’ and the Agency Heads’ annual assessment of and report on internal control, as required by Interior’s policy in support of the Federal Manager’s Financial Integrity Act (FMFIA).

1.2.3. Interior's Internal Control Compliance Requirements

Interior has established the following objectives for the ICP to promote a common understanding that management has a fundamental responsibility for achieving results. Interior’s overall objectives for the Program are twofold:

a) To ensure that a sound system of internal controls exists in all programs, operations, organizations, and functions that meet the objectives and requirements of FMFIA and OMB Circular A-123, as revised; and,
b) To implement an effective, efficient, and systematic approach to assessing internal controls that integrates with other management improvement initiatives within Interior.

The Interior’s specific objectives for the internal control program are to ensure that bureaus/offices are:

a) Operating efficiently and effectively;
b) Managing and protecting resources;
c) Complying with laws and regulations;
d) Sustaining effective controls over financial reporting;
e) Using reliable program, IT, and/or financial information for day-to-day decision making; and,
f) Achieving stated program performance goals.

For Interior to have an effective internal control program, management and staff must have an understanding and commitment to controls. Although responsibility for controls lies with management, all employees have a role in the effective and efficient operation of controls established by management. In this regard, management at all levels is responsible for reasonably assuring that:

a) Programs achieve the intended results;
b) Resource use is consistent with the agency mission;
c) Programs and resources are protected from waste, fraud, and abuse;
d) Laws and regulations are followed; and,
e) Reliable and timely information is obtained, maintained, reported, and used for decision making.

1.2.4. Authority

The authority for establishing and maintaining agency controls is established in the Accounting and Auditing Act of 1950 (U.S.C. 3512), as amended by the *Federal Financial Managers' Improvement Act of 1982* (FMFIA). The FMFIA, which is implemented by OMB Circular A-123, requires agencies to conduct an ongoing review of internal controls and to report annually on the adequacy of agencies' programs, operations, and financial reporting for internal control systems. Under authority provided by the *Government Management Reform Act of 1994* (GMRA), Interior's annual assurance statement on compliance with FMFIA is incorporated into Interior's Annual Financial Report (AFR). Appendix A to A-123 requires the submission of an additional assurance statement as of June 30 each year for controls over financial reporting (see Section 2 for more information on Appendix A). Interior managers should maintain environments where internal controls are understood, encouraged, and implemented.

Other acts which provide authority include the *Government Performance and Results Modernization Act of 2010* (GPRA); the *Chief Financial Officers Act of 1990* (CFO Act); *Federal Financial Management Improvement Act of 1996* (FFMIA); the *Federal Information Security Management Act of 2002* (FISMA); and the *Improper Payments Elimination and Recovery Improvement Act of 2012* (IPERIA).

1.3. GOVERNANCE STRUCTURE

Interior's internal control organizational structure provides for an integrated approach and interaction of many personnel from diverse disciplines. The structure starts with the Secretary, descends to the program Assistant Secretary, then to the bureau/office director, and finally to the assessable unit manager. Roles and responsibilities of key components of the Internal Control Program are described below.

1.3.1. Roles and Responsibilities

The roles and responsibilities of the key personnel of the Program help contribute to a successful achievement of Departmental mission and goals. Management recognizes the importance of internal controls to ensure efficient and effective programs and operations within their organizations and emphasizes an integrated, risk-based, systematic approach to assess them. Further, management should ensure that resources are available to assess controls and correct deficiencies.

Secretary — establishes the internal policy direction for the Internal Control Program and submits the Annual Financial Report (AFR) to the President and the Congress in November of each year that includes an annual FMFIA assurance statement as of September 30 of each year.

Assistant Secretary - Policy, Management and Budget (A/S-PMB) and Chief Financial Officer (CFO) — has operational responsibility for the Internal Control Program. The CFO Act placed responsibility for internal controls with the agency CFO to ensure Interior's compliance with A-123, Appendix D, FMFIA, the CFO Act, FFMIA, and GPRA.

Office of Inspector General (OIG) — is responsible for performing routine evaluations of internal controls within the scope of internal audits, as part of the OIG overall program of audits, evaluations, and investigations, and reporting the results in its semi-annual reports to Congress. In addition, the OIG annually reviews bureau/office administrative and accounting controls as part of the financial statement audits.

Program Assistant Secretaries (ASs) /Solicitor/ Bureau/Office Directors — are responsible for the various bureau/office programs within their purview and have Department-wide responsibilities for internal control as members of the Senior Management Council which, in DOI, is performed by the Principals Operating Group (POG). They are encouraged to establish internal control and audit follow-up councils or oversight groups in their respective organizations to coordinate and monitor internal control and audit follow-up requirements for their bureau/office programs. Such councils or oversight groups may be used to implement the responsibilities for internal control which, at a minimum, are:

- Institutionalizing the internal control process within their organizations;
- Establishing priorities in identifying, correcting, and reporting of internal control material weaknesses and accounting non-conformances;
- Ensuring that funding to correct identified deficiencies is addressed in the budget formulation and execution process;
- Establishing a quality assurance process that permits the responsible official to provide reasonable assurance to the Secretary that the objectives of the FMFIA are being achieved; and,
- Chaired by the A/S-PMB.

Deputy Ass and Bureau/Office Deputy Directors — comprise the Senior Assessment Team performed by the DOI Deputy Operating Group (DOG), which is chaired by the A/S-PMB. They are responsible for establishing and maintaining the system of internal control within their bureaus/offices. This includes determining that the system of control is consistent with the standards prescribed in OMB Circular A-123, which are drawn in large part from GAO's *Standards for Internal Control in the Federal Government*. This includes determining that the systems of control are functioning as intended; are properly documented; modifying the control systems, as appropriate, for changes required; and ensuring that the type, number, and quality of control evaluations conducted are sufficient to provide assurance in disclosing the existence of any internal control weaknesses or accounting systems non-conformance.
Bureau/office directors are also responsible for:

- Determining annually which programs or administrative functions should be subject to a formal review in order to supplement management's judgment as to the adequacy of internal controls;
- Ensuring Departmental internal control guidelines issued by the Office of Financial Management (PFM), the Office of Acquisition and Property Management (PAM), the Office of the Chief Information Officer (OCIO), and other Departmental Offices are implemented;
- Allocating adequate resources to evaluate control systems;
- Developing procedures, documentation, training, and reporting requirements necessary to review, establish, maintain, test, improve, and report on control systems within bureau/office programs and operations;
- Reporting to the A/S-PMB, in consultation with the program Assistant Secretary, internal control deficiencies identified in audit reports, internal reviews, and from other sources;
- Specifying employee accountability by including program-specific internal control elements and standards in all managers' performance evaluations;
- Ensuring timely correction and validation of all identified program and operational deficiencies, whether material or nonmaterial; and,

Program Managers / Assessable Unit Managers — Are responsible for ensuring compliance with requirements for internal controls for their programs. Specifically, they must undertake, within their programs, the duties listed above for bureau/office Directors including:

- Ensuring Departmental internal control guidelines are implemented;
- Performing risk assessments;
- Documenting program processes and controls;
- Preparing and conducting reviews of programs (includes control testing and documenting results);
- Implementing and tracking Corrective Action Plans (CAPs), as necessary;
- Certifying corrective actions have been implemented and completed; and,
- Providing assurance to the bureau/office Director.

Office of Financial Management (PFM) — PFM is responsible for:

- Recommending internal control policies and procedures;
- Providing oversight and guidance to the bureaus/offices concerning reviews, evaluations, tracking of CAPs for detected Material Weaknesses, and maintenance of effective controls; and,
- Managing, directing, and evaluating Interior's reporting under A-123, FMFIA, FFMIA, and the CFO Act.

Office of Acquisition and Property Management (PAM) — PAM is responsible for:

- Developing and issuing control evaluation guidelines for acquisition, Federal assistance, and property management functional areas;
- Assessing the results of bureau/office control evaluations in these areas;
- Providing PFM an annual summary assessment of the adequacy of bureau/office controls in these functional areas;
- Overseeing, monitoring, assessing, and recommending the completion of bureau/office corrective action plans addressing acquisition and property management material weaknesses; and,
- Advising PFM and A/S-PMB regarding the closure of bureau/office recommendations, as applicable.

Office of the Chief Information Officer (OCIO) — The OCIO is responsible for:

- Developing and issuing control evaluation guidelines for conducting reviews of information technology general support systems and major applications;
- Assessing the results of bureau/office control evaluations in these areas;
- Providing PFM with an annual summary assessment of the adequacy of bureau/office controls in these areas;
- Reviewing corrective action plans for identified Information Security deficiencies; and,
- Advising PFM and the A/S-PMB regarding the closure of bureau/office IT recommendations.

The **Internal Control Workgroup** is comprised of bureau/office internal control coordinators, bureau/office finance representatives, and representatives from various Departmental offices. The Group meets regularly to discuss the status of the assessments of internal controls over both programs and financial reporting and related issues.

Several other components of Interior also play a key role in the management of the internal control processes. These components include the Chief Financial Officers Council, the Executive Steering Committee for the Financial and Business Management System, and the various specialty groups that meet regarding specific matters (Finance Officers’ Partnership, Acquisition Council, etc.).

To promote the Internal Control Program in bureaus/offices, senior management leadership directs the planning, reviewing, and reporting for internal control overall 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/office key internal control functions should be documented.

See 340 Departmental Manual (DM) 1 (for detailed information on the roles and responsibilities of the A/S-PMB, Inspector General, Assistant Secretaries/Solicitor, bureau/office Directors, and others in Interior’s internal control process.

1.4. BENEFITS OF A STRONG INTERNAL CONTROL REVIEW PROCESS

Management is responsible for developing and maintaining internal control activities (controls) that comply with the following GAO/Committee of Sponsoring Organizations (COSO) standards:

- Control Environment – sets the tone of an organization influencing the control consciousness of its employees; in other words, the tone at the top.
- Risk Assessment – identification and analysis of risks to achievement of program objectives, helping to determine how the risks should be managed.
- Control Activities – 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 –the activities required to identify and communicate information in a timeframe that enables employees to carry out their responsibilities and take actions.
- Monitoring – the process to assess the quality of the internal control system's performance over time, including regular management and supervisory activities.

Strong internal controls are not just about compliance, but about performance. When implemented correctly, internal control reviews can improve the overall performance of an organization and effect the change required to meet or exceed mission goals. Ultimately, when organizations adopt internal control reviews into their culture as a tool for strengthening their daily operations, compliance becomes a by-product of high performance. By implementing a strong internal control review process, and conducting reviews in a manner consistent with the guidance provided in this document, Interior's programs, activities, and functions should:

- Improve overall performance and effectiveness in achieving organizational goals;
- Gain an enhanced understanding of its organizational risk exposure;
- Gain an understanding of organizational business processes and internal control activities;
- Inform, support, and/or justify funding requests and decisions;
- Be more efficient by identifying and removing unnecessary or ineffective internal control activities;
- Build a culture of continuous improvement into ongoing operations; and
- Comply with applicable laws, regulations, policies, and guidance.
- Minimize risk of fraud, waste, unauthorized use and/or misappropriation of funds.

There are other benefits that result from strong internal control reviews, such as the elimination of manual processes and identification of improvement opportunities. These benefits are identified through internal control reviews, as described in the following sections of this document.

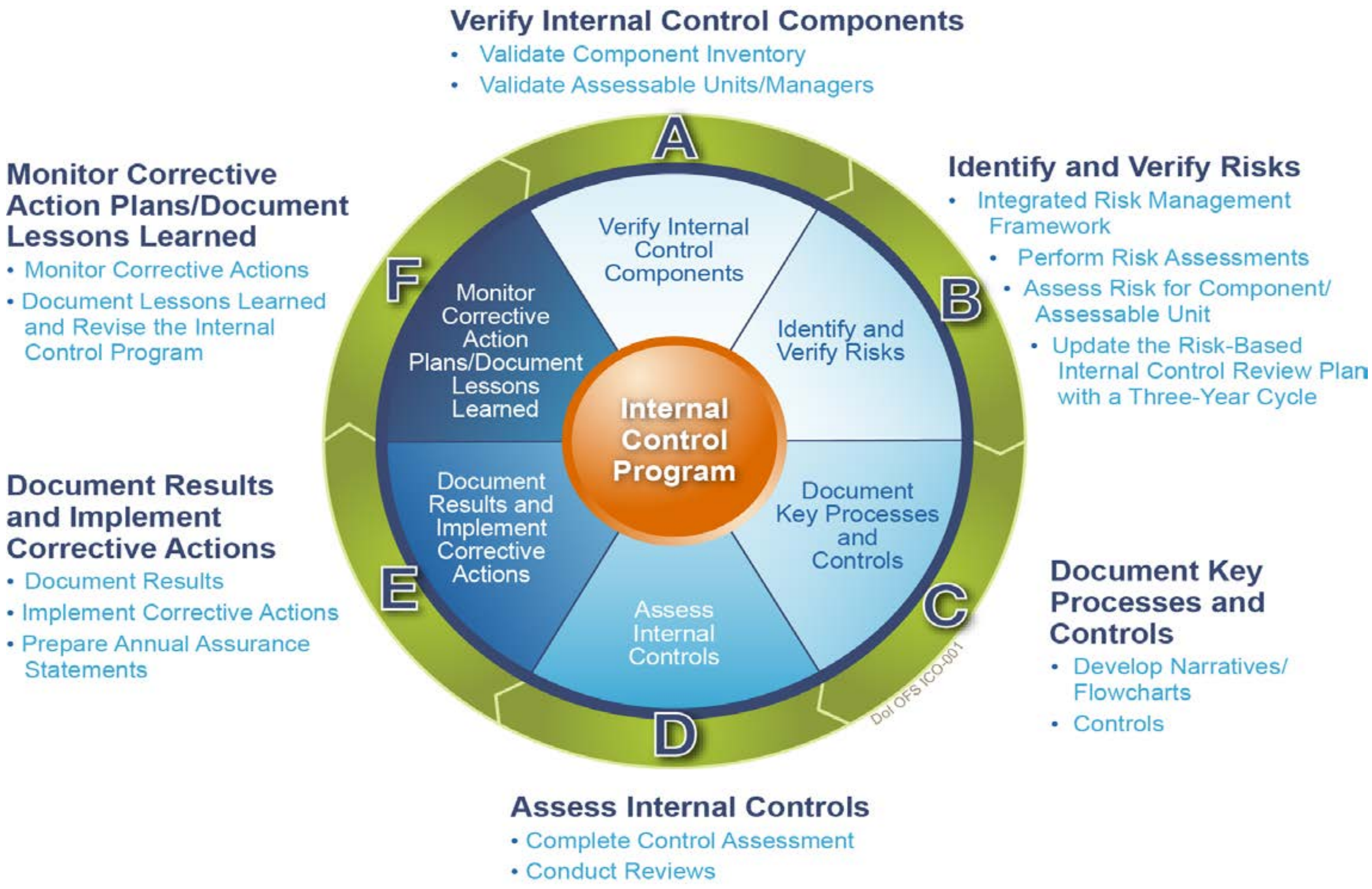
1.5. INTRODUCTION TO THE INTERNAL CONTROL CYCLE

Internal control activities should be considered part of a continuing cycle of improvement -- assessing the risks associated with each program component, identifying controls to mitigate these risks, and testing controls to ensure they are working effectively. Additionally, internal control should be an integral part of the cycle that occurs each year for planning, budgeting, and managing. The following steps comprise the Internal Control Program cycle for 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

This document is designed to go beyond the Internal Control Program Cycle showing Program Managers the "how to" of planning an internal control review; documenting key business processes and control activities; assessing internal controls; reporting review results and correcting findings; and concluding the internal control review. Figure 1 illustrates this cycle.

FIGURE 1: INTERIOR'S INTERNAL CONTROL PROGRAM CYCLE


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 Action Plans/Document Lessons Learned
Internal Control Program
DoI OFS ICO-001

Verify Internal Control Components
- Validate Component Inventory
- Validate Assessable Units/Managers

Identify and Verify Risks
- Integrated Risk Management Framework
- Perform Risk Assessments
- Assess Risk for Component/ Assessable Unit
- Update the Risk-Based Internal Control Review Plan with a Three-Year Cycle

Document Key Processes and Controls
- Develop Narratives/ Flowcharts
- Controls

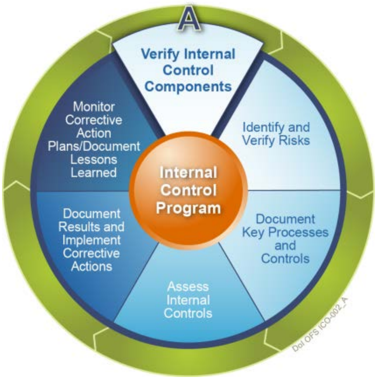
Assess Internal Controls
- Complete Control Assessment
- Conduct Reviews

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

Monitor Corrective Action Plans/Document Lessons Learned
- Monitor Corrective Actions
- Document Lessons Learned and Revise the Internal Control Program

2. STEP A: VERIFY INTERNAL CONTROL COMPONENTS

2.1. PURPOSE


A
Verify Internal Control Components
Identify and Verify Risks
Document Key Processes and Controls
Assess Internal Controls
Document Results and Implement Corrective Actions
Monitor Corrective Action Plans/Document Lessons Learned
Internal Control Program
DoI OFS ICO-002_A

The purpose of verifying internal control components and planning internal control reviews is to encourage Interior's personnel to dedicate adequate time for determining what organization should be reviewed, who will perform the review, the timing of the review, the frequency of the review, and the type of review to be performed.

During the initial phase of the internal control review process, senior executives identify specific programs, activities, and functions to be included in the component inventory. Senior executives also designate an assessable unit manager, typically the Program Manager, responsible for completing the internal control reviews for their respective areas. The assessable unit manager is responsible for the following planning activities:

- Identifying the organization’s inventory for their respective area (Component, Assessable Unit) and providing that data to their internal control coordinator (ICC);
- Determining whether an Internal Control Review is necessary or if an external review (e.g. Alternative Internal Control Review (AICR)) can be leveraged;
- Determining the schedule and preparing a timeline for the review;
- Determining the scope (i.e., the extent, breadth, and depth) of the review;
- Managing stakeholder communication and coordination; and
- Confirming that adequate resources have been provided to conduct the review.

Subsequent to planning the internal control review, assessable unit managers are responsible for coordinating the documentation of key business processes and control activities. Additionally, assessable unit managers are responsible for assessing controls, evaluating results, and determining corrective actions. Each of these activities is described in detail in the subsequent chapters of this document.

2.2. VERIFY INTERNAL CONTROL COMPONENTS

This step of the cycle includes validating the component inventory and validating the component and assessable unit managers. In order to complete an effective internal control review, it is necessary to first identify the organizations and individuals that exist within the bureau. Interior's senior executives are responsible for applying criteria to their respective organizations to determine what programs, activities, or functions comprise a component, assessable unit, and sub-assessable unit. This information is recorded in the bureau's/office's component inventory, which is updated and submitted to PFM annually, using the Department’s template.

The following sections contain criteria that should guide senior executives in identifying the bureau components and managers responsible for conducting internal control reviews.

2.2.1. Validate the Component Inventory

Components are the major programs, administrative activities, organizations, or functional subdivisions, within the bureau/offices, that require one or more separate systems of internal control. Components should be aligned with the bureau/office organizational structure, constitute a significant portion of their administrative activities or budget, and should perform a unique function or functions to achieve a specific set of objectives. The component inventory should align with the bureau's/office's mission and strategic plan and can provide management with a comprehensive view of their organizational entities. This can be accomplished by reviewing the bureau's/office's organizational chart, budget alignment, and structure used for Activity Based Costing (ABC). The organization chart is a starting point for identifying its components. Additional criteria that should be used to identify components include the following:

- **Leadership** - Components are led by senior executives possessing knowledge of the broader risks to the organization and accountable for the organization's operations.
- **Political Visibility** - Components should have Department-level visibility. In other words, managers at the component-level should have regular interaction with senior leadership.
- **Comprised of Multiple Assessable Units** - Components usually consist of multiple assessable units.

The following are examples of bureau/office components.

Most bureaus/offices have the following components within their organization:

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

Examples of other components include the following organizations:

1. Regional Operations
2. Safety and Security
3. Programs

2.2.2. Validate Assessable Units

An assessable unit is a subdivision of a component. An assessable unit can be the program, activity, or function within the component that is significant to Interior's operations or budget. A clear line of authority should exist between an assessable unit and the component, and assessable unit managers should report directly to component managers. Assessable units usually exist below the organizational chart level...Each assessable unit should have an assessable unit manager who will be responsible for ensuring that appropriate risk assessments and control testing are performed and documented. It is possible that not all assessable units will be subject to a review – this should be a risk-based decision.

The following excerpt describes the characteristics of an assessable unit:

An assessable unit should:

- Have well-defined management boundaries distinct from the component because its operations are measured against specific program objectives, and
- Be large enough to be meaningful when describing how Interior achieves its mission objectives.

Each of these assessable units may have a manager designated as the lead person for that assessable unit. Continuing with the example given above, several components have been identified: Law Enforcement, Human Capital, Labor Relations and Information Resources. Within one component, Human Capital, the following assessable units may exist:

1. Benefits Processing
2. Security and Safety
3. Employee Training
4. Labor Relations

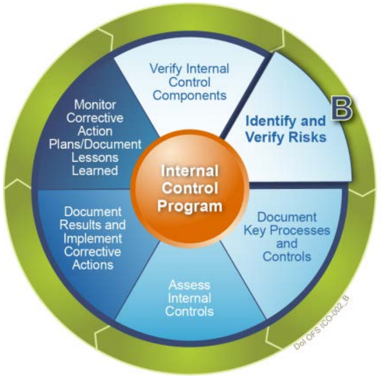
The following are additional considerations that should be used when determining whether a program, activity, or function is an assessable unit. Will the bureau/office fail to meet its mission objectives without this program, activity, or function? Is there currently adverse publicity relating to the program, activity, or function? Is there a strong potential for adverse publicity in the future? Does the program manage a significant level of organizational assets or represent a significant source of cost or revenues?

It is important to review and validate existing components/assessable units, identify new components/assessable units, and refine the component/assessable unit inventory structure to better support the bureaus' mission or organization each year.

2.2.3. Documenting Components and Assessable Units

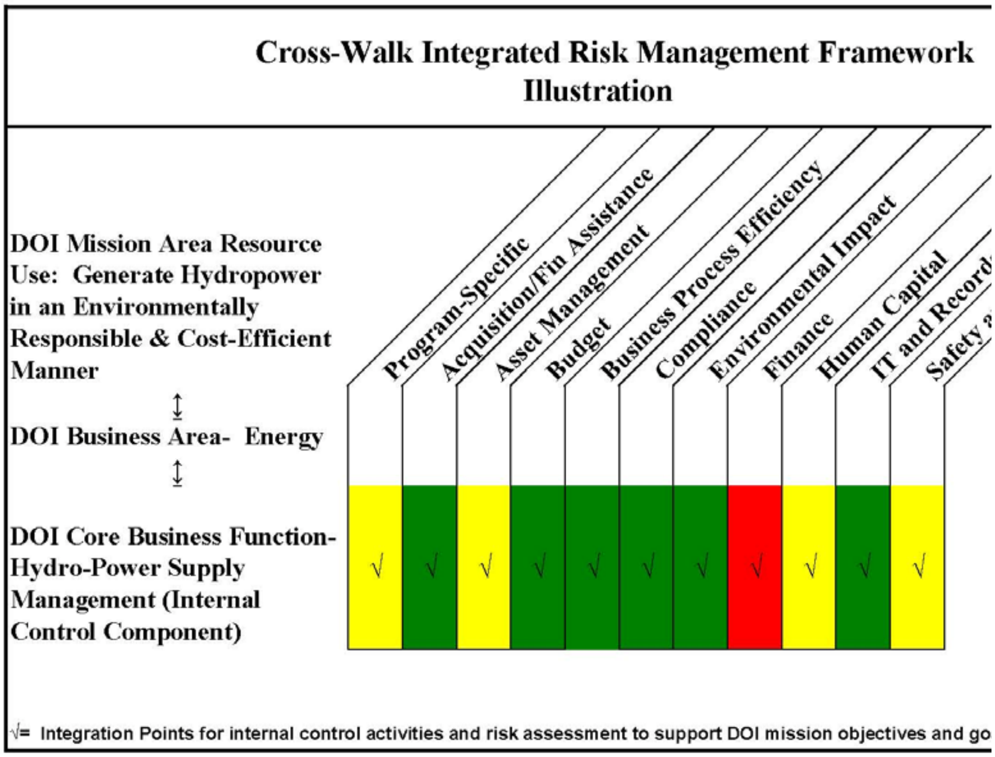
The inventory of components and assessable units is included in each bureau's Component Inventory and Internal Control Review Plan based on a three-year cycle, a sample of which is provided in the attachments to the handbook. Each bureau/office must use the template provided by PFM annually to perform the following steps: (1) identify components and assessable units; (2) record the risk associated with each component and assessable unit in the Internal Control Review Plan based on a three-year cycle; and (3) identify the schedule for conducting internal control reviews. Steps (2) and (3) are completed after the risk assessment is performed, described further in the following section.

3. STEP B: IDENTIFY AND VERIFY RISKS


Verify Internal Control Components
Identify and Verify Risks
B
Document Key Processes and Controls
Assess Internal Controls
Document Results and Implement Corrective Actions
Monitor Corrective Action Plans/Document Lessons Learned
Internal Control Program
DoI OFS ICO-002_B

3.1. INTEGRATED RISK MANAGEMENT FRAMEWORK

Interior has implemented an integrated risk management framework to assess risk throughout the programs. The framework integrates Interior's mission areas and outcome goals, and business model. 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 across the bureau's/office's risk assessments.



Cross-Walk Integrated Risk Management Framework Illustration

	Program-Specific	Acquisition/Fin Assistance	Asset Management	Budget	Business Process Efficiency	Compliance	Environmental Impact	Finance	Human Capital	IT and Record	Safety a
DOI Mission Area Resource Use: Generate Hydropower in an Environmentally Responsible & Cost-Efficient Manner ↕ DOI Business Area- Energy ↕											
DOI Core Business Function- Hydro-Power Supply Management (Internal Control Component)	🟨 √	🟩 √	🟨 √	🟩 √	🟩 √	🟩 √	🟩 √	🟥 √	🟨 √	🟩 √	🟨 √

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

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

To determine whether an assessable unit or sub-assessable unit requires an internal control review, managers must first identify the risks facing the assessable unit, carefully weigh the risks, and use management judgment for selecting the appropriate course of action. Risk, as defined within the context of an internal control review, is the possibility that an event or activity (or lack thereof) could occur resulting in an adverse outcome. Risk is measured in terms of the likelihood of an adverse event occurring, and the relative impact caused by the event.

To enable Interior's management to effectively capture, document, and analyze these risks, personnel should use the integrated risk rating tool. The instructions for using this tool and a sample risk questionnaire can be found in the attachments to this handbook. When reviewing the results, management should use their best judgment as to what the results mean and how to proceed. While risk indicators are very useful, management should not substitute their judgment for indicators provided in the integrated risk rating tool questionnaire.

3.1.1. Completing a Risk Assessment

Performing a risk assessment for each assessable unit and component is required. The Program Manager is responsible for completing a risk assessment using an approved risk rating tool or questionnaire, which is designed to capture risk and control information across a variety of operational risk categories. Some bureaus currently employ the IRRT as a web-based tool, while others use a spreadsheet-based excel IRRT tool. The tool a bureau/office uses should provide an assessment of risk that conforms to Departmental definitions and uses similar terminology and calculations. The general steps required to complete a risk assessment are as follows:

1. Confirm the list of components and assessable units with management;
2. Identify and confirm the risk categories and specific risks relevant to each organization;
3. Perform the risk assessment using a risk rating tool; and
4. Using management judgment, confirm the risk for component/assessable units identified in the tool is reasonable.

For additional information related to the Departmental template (e.g., the Integrated Risk Rating Tool), refer to the instructions provided in the attachments to this handbook.

The results of a risk assessment should be used for several purposes. First, the results should be used by each manager to identify areas that require further examination. It may also be used by managers to justify reducing the frequency of reviews currently being performed. The results of a risk assessment will be used to help Interior's leadership identify trends in risks across the organization for further inquiry and as justification that it is performing an organization-wide risk analysis.

3.1.2. Risk Definitions and Terminology

Interior has chosen to define risk as the probability that events could occur or might not occur and, as a consequence, result in adverse outcomes. This definition is consistent with guidance provided by OMB, the Government Accountability Office (GAO), and other governing bodies. Evaluation of risk is a judgmental review by bureau/office officials of the susceptibility of components and assessable units to the occurrence of inefficiency, ineffectiveness, and the occurrence of waste, loss, unauthorized use, and/or misappropriation of assets. The bureau/office should evaluate management's processes for determining the level of risk related to programs and internal controls used to support the achievement of organizational goals.

Risk challenges can include strategic, traditional, irregular, catastrophic, and disruptive risks. Management should also consider conditions described in auditor-identified findings, noncompliance with laws and regulations, and issues found during internal control reviews. The types of risks to be considered include:

- Inherent Risk (I) — 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 (C) — Control risk is the risk that controls may fail to prevent or detect identified inherent risks.
- Residual Risk (R) — Residual risk is the risk that remains after management's response to risk (considering controls that are in place). Mathematically, residual risk is calculated simply as: R = I – C.
- Fraud Risk — Fraud risk is risk that there may be a significant vulnerability that causes appropriated funds or Government assets to be wasted, misused, or converted for personal use, preventing the program from achieving its mission, goals, and/or objectives. Fraud Risk should be considered for all risk categories.

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

- The consequence (impact) of the risk;
- The likelihood of occurrence; and,
- Management's capacity/decision in acceptance of risk.

These factors are further defined as follows:

Likelihood of occurrence:

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

Consequence of impact:

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

Risks calculated using a scale of likelihood and impact should be plotted on a two dimensional chart similar to the following:

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

The Department introduced the Integrated Risk Rating Tool (IRRT) to each bureau/office as a consistent means of assessing risk throughout the Department. This spreadsheet-based tool is an automated way to assess risk described in this section. Unless other arrangements are made with PFM, 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. 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 OMB Circular A-123, enhancing the concept of integration.

3.1.3. Reviewing the Risk Ratings

Program and senior management should aggregate risk scores and provides overall risk ratings for each assessable unit and component. The ratings are intended to help management: (1) understand the risks their organization faces in the course of everyday business, (2) understand how well these risks are being mitigated, and (3) determine which risks require additional attention through an internal control review. After risk assessment ratings have been completed, managers and senior leaders should hold a risk management meeting to document and consider the following actions:

- Determine if the inherent risk is correctly defined;
- Accept, reject, and prioritize risks;
- Confirm whether the inherent risk rating is appropriate;
- Confirm that the N/A listed categories do not apply;
- Resubmit the IRRT questionnaire for any categories listed as N/A, which do apply;
- Confirm that the answers provided in the IRRT questionnaire are correct for opportunities for improvement, entity level, and efficiency;
- Determine if an internal control review (ICR) or alternative internal control review (AICR) should be performed for risks rated as “high” or “medium”;
- Meet with senior management to discuss entity-level risks rated as high or medium; and,
- Evaluate the assessable unit’s processes and procedures for a “medium” or “high” (yellow or red) risk.

3.1.4. Update the Internal Control Review Plan Based on a Three-Year Cycle

Validating each bureau’s/office’s annual comprehensive, risk-based internal control review plan based on 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.

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 until the deficiencies are corrected. The test schedule should be reflected on the three-year plan (see attachments to this handbook). Some information security controls must be tested annually as discussed in the FISMA.

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

Bureau/office personnel should look for opportunities to integrate, coordinate activities, and leverage internal control reviews already being conducted elsewhere in the bureau/office. For instance, business processes and related information systems that are key to 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. PAM 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 information security and acquisition programs to determine which program-related areas are of the highest risk and should be assessed.

As another example, if the 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.

If bureaus/offices need to defer, delay, or cancel any reviews from the three-year plan, they must justify, in writing, to PFM the reason for these changes and explain how these changes do not weaken support for the assurance statement. Requests must come from the 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.

3.2. OVERVIEW OF INTERNAL CONTROL REVIEWS

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 internally by the assessable unit manager is considered an ICR. A review conducted by other outside sources (such as the OIG, GAO, or independent contractor) is considered an AICR. Management may use other sources of information for planning purposes and to avoid duplication of conducting reviews. Other 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 A-123, Appendix D, *Compliance with the Federal Financial Management Improvement Act of 1996*, or any other system reviews (ICR).

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) – A DFR is a targeted review which is mandated by the Department and performed by the bureaus/offices which tests certain controls within a business process. To comply with statutory requirements, directives and risk-based analysis, some of the Department’s Offices, such as the OCIO or PAM, may prescribe selected DFRs for information systems, property, financial assistance (i.e., grants and cooperative agreements), acquisition management and other functional areas deemed necessary. These DFRs should be treated as a subset of an ICR. Guidance for conducting and reporting the results of these reviews will be provided by the responsible offices.

Use the attachments to the handbook to provide the updated component /assessable unit inventory, the risk associated with each component and assessable unit, and an updated internal control review plan based on a three-year cycle. The schedule of key milestone dates, re-issued each year with current dates, has the due date for this submission. The plan must identify test plan schedules for all components in a bureau’s/office’s inventory regardless of when that component will be reviewed.

3.2.1. Definition of an Internal Control Review

An internal control review is defined as any audit, review, evaluation, or inspection performed by internal individuals, groups or teams that follows the steps and processes for the internal control cycle. It is an in-depth examination of internal controls established and used by an assessable unit to meet a program's goals and objectives. Administrative, financial, technical, and programmatic activities and functions are subject to review. Managers are responsible for organizing a team or a workgroup to conduct the reviews in accordance with Interior's annual guidance. Reviews should be scheduled periodically to examine: (1) significant and material internal control weaknesses; (2) activities with high operational risks; (3) other areas of concern to management, such as improving the efficiency or effectiveness of programs; and (4) compliance with laws and regulations.

3.2.2. Definition of an Alternative Internal Control Review

Alternative Internal Control Reviews are defined as an audit, review, evaluation or inspection conducted by outside sources (such as the OIG, GAO, or independent contractor). The main difference between an ICR and an AICR is who conducts the review.

To consider whether an ICR or AICR supports the Annual Assurance Statement, the following criteria should be met:

- Be planned to consider the scope of the review to include the period covered and the extent of monitoring, testing, verification, and/or validation to be performed;
- Contain objectives or purposes of the review or report that align with and demonstrate compliance with Internal Control Program objectives;
- Identify the staff performing the review;
- Contain evidence that the review conducted demonstrates compliance with laws and regulations and/or that specific monitoring and testing was performed to determine compliance with the purpose/objectives of the review;
- Contain adequate documentation to support any conclusions drawn or deficiencies noted in a written format;
- Confirm deficiencies are reported to the appropriate manager responsible for taking action;
- Confirm that corrective actions are in place for each noted deficiency; and,
- Identify a person responsible for taking corrective action and a target date to address the deficiencies noted.

Bureaus/offices should avoid duplicating reviews that assess the same internal controls and should coordinate efforts with other evaluations to the extent possible.

3.2.3. Determining Whether to Perform an Internal Control Review

The following questions should be answered to determine whether to perform an internal control review of key business processes (as defined in section 4) for the program, activity, or function:

- **Risk** - Are the risks to your program, activity, or function (as defined in the Integrated Risk Rating Tool) high or medium? A high or medium risk, in one of the risk categories, indicates that an Internal Control Review should be performed because a risk exists that may prevent your program, activity, or function from achieving its objectives. A good indication of a high risk program may include findings from previous reviews or external audits.
- **Effectiveness and Efficiency** - Would your program, activity, or function benefit from having a structured approach to evaluating operating effectiveness and efficiency? If your program, activity, or function would benefit from a structured approach for evaluating operating effectiveness and efficiency, this indicates that an Internal Control Review should be performed.
- **Change** - Has the need for significant change been identified in your program, activity, or function? If your program, activity, or function has identified a need for significant change, this indicates that an internal control review should be performed.

- **Compliance -** Has your program, activity, or function had difficulty complying with laws, regulations, or policies? If your program, activity, or function has had difficulty complying with laws, regulations, or policies, this indicates that an Internal Control Review should be performed.
- **Political Sensitivity** - Is your program, activity, or function politically sensitive or highly visible to the public? If your program, activity, or function is highly visible to the public, this indicates that an Internal Control Review should be performed.
- **Structure** - Is the program, activity, or function new? Could your program, activity, or function benefit from having a comprehensive understanding of its business processes? If your program, activity, or function is new or could benefit from having a comprehensive understanding of its business process, this indicates that an Internal Control Review should be performed.
- **Documentation** - Does documentation describing the operations of your program, activity, or function exist? Is documentation that describes ongoing operations and processes difficult to obtain, or is the documentation unclear? If documentation describing you key business processes does not exist, this indicates that an Internal Control Review should be performed.

Answering to these questions should assist managers with determining whether to perform an internal control review or to leverage an alternative internal control review. However, managers should always use their best judgment. Since internal control reviews are intended to be highly structured and thorough, it is strongly suggested that a full internal control review be performed if an alternative internal control review does not already exist.

3.3. PLANNING FOR AN INTERNAL CONTROL REVIEW

Planning for an internal control review is not required, but strongly suggested. The assessable unit manager conducting the review should prepare a timeline for the high-level tasks that need to be performed. This should include confirming the tasks that need to be completed with the assessment team, the relationships among the tasks, task durations (lengths), milestones, and task completion dates.

Immediately following the end of the fiscal year, the manager should begin preparing a timeline for the internal control review. The deadline for completing internal control reviews is August 31st of each year, in accordance with Interior's annual guidance. A simple Gantt chart, which can be included in the internal control review's Projects and Communications Plan, is provided below illustrating the results for planning a review.

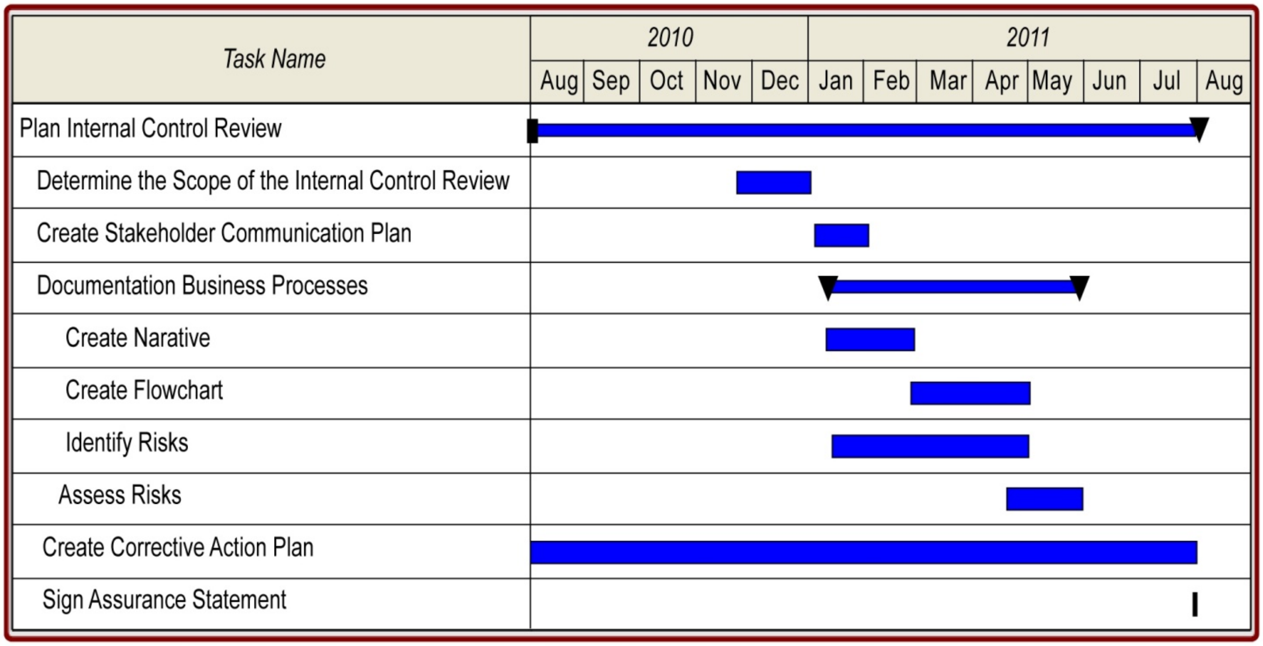


FIGURE 2: SAMPLE GANTT CHART

3.3.1. Key Tasks for an Internal Control Review

The following table outlines the key tasks for an internal control review and an alternative internal control review.

Starting a New Internal Control Review	Modifying an Existing Review
1. Complete Integrated Risk Rating Tool 2. Assess risks 3. Plan the review, including the identification of review objectives 4. Identify key business processes 5. Complete business process documentation including: (1) Narrative, (2) Flowchart, and (3) Control Matrix 6. Identify and assess key controls 7. Prepare a summary of findings and recommendations 8. Identify corrective actions and complete corrective action plan 9. Report results 10. Monitor corrective action progress 11. Document lessons learned 12. Provide the summary of findings and recommendations, as well as corrective actions to Senior Management.	1. Update the previously completed integrated risk rating tool, as needed 2. Identify required changes to existing review 3. Follow steps for a new internal controls review 4. Report results 5. Provide the review reports to Senior Management 6. Monitor corrective action progress

3.4. IDENTIFYING THE GOALS OF THE ASSESSABLE UNIT (ORGANIZATION)

Identifying the goals of an internal control review are strongly suggested, but not required. In order to properly conduct a review, the mission and goals of the organization must first be clear. Typically, organizational mission and goals can be found in a mission statement, policy, or guidance. As part of the review, these goals should be identified and documented to provide a basis for determining if internal controls are successful. By identifying the goals of the assessable unit, prior to conducting the Internal Control Review, the assessable unit manager will be able to compare the results of the review to the stated goals of the organization to create an actionable plan for the future. When identifying the mission of an organization, the following questions should be answered:

- **Mission** - What is the objective of the organization/assessable unit?
- **Goals** - How does management know if the assessable unit / organization is successfully achieving its mission (i.e. what measures of success are used to determine if an organization successfully achieved its mission?)?

The following is an example of the assessable unit mission and goals:

Mission: The mission of the Emergency Management program is to save lives, protect property and the environment by influencing human behavior through implementation of mitigation, preparedness, response, and recovery activities.

Goals: The goal of the Emergency Management program is to achieve our stated mission through the following:

1. Confirming that Emergency Action Plans for dams, Continuity of Operations Plans, Occupant Emergency Plans and Communications Directories are in place and updated on an annual basis
2. Conducting emergency exercises, for a third of the emergency plans on an annual basis, so that 100% of the emergency plans are tested in a three-year period
3. Confirming that members of the Emergency Management program are adequately trained, cross trained, and informed of their responsibilities
4. Coordinating regular communication with Emergency Management program managers to maintain group cohesion and consistent documentation
5. Continuously improving the program by identifying corrective actions, based on lessons learned in emergency exercises and actual emergency events, and completing them in a timely manner

3.4.1. Articulating Objectives of the Internal Control Review

After identifying the mission and goals of the assessable unit, the assessable unit manager should identify objectives for the internal control review. The objectives of the Internal Control Review should directly correlate to the goals of the assessable unit. The assessable unit manager should articulate the objective of the internal control review, and in doing so, the manager should consider the following questions:

- How can the internal control review demonstrate the assessable unit is achieving its goals?
- What information do I want to get out of this review?
- What information is most useful to the organization?
- What needs to be achieved by the organization?
- What requirements should the organization meet?
- Are there any specific compliance requirements that should be addressed?

Once the assessable unit manager has articulated the purpose of the organization, what the organization expects to accomplish, and what the organization needs to succeed, the manager will identify the goals and objectives of the Internal Control Review.

Assessable unit managers should consider using the SMART mnemonic when identifying goals for their internal control review. A SMART objective is specific, measurable, achievable, results-oriented, and time-bound. The SMART mnemonic will assist the assessable unit manager with defining objectives. The following explains the steps to create SMART objectives:

- **Specific** - Objectives should be specific. If a goal is specific, it has a much greater chance of being accomplished. A specific goal answers the six "W" questions: Who, What, Where, When, Which, and Why.
- **Measurable** - Establish criteria for measuring progress for each goal. Measuring progress can help keep assessable unit managers on track and provide a sense of accomplishment when objectives are met. If possible, these measures should be quantitative.
- **Achievable** - Objectives should be achievable and realistic. Objectives should be something that Managers are both willing and able to meet.
- **Results-oriented** - Objectives should be measured based on outputs or results.
- **Time-bound** - Objectives should be restricted to a timeline. There should be milestones between the beginning and end to ensure assessable unit managers are on track to accomplishing the objectives they have set out for the organization.

The following is an example of an Internal Control Review objective for the Emergency Management program:

Review Objective: The purpose of the internal control review is to confirm that emergency action plans for dams, continuity of operations plans, occupant emergency plans and communications directories have been reviewed and updated on an annual basis and certified by management.

3.4.2. Internal Control Review Objectives Template

To gain the most benefits from an Internal Control Review, it is important to first articulate the goals of the organization and to describe the objectives of the review in a structured and formal manner. This can be completed through use of the internal control review objectives template. The objectives template summarizes the mission and goals of the organization, and describes what the review seeks to confirm as described in the objectives.

3.4.3. Objectives Statement Template Instructions

<u>Who is responsible for preparing the objectives statement?</u>

The assessable unit manager is responsible for preparing or delegating responsibility for preparing the objectives statement.

<u>What type of information and level of detail should be included?</u>

The following guidance describes the primary elements of the objectives statement template and how to complete it. Note the letter associated with each item in the bulleted list below (e.g., A, B, C) has a corresponding reference on the sample objectives template presented in section 3.4.4 of this document.

A. Background Information - This section of the objectives statement includes standard information, including: Directorate, Region, Area Office, Organization or Program, Mission Area(s), Assessable Unit and Assessable Unit Manager(s).
B. Mission - This section of the objectives statement describes the goal of the assessable unit.
C. Goals - This section describes what the assessable unit must accomplish to successfully achieve its mission.
D. Internal Control Review Objectives - This section is tied directly to the goals of the organization. It provides specific measures that will be assessed during the review.

3.4.4 Internal Control Review Objectives Statement Example

	Organizational Mission, Goals, and Internal Control Review Objectives	
	Directorate:	Safety Division
	Region:	Northwest
	Area Office:	Portland
A	**Organization or Program:**	Programs and Emergency Management Office
	Mission Area(s):	Support Programs
	Business Process (i.e., Assessable Unit):	Emergency Action Plan & Continuity of Operations
	Business Process (i.e., Assessable Unit) Manager(s):	Program Manager
B	**Mission:** The mission of the Emergency Management (EM) program is to save lives, protect property and the environment by influencing human behavior through implementation of mitigation, preparedness, response, and recovery activities.	

C

Goals:
The goal of the EM program is to achieve our stated mission goals through the following:

1. Confirming that emergency plans Emergency Action Plans (EAPs) for dams, Continuity of Operations (COOP) Plans, Occupant Emergency Plans (OEPs) and Communications Directories are in place and updated on an annual basis
2. Conducting emergency exercises, for a third of the emergency plans on an annual basis, so that 100% of the emergency plans are tested in a three-year period
3. Confirming that members of the EM program are adequately trained, cross trained, and informed of their responsibilities
4. Coordinating regular communication with EM program managers to maintain group cohesion and consistent documentation
5. Continuously improving the program by identifying corrective actions, based on lessons learned in emergency exercises and actual emergency events, and completing them in a timely manner

D

Internal Control Review Objectives:
The purpose of this internal control review is to confirm that adequate internal controls are in place to achieve the stated goals. The review will focus on documenting and assessing the controls embedded within the key business processes and internal control activities used to achieve the stated goals. The specific objectives of this internal control review include confirming the following:

1. Emergency action plans for dams, continuity of operations plans, occupant emergency plans and communications directories have been reviewed and updated on an annual basis and certified by management.
2. Scheduled exercises have been completed and documented in a timely manner.
3. Adequate training has been provided to EM team members.
4. Documentation is consistent between regions, and it is adequately retained for future reference.
5. EM management and staff are fully engaged and aware of their responsibilities.
6. Corrective actions have been identified, written into a formal plan, tracked appropriately, and executed in a timely manner.

3.5. IDENTIFYING THE REVIEW TEAM

After key business processes have been identified, the Assessment Team responsible for performing the internal control review should be identified.

3.5.1. Internal Control Review Manager’ (Assessable Unit Manager) Responsibilities

The Internal Control Review manager, typically the manager over each assessable unit, is responsible for leading the internal control review or for delegating the responsibility to a staff member. The assessable unit manager should have in-depth knowledge of the program, activity, or function being reviewed, the capacity to affect change through budget requests, and the technical background and experience to understand issues critical to the assessable unit. The assessable unit manager has the authority to delegate the responsibility for conducting the internal control review.

3.5.2. Internal Control Review Assessment Team Members' Responsibilities

The Internal Control Review Assessment Team includes the assessable unit manager, as well as additional members that are selected by the assessable unit manager. Members of the Internal Control Review Assessment Team should: (1) have a working knowledge of the assessable unit's overall processes; (2) have experience performing internal control reviews; and (3) have an understanding for performing and conducting an internal control review. The following is an example of a well-balanced Internal Control Review Assessment Team:

Team Member A - Team Member A is the assessable unit manager. The manager leads the team in executing the internal control review.

Team Member B - Team Member B has previously supported internal control review teams and understands the required processes and documentation.

Team Member C - Team Member C has technical expertise regarding the processes being reviewed.

Team Member D - Team Member D is a manager with responsibility for several key business processes that are being reviewed. Team member D has a strong understanding of the key business process.

*Team compositions will vary depending on the size and location of the assessable unit being reviewed, and the availability and experience of the personnel available to support the review.

3.5.3. Internal Control Review Stakeholders

"Internal control review stakeholders" is a generic term for all of the personnel involved in the review. These other personnel help document key business processes, provide information for the review, and include review team members as well.

3.6. MANAGING AND COORDINATING STAKEHOLDER COMMUNICATIONS

Communicating with Internal Control Review stakeholders is critical to a successful Internal Control Review. Without stakeholder support, the Internal Control Review will be difficult to complete and the results may be unreliable or misleading. Therefore, it is important to communicate the benefits of the Internal Control Review to stakeholders and to maintain communication with them as the project progresses. In order to effectively plan and coordinate stakeholder communication and involvement, it is strongly suggested the Internal Control Review Assessment Team prepare a communications plan and conduct a formal kick-off meeting prior to initiating the review. The steps for creating a communication plan are discussed in the next few sections.

3.6.1. Creating a Communications Plan

The communications plan is designed to engage internal review control stakeholders, gain their support, and coordinate their involvement. Cooperation and participation of internal control review stakeholders starts with visible sponsorship at DOI's highest levels. The communications plan outlines the communication methods (e.g. distributing formal memoranda; sending emails to stakeholders; and conducting interviews and teleconferences) that can be used to keep internal control review stakeholders informed of progress. It also informs internal control review stakeholders of their responsibilities, as well as important scheduling events, such as upcoming activities and milestones.

The plan should outline the suggested frequency of messages to internal control review stakeholders, as well as the communication roles and responsibilities of stakeholders. The communication methods defined in the communications plan are suggestions. The assessable unit manager should determine what communication methods and frequency are appropriate for the assessable unit being reviewed.

The objectives of the communications plan include the following:

- Explaining the context and benefits of a strong Internal Control Review;
- Gaining internal control review stakeholder support for the project;
- Informing internal control review stakeholders of the schedule and upcoming activities so they are prepared to assist the Internal Control Review Assessment Team in meeting deadlines;
- Creating awareness concerning the requirements and impacts of the Internal Control Review;
- Establishing an approach that provides communications to internal control review stakeholders at various levels in a structured, consistent manner; and
- Presenting stakeholders with the opportunity to provide candid and timely feedback.

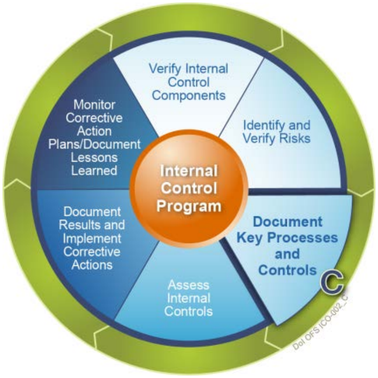
3.6.2. Conducting an Internal Control Review Kickoff Meeting

After forming the Internal Control Review Assessment Team, the assessable unit manager should host a kickoff meeting. This meeting should introduce the scope and objectives of the Internal Control Review, as well as outline the roles and responsibilities of team members. Key actions for the meeting include documenting attendees and taking meeting minutes to capture key decisions, as well as actions items and next steps. Meeting participants should bring documentation pertaining to the establishment and governance of their organization. This includes items such as policies, executive orders, laws, and any other documentation that guides the regular operation of the organization.

4. STEP C: DOCUMENT KEY PROCESSES AND CONTROLS

4.1. OVERVIEW

Documenting key business processes and controls is required. The process for documenting key business processes and control activities is designed to complement existing reviews being performed within the bureaus (i.e., contract services reviews or comprehensive facility reviews). The Internal Control Review Assessment Team, led by the assessable unit manager, is responsible for gathering and organizing information regarding Interior's key business processes. If adequate documentation does not exist, it is necessary to formally document the key business processes. The documentation, when completed, should clearly demonstrate the following: (1) the process starting point; (2) the process end point; (3) the relationships of activities within the process; (4) how the objectives of the organization being reviewed are achieved; and (5) the key activities (i.e. internal controls) that mitigate the risks to achieving the objectives of the organization being reviewed.


Verify Internal Control Components
Identify and Verify Risks
Document Key Processes and Controls
C
Assess Internal Controls
Document Results and Implement Corrective Actions
Monitor Corrective Action Plans/Document Lessons Learned
Internal Control Program
DoI OFS ICO-002_C

It is suggested that the Internal Control Review Assessment Team use the following templates to document key business processes:

- **Narrative Template** - Articulates key business process steps in a logical, often sequential, format;
- **Flowchart Template** - Depicts the activities of the narrative, including relationships between activities and internal controls. Since not all processes are linear, the flowchart can demonstrate relationships between activities that are not linear; and
- **Control Matrix Template** - Provides specific details related to internal controls such as the control description, the frequency with which the control is performed, whether it is manual or automated, and if it is preventative or detective.

4.2. IDENTIFYING KEY BUSINESS PROCESSES

To meet Departmental requirements, each assessable unit is responsible for identifying the key business processes, as well as the controls within the process, that mitigate the risks identified in the risk assessment. Key business processes are those groups of related activities, performed by Interior's personnel, which are critical to the assessable unit's ability to achieve its mission-related objectives.

4.3. NARRATIVE TEMPLATE DESCRIPTION

A narrative describes the steps in a process in a logical, often sequential, format. Interior's Annual Guidance requires that assessable units provide detailed narratives of their key business processes "from the point of origin to the point of product or service, as well as to financial reports, in order to capture all operational functions, transaction types, service providers, and systems that are elements of the process." A suggested narrative format sample is provided in the attachments to this handbook and instructions for using the narrative template are provided below.

The narrative should describe important activities in as much detail so that a person who is unfamiliar with the process is able to understand the major activities and objectives. To the degree possible, the narrative should group and describe activities that follow a linear progression. The narrative template below assists assessable units in meeting Interior's requirements by providing a standardized format for creating flowcharts.

4.3.1. Narrative Template Instructions

<u>Who is responsible for preparing a narrative?</u>
The assessable unit manager is responsible for preparing or delegating responsibility for preparing the narrative.

<u>What type of information and level of detail should be included?</u>
The following guidance describes the primary elements of the narrative and how to complete the narrative template shown below. Note the letter associated with each item in the bulleted list below (e.g., A, B, C) has a corresponding reference on the sample narrative template presented in this section.

A. **Background Information** - This section of the narrative includes standard information, including: Process Title, Purpose, Scope, and Stakeholder(s).
B. **Key Business Process Narrative Description** - This section of the narrative provides a brief overview of the key business processes, including: Process Overview, Frequency, and the Name of the Preparer.
C. **Narrative Steps** - In order to facilitate ease of readability and provide structure, the narrative should be documented as a series of logical steps. The steps should be detailed enough so that a person who is unfamiliar with the process is able to understand the major activities and objectives.
D. **Process Owner(s)** - The process owner is the person responsible for performing a step or multiple steps in the narrative. A key business process will typically involve multiple process owners.
E. **Documents/Reports/Systems Used** - This section of the narrative exists to capture the documents, reports, or systems used in performing or executing the key business process.
F. **Frequency (Continuous, Once, Daily, Weekly, Monthly, Quarterly, Annually)** - This section of the narrative exists to document how often each step in the process is performed.
G. **Decision Point** - If a step in the process is a decision point rather than an activity, the person completing this step should enter "[Decision Point]" in the beginning of the text so that it is easily identifiable.
H. **Identification of Internal Control Activities** - An internal control is a program, activity, or function that is used to mitigate risk. In the context of programmatic or functional operations, internal controls are either preventative or detective (i.e., reactive). Internal controls may include reviews, inspections, action plans, monitoring activities, passwords, security procedures, IT restrictions, or formal authorizations (e.g., a signature to confirm a document has been reviewed). In the absence of internal controls, risks may not be adequately mitigated and, as a result, organization objectives may not be achieved. When

differentiating between an internal control activity and a regular activity, ask the question: "If this activity or procedure ceased to be performed, would the potential for an adverse outcome increase?" If the answer to this question is “yes,” then it is likely the activity is an internal control. Financial controls address adverse outcomes related to material misstatements. Internal control activities should be identified within the narrative using a symbol or indicator of choice (i.e., (C)).

4.3.2. Narrative Example

Process:	Continuity of Operations Planning
Purpose:	The purpose of the Continuity of Operations Planning (COOP) process is to confirm that Continuity of Operations Plans (COOPs) are in place so that the bureau/office will continue to function in the event of a disaster.
A **Scope:**	DOI Office of Management & Budget (OMB) Circular A-123 Internal Controls Review for the period October 1, 2008 through June 30, 2009.
Key Process Stakeholders, Stakeholder Title:	Continuity of Operations Planning (COOP) Coordinator
B **Key Business Process Narrative Description:**	The COOP Program is within the Safety Directorate and is centrally managed from the Arlington office. It consists of multiple COOP Coordinators within each region / area office.
Frequency of Process: F	This process is performed every three years, with several control activities performed on a monthly and weekly basis.
Preparer:	Regional COOP Coordinator

C

Number	Process: COOP	Process Owner(s)	Notes
1.1.1	<u>Conduct regular status meetings with COOP Coordinators</u> - The COOP Coordinator (COOPC) conducts regular meetings / conference calls with the Regional COOP Coordinators to discuss the current status of the program. Each region is represented.	COOP Coordinator (COOPC) D	
1.1.2	<u>Discuss planning, updating, and executing annual Continuity of Operations Planning (COOPs) Plans</u> - The COOPC discusses the requirements for the program with regional / area / Arlington office COOP Coordinators at the regular conference calls. Topics of discussion include the following: (1) training requirements; (2) status of actions to update the COOPs; (3) changes in requirements for the program; and (4) COOP exercises.	COOPC	

1.1.3	Assemble COOP Planning Team - The COOPC organizes a team of individuals who will participate in planning, drafting, executing and revising the COOP for the Arlington area offices. The team of individuals selected by the COOPC will be responsible for assisting with COOP development and execution of training exercise. In the event of an emergency situation, these individuals will also be responsible for carrying out the COOP.	COOPC	
1.1.4	G [Decision Point] - Does a plan already exist? Yes, proceed to step 1.1.10. No, proceed to step 1.1.5.	COOPC	
1.1.5	Conduct planning meetings - The COOPC assembles a team of COOP stakeholders to create a COOP plan if one does not exist.	COOPC	
1.1.6	Verify that the critical planning elements are met during planning meetings - The COOPC conducts a meeting to discuss development of a plan, if a COOP does not already exist. If a COOP exists, then the manager begins the process of training the COOP participants (step 1.1.5). The COOPC is responsible for confirming that the following critical planning elements are discussed at the meeting: E Staffing - A roster of personnel responsible for creating, executing, and updating COOPs at each critical location, who are properly trained and credentialed in their area of responsibility. Guidance - Guidance pertinent to planning the COOPs, including directives, standards, executive orders, or policies. It is especially important the COOP coordinators be made aware of any updates or changes to new guidance. Critical Functions - A list of [Bureau's] organizational functions which cannot be interrupted for more than 12 hours and must be continued for greater than 30 days.	COOPC	
1.1.7	[Decision Point] - Were the critical planning elements met? No, proceed to step 1.1.5. Yes, proceed to step 1.1.8.	COOPC / COOP Team Members	
1.1.8	Design COOP Plan - During the planning meeting (or shortly thereafter), COOP team members are responsible for creating COOPs that meet the standards as outlined in the guidance noted in the "Laws, Regulations, Policies or Directives and Standards" section. These standards have been summarized as follows:	COOPC / COOP Coordinators	

	• Essential Functions List - A list of essential functions that documents agency "interdependencies," those organizations that rely on the Bureau, as well as the Bureau's resource requirements. • Orders of Succession and Delegations of Authority - Succession for key positions and delegations of authority to confirm authorities are in place to execute essential functions. • Alternate Operating Facilities - A list of alternate facilities. • Vital Records - Descriptions of vital records, systems, and databases, their location and how they can be accessed. • COOP Activation Process - The decision process for activation of COOP plans during “no-warning” and “warning” scenarios. This should include contact numbers, radio call signs, or other information needed to implement critical communications system, and maintenance of contact lists. • Notification and Deployment Procedures and Checklists - The procedures and checklists needed to notify alternate facilities managers, COOP team members, senior leadership and others upon COOP activation. This should include instructions for movement of personnel and other resources including “drive-away” kits to the alternate facility. • Initial Operating Capability Procedures and Materials - The procedures, reference materials, and checklists needed to ensure COOP team members and alternate facilities reach operational status within 12 hours. This should include delineation of responsibilities for COOP team members, alternate facility reception and orientation, and the establishment of formal communications. • Alternate Facility Operations Procedures - Procedures and/or checklists as needed to order necessary equipment and supplies that are not pre-positioned; manage situation tracking and implementation of essential functions; and provide ongoing communications with other organizational units, non-deployed personnel,		

	other agencies, critical customers, and the public. - Reconstitution Procedures - Procedures and/or checklists for plans to redeploy personnel and transition to normal operations.		
1.1.9	Review the COOP Plan for accuracy and completeness and validate that the COOP Plan meets applicable requirements - Management reviews the COOP Plan to confirm that is has been updated and meets the required standards, as outlined in FAC 05-01. As proof of review, management signs the COOP Plan cover page. (C)	COOPC	
1.1.10	[Decision Point] - Is the COOP Plan approved? No, proceed to step 1.1.8. Yes, proceed to step 1.1.11.	COOPC	
1.1.11	Provide COOP participants with applicable required training - The COOPC provides training to COOP participants to confirm they have the knowledge necessary to carry out the COOPs. (C)	COOPC	

4.4. FLOWCHART TEMPLATE DESCRIPTION

A flowchart is a graphical representation of the steps described in the narrative. The purpose of the flowcharts is to identify control points in the process and the control activities performed by the users. Flowcharts provide details of activities, tasks, responsibilities, and key decision points in a given process. 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 divided by "swim lanes" that contain descriptive shapes. Each shape represents a particular occurrence within the process. Specific process activities, decision points or references are all described within the shapes. The movement of a process model travels from left to right in a timeline fashion.

Specific definitions of the various elements contained within the flowchart presentation are as follows:

- **Swim Lanes.** Indicate the specific entity or organizational unit responsible for handling a process or making a decision. Swim lanes are presented horizontally with titled position marked vertically on the left side of the flowchart.
- **Phases.** Specific phases are identified as a set of activities grouped together. Separate phases can be shown on the same flowchart, divided by a vertical line.
- **Shapes.** The specific shapes are symbols meant to identify actions or documents.

A flowchart template is provided in the attachments to this handbook. Details on how to prepare a flowchart, as well as an example of a completed flowchart, are also provided in the attachments to this handbook and below.

4.4.1. Flowchart Template Instructions

<u>Who is responsible for preparing the flowchart?</u>
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:

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

What are all the shapes?

The flowchart is comprised of basic shapes, each representing a particular activity or step. For example, manual activities are represented by a box. A decision is represented by a diamond. While some organizations may be familiar with flowcharting principles, and some may have flowcharting software, many organizations have not had exposure to flowcharting. In Excel, all basic flowchart shapes, including titles, can be inserted from the drawing toolbar. This will open the drawing toolbar. Click on "insert," and then click on "shapes" and select the shape you wish to insert. Click on the appropriate shape, as explained in the flowchart template, and then click onto the worksheet.

How do the shapes fit together to make the flowchart?

1. Each step in the narrative should correspond with a symbol in the flowchart. For each step, the symbol used depends on what is occurring in the corresponding narrative step (i.e., if the step is an activity, then a square symbol is used).
2. Number the shape to match the numbering convention in the narrative, and label the symbol. Labels should be short, but descriptive, and should begin with a verb.
3. Insert the appropriate flowchart shape for the next step described in the narrative.
4. Connect symbols with "connector arrows."
5. Repeat steps 1 through 4 until the entire process is documented.

What type of information and level of detail should be included?

The following guidance is provided to describe the components of the flowchart and how to complete the flowchart template, which can be found in the attachments to the handbook. Note the letter associated with each item in the bulleted list below (e.g., A, B, C) has a corresponding reference on the sample flowchart template presented in this section. Additional flowchart symbols currently used within Interior are referenced in the attachments to the handbook.

A. **Background Information** - This section of the flowchart includes standard information, including: Scope, Process Stakeholders, and Process Overview.
B. **Connector Table** - This section of the flowchart serves as a reference point for on-page and off-page connectors.
C. **Process/Basic Activity** - This section of the flowchart should be used to document each step of the process in the form of a symbol. No decisions are made in these steps.
D. **Hardcopy Document** - This symbol in the flowchart represents any hardcopy document(s) used or referenced in the process.
E. **Decision Point** - When a decision is being made, a diamond is used. The corners of the diamond lead to the different options. To be consistent, horizontal lines coming out of the diamond corners should represent the same decision throughout the Flowchart, as should all vertical lines.
F. **Control Process/Basic Activity (Control Point)** - This symbol represents an internal control activity. It resembles a black flag with the letter "C" in order to differentiate it from the other steps in the process.
G. **System** - While a system is not presented in the sample flowchart, the symbol for a system (typically a cylinder) represents a system (i.e., computer, scanner, telephone, or other equipment, software, or hardware) that is used during the process. It is normally "attached" to a step to demonstrate that it is used as part of the step.
H. **Connecting Arrows** - Arrows are used to show the flow of information or data and the order in which steps within the process are performed.

4.4.2. Flowchart Example

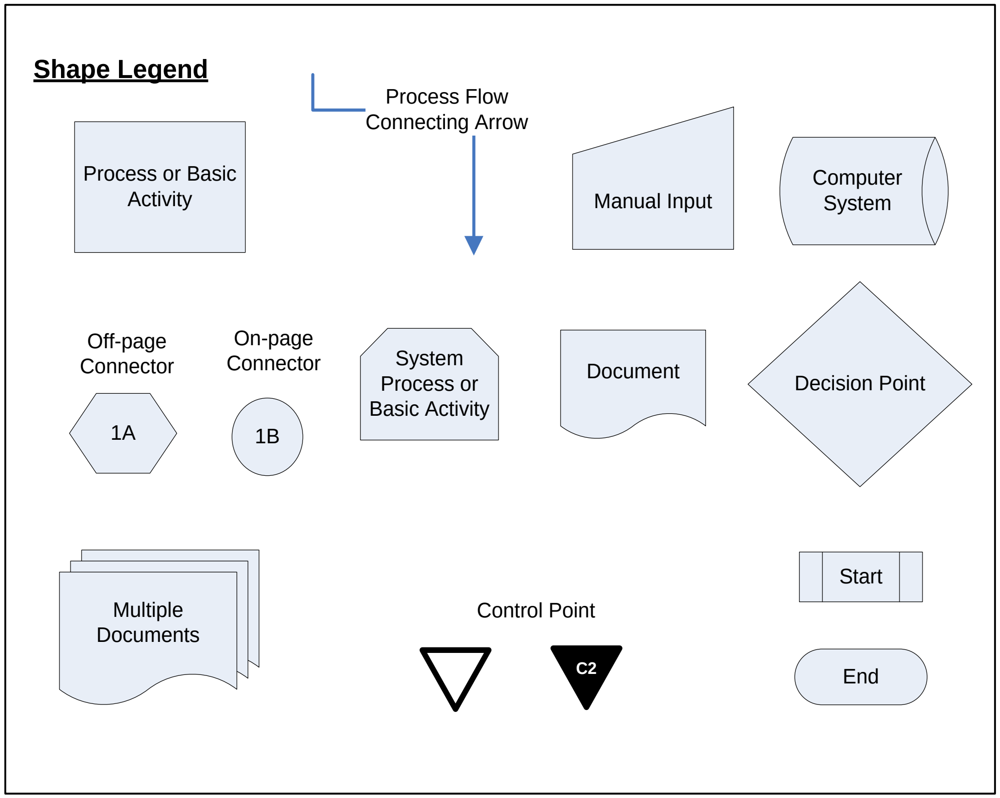
OMB Circular A-123, Appendix A – Business Process Flowchart
Business Process: Continuity of Operations Planning (COOP)

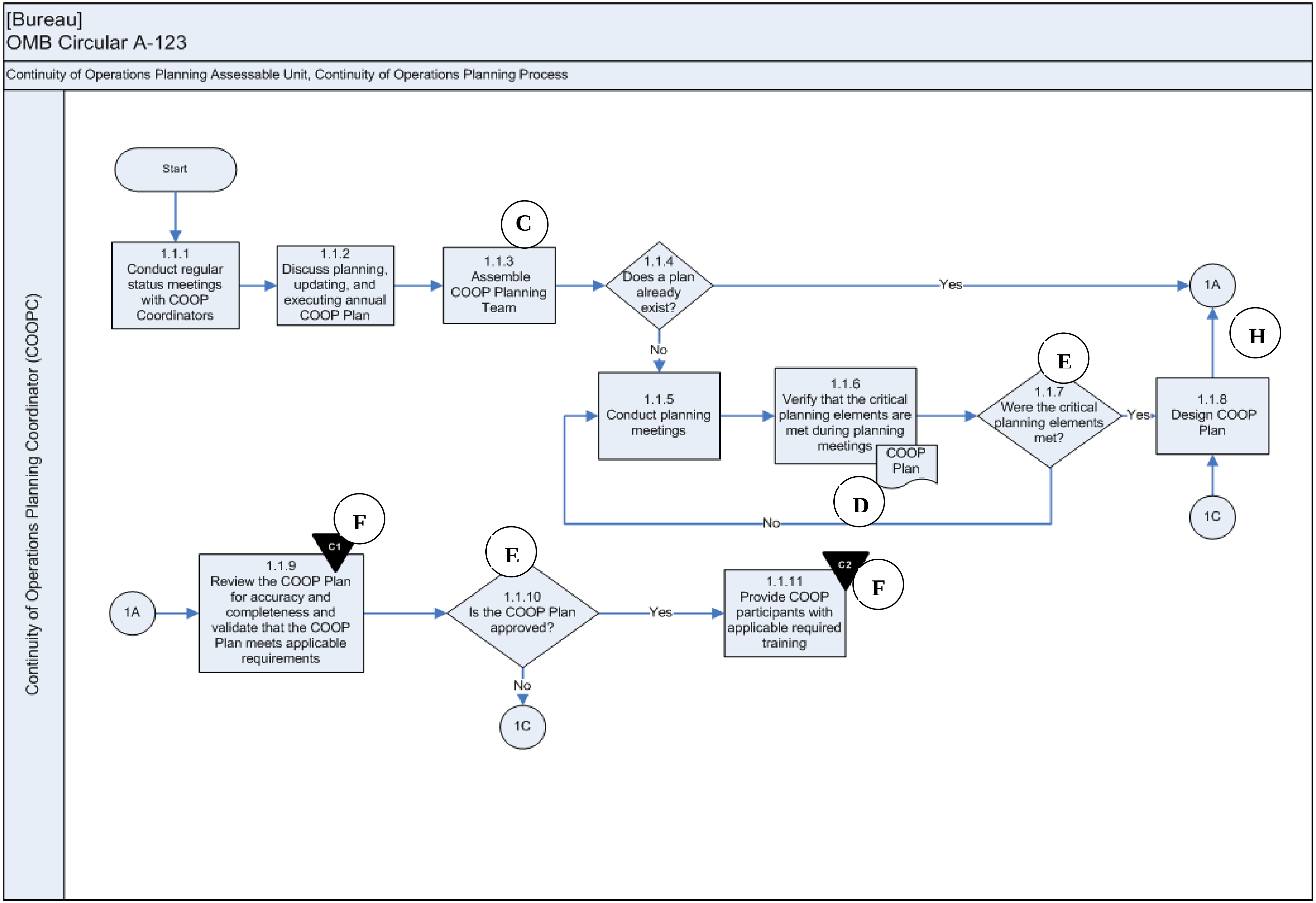
A

Scope:	DOI Office of Management & Budget (OMB) Circular A-123 Internal Controls Review for the period October 1, 2008 through June 30, 2009.
Key Process Stakeholders, Stakeholder Title:	Continuity of Operations Planning (COOP) Coordinator
Process Overview:	The COOP Program is within the Safety Directorate and is centrally managed from the Arlington office. It consists of multiple COOP Coordinators within each region / area office.

B

Connectors	**Start**		**Finish**	
	Flowchart	Page Number	Flowchart	Page Number
1A	1	1	1	1
1C	1	1	1	1




[Bureau]
OMB Circular A-123
Continuity of Operations Planning Assessable Unit, Continuity of Operations Planning Process
Continuity of Operations Planning Coordinator (COOPC)
Start
1.1.1 Conduct regular status meetings with COOP Coordinators
1.1.2 Discuss planning, updating, and executing annual COOP Plan
C
1.1.3 Assemble COOP Planning Team
1.1.4 Does a plan already exist?
Yes
1A
H
No
1.1.5 Conduct planning meetings
1.1.6 Verify that the critical planning elements are met during planning meetings
COOP Plan
D
E
1.1.7 Were the critical planning elements met?
Yes
1.1.8 Design COOP Plan
No
1C
F
C1
1A
1.1.9 Review the COOP Plan for accuracy and completeness and validate that the COOP Plan meets applicable requirements
E
1.1.10 Is the COOP Plan approved?
Yes
C2
F
1.1.11 Provide COOP participants with applicable required training
No
1C

4.5. CONTROL MATRIX TEMPLATE OVERVIEW

A control matrix is used to record internal control activity details beyond what is captured in the narrative and flowchart. The control matrix documents information about each internal control activity, such as the control description, the frequency with which the control is performed, whether it is manual or automated, and if it is preventative or detective. A control matrix template is provided in the attachments to this handbook. Details on how to prepare a control matrix, as well as an example of a completed control matrix, are provided below.

4.5.1. Control Matrix Template Instructions

Who is responsible for preparing the control matrix?

The assessable unit manager is responsible for preparing or delegating responsibility for preparing the control matrix.

What type of information and level of detail should be included?

The following guidance describes the primary elements of the control matrix and how to complete the control matrix template provided in the attachments to the handbook. Note, the letter associated with each item in the bulleted list below (e.g., A, B, C) has a corresponding reference on the sample control matrix template presented in this section.

A. **Background Information** - This section of the control matrix includes standard information, including: Bureau, Component, Assessable Unit, Preparer, and the Preparer's Phone Number.

B. **Control Number** - This is the number previously assigned to the internal control in both the narrative and flowchart.

C. **Risk Being Mitigated** - Internal controls are implemented to mitigate risks. Risks are identified through completion of the Integrated Risk Rating Tool. To identify the risks that the internal control is mitigating, ask the following question: "If this activity or procedure ceased to be performed, would the potential for an adverse outcome increase?" In some cases, internal controls are performed as a matter of habit or expectation of the agency, but may no longer serve a legitimate purpose. In many cases, if an internal control activity is not performed, the consequences may be severe (e.g., not protecting a cash drawer with a lock and key could result in theft, or not replacing a degraded transformer bushing could result in a power failure).

D. **Control Activity Description** - The internal control activity description is generally written as a step-by-step guide to performing the internal control. The description should answer the "5 W's." In other words, what activities are included in the step? Who performs the step? When is the step performed? Where is the step performed? Why is the step performed?

E. **Evidence of Control Activity (Supporting documentation, Reports, etc.)** - Evidence of an internal control activity is proof the control was performed. For example, if a manager reviews a report on a monthly basis (i.e., performs an internal control activity), evidence of the manager's review may be the manager's signature, initials, or an e-mail stating that the report was reviewed.

F. **Manual or Automated (M or A - If A, note system)** - Internal controls are automated or manual. Automated internal controls are information system-driven and are performed without human intervention. For example, password restricted access to a database is an automated internal control. Manual internal controls include all other activities, such as reconciliations and management reviews.

G. **Control Type (Preventative, Detective/Reactive, and Sub-type)** - Preventative internal controls are designed to proactively address risks. For example, an automated computer message informing a user that s/he is unable to log into a system is preventative. Maintenance reviews are also preventative internal control activities. Detective/reactive internal controls identify issues after they have occurred. For example, continuity of operations plans for natural disasters are reactive. They mitigate the consequences of a risk event after the major risk event has occurred. Additionally, controls can be further defined as one of the following sub-types:

- **Authorization -** Authorization controls include documented proof that policies, procedures, Directives and Standards, or master files exist and demonstrate that an individual is authorized to make certain decisions. For example, a master file demonstrating authorization to access a database is a sub-type of control. Authorization controls are the rules that allow an individual to have approval authority.
- **Approval** - Approval controls include documented proof that a transaction or decision was made by an individual with the appropriate authority. For example, if a manager is authorized to sign acquisition requests for new equipment, and the manager signs the AR, this is proof that the acquisition was appropriately approved.
- **Segregation of Duties** - Segregation of duties controls include the proper assignment of responsibilities to individuals to prevent a conflict of interest in decision making. If an employee has the ability to both perpetrate and conceal errors or fraud in the normal course of business, then there is an improper segregation of duties within the process.
- **Design and Use of Documents and Records** - Design and use of documents and records controls include pre-numbering forms, marking documents as they are reviewed, and cancelling documents after processing them. For example, a manager receives and pays an invoice for purchased equipment. The manager stamps the invoice as "paid" when complete, preventing a duplicate payment for the same invoice.
- **Adequate Safeguard Over Access to and Use of Assets and Records** - Adequate safeguard over access to and use of assets and records controls include protecting assets from physical harm, loss, misuse, or unauthorized alteration. For example, restricting the use of program vehicles to work-related activities by requiring employees to sign the vehicle in and out prevents the vehicles from being misused.
- **Independent Checks** - Independent checks controls include checking the validity, accuracy, and completeness of processed data. Records should be reconciled and reviewed periodically. For example, an employee in the field office should periodically inspect the assets controlled by the field office and compare the results with inventory records.
- **Summarization of Accounting Data** - Summarization of accounting data controls are designed to ensure financial transactions are properly recorded and adjustments receive the proper approval. For example, prior to posting the journal entries to the general ledger, a manager should compare the journal entry with the supporting documentation to ensure the information the completeness and accuracy of the data.

- **Rights and Obligations** - Rights and obligations controls are designed to ensure that the organization has ownership and rights to its assets at a given date and that the organization's legal obligations are properly recorded. Reported data should be compared to authorization forms, titles, contracts, etc. to confirm the assets and liabilities were recorded properly in the financial statements.
- **Presentation and Disclosures** - Presentation and disclosure controls are not normally included in programmatic reviews. These controls are designed to ensure the organization is properly classifying and describing accounts in the financial statements, the financial statements are in accordance with GAAP, and the footnotes disclose the proper amount of information. For example, a manager references policies and procedures for properly disclosing financial and non-financial information in the financial statements. This will ensure that the information is presented in accordance with GAAP.
- **System Controls** - System controls include preventing unauthorized users from accessing and making changes to the system. If an unauthorized user attempts to make changes in a mission-critical system, the system should either reject the user's changes or not provide the user with the opportunity to make the changes. This will ensure that only authorized users have access and control over the system**.**

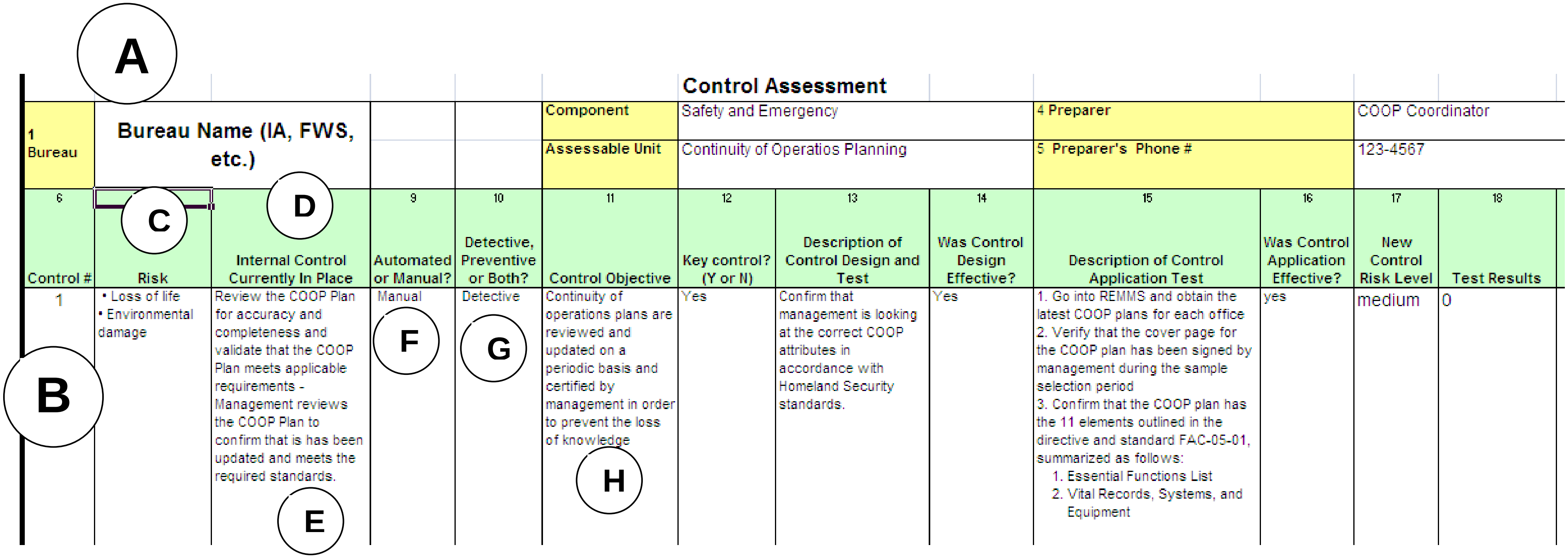
H. **Control Objective** - The control objective is the stated outcome of the control activity. The objective is typically the outcome that will be tested. For example, submission of an accurate time sheet can be a control objective for the time sheet review control.

I. **Frequency (Continuous, Once, Daily, Weekly, Monthly, Quarterly, Annually)** - The frequency should be used to describe how often the control activity is performed. Although not provided in this template, the frequency should be described somewhere in the control matrix to assist with testing the control. For example, many people review their bank statements monthly. Checking a bank statement is a monthly internal control to confirm the account is accurate.

J. **Key Control -** Key controls are those controls that must function in order for an organization to achieve its stated goals and objectives. Key controls often are critical activities without which an organization would not be able to function or would not achieve its goals. Typically, organizations only test key controls.

K. **Columns 13 through 18 of the template -** These columns are captured in the "Test Template." However, they have been presented in this format to demonstrate how controls and control tests can be documented in the same template.

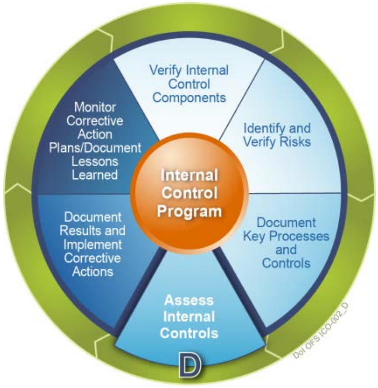
4.5.2. Control Matrix Example - Control Description



Control Assessment

1 Bureau	Bureau Name (IA, FWS, etc.)				Component	Safety and Emergency			4 Preparer		COOP Coordinator	
					Assessable Unit	Continuity of Operatios Planning			5 Preparer's Phone #		123-4567	
6			9	10	11	12	13	14	15	16	17	18
Control #	Risk	Internal Control Currently In Place	Automated or Manual?	Detective, Preventive or Both?	Control Objective	Key control? (Y or N)	Description of Control Design and Test	Was Control Design Effective?	Description of Control Application Test	Was Control Application Effective?	New Control Risk Level	Test Results
1	• Loss of life • Environmental damage	Review the COOP Plan for accuracy and completeness and validate that the COOP Plan meets applicable requirements - Management reviews the COOP Plan to confirm that is has been updated and meets the required standards.	Manual	Detective	Continuity of operations plans are reviewed and updated on a periodic basis and certified by management in order to prevent the loss of knowledge	Yes	Confirm that management is looking at the correct COOP attributes in accordance with Homeland Security standards.	Yes	1. Go into REMMS and obtain the latest COOP plans for each office 2. Verify that the cover page for the COOP plan has been signed by management during the sample selection period 3. Confirm that the COOP plan has the 11 elements outlined in the directive and standard FAC-05-01, summarized as follows: 1. Essential Functions List 2. Vital Records, Systems, and Equipment	yes	medium	0

5. STEP D: ASSESSING INTERNAL CONTROLS


Verify Internal Control Components
Identify and Verify Risks
Document Key Processes and Controls
Assess Internal Controls
D
Document Results and Implement Corrective Actions
Monitor Corrective Action Plans/Document Lessons Learned
Internal Control Program
DoI OFS ICO-002_D

5.1. OVERVIEW OF THE INTERNAL CONTROL TEST PLAN

Assessing internal controls is required. Internal controls should be periodically assessed to determine if they are designed properly and operating effectively (i.e., helping the organization achieve its objectives). The following section describes a suggested approach for evaluating internal control design and operating effectiveness.

5.2. INTERNAL CONTROL TEST PLAN DESCRIPTION

The internal control test plan documents the steps necessary to identify and evaluate key internal control activities. A sample internal control test plan is provided in the attachments to the handbook. Details on how to prepare the internal control test plan, as well as a completed example, are provided below.

5.2.1. Internal Control Test Plan Instructions

Who is responsible for preparing a test plan?
Assessable unit managers are responsible for preparing or delegating responsibility for preparing the internal control test plan. Assessing internal controls requires an understanding of how internal controls may fail, so it is important that internal control assessments be performed by properly trained and experienced individuals.

What type of information and level of detail should be included?
The following guidance describes the primary elements of the internal control test plan and how to complete the template provided in the attachments to the handbook. Note the letter associated with each item in the bulleted list below (e.g., A, B, C) has a corresponding reference on the sample internal control test plan in this section.

A. **Background Information** - This section of the test plan includes standard information, including: Bureau, Component, Assessable Unit and Business Process, Preparer, Preparer's Phone Number, and Related Account Line.
B. **Control Number** -This is the number previously assigned to the internal control in both the narrative and flowchart. It is the same number that appears in the first column of the control matrix.
C. **Nature of Review (Observation, Inspection, Interview, Reperformance)** - The nature of the review refers to the method the reviewer uses to evaluate the operating effectiveness of an internal control. When determining the nature of a review, answer the following question: "What is the most effective method for determining if an internal control activity is failing?" There are four suggested answers to this question: observation, inspection, interview, and re-performance, each of which is described in detail below.
    - **Observation** - An observation is conducted by watching someone perform an internal control activity in the normal course of their duties. Observation of the internal control activity provides evidence that the control was properly performed during the

observation; however, it provides no evidence that the internal control was in operation at any other time.

- **Inspection** - An inspection is conducted by examining documents or records for evidence (e.g., the existence of initials or signatures) that an internal control activity was performed. Inspection, while heavily relied upon for internal control verification, is not always conclusive (e.g., a signature or initials on a document does not necessarily mean an individual reviewed the document).
- **Interview** - An interview is conducted by making oral or written inquiries of personnel involved in performing a control to determine how the internal control activity is performed. Open-ended questions, as opposed to "yes" or "no" questions, are preferred (e.g., "Tell me how you determine when to replace switchgear?").
- **Re-performance** - Re-performance entails performing the internal control activity to assess whether the same results are achieved or conclusions reached as when the control was initially performed. It provides the highest level of assurance. While re-performing controls provides the highest levels of assurance, doing so is often difficult, costly, and/ or time consuming to perform. Re-performance should be used only in circumstances where the benefits are substantial relative to the level of effort required (e.g., performing a network penetration test on a restricted information system, or a physical security test on a restricted building, to assess whether if the systems/facilities can be breached).

D. **Sample Selection Periods** - The period from which the sample is selected should match the period covered by the Annual Assurance Statement. For example, if an assessable unit is reviewing internal controls to provide feedback for the current year's Annual Assurance Statement, the start date of sample documents to be reviewed should not be before October 1 of the current fiscal year. For example, it would not be appropriate to review a document for a signature from a previous fiscal year, if the internal control being tested must be relied upon for the current year's Annual Assurance Statement.

E. **Population** - The population is the total number of items from which the assessable unit manager may draw. For example, if an internal control is performed monthly, the population from which a sample may be drawn is twelve.

F. **Sample Size** - The sample size is based on the frequency with which the internal control activity is performed. Selecting the sample size requires management judgment. As the risk a control mitigates increases, so should the sample size. Although management guidance may vary, the following sample sizes are generally sufficient for reviewing internal controls:

How Often is the Control Performed?	Typical Number of Times to Test Controls	Factors to Consider When Deciding the Extent of Testing
Annually	1	• Complexity of the control • Significance of judgment in the control operation • Level of competence necessary to perform the
Quarterly	2	
Monthly	2 to 5	

How Often is the Control Performed?	Typical Number of Times to Test Controls	Factors to Consider When Deciding the Extent of Testing
Weekly	5 to 15	control • Frequency of operation of the control • Impact of changes in volume or personnel performing the control • Importance of the control
Daily	20 to 40	
Multiple Times a Day	25 to 60	

G. **Evaluation of Design Effectiveness and Steps to Assess Control Effectiveness** - Assessing the design effectiveness of an internal control allows the Internal Control Review Assessment Team to determine if the internal control mitigates identified risks. The steps for assessing internal control design effectiveness should explain how each internal control activity is assessed. The steps should be logical, manageable, and easily understood. When evaluating the design effectiveness of the internal control, ask the following question: "Is something being overlooked or missed by the internal control?" If the answer to this question is yes, then there is likely a design deficiency. When assessing the internal control operating effectiveness, the internal control is assumed to be designed properly, and it is being tested to determine if it is being consistently performed. When assessing internal control operating effectiveness, answer the following question: "Is the internal control being performed, and is it being performed as it was supposed to be performed?" If the answer to this question is no, then it is not operating effectively and should be corrected.

Person Performing Review - The person reviewing an internal control should be competent, objective, and should not be the person that performs the internal control or a subordinate to the person who performs the internal control.

H. **Date Review Completed** - This is the date that the review was completed.

I. **Control Finding (Pass or Fail, Control Deficiency, Reportable Condition, Material Weakness)** - The internal control finding is based on the outcome/results of the Internal Control Review. One of the following options must be selected for each control assessed.

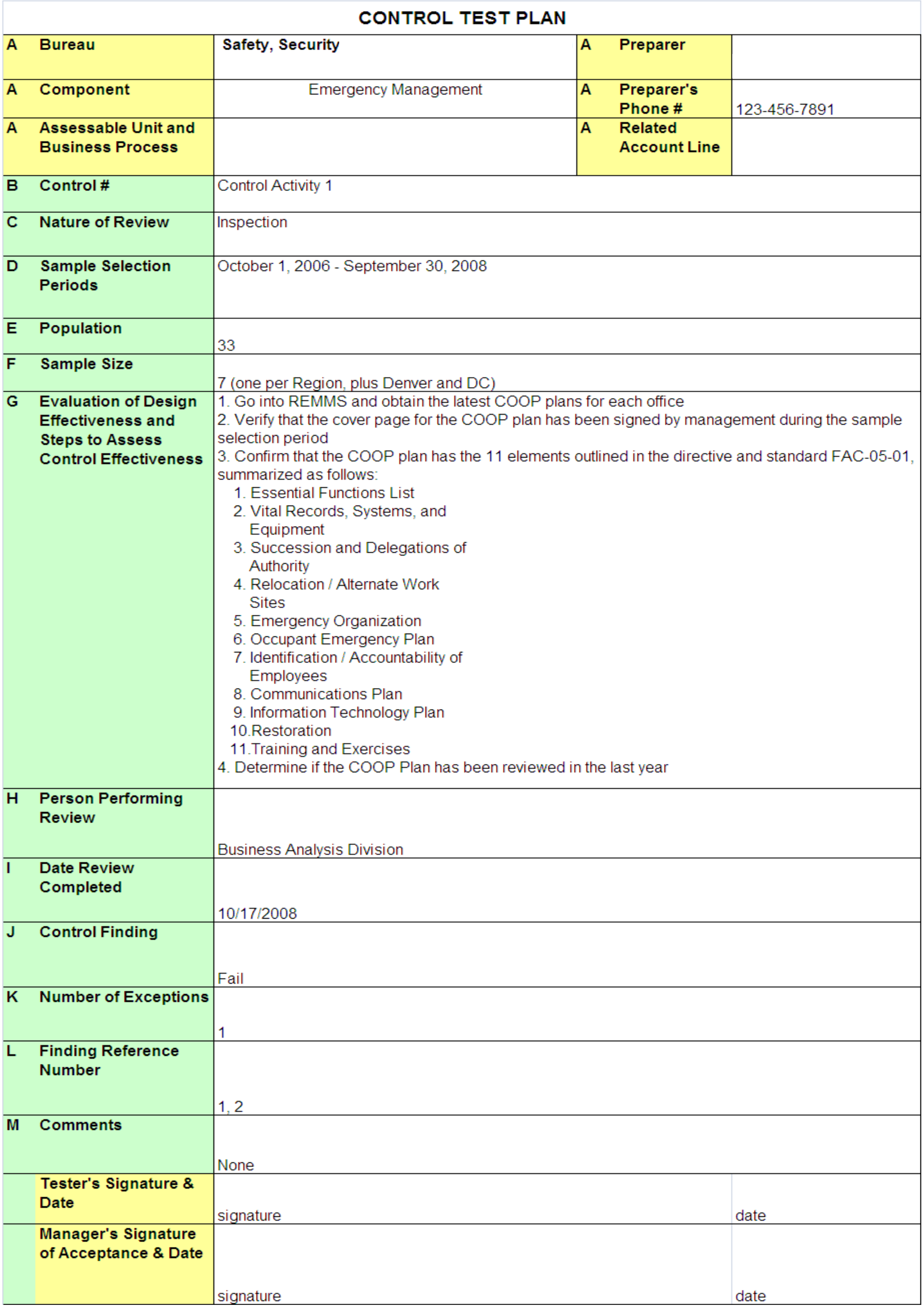
- **Pass or Fail** - The internal control is/is not designed appropriately and/or is/is not operating effectively.
- **Control Deficiency –** The internal control is either improperly designed, or it is operating ineffectively (i.e., not being performed). This exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect a risk to organizational operations in a timely manner.
- **Reportable Condition** - A control deficiency or combination of control deficiencies that in management’s judgment represent significant deficiencies in the design or operation of internal control that could adversely affect the organization’s ability to meet its ability to operate.

- **Material Weakness** - Reportable conditions have been identified within the same component or assessable unit, which individually, **or collectively,** may cause a major failure within the program/bureau. Specifically, this exists when a reportable condition, or combination of reportable conditions, is considered significant enough by the agency head to be reported outside the agency. A material weakness is included in the annual FMFIA assurance statement and reported in the agency financial report.

J. **Number of Exceptions** - This refers to the number of controls tested for a particular attribute that did not have evidence that the control was performed correctly and/or performed recently. In other words, if an attribute being tested was not performed correctly in one of the sample items, that sample failed the test. The total number of failures for each attribute tested is the number of exceptions accumulated for the testing of one attribute. If the number of exceptions exceeds established thresholds, generally three or more for the same control, then a finding should be reported in the summary of findings and recommendations. Example: Acquisition is testing a control which states that for all sole source contracts a justification for the sole source is part of the contract file. If this is a monthly occurrence, an acquisition office would review 2-5 files where sole source vendors were selected. Two out of the selected files do not contain a sole source justification document. Therefore, there are 2 exceptions in this sample and a deficiency exists in the performance of the control.

K. **Finding Reference Number** - Each "control deficiency," "reportable condition," or "material weakness" should be given a reference number for tracking purposes. This number will carry over to the summary of findings and recommendations to help track the finding and corrective actions.
Comments - This section of the internal control assessment portion of the control matrix is where the person performing the internal control review may provide additional comments regarding the internal control being assessed.

5.2.2. Internal Control Test Plan Example

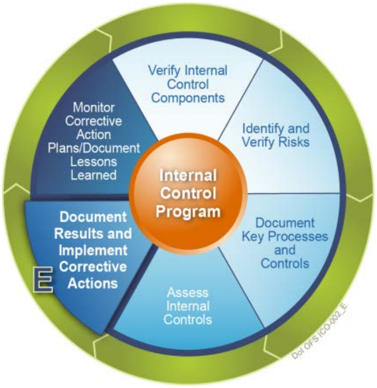


CONTROL TEST PLAN

A	Bureau	Safety, Security	A	Preparer	
A	Component	Emergency Management	A	Preparer's Phone #	123-456-7891
A	Assessable Unit and Business Process		A	Related Account Line	
B	Control #	Control Activity 1			
C	Nature of Review	Inspection			
D	Sample Selection Periods	October 1, 2006 - September 30, 2008			
E	Population	33			
F	Sample Size	7 (one per Region, plus Denver and DC)			
G	Evaluation of Design Effectiveness and Steps to Assess Control Effectiveness	1. Go into REMMS and obtain the latest COOP plans for each office 2. Verify that the cover page for the COOP plan has been signed by management during the sample selection period 3. Confirm that the COOP plan has the 11 elements outlined in the directive and standard FAC-05-01, summarized as follows: 1. Essential Functions List 2. Vital Records, Systems, and Equipment 3. Succession and Delegations of Authority 4. Relocation / Alternate Work Sites 5. Emergency Organization 6. Occupant Emergency Plan 7. Identification / Accountability of Employees 8. Communications Plan 9. Information Technology Plan 10.Restoration 11.Training and Exercises 4. Determine if the COOP Plan has been reviewed in the last year			
H	Person Performing Review	Business Analysis Division			
I	Date Review Completed	10/17/2008			
J	Control Finding	Fail			
K	Number of Exceptions	1			
L	Finding Reference Number	1, 2			
M	Comments	None			
	Tester's Signature & Date	signature			date
	Manager's Signature of Acceptance & Date	signature			date

6. STEP E: DOCUMENTING RESULTS AND IMPLEMENTING CORRECTIVE ACTIONS

6.1. OVERVIEW


Verify Internal Control Components
Identify and Verify Risks
Document Key Processes and Controls
Assess Internal Controls
E
Document Results and Implement Corrective Actions
Monitor Corrective Action Plans/Document Lessons Learned
Internal Control Program

Documenting the results of an internal control review and implementing corrective actions after identifying deficiencies is required. Assessable units are required to take action to improve internal controls that are not operating effectively. As part of this process, the Internal Control Review Assessment Team and assessable unit manager uses assessment results to draft recommendations and to implement process improvements (i.e., corrective actions). This chapter describes the process for summarizing and reporting findings, as well as the process for creating recommendations and implementing corrective actions. The process for implementing corrective actions covers the following: (1) providing a method for assessable unit managers to track corrective action progress; (2) assigning process improvement/corrective action responsibility to the assessable unit personnel; and (3) providing a basis of comparison for future internal control reviews.

6.2. CORRECTIVE ACTION PLAN TEMPLATE DESCRIPTION

The template provided in the attachments to this handbook provides a format for preparing a summary of internal control review findings, as well as recommendations for process improvement. The template, referred to as a summary of findings and recommendations, should be completed for the internal control review. Each individual finding should have its own summary and recommendation for corrective action.

6.2.1. Corrective Action Plan Template Instructions

Who is responsible for preparing the Summary of findings and recommendations?
The assessable unit manager is responsible for preparing or delegating responsibility for preparing the summary of findings and recommendations.

What type of information and level of detail should be included?
The following guidance describes the primary elements of the corrective action plan template and how to complete the corrective action plan template provided in the attachments to the handbook. Note the letter associated with each item in the bulleted list below (e.g., A, B, C) has a corresponding reference on the sample summary of findings and recommendations template in this section.

A. **Background Information** - This section of the summary of findings and recommendations includes standard information, including: Bureau, Component, Assessable Unit and Business Process, Preparer, and Preparer's Phone #.
B. **Report Title** - This section includes information pertaining to the finding and recommendation.

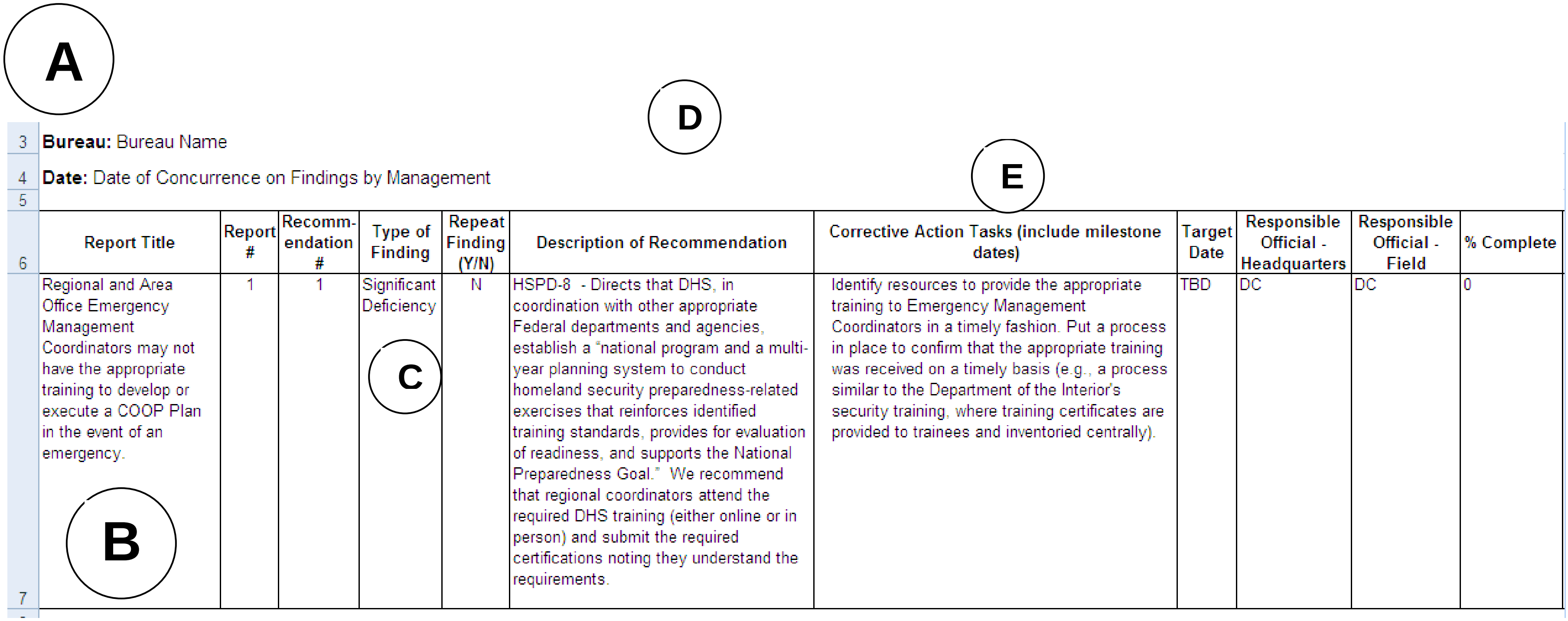
C. **Type of Finding** - This section indicates the severity of the finding and provides the same information as in the "Control Finding" field in the Control matrix. As indicated in the chapter for conducting control assessments, the level should be classified as one of the following:

- **Control Deficiency** - The internal control is either improperly designed, or it is operating ineffectively (i.e., not being performed). This 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 a risk to organizational operations in a timely manner.
- **Reportable Condition -** A control deficiency or combination of control deficiencies that in management's judgment represent significant deficiencies in the design or operation of internal control that could adversely affect the organization's ability to meet its ability to operate.
- **Material Weakness** - Reportable conditions have been identified within the same component or assessable unit, which individually, **or collectively,** may cause a major failure within the program/bureau. Specifically, this exists when a reportable condition, or combination of reportable conditions, is considered significant enough by the agency head to be reported outside the agency. A material weakness is included in the annual FMFIA assurance statement and reported in the agency financial report.

D. **Description of Recommendation** - The recommendation should directly address the failure and its severity. The recommendation should summarize the actions that need to be taken.

E. **Corrective Action Tasks -** Corrective action tasks further define the steps necessary to accomplish the recommendations.

6.2.2. Summary of Findings and Recommendations Example



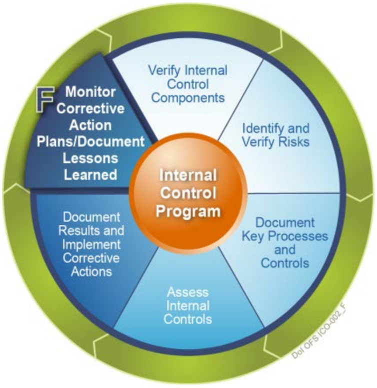
3 **Bureau:** Bureau Name

4 **Date:** Date of Concurrence on Findings by Management

5

Report Title	Report #	Recomm-endation #	Type of Finding	Repeat Finding (Y/N)	Description of Recommendation	Corrective Action Tasks (include milestone dates)	Target Date	Responsible Official - Headquarters	Responsible Official - Field	% Complete
Regional and Area Office Emergency Management Coordinators may not have the appropriate training to develop or execute a COOP Plan in the event of an emergency.	1	1	Significant Deficiency	N	HSPD-8 - Directs that DHS, in coordination with other appropriate Federal departments and agencies, establish a "national program and a multi-year planning system to conduct homeland security preparedness-related exercises that reinforces identified training standards, provides for evaluation of readiness, and supports the National Preparedness Goal." We recommend that regional coordinators attend the required DHS training (either online or in person) and submit the required certifications noting they understand the requirements.	Identify resources to provide the appropriate training to Emergency Management Coordinators in a timely fashion. Put a process in place to confirm that the appropriate training was received on a timely basis (e.g., a process similar to the Department of the Interior's security training, where training certificates are provided to trainees and inventoried centrally).	TBD	DC	DC	0

7. STEP F: MONITORING CORRECTIVE ACTIONS AND DOCUMENTING LESSONS LEARNED


F
Monitor Corrective Action Plans/Document Lessons Learned
Verify Internal Control Components
Identify and Verify Risks
Document Key Processes and Controls
Assess Internal Controls
Document Results and Implement Corrective Actions
Internal Control Program

7.1. OVERVIEW

Monitoring the status of organizational controls on an ongoing basis is required. This chapter provides guidance for monitoring corrective actions and concluding the Internal Control Review, including conducting a close-out meeting, and documenting lessons to improve future years' performance.

7.1.1. Monitoring Corrective Actions

Monitoring the status of corrective actions is an ongoing activity and should be incorporated into the normal course of business. Monitoring should occur through routine management meetings, and require the use of ongoing status reports. These reports should be retained to demonstrate that corrective actions are being carried out and to confirm that management has accomplished its goals outlined in the planning stages of the review.

7.1.2. Planning the Close-out Meeting

The purpose of the internal control review close-out meeting is to discuss difficulties and successes in executing an Internal Control Review. The close-out meeting should be used to document lessons learned and actionable steps for improving future processes. Stakeholders that should attend the close-out meeting include the assessable unit manager, assessment team, and stakeholders.

7.1.3. Close-out Meeting Topics of Discussion / Lessons Learned

The close-out meeting should be structured to elicit feedback related to the following topics/questions:

Overall Review

- *What went well during the Internal Control Review?*
- *What should change in the next Internal Control Review?*
- *Were the results of the Internal Control Review meaningful?*

Stakeholder Management and Communications

- *Were internal control review items(i.e. best practices, findings) communicated to personnel effectively and in a timely manner?*
- *Were issues that arose during the Internal Control Review addressed in a timely manner?*
- *What would the internal control Assessment Team change regarding its interactions with the internal control review Stakeholders next time?*
- *Were the communication methods effective?*

Assessment Team

- *Did the internal control Assessment Team have a clear understanding of their roles and responsibilities?*
- *Did personnel have the right experience and/or knowledge to perform their responsibilities?*
- *Were there enough personnel dedicated to the internal control review? Too many?*

Review Process

- *Was the internal control review guidance clear?*
- *Were enough resources dedicated to the internal control review?*

Responses to these questions should be documented and distributed to meeting participants so that the internal control review process can be improved in future years. The following example provides a suggested format for documenting the lessons learned:

Focus Area	Comment	Lesson Learned / Going Forward
Stakeholder Management and Communications	The initial internal control review Kickoff Memo from the Assessable Unit Manager (or internal control review team lead) was well timed and provided adequate detail regarding the internal control review process enabling stakeholders to understand their roles and responsibilities.	Continue to send the internal control review Kickoff Memo prior to initiating the internal control review.
	Meeting minutes were not posted on the review website in a timely manner.	Consider emailing the meeting minutes to the internal control review team to improve the timeliness of communications.

Section 2
Guidelines to Evaluate Internal Control over Financial Reporting

Interior continues its efforts to enhance its comprehensive, risk-based, integrated Internal Control Program. Developing a comprehensive assessment plan to evaluate internal control over financial reporting is essential to effective implementation of OMB Circular A-123, *Management's Responsibility for Internal Control*, revised 2004. The revision added Appendix A: *Internal Controls over Financial Reporting*. Bureaus/offices are responsible for establishing and maintaining the operational effectiveness and design of Interior's internal control environment. This requires evaluating, testing, and improving internal controls.

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. In addition, Appendix A requires:

- Management to use a separate materiality level when assessing internal control over financial reporting; and,
- Management to specifically document the process and methodology used to evaluate the design and operating effectiveness of internal control over financial reporting.

Interior is using a Department-wide approach whereby analysis of the Department-wide financial statements and identification of the significant financial statement line items helps determine which business processes each bureau/office will review. Only those controls needed to provide sufficient evidence for assurance on the internal control over financial reporting are evaluated.

Interior's framework for the assessment is based on the *Standards for Internal Control in the Federal Government*, issued by the Government Accountability Office (GAO) in November 1999 (GAO/AMD-00-21.3.1 and outlined in OMB Circular A-123). These standards, referred to as the "Green Book," are based on the *Integrated Framework of Internal Control* issued by the Committee of Sponsoring Organizations (COSO). The COSO framework is the most widely applied model in the United States. COSO defines internal control as a process designed to provide reasonable assurance of achieving objectives in three areas:

1. Effective and efficient operations;
2. Reliable financial reporting; and,
3. Compliance with applicable laws and regulations.

The COSO framework presents five interrelated components, each spanning the three objectives: control environment, risk assessment, control activities, information and communication, and monitoring. COSO uses a matrix to illustrate the direct relationship between objectives, activities, and control components. The third dimension of the matrix is those units or activities that relate to internal control.

Interior has adapted a five step process to implement Appendix A. The process is based on the Chief Financial Officer's Council implementation guidance for Appendix A. The five steps are:

1. Planning
2. Evaluating Controls at the Entity Level
3. Evaluating Controls at the Process Level
4. Testing Controls at the Transaction Level
5. Concluding, Reporting, and Correcting

2.1 Planning

Planning is a critical step in the process. A well planned process will ensure the efficient use of resources and a high quality product. The key steps for planning are:

A. Overall Approach: A Top-Down Focus

Under OMB Circular A-123, the support for management's assurance statement should not begin in independent review areas that eventually work their way up the chain of command. Instead, Interior uses a top-down approach focusing on the assurance at the Department-wide level. This approach begins with the Interior'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.

Interior has established an integrated organizational structure to implement the Internal Control Program over financial reporting. This structure starts with the Secretary and descends to the program Assistant secretary, the Bureau/Office Director, and finally the program manager. Roles and responsibilities of key components of the Internal Control Program are described below.

B. Roles and Responsibilities

Roles and responsibilities have been assigned to the following groups:

1. **Principal Operating Group**
The Principals Operating Group (POG) performs the Senior Management Council function as required by OMB Circular A-123. The POG is chaired by the Assistant Secretary - Policy, Management and Budget (PMB) and is comprised of all the Assistant Secretaries, Bureau Directors and the Assistant Secretary – PMB - Chief Information Officer and the Assistant Secretary – PMB – Chief Financial Officer.

The POG's role is to:

- Support DOI's commitment to internal controls – both financial and programmatic
- Ensure your bureau/office has an adequate internal control program - a continuous cycle of assessment, improvement, and reporting
- Each bureau/office - asserts annually that internal controls comply with requirements of the Federal Managers' Financial Integrity Act and OMB Circular A-123
- Oversee detailed management by the Deputies Operating Group.

2. **Deputy Operations Group**
The Deputy Operations Group (DOG) performs the duties of the Senior Assessment Team as defined in OMB Circular A-123. The DOG is chaired by the Assistant Secretary – PMB – Chief Financial Officer and is comprised of the Deputy Assistant Secretaries, Bureau Deputy Directors, Assistant Secretary – PMB - Chief Information Officer and the Office of Inspector General (advisory role). The DOG's role is to:

- Determine scope of assessment, i.e., those financial reports covered by the assessment and processes that impact those reports.
- Ensure that internal control assessment objectives are clearly communicated throughout the Department.
- Ensure that assessment is carried out in a thorough, effective, and timely manner (effective project management).
- Identify and ensure adequate funding and resources are made available.
- Identify staff and secure contractors to perform the assessment.
- Ensure that staff and contractor personnel are adequately trained.
- Determine assessment design and methodology.
- Ensure that adequate policies and procedures are in place to document assessment design, methodology, and results.
- Analyze results of testing and assessment.
- Report on results of assessment.
- Monitor progress of implementing corrective actions.

3. **Bureau/Office Senior Assessment Team (SAT)**
The duties of the Bureau/Office SAT are to:

- Ensure that the assessment objectives are clearly communicated throughout the bureau/office;
- Provide training to personnel involved in the assessment process,

- Ensure that the assessment is executed in a thorough, effective, and timely manner;
- Identify and ensure adequate funding and resources are made available and appropriate staff and/or contractors have been identified to perform the assessment; and,
- Review the assessment results, classification of deficiencies, and adequacy of the corrective action plans.

4. Office of Financial Management (PFM)

PFM is responsible to:

- Provide staff assistance to the POG and DOG;
- Recommend risk-based internal control policies and procedures;
- Provide oversight and guidance to the bureaus/offices concerning the review, evaluation, and maintenance of effective controls;
- Provide training tools to bureaus/offices and facilitate the sharing of training materials among the bureaus/offices.
- Manage, direct, and evaluate Interior's reporting under OMB Circulars A-123 and A-127, the FMFIA, the Federal Financial Management Improvement Act (FFMIA), and the Chief Financial Officers Act, as amended (CFO Act); and,
- Issue the annual guidance on the *Integrated Internal Control Program.*

5. Internal Control Workgroup

The Internal Control Workgroup is comprised of PFM and bureau/office staff directly responsible for implementing the OMB Circular A-123. Duties of the Internal Control Workgroup are to:

- Determine planning and reporting materiality;
- Suggest qualitative materiality factors;
- Solve, collectively, operational problems and issues;
- Respond to audit requests and findings;
- Ensure consistency and timeliness of deliverables; and,
- Develop operational policy and procedures.

C. Assessment Documentation

Documentation to support the planning, evaluating, testing, and reporting phases of the internal control assessment should be created, maintained and be readily available for review. The level of detail of the documentation should ensure management understands the entire financial reporting process and can identify how processes related to financial reporting assertions, potential errors or misstatements and control objectives.

Documentation should be prepared in sufficient detail to provide a clear understanding of it purpose, source and the conclusions reached. Documentation must contain sufficient information to enable a knowledgeable person with no previous connections to the assessment to understand the nature, timing, extent and results of the procedures performed, evidence obtained and conclusions reached, and to determine who performed the work and the date the work was completed. As a general rule, working papers should include the purpose, source, scope, conclusion, and the reviewer's and preparer's name and date.

Standard templates will be provided as necessary by PFM. These will include forms for documentation of business processes, testing, and reporting and should be used as much as possible. The use of standardized forms will allow for an easier comparison of processes and controls across bureaus/offices, encourage the use of a common internal control language at Interior, and assist in exporting best practices.

D. Establish the scope/identify significant financial reports

The scope of significant financial reports to be considered under OMB Circular A-123 Appendix A determines both the breadth and depth of financial reporting. Appendix A provides management with 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:

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

The following steps need to be completed:

- ➢ Bureaus/offices should determine what financial reports are significant. Please note that the first two statements 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/office should document the process used to select the report and why it is significant to the bureau/office.

E. 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.

1. Quantitative materiality factors

a. Quantitative Materiality Base

The materiality base is the element of the financial statements or report that is most significant to the primary users of the statements. The Department uses the greater of adjusted total assets (net of adjustments for intra-governmental balances and offsetting balances) or expenses (total gross costs).

b. Planning Materiality

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

c. Design Materiality

The design materiality is the portion of planning materiality allocated to line items and related disclosures. The provide an allowance for aggregation of misstatement across the individual accounts comprising each line item and for detection risk, design materiality should be one-third of planning materiality. ("Detection risk" is the risk that control activities will fail to detect a material misstatement).

d. DOI Testing Materiality

Interior's design materiality for Management's assessment of internal controls should be lower than that for a financial statement audit. Therefore, the DOI materiality for purposes of OMB A-123, Appendix A, will be calculated at 90 percent of the design materiality. 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.

Interior 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]

[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*

2. 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 Notices of Findings and Recommendations received by the bureaus/offices should also be considered. Although a finding may not be material to the account balance, it may indicate an underlying problem that should be of concern as management determines the materiality of each line item. Changes in business process, accounting standards, and/or in format reporting standards are considered qualitative factors that should be considered when determining material items, lines, or processes to be tested.

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 received by the bureaus/offices
- Political sensitivity of a program or balance.

The following steps need to be completed:

- ➢ PFM will provide the quantitative materiality by financial statement line item and bureau/office.
- ➢ Bureaus/offices should determine and document if any additional financial statement line items and footnotes are significant.

F. Determining Key Processes Supporting Material Line Items

Business processes are the foundation of the internal control assessment and support significant material balances on the financial reports. 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 with Treasury and Investments Management process are:

- 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 revisit process memoranda, flowcharts, and any other analyses that are available.

A standard list of business processes and sub-processes for financial reporting based on the Financial and Business Management System nomenclature has been developed.

The following steps need to be completed:

- ➢ Bureau/office should review the list of identified business processes and sub-processes and determine if any changes are necessary.
- ➢ Bureau/office should complete the crosswalk between significant line items and business processes and sub-processes.

G. Financial Reporting Assertions

Internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reports. The CFO Council's *Implementation Guide for OMB Circular A-123, Management's Responsibility for Internal Control, Appendix A* provided five financial reporting assertions:

- **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.
- **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.

- **Rights and Obligations:** The entity holds or controls the rights to assets and liabilities are the obligations of the entity at a given date.
- **Completeness and Accuracy:** All transactions and events that should have been recorded are recorded in the proper period. Amounts and other data relating to recorded transactions and events have been recorded appropriately.
- **Valuation or Allocation:** 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.

Risks are associated with each type of assertion; the team 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.

The following step needs to be completed:

➢ Bureaus/offices should identify the financial reporting assertions to each material line item on the Business Process crosswalk.

H. Risk Assessment For Financial Reporting

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

- **Inherent Risk** — the susceptibility of an assertion to misstatement, assuming there are no related specific control activities. Inherent risk factors include: the nature of the agency’s programs, transactions, and accounts and whether the agency had significant audit findings.
- **Control Risk** — the risk that misstatements will not be prevented or detected by the agency’s internal control (assessed separately for each significant financial statement assertion in each significant cycle or accounting application).
- **Combined Risk** — the likelihood that a material misstatement would occur (inherent risk) and not be prevented or detected on a timely basis by the agency’s internal control (control risk).
- **Fraud Risk** — the risk that there may be fraudulent financial reporting or misappropriation of assets that causes a material misstatement of the financial statements.

Interior has developed a risk assessment tool that provides a consistent methodology to assess risk across all bureaus/offices. Bureaus/offices will use the results of the risk assessments to determine the testing cycle for business processes. Those business processes rated as high risk should be tested annually.

The following step needs to be completed:

- Bureaus/offices will use the risk assessment tool to determine and document the risks for each business processes. Based upon the results, additional business processes may need to be assessed.

I. Documentation

Once key business processes are identified, they must be described in detail in order to perform an in-depth control analysis. The vehicles most suited to document the processes are the business process memoranda, flowchart, and control matrix.

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

Additionally, business process memos should clearly identify key manual controls and workarounds. Key manual controls identified in the business process memos should be traceable from the business process memos 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 memos and flowcharts.

Key manual controls, which mitigate known IT control gaps or failures, should be clearly marked as a workaround. Also, please indicate the system (e.g., FBMS or other system) 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.

Flowcharts of the business process should be developed based on these process memoranda. The controls should also be identified and numbered on the flowchart to correspond with the process memoranda numbering.

Control Matrixes 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.

The following step needs to be completed:

- Bureaus/offices should develop or update business process memoranda, flowcharts, and control matrixes for each key business process.

2.2 Evaluating 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 GAO Internal Control 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 are 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 accomplish 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. Specific control activities include such items as management review and approval; physical control of assets; exception and edit reports when exceptions are cleared; reconciliations; and segregation of duties.

- **Monitoring** — Internal control monitoring should assess the quality of performance over time. This is done by implementing procedures to monitor internal control on a continuous basis. 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. Interior has developed a tool that can be used to evaluate the entity level controls.

The following steps need to be completed:

- ➢ PFM will provide bureaus/offices the entity level tool.
- ➢ Bureaus/offices will use the entity level tool to evaluate the entity level controls and document the results.

2.3 Evaluating 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 quality of the controls is more important than the number of controls.

A. 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;
- Documenting the assessment process.

A key control is a control whose failure would result in a potential for a material misstatement of the financial statements. Bureaus/offices are responsible for identifying key controls in each of the key business processes. The key controls should be documented on the business process control matrix.

The following step needs to be completed:

- ➢ Bureaus/offices should identify the key controls for each business process on the control matrix and provide the documentation to PFM. See Attachment for control matrix formats.

B. Process owner's concurrence on the documentation of controls

Personnel responsible for a respective business processes should review and approve the process memoranda, flowcharts, and control matrixes. 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 memoranda and controls by the process owner is adequate).

C. Understanding 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 that no changes were made in the 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-performing a given procedure, 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 to consider include:

- 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; and/or,
- 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 an explanation of procedures followed;
- Validate process flowcharts and narratives prepared by program managers;
- Analyze controls design and identify any gaps; and,
- Identify recommendations for corrective actions for gaps.

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

- Names of any persons interviewed;
- Specific items selected for evaluation;
- Results of the evaluation that include a conclusion on the effectiveness of the control design; and,
- 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. Further testing of transactions subject to such controls help determine if any actual loss, fraud, error, improper payment, or noncompliance occurred.

D. Service Organizations

Service organizations that provide significant financial services to Interior 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 service organizations that have a role in handling significant financial transactions may have an assessment completed in accordance with the

Statement on Standards for Attestation Engagements No. 16, *Reporting on Controls at a Service Organization* (SSAE 16) and provide the report to user organizations. The SSAE 16 report provides user management with the information about the service organization's controls to help the user organization assess and address the risks associated with an outsourced service.

AU Section 324 indicated that a service organization's services are part of the User's information system if they affect the following:

- The classes of transactions in the entity's operations that are significant to the financial statements;
- The procedures, both automated and manual, by which transactions are initiated, authorized, recorded, processed, and reported from their occurrence to their inclusion in the financial statements;
- The related accounting records (whether electronic or manual), supporting information, and specific accounts in the financial statements involved in initiating, recording, processing, and reporting transactions;
- How the entity's information system captures other events and conditions that are significant to the financial reports;
- The financial reporting process used to prepare Interior's financial statements, including significant accounting estimates and disclosures.

PFM will identify those service organizations that process significant financial transactions to more than one bureau/office. PFM will then contact those service organizations and request copies of SSAE 16 reports. PFM will inform bureaus/offices of these actions so that multiple requests for the same report are not made to the service organization. Bureaus/offices will be responsible for obtaining SSAE 16 reports from service organization that only provide a service to their bureau/office.

Bureaus/offices are responsible for reviewing and evaluating the SSAE 16 Reports obtained by service providers. The reviews should:

a. 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;
b. Determine whether the report is sufficient in scope;
c. Obtain an understanding of controls at the service provider that are relevant to the bureau/office's portion of the assessment;
d. Obtain an understanding of controls that the bureau/office has over activities of the service provider;
e. Obtain evidence that relevant controls at the service provider operate effectively, and if that is the case, no further testing of those controls is required; and,
f. Address agency control considerations identified in the SSAE 16 Report.

In addition, roll forward memoranda from the service provider for the gap between the end of the period in the SSAE 16 Report and the end of the fiscal year should also be obtained and reviewed by the bureau/office. Documentation of the SSAE 16 reviews should be maintained by the bureau/office.

Not all service organizations have SSAE 16 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.

The following steps need to be completed:

- PFM will provide a listing of SSAE 16 reports Interior expects to receive and the bureau/office responsible for obtaining the report from the service organization.
- PFM will provide to bureaus/offices with a SSAE 16 Review Checklist.
- Bureaus/offices will review SSAE16 Reports and document the review on the Checklist.

E. Understanding the IT Infrastructure and Associated Risks

Interior relies on information technology (IT) to perform its missions and manage processes. IT also plays an important role in the development of internal control over financial reporting. It is critical that technology based controls are also assessed. Bureaus/offices 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:

1. 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. Interior 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.

2. 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 Interior'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 Interiorwide 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.

3. 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

Refer to Section 3 of the Internal Control and Audit Follow-up Handbook for more in-depth information on Interior's IT systems and programs.

2.4 Testing at the Transaction Level

A. 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 memoranda 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 memoranda, 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 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.

B. Risk-Based Approach

Bureaus/offices may 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 3 years. Specifically, risk-based testing is permitted under the following circumstances:

1. 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).

2. 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.

3. 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 3 years and no deficiencies have been found.

The following steps need to be completed:

- ➢ Bureaus/offices should document the risk-based testing plan and how it complies with the above requirements.

C. 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 monthly).
- 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-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.

D. Timing of Testing

The bureau/office should schedule testing to occur throughout the year or quarterly for those controls that coincide with the 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.

E. 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.

The suggested sample sizes from the CFO Council's Implementation Guide are in the following table with examples:

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

To generate the selection, a random number generator should be used. In the case of less frequent occurrences, a representative selection could used instead.

F. Test the Key Controls

Key controls should be tested to determine if they are operating effectively. Determine whether the controls have been applied adequately using a sample of transactions processed throughout the period as indicated in the sampling plan. Samples should be selected from the complete population of transactions for which controls are to be tested.

Detailed documentation of the testing of key controls will support the determination that controls performed as designed and allow others to duplicate the testing if needed. Exceptions noted during testing would indicate when the key controls were operating ineffectively.

2.5 Concluding, Reporting, and Correcting

A. 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 that 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 with the opportunity to remedy the deficient controls prior to Interior's assessment date.

OMB Circular A-123, Appendix A includes the following definitions of deficiencies:

- **Internal Control Deficiency** – exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements in a timely manner.

- **Reportable Condition** – an internal control deficiency, or a combination of deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements, or other significant financial reports, that is more than inconsequential and will not be prevented or detected.

- **Material Weakness** – A reportable condition, or combination of reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected.

B. 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. The deficiency-level determination should be properly documented. When all results have been reported, management can then make the determination if the consolidation of deficiencies is incidental, consolidated 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 is found to be operating effectively, the bureau/office can decide not to report the deficiency.

1. **Issue Log**
All control failures identified during testing should be noted on the issue log. Bureaus/offices must review the test results and consider the likelihood and degree of potential for misstatement in order to assign the level of deficiency to be reported. When all the results are reviewed, management must make a determination if the consolidation of deficiencies are incidental, reportable, or rise to the level of material weakness for reporting in the assurance statement.

The following steps need to be completed:

- PFM will provide to bureaus/offices an issue log
- Bureaus/offices will complete the issue log and provide a copy to PFM as noted in the Monthly Status Report on A-123, Appendix A, provided with the annual guidance.

2. **Reporting required as of June 30**
Interior is required to provide a statement of assurance over the effectiveness of internal controls over financial reporting as of June 30, including an explicit conclusion as to whether the internal controls over financial reporting are effective.

3. **Reporting required as of September 30**
As discussed above, the assessment of internal control over financial reporting is as of June 30. If a material weakness is discovered by June 30, but corrected by September 30, a statement identifying the material weakness, the corrective action taken, and that it has been resolved by September 30 must be added to the assurance statement. If a material weakness is discovered after June 30 but prior to September 30, the statement identifying the material weakness should be updated to include the subsequently identified material weakness.

4. **Changes in Status between June 30 and September 30**
Review Interior'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 end of the fiscal year (September 30). Attempting to correct control deficiencies as they are identified benefits Interior 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 Interior's mission or programs;
    - Reorganizations or other changes to Interior'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/office 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 Interior's financial reports.

The following steps need to be completed:

- ➢ PFM will provide to bureaus/offices a template for the Statement of Assurance on Internal Controls over Financial Reporting.
- ➢ Bureaus/offices will complete the applicable statement and provide the signed document to PFM by the due date.

5. Correcting Deficiencies and Weaknesses

Bureaus/Office should develop a corrective action plan (CAP) for all deficiencies identified during the testing process. The CAP should include actions that will correct the underlying cause of the deficiencies. Interior has developed a standard CAP template that should be used. PFM will monitor the CAP progress for significant deficiencies and material weaknesses.

The following steps need to be completed:

- Bureaus/offices will develop a CAP for each deficiency identified during the testing process.
- Bureaus/offices will provide PFM with CAPs for material weaknesses and significant deficiencies on a quarterly basis.
- PFM will monitor implementation of the submitted CAPs.

SECTION 3

FINANCIAL SYSTEMS/INFORMATION SECURITY

3.1 OVERVIEW

In accordance with 340 DM 1.5.F, Exhibit 1, this section of the Internal Control and Audit Followup Handbook is designed to provide guidance and to establish policy and process procedures for the information security community within Interior for conducting the necessary Internal Control Reviews (ICRs) for operational information systems and information security programs.

As identified in Federal Regulations and OMB Circulars, referenced in Section 3.4 below, Interior is required to conduct an ongoing review of internal controls and report annually on the adequacy of the Interior's security program and operational information systems.

A major part of the ongoing review process of internal controls includes agency program management, financial management, and the supporting information systems and networks. All information systems (otherwise known as major applications and general support systems) shall undergo an ICR annually to comply with the regulation(s) and OMB directives. The ICR of information systems and security programs directly supports and substantiates the annual assurance statement signed by the Secretary of the Interior.

It is paramount that Bureaus/Offices streamline the ICRs of their systems and consolidate reporting requirements to facilitate more efficient reporting and use of financial and human resources. Internal review processes and reporting requirements shall be evaluated to identify overlap and to eliminate duplication where reviews can satisfy multiple requirements.

This section provides detailed guidance for conducting ICRs of information systems and details roles and responsibilities and fiscal year activities.

For the purposes of this section, the following acronyms and terms are defined for use.

- OCIO – Office of the Chief Information Officer (CIO), an organization under the Office of the Secretary.
- CSD – Cyber Security Division, an organization under the OCIO.
- OCIO ICR Coordinator – A designated "ICR" official in the Cyber Security Division of the OCIO.

➢ 3.2 Roles and Responsibilities

Bureau/Office Directors have the overall responsibility to monitor progress associated with the mitigation of material weaknesses, non-compliance issues, and other problem areas identified in OIG, GAO, Departmental, and independent reviews. To facilitate the correction of the identified problem areas, an "early warning system" shall be developed for the internal control and audit followup program to ensure that Interior management is advised of impending problems and recommended solutions that shall ensure that the Bureau/Office can complete remedial actions planned for the current fiscal year. This system shall include the Plan of Actions and Milestones (POA&M) process.

The following roles and responsibilities are defined for the ICRs of information systems and information security programs:

- Departmental CIO — Responsible for the overall ICR program for information systems and information security program for Interior. Provides the department-level assurance statement over information security to the Secretary of the Interior.
- OCIO ICR Coordinator — Responsible for preparing and coordinating annual guidance and Department level reporting relating to ICRs of information systems and the information security program for Interior. This position is designated to a member of the Cyber Security Division in the OCIO.
- Bureau/Office CIOs — Responsible for the overall ICR effort within their respective Bureau/Office. Provides the Bureau-/Office-level assurance statement over information security to their respective Bureau/Office Director.
- Bureau/Office Chief Information Security Officers (BCISO) — Responsible for the coordination of ICRs of information systems and the information security program within their respective Bureau/Office. Reviews the ICR plan and assurance statement ensuring they are complete and accurate. Responsible for ensuring that weaknesses are tracked in accordance with regulation, policy, and the POA&M process.
- Bureau/Office Information Security ICR Lead — Responsible for conducting the assessment of the Bureau/Office information security program. Prepares Bureau-/Office-level ICR plan and assurance statement for the Bureau/Office CIO's signature.
- System Owners — Responsible for conducting ICRs of their assigned information systems, entering the data into the Interior ICR tracking application (CSAM) and reporting ICR results. Responsible for ensuring that weaknesses are managed in accordance with regulation, policy, and the POA&M process.
- Information System Security Officers — Responsible for assisting the ICR Lead and the System Owner as required.

3.3 Executing Internal Control Reviews for Information Systems and Information Security Programs

a) Policy: Internal Control Reviews (ICRs) of all information systems and information security programs shall be conducted on an annual basis in accordance with and in support of Federal Managers' Financial Integrity Act of

1982, OMB Circular A-123, Federal Information Security Management Act of 2002, OMB Circular A-130, and National Institute of Standards and Technology (NIST) Special Publications (SP) 800-100, 800-37, and 800-53.

b) Scope: All Interior operational information systems and information security programs.

c) Definitions:

c.1 The term "information system" refers to either a major application or general support system with a defined security accreditation boundary as described in the NIST "Certification and Accreditation Guide" (NIST SP 800-37).

c.1.1. The term "major application" means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the system in which they operate (either a major application or general support system). Source: OMB Circular A-130 Appendix III

c.1.2. The term "general support system" or "system" means an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency wide backbone, a communications network, a Departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO). Source: OMB Circular A-130 Appendix III

c.1.3. The process of uniquely assigning information resources ("information resources" consist of information and related resources, such as personnel, equipment, funds, and information technology) to an information system defines the "security accreditation boundary" for that system. Source: NIST Special Publication 800-37

Material Weakness – A reportable condition, or combination of reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected. (IC-8)

c.1.4 Significant Deficiency **-** is 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. A significant deficiency under FISMA is to be reported as a material weakness under the Federal Managers Financial Integrity Act (FMFIA) and as a lack of substantial compliance under the Federal Financial Management Improvement Act (FFMIA). (OMB M 08-21)

c.1.5. Non-conformance – A condition in which financial management systems do not substantially conform to financial systems requirements. Financial management systems include both financial and financially related (or mixed) systems. The OIG often terms this as a non-compliance issue. (IC-8)

c.1.6. Non-material weaknesses – Control problems that can be corrected at the Bureau/Office level without the approval or attention of the next higher level or management. (IC-8) also;

Reportable Condition – A reportable condition exists when a security or management control weakness does not rise to level of a significant deficiency, yet is still important enough to be reported to internal management. A security weakness not deemed to be a significant deficiency by agency management, yet affecting the efficiency and effectiveness of agency operations, may be considered a reportable condition. However, due to lower risk, corrective action may be scheduled over a longer period of time. A reportable condition under FISMA is not reported as a material weakness under FMFIA.

d) Policy and Process:

d.1. Bureau/Office CIOs shall ensure ICRs are conducted for all operational information systems for their Bureau/Office identified within the CSAM C&A tracking web application as an accreditation boundary.

Any discrepancies between the CSAM web application and those systems actually in operation shall be promptly resolved and any necessary updates completed.

d.2. Bureau/Office CIOs shall formalize and execute plans to review all of the information systems and the information security programs for which they have responsibility. Plans shall be submitted by each Bureau/Office to the OCIO ICR coordinator in accordance with annual guidance.

d.2.1 The plan shall include a list of all operational information systems for the Bureau/Office.

d.2.2. The plan shall include a reasonable schedule with defined dates and the appropriate designated resources for each of the major functions of the ICR.

d.2.3. The plan shall demonstrate a schedule that meets the date requirements for delivery of the reports to the Department.

d.2.4. The plan shall include the contact information for the information security ICR Lead and the Bureau/Office financial management control testing point of contact.

d.3. ICRs for all information systems and information security programs shall be completed and submitted to the OCIO ICR Coordinator in accordance with annual guidance.

d.3.1 The ICR of each information system shall be conducted in accordance with the annual OCIO directive providing guidance for that fiscal year.

d.3.2. An Assurance Statement memorandum providing the results of the internal control review for all systems and the overall Bureau/Office information security program shall be addressed to the Bureau/Office Director with a courtesy copy to the Departmental CIO and OCIO ICR Coordinator.

d.3.3. All material weaknesses, significant deficiencies, and non-conformance weaknesses (where compensating controls do not fully mitigate the weakness) that are found during the ICR shall be recorded in the assurance statement memorandum. All unmitigated weaknesses, regardless of their severity, shall be recorded in the respective information system's of information security program Plan of Action and Milestones (POA&M) report.

d.4. The OCIO ICR coordinator shall validate that ICRs have been submitted for each system identified in the CSAM web application. The respective Bureau/Office BCISO and Bureau/Office CIO Will be notified of any missing ICR's.

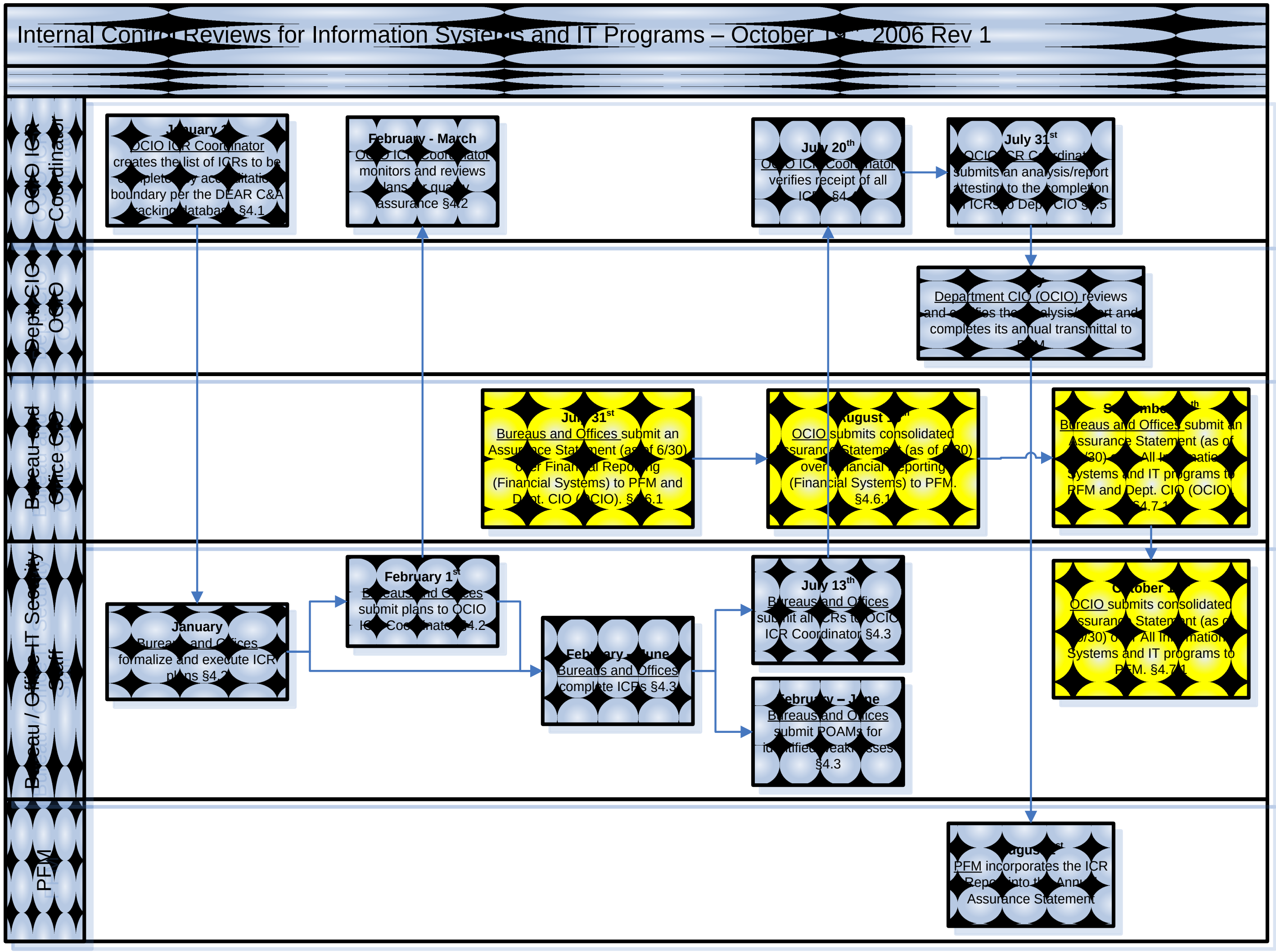
d.5. The OCIO ICR coordinator shall assess all Bureau/Office ICRs for quality and completeness with the respective requirements and shall attest as to whether all ICRs have been completed for all identified (per DEAR) information systems and information security programs.

e) <u>Bureau and Office Assurance Statements</u>

e.1. All Bureau/Office ICRs over financial reporting shall be completed on or before the date specified in the annual guidance. This includes required reviews for financial information systems. Bureau/Office assurance statements over financial reporting as of June 30th must be submitted to

PFM on or before July 31st. Bureau/Office CIOs shall provide their assurance statement to the Bureau/Office Director to support the overall Bureau/Office assurance statement to the Secretary on or before the date specified in annual guidance. The assurance statement must address compliance with FFMIA for financial information systems and follow the template provided in OCIO guidance.

e.2. All reviews of non-financial programs or operations planned shall be completed on or before the date specified in annual guidance. The Bureau/Office annual assurance statement over all security programs and operations, including information systems, as of September 30th, must be submitted to PFM on or before September 28th. Bureau/Office CIOs shall provide their assurance statement to the Bureau/Office Director to support the overall bureau or office assurance statement to the Secretary on or before the date specified in annual guidance. This statement should include an update to the June 30th assurance statement over financial reporting, verifying that key financial reporting controls have either no reportable changes between June 30th, and September 30th, that all reportable material weaknesses have been corrected, or that any uncorrected weaknesses have a POA&M created, resources allocated, and a corrective actions plan in place.



Internal Control Reviews for Information Systems and IT Programs – October 19th, 2006 Rev 1

January 1
OCIO ICR Coordinator creates the list of ICRs to be completed by accreditation boundary per the DEAR C&A tracking database §4.1

February - March
OCIO ICR Coordinator monitors and reviews plans for quality assurance §4.2

July 20th
OCIO ICR Coordinator verifies receipt of all ICRs §4.4

July 31st
OCIO ICR Coordinator submits an analysis/report attesting to the completion of ICRs to Dept CIO §4.5

Department CIO (OCIO) reviews and certifies the analysis/report and completes its annual transmittal to PFM

July 31st
Bureaus and Offices submit an Assurance Statement (as of 6/30) over Financial Reporting (Financial Systems) to PFM and Dept. CIO (OCIO). §4.6.1

August 15th
OCIO submits consolidated Assurance Statement (as of 6/30) over Financial Reporting (Financial Systems) to PFM. §4.6.1

September 15th
Bureaus and Offices submit an Assurance Statement (as of 6/30) over All Information Systems and IT programs to PFM and Dept. CIO (OCIO). §4.7.1

January
Bureaus and Offices formalize and execute ICR plans §4.2

February 1st
Bureaus and Offices submit plans to OCIO ICR Coordinator §4.2

February – June
Bureaus and Offices complete ICRs §4.3

July 13th
Bureaus and Offices submit all ICRs to OCIO ICR Coordinator §4.3

February – June
Bureaus and Offices submit POAMs for identified weaknesses §4.3

October 1
OCIO submits consolidated Assurance Statement (as of 6/30) over All Information Systems and IT programs to PFM. §4.7.1

August 31st
PFM incorporates the ICR Report into the Annual Assurance Statement

3.4 Statutory and OMB Requirements Outline

Federal Regulations

- **FISMA (Federal Information Security Management Act of 2002)**

  The E-Government Act (Public Law 107-347) passed by the 107th Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The information security program must include:

  - **Periodic assessments of risk**, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;
  - **Policies and procedures** that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system;
  - **Subordinate plans** for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
  - **Security awareness training** to inform personnel (including contractors and other users of information systems that support the operations and assets of the agency) of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks;
  - **Periodic testing and evaluation** of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
  - **A process for planning, implementing, evaluating, and documenting** remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency;
  - **Procedures for detecting, reporting, and responding** to security incidents; and
  - **Plans and procedures to ensure continuity of operations** for information systems that support the operations and assets of the agency.

44 U.S.C. §§ 3541, 3544

§ 3541 Purpose — The purpose of FISMA is to:

(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.

§ 3544 Federal agency responsibilities — The head of each agency shall

(a)(1) Be responsible for

(A) providing information security protections;

(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes.

(2) Ensure that senior agency officials provide information security for the information and information systems that support the operations assets under their control, including through;

(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards for information security classifications;

(C) implementing policies and procedures to reduce risks to an acceptable level; and

(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.

(3) Delegate to the agency CIO the authority to ensure compliance with the requirements imposed on the agency, including:

(A) ***CISO -*** designating a senior agency information security officer;

(B) ***Security Program -*** developing and maintaining an agency wide information security program;

(C) ***Policies -*** developing and maintaining information security policies, procedures, and control techniques;

(D) ***Training -*** training and overseeing personnel with significant responsibilities; and

(E) assisting senior agency officials concerning their responsibilities.

(4) Ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements

(5) Ensure **CIO reports annually** to the agency head on the effectiveness of the agency information security program

(b) Implement information security program that includes

(1) ***Risk Assessment -*** periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency

(2) ***POA&M -*** a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency

(3) ***Incident Response -*** procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued

(c) ***Agency Reporting -*** each agency shall

(1) report annually on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements

(2) address the adequacy and effectiveness of information security policies, procedures, and practices

(3) report any significant deficiency in a policy, procedure, or practice identified

(d) ***Performance Plan***

(1) each agency shall include a description of (A) the time periods, and (B) the resources, including budget, staffing, and training, that are necessary to implement the program.

(2) The description shall be based on the risk assessment.

- **OMB Circular A-130** — OMB A-130 establishes “security guidance” for Federal systems, issued in response to the Paperwork Reduction Act of 1980 (P.L. 104-13 and 44 U.S.C. Chapter 35, which established "a broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner”).

a. A minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123

b. Authorization of a system to process information. By authorizing a system, a manager accepts the risk association with it. Management authorization is based on an assessment of management, operational, and technical controls

OMB Circular A-130 Appendix III

A. Requirements

1. Purpose – establishes a minimum set of controls to be included in Federal automated information security programs
2. Definitions
3. Automated Information Security Programs. Implement policies, standards and procedures. At a minimum, agency programs shall include the following controls in their general support systems and major applications:

a. General Support Systems

1) Assign Responsibility for Security.

2) System Security Plan. Shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35). Security plans shall include:
   - a) Rules of the System.
   - b) Training.
   - c) Personnel Controls.
   - d) Incident Response Capability.
   - e) Continuity of Support.
   - f) Technical Security.
   - g) System Interconnection.

3) Review of Security Controls. When significant modifications are made to the system, but at least every three years.

4) Authorize Processing. Use of the system shall be re-authorized at least every three years.

b. Major Applications
   1) Assign Responsibility for Security.
   2) Application Security Plan. Shall be incorporated into the strategic IRM plan required by the PRA. Application security plans shall include:
      - a) Application Rules.
      - b) Specialized Training.
      - c) Personnel Security.
      - d) Contingency Planning.
      - e) Technical Controls.
      - f) Information Sharing.
      - g) Public Access Controls.
   3) Review of Application Controls. Perform an independent review or audit of the security controls in each application at least every three years.
   4) Authorize Processing.

4. Assignment of Responsibilities.

5. Correction of Deficiencies and Reports
   a. Agencies shall correct deficiencies which are identified through the reviews.
   b. **Reports on Deficiencies**. In accordance with OMB Circular A-123, material deficiencies shall be included in the annual FMFIA report. Less significant deficiencies shall be reported and progress on corrective actions tracked at the agency level.
   c. Summaries of Security Plans. Agencies shall include a summary of their system security plans and major application plans in the strategic plan required by the Paperwork Reduction Act.

➢ **GISRA (Government Information Security Reform Act of 2000)** — FISMA replaced GISRA.

- **CSA (Computer Security Act of 1987)** — FISMA repealed CSA.

- **ITMRA (Information Technology Management Reform Act of 1996) / CCA (Clinger-Cohen Act)** — ITMRA/CCA assigns the head of each agency the responsibility to assess Information Technology (IT) resources and makes him/her responsible for effectively managing the risks of IT investments. Recent amendments to this CCA included in the Intelligence Reform and Terrorism Prevention Act of 2004 have created mandatory security responsibilities for the agencies and their CIO.

  a. Requires an inventory of all computer equipment under agency's control; and maintenance of an inventory of any such equipment that is excess or surplus property.
  b. Includes security as a requirement for systems planning and acquisition by agencies.
  c. Provides OMB greater authority in guiding agencies on information security issues, with some specific exemptions.
  d. Codifies the Chief Information Officer responsibility for the security of the information technology architecture.

- **OMB Circular A-11, Preparation, Submission, and Execution of the Budget** — OMB Circular A-11 provides guidance to agencies on how to prepare annual budget submissions. Part 1 provides an overview of the budget process. Part 2 covers development of the President's Budget and describes how to prepare and submit materials required for OMB and Presidential review of agency requests and for formulation of the FY 2007 Budget, including development and submission of performance budgets for FY 2007. The performance budget replaces the annual performance plan required by the Government Performance and Results Act.

  a. Submit a Report on Information Technology to OMB (OMB Circular A-11, Exhibit 53). Per Exhibit 53, agencies are required to have major IT investments within 10% of cost, schedule, and performance objectives.
  b. Submit an OMB Circular A-11 Exhibit 300 for each major IT system. Exhibit 300 requires information on plans and justifications for major acquisitions as identified in OMB Circular A-11, Section 300: Any information technology system reported as a major system in Exhibit 53 (Parts 1, 2, 3, and 4) must also be reported on Exhibit 300;
  c. Ensure information and systems are secure and that security is part of the management of the process from initial concept and throughout the entire life cycle of the investment. Agencies must also protect privacy in a manner consistent with relevant laws and OMB policies, including privacy impact assessments where appropriate.

- **FMFIA (Federal Managers Financial Integrity Act of 1982) (**31 U.S.C. 3512 et seq.) — FMFIA requires agencies to establish and maintain internal control. The requirements of FMFIA serve as an umbrella under which other reviews, evaluations and audits should be coordinated and considered to support management's assertion about the effectiveness of internal control over operations, financial reporting, and compliance with laws and regulations.

  Evaluate and report annually on the control and security of financial systems contained within each agency.

  Amendment to the Accounting and Auditing Act to require ongoing evaluations and reports of the adequacy of the systems of internal accounting and administrative control.

  (d)(2) OMB shall establish guidelines for the evaluation by agencies of their systems of internal accounting and administrative control to determine such systems' compliance with requirements.
  (3) By December 31 of each year, the head of each executive agency shall prepare a statement –
  (A) that the agency's systems of internal accounting and administrative control fully comply with the requirements; or
  (B) that such systems do not fully comply with such requirements.
  (4) …include a report in which any material weaknesses in the agency's systems of internal accounting and administrative control are identified and the plans and schedule for correcting any such weakness are described.

- **OMB Circular A-123, Management's Responsibility for Internal Control** — OMB Circular A-123 provides guidance to agencies and Federal Managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal control to meet the requirements of the Federal Managers' Financial Integrity Act (FMFIA) of 1982, OMB revised internal controls in Section II to better align with current standards.

  a. Identifies security as a necessary component to all internal controls. Specifically, "the safeguarding of assets is a subset of all of those objectives." Internal control should be designed to provide reasonable assurance regarding prevention of or prompt detection of unauthorized acquisition, use, or disposition of assets;
     b. Requires a separate section (Section III) and a listing of statutes for agencies to consider when assessing internal control; and
     c. Introduces a new assurance statement on the effectiveness of internal control over financial reporting, which will be a subset of the overall FMFIA assurance statement.

- **OMB Circular A-127, Financial Management Systems** — OMB A-127 prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems.

- **FFMIA (Federal Financial Management Improvement Act of 1996)** (31 U.S.C. 3512) — FFMIA requires agencies to have financial management systems that substantially comply with the Federal financial management systems requirements, standards promulgated by the Federal Accounting Standards Advisory Board (FASAB), and the U.S. Standard General Ledger (SGL) at the transaction level. Financial management systems shall have general and application controls in place in order to support management decisions by providing timely and reliable data.

  a. Develop and implement general and application controls compliant with guidance provided by FASAB and SGL;
  b. Make a determination annually about whether the agency's financial management systems substantially comply with FFMIA; and
  c. Develop a remediation plan if systems are found to be non-compliant with FFMIA, and determine whether the deficiencies must be reported pursuant to FMFIA.

- **PRA (Paperwork Reduction Act)** — Amended by GPEA.

- **GPEA (Government Paperwork Elimination Act)** — GPEA enacted to make government service delivery more efficient while ensuring baseline standards for electronic signatures across federal agencies.

  Perform business case analysis, cost/benefit analyses, technology assessments, and risk assessments to determine which technologies, systems, and procedures best support compliance with GPEA.

- GPRA (Government Performance and Results Act) — GPRA requires strategic plans and goals to be integrated into: (i) the budget process; (ii) the operational management of agencies and programs; and (iii) accountability reporting to the public on performance results, and on the integrity, efficiency, and effectiveness with which they are achieved. The primary purpose is to assess program effectiveness and improve program performance.

  Develop strategic plans, set performance goals, and report annually on actual performance compared to the goals relating to agency budget, operational management, and reporting to the public on performance results.

National Institute of Standards and Technology

- **Federal Information Processing Standard (FIPS) 199** – Standards for Security Categorization of Federal Information and Information Systems
- **FIPS 200** – Minimum Security Requirements for Federal Information and Information Systems
- **Special Publication (SP) 800-16** – Information Technology Security Training Requirements: A Role- and Performance-Based Model
- **SP 800-18** – Guide for Developing Security Plans for Federal Information Systems
- **SP 800-23** – Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- **SP 800-30** – Risk Management Guide for Information Technology Systems
- **SP 800-34** – Contingency Planning Guide for Information Technology Systems
- **SP 800-37** – Guide for the Security Certification and Accreditation of Federal Information Systems
- **SP 800-39** – DRAFT Managing Risk from Information Systems: An Organizational Perspective
- **SP 800-47** – Security Guide for Interconnecting Information Technology Systems
- **SP 800-50** – Building an Information Technology Security Awareness and Training Program
- **SP 800-53** – Recommended Security Controls for Federal Information Systems
- **SP 800-53A** – Guide for Assessing the Security Controls in Federal Information Systems
- **SP 800-55** – Performance Measurement Guide for Information Security
- **SP 800-60** – Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) – Volume 1: Guide Volume 2: Appendices
- **SP 800-61** – Computer Security Incident Handling Guide
- **SP 800-64** – Security Considerations in the System Development Life Cycle
- **SP 800-65** – Integrating IT Security into the Capital Planning and Investment Control Process
- **SP 800-88** – Guidelines for Media Sanitization
- **SP 800-100** – Information Security Handbook: A Guide for Managers
- **SP 800-115** – Technical Guide to Information Security Testing and Assessment

➢ 3.5 Reporting Requirements

1. **FISMA**
   a. What: Annual reporting defined in OMB memorandum (OMB releases guidelines each fiscal year)

   b. Who: Annual OMB Memorandum
   Section A – no reporting
   Section B – Agency CIO (delegated to CSD, OCIO)
   Section C – IG
   Section D – Privacy Officer

   c. When: Annually at the end of the fiscal year, as directed in OMB FISMA reporting guidance

   d. How: Using the OMB Guidance and OMB Cyber Scope automated reporting tool, completed and transmitted (hard copy and electronic). Tools used to gather inputs for section B include DEAR, DOI CIRC, Department policy, online training reports, and data calls using various office automation tools include Word and Excel. OCIO/CSD collects all input and prepares and coordinates the Secretary's letter to OMB. When directed by OMB, OCIO/CSD later prepares, coordinates, and transmits the FISMA report to the GAO and Congress.

2. **OMB A-130 Appendix III**
   a. What: No extra reporting requirements.
   b. Who: N/A
   c. When: N/A
   d. How: N/A

5. **ITMRA/CCA**
   a. What: No extra agency reports required.
   b. Who: N/A
   c. When: N/A
   d. How: N/A

6. **OMB A-11**
   a. What: 1) Report on resources for financial management activities (Exhibit 52).
   2) Submit a Report on Information Technology to OMB (Exhibit 53).
   3) Submit an Exhibit 300 for each major IT system. Any information technology system reported as a major system in Exhibit 53 (Parts 1, 2, 3, and 4) must also be reported on Exhibit 300.

b. Who: 1)
2)
3)
c. When: 1)
2)
3) 2007: August 30, 2007 [?]
d. How: 1)
2)

7. FMFIA

a. What: Statement that the agency's systems of internal accounting and administrative control fully comply with requirements
b. Who: Department Secretary
c. When: Annually, September 30
d. How: The Assistant Secretaries provide a statement to PMB for each Bureau

8. A-123

a. What: Assurance statement of internal control along with a report on identified material weaknesses and corrective actions.
1) Bureaus/Offices submit material weakness corrective action progress and OIG and GAO audit recommendation implementation status reports
b. Who: Department Secretary
1) Bureau/Office management director and/or Assistant Secretary if appropriate.
c. When: Appendix A is due to OMB June 30 — September 30 weaknesses are updated
1) Monthly for audited financial statement material weakness and noncompliance issues
2) Quarterly (January, April, July, and September) for non financial statement weaknesses
d. How: The assurance statement is submitted in PAR
1) Bureaus/Offices submit quarterly status reports to PFM

9. A-127

a. What: No specific reporting requirements.
b. Who: N/A
c. When: N/A
d. How: N/A

10. FFMIA

a. What: Report to the OMB regarding implementation of FFMIA
b. Who: Secretary of the Interior
c. When: Annually, as of September 30
d. How: In the Annual Financial Report

SECTION 4
AUDIT FOLLOWUP PROGRAM

4.1 Overview

Audit Followup is the process of ensuring that Office of Inspector General (OIG) and Government Accountability Office (GAO) audit recommendations are implemented in a timely manner and that disagreement regarding audit findings and corrective actions between management and the OIG are resolved. Office of Management and Budget (OMB) Circular A-50, "*Audit Followup*," (see Exhibit 12) directs each federal agency to "establish systems to assure the prompt and proper resolution and implementation of audit recommendations."

Interior firmly believes that timely implementation of OIG and GAO audit recommendations is essential to improving efficiency and effectiveness of its programs and operations, as well as achieving integrity and accountability goals. To demonstrate the importance of its commitment to the timely implementation of OIG and GAO audit recommendations, Interior has established a goal for meeting the requirements of the Government Performance Results Act (GPRA). The GPRA goal is based on the number of audit recommendations at the beginning of the fiscal year that have targeted implementation dates during the fiscal year as well as any audit recommendations referred during the fiscal year with target implementation dates during the fiscal year. The Departmentwide performance goal is 85%.

Interior has established a comprehensive audit followup program to ensure that policy and direction regarding the resolution and implementation of audit recommendations is promulgated for the Interior's managers, that audit recommendations are implemented in a timely and cost-effective manner, and that disallowed costs and other funds due the Federal government from contractors and grantees are collected or offset, as appropriate.

This section of the handbook discusses the roles and responsibilities of all components of the audit followup process, procedures for responding to audit reports, the Interior's audit followup tracking system, reporting, and references to key OMB, GAO, and Departmental guidance pertaining to the Audit Followup Program.

<u>Roles and Responsibilities</u>

Interior's Audit Followup Program provides for the clear responsibility of all components involved in reviewing, responding to, and implementing audit recommendations in a timely and effective manner. These roles and responsibilities are outlined below and in Section 1.4A of Departmental Chapter 361 DM 1.

- **The Office of Inspector General (OIG)**

The OIG, under the general supervision of the Secretary, is responsible for independently verifying, conducting, supervising, and issuing audit, evaluation, inspection, and verification reports of programs, operations, activities, and functions conducted by Interior as well as programs funded by Interior. The OIG is also responsible for conducting or supervising audits of insular area governments' programs and operations. It determines when audits can be completed by organizations outside the OIG (such as state and local auditors). In addition, the OIG issues audit reports that have been conducted by the OIG or that have been conducted by other auditing entities.

- **The U.S. Government Accountability Office (GAO)**

GAO is the investigative arm of Congress that supports the Congress in meeting its constitutional responsibilities and assists in improving the performance and ensures accountability of the Federal government for the benefit of the American people.

- **Assistant Secretary - Policy, Management and Budget (A/S-PMB)**

The A/S-PMB is the Interior's Chief Financial Officer (CFO), and, as such, discharges the authority of the Secretary for all phases of management and administrative activities. The A/S-PMB is a principal policy advisor to the Secretary and also the Chair of the Management Excellence Council which serves as the, Internal Control and Audit Followup (ICAF) Council. As Interior's Audit Followup Official, the Assistant Secretary is responsible for overseeing Interior's Audit Followup Program, including the resolution of disputed audit recommendations and corrective actions.

- **Office of Financial Management (PFM)**

The A/S-PMB has delegated day-to-day responsibility for conducting the responsibilities of the Audit Followup Program to the Office of Financial Management (PFM). PFM is responsible for establishing the Interior's policy regarding the Interior's Audit Followup Program, for assisting the Audit Followup Official in resolving disputed audit recommendations, for establishing and maintaining the Interior's audit followup tracking system, and for providing training and technical assistance to Bureaus/Offices regarding the Interior's Audit Followup Program.

- **Departmental Management (Program Assistant Secretaries and Bureau/ Office Directors)**

Assistant Secretaries and Bureau/Office Directors are primarily responsible for responding to and ensuring the implementation of audit recommendations. They are responsible for designating an Audit Liaison Officer (ALO) to conduct the day-to-day audit and audit followup functions and for ensure that systems are in place that provide for the prompt and thorough response to and implementation of audit recommendations.

- **Audit Liaison Officers**

Audit Liaison Officers, appointed by program Assistant Secretaries and/or Bureau/Office Directors, serve as points of contact for all audit activities within their organizational component.

- **Management Excellence Council/Internal Control and Audit Follow-up Council**

The Council is chaired by the A/S-PMB and is comprised of Assistant Secretaries, the Solicitor, the Inspector General (ex officio), the Deputy Assistant Secretary – Budget and Business Management, the Chief Information Officer, and the Senior Procurement Official. The Council's responsibilities are to:

- Ensure Interior's commitment to an appropriate internal control environment;
- Approve Interior's implementation plan for assessing and reporting on internal controls over financial reporting;
- Assess and monitor correction of deficiencies in internal control;
- Identify and ensure correction of systemic weaknesses;
- Review and approve management's annual assertion on the effectiveness of internal controls over financial reporting;
- Recommend to the A/S-PMB which control deficiencies are material and must be disclosed in the annual Federal Managers Financial Integrity Act (FMFIA) assurance statement and Annual Financial Report (AFR);
- Oversee implementation of corrective actions related to material weaknesses; and,
- Determine when sufficient action has been taken to declare a material weakness corrected.

- **Senior Assessment Team/Management Initiatives Team**

The duties of the Senior Assessment Team are performed by the Interior's Management Initiatives Team (MIT) chaired by the A/S-PMB and comprised primarily of Deputy Assistant Secretaries and Bureau Deputy Directors. The team is responsible to:

- Ensure that assessment objectives are clearly communicated throughout the agency;
- Ensure that adequate funding and resources are made available to comply with the requirements of OMB Circular A-123, as revised;
- Ensure that assessments are planned, conducted, documented, and reported upon in a thorough, effective, and timely manner;
- Identify staff and/or secure contractors to perform assessments;
- Determine the scope of assessments and materiality thresholds in accordance with the requirements of OMB Circular A-123, as revised; and,
- Determine or approve assessment design and methodology for each entity and the Interior.

4.2 Accountability and Reporting

Interior places a high priority on improving and promoting accountability and integrity in Interior’s Audit Followup Program and in achieving Government Performance and Results Act (GPRA) performance goals. To evaluate the effectiveness of the Audit Followup Program and Interior’s managers and program officers in implementing audit recommendations, PFM works in partnership with Bureaus/Offices, the OIG, and the GAO to monitor and track activities to ensure the prompt resolution and implementation of audit recommendations and to reduce any backlog of unimplemented audit recommendations. Corrective action plans (CAPs), periodic reporting, and progress meetings provide opportunities to monitor the effectiveness of the Audit Followup Program.

Corrective Action Plans

The development of CAPs and target implementation dates precedes periodic reporting; however, it is integral to Interior’s Audit Followup Program. As indicated in OMB Circular A-50, responses indicating agreement on final reports shall include planned corrective actions and, where appropriate, target completion dates for achieving those actions. To facilitate prompt implementation of recommendations and to reduce slippage, bureaus/Offices must make every effort to:

- Provide responses to recommendations that include target completion dates;
- Ensure that subject matter experts are involved in establishing the target dates;
- Ensure that current and future financial resources are considered and set aside in establishing those dates;
- Ensure that human resources (headquarters and field-level, if applicable) are assigned to ensure completion of the required actions; and
- Ensure that monthly/quarterly milestones are achieved.

Monthly Status Reports

Bureaus/Offices are required to provide the status of the following items on a monthly basis:

- Financial statement audit material weaknesses
- Financial statement audit noncompliance issues

Information from these reports is included in PFM's monthly scorecard reports to senior management. Bureau/Office status report formats should adhere to the PFM annual guidance regarding open audit recommendations identified as material weaknesses and reportable conditions.

Monthly updates must be signed by a Bureau/Office Director or Assistant Director for Administration, as appropriate (some bureaus have been directed to have this information routed through their respective Assistant Secretary before submission to PFM).

Quarterly Status Reports

An updated corrective action plan is to be provided within 15 days of the end of a quarter (expect for the 4th quarter, which must be submitted by the last day of the quarter) on the status of the following:

- Financial statement audit material weaknesses
- Financial statement audit noncompliance issues
- All other referred OIG and GAO recommendations
- Questioned cost in tracking
- Status of external audit reports with disallowed costs.

Quarterly updates must be signed by a Bureau/Office Director or Assistant Director for Administration, as appropriate (some bureaus have been directed to have this information routed through their respective Assistant Secretary before submission to PFM). Information from these reports will also be included in PFM's quarterly scorecard reports to senior management (with copies to the Bureaus/Offices).

Closing OIG and GAO recommendations

Closure documentation must include adequate supporting documentation. If adequate documentation is not included with the closure request, PFM will require additional information and the closure will be delayed. PFM provides the decision on the closure of OIG recommendations/audits to the appropriate Bureaus/Offices and the OIG.

Bureaus/Offices are not restricted to providing notice of implementation of audit reports/recommendations via monthly/quarterly reports; Bureaus/Offices are encouraged to notify PFM of implementation along with the submission of appropriate documentation throughout the year.

Where targeted implementation dates for pending audit recommendations has slipped, a memorandum to PFM requesting an extension of the target implementation date. This request must contain a concise statement of the reasons for the delay and provide a revised target date(s).

Mid-Year and Year-End Progress Meetings

Bureaus/Offices are required to participate in mid-year and year-end progress meetings with PFM, PMB, and the OIG; these meetings are usually held in May and October, respectively. The purpose of the meetings is to review program status and discuss and resolve other pertinent audit followup issues. Additional progress meetings will be scheduled as necessary by PFM.

A senior management official with the authority to make decisions regarding policy issues that affect audit recommendations should be in attendance. It is recommended that individuals designated with the responsibility to correct material weaknesses/noncompliance issues attend these meetings.

Management Excellence Council/Internal Control and Audit Followup (ICAF) Council Meetings (Senior Management Council)

If issues arise as a result of an audit recommendation(s) that cannot be resolved, such as between the Bureau/Office and the OIG, PFM determines whether these issues should be elevated to the ICAF Council for final decision. If it is determined that audit issues need to be elevated to the A/S–PMB and the ICAF Council, PFM will prepare a list of the issues for which agreement/resolution could not be achieved and will schedule the ICAF Council meeting.

Annual Financial Report

One of the purposes of the Chief Financial Officers (CFO) Act of 1990 is to ensure the production of reliable and timely financial information for use in the management and evaluation of Federal programs. The Government Management Reform Act (GMRA) of 1994 furthered the objectives of the CFO Act by requiring all Federal agencies to prepare and publish annual financial reports.

The objective of the Annual Financial Report (AFR) is to provide complete and concise financial and performance information concerning the effectiveness of Interior in achieving its financial program objectives. A component of the AFR is a compliance section that discusses the ICAF program and provides performance data and statistics regarding the effectiveness of Bureaus/Offices in meeting the requirements of pertinent laws and regulations pertaining to the FMFIA.

The AFR also includes key performance measurement data in accordance with GPRA. The GPRA requires that all Federal agencies: (1) Define long-term goals; (2) set specific annual performance targets; and (3) annually report actual performance compared to targets. Interior has elected to publish the AFR and the Annual Performance Report (APR) in lieu of a combined Performance and Accountability Report. The AFR will include key performance indicators and the APR will provide detailed information on Interior's performance goals.

In accordance with the GPRA, Interior has established an objective to resolve audit findings in a timely manner. The AFR includes the FMFIA required September 30 assurance statement which incorporates the June 30, Appendix A Assurance Statement.

Timeframes for Audit Responses

The appropriate response times for OIG, GAO, and other audits are:

Type of Report	Draft Reports	Final Reports
OIG Reports	30-45 calendar days	30 calendar days
Financial Statement Audits	14 calendar days	30 calendar days
GAO Reports	7-30 calendar days	60 calendar days
External Audits	n/a	90 calendar days

4.3 Internet References for OMB Circulars

The following OMB circulars applicable to internal/external audits and referenced in this section may be obtained from the OMB web-site: **www.whitehouse.gov/omb/circulars.**

OMB Circular A-50, *Audit Followup* — This circular provides the policies and procedures for use by executive agencies when considering reports issued by the Inspectors General, other executive branch audit organizations, GAO, and non-Federal auditors where follow-up is necessary.

OMB Circular A-110, *Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations* — This circular sets forth standards for obtaining consistency and uniformity among Federal agencies in the administration of grants to and agreements with institutions of higher education, hospitals, and other non-profit organizations.

OMB Circular A-133, *Audits of States, Local Governments, and Non-Profit Organizations* — This circular, issued pursuant to the Single Audit Act of 1984, Public Law 98-502, and the Single Audit Act Amendments, Public Law 104-156, sets forth standards for obtaining consistency and uniformity among Federal agencies for the audit of States, local governments, and non-profit organizations expending Federal awards.

SECTION 5
OFFICE OF INSPECTOR GENERAL
AUDITS, INSPECTIONS AND EVALUATIONS REPORTS

5.1 Overview

The mission of the Office of Inspector General (OIG) is to promote excellence, integrity, and accountability in the programs, operations, and management of the U.S. Department of the Interior. The OIG, Office of Audits, Evaluations, and Inspections conducts, supervises, and coordinates reviews that:

- Measure Interior programs and operations against best practices and objective criteria to determine if the programs and operations are effective and efficient, achieve the desired results, and/or operate in accordance with applicable laws and regulations.
- Evaluate the revenues and expenditures of the Insular Area Governments of Guam, Commonwealth of the Northern Mariana Islands, the U.S. Virgin Islands, and American Samoa; and Interior funds provided under Compacts of Free Association between the U.S. Government and the Federated States of Micronesia, the Republic of the Marshall Islands, and the Republic of Palau.
- Provide information to or respond to data requests by the Congress, the Office of Management and Budget, and Interior management about Interior's operations.
- Examine Interior financial statements to determine if they are presented fairly and are in accordance with accounting principles.
- Reviews Interior grants and contracts awarded to state, local, Indian tribal, and Insular area governments; for-profit and non-profit organizations; and educational institutions to determine if services have been provided in accordance with the agreements and if costs incurred are eligible for Interior I reimbursement.
- Follow up on prior audit recommendations to determine if the recommendations have been effectively implemented and if any original recommendations need to be reinstated or new recommendations are warranted.
- Oversee the work of non-federal auditors to determine if the work that is performed is in accordance with applicable standards.
- Serve as the federal audit agency responsible for determining compliance with the Single Audit Act of 1984, as amended, by certain state, local, Indian tribal, and Insular area governments; and non-profit organizations as designated by the Office of Management and Budget.

5.2 General Audit Process

The audit process (see Attachment 1) begins with a memorandum from the OIG to the appropriate management official (either an Assistant Secretary or a Bureau/Office director) announcing the start of an audit. An entrance conference is coordinated between the OIG and appropriate management whether Departmentwide or Bureau/Office specific.

The entrance conference provides the OIG with an opportunity to discuss the scope and objectives of the audit. The OIG will also indicate the type of review such as audit, inspection or evaluation. Generally, after the entrance conference audit work will begin.

The OIG holds an exit conference with management officials after the field work is completed. The OIG will discuss preliminary audit findings and may ask for additional information prior to the issuance of a draft audit report. Management officials are encouraged to use the exit conference as an opportunity to thoroughly review and discuss preliminary findings with the OIG, to voice objections or concerns with the preliminary audit findings, and to consider issues that may impact the implementation of audit recommendations (such as the availability of funds needed to implement audit recommendations or the need to publish regulations).

Audit Type	Response Time for Draft Report	Recommendations Referred to PFM for Tracking
Performance	30 days	Yes
Inspection	30 days	Yes
Evaluation	30 days	Yes
Financial	30 days	Yes

Draft reports allow management officials the opportunity to review audit, inspection, or evaluation findings and provide comments that are incorporated into the final report. If the OIG and management official cannot agree on proposed corrective actions or if management disagrees with the OIG's findings, the OIG will refer the final report recommendations to PFM (through the Assistant Secretary – Policy, Management and Budget) for resolution.

If the OIG audit report contains an OIG's assessment of the monetary impact of findings, such as funds to be put to better use, or potential additional or unpaid revenue, Bureaus are expected to indicate agreement or disagreement with the OIG's assessment of the monetary impact of the findings in the response to the audit report.

5.3 Recommendation Referral and Tracking

The OIG obtains and reviews management's official response to the report recommendations. Based on management's response, the OIG classifies each recommendation into the following categories:

Recommendation Category	Referred to PFM for Tracking	Management Official Actions
Resolved and implemented	No	No additional actions required
Resolved and not implemented	Yes – for tracking of implementation	• Develop corrective action plan. • Provide monthly/quarterly status reports to PFM, as appropriate. • Provide supporting documentation to PFM for closure.
Unresolved	Yes – for resolution and implementation, if appropriate	Additional information may be required from management and/or Departmental program policy office.

The OIG refers recommendations for resolution and/or tracking of implementation to PFM via a referral memorandum. PFM inputs the report data and recommendations into its Internal Control and Audit Followup Tracking System (ICAF-TS) and notifies the appropriate management official and Audit Liaison Officer (ALO) of the referred recommendations. PFM considers the date of the OIG referral memorandum as the date of management decision. PFM tracks unimplemented recommendations until the management official provides PFM with sufficient documentation to support the closure of the recommendation.

After the OIG refers an audit report to PFM for tracking, the OIG does not close the audit report in its tracking system until notified by PFM that the recommendation has been implemented and closed. All tracking is the responsibility of PFM. All correspondence pertaining to the referred report must be provided to PFM.

The OIG also refers to PFM for resolution the audits for which management has not responded within the specified timeframe (30 calendar days for a final internal audit report) or audits for which the OIG and management cannot come to an agreement on the recommendation itself or on the management's proposed actions to correct the recommendation. PFM then assumes the responsibility for requesting and receiving management's response and making the final determination of the adequacy of the response. If management responds that all corrective actions have been taken and PFM concurs, PFM closes the report and notifies management, the ALO, and the OIG of the closure. If all corrective actions have not been taken, the report is entered into the ICAF-TS and monitored through final action.

Note: The scope of OIG audits of insular areas includes federal and local funding; the OIG refers to PFM for tracking only those recommendations that involve federal funds and programs.

5.4 Corrective Action Plans

The Bureau/Office management official must develop detailed corrective action plans to implement the recommendations identified in an audit report. A corrective action plan (CAP) must include the following:

- Description of the recommendation as stated in the audit report;
- Tasks/steps that will be completed to implement the recommendation;
- Target dates of implementation of corrective action steps;
- Responsible officials for completing the corrective action steps; and,
- Metrics to measure implementation of the corrective action steps

Attachment 2 is a template that can be used to develop the corrective action plan. This template is also used for reporting the status of open recommendations to PFM. The corrective action plan must be developed within 60 days after the final report is issued.

Bureaus/Offices may find it necessary to develop a more detailed corrective action task plan to implement a recommendation. For instance, it may be helpful to include an estimate of the funding necessary to complete the corrective action steps. These detailed plans should be maintained internally within the Bureau/Office; PFM will request a copy of the detailed plan, if necessary.

Interior's goal is to complete all corrective actions within one year of the date the recommendation was referred to PFM. If the proposed completion date will exceed one year, the Bureau/Office must provide PFM with a detailed explanation justifying the need for an extension.

Due dates for recommendations referred from the Bureau/Office annual financial statement audit are different than the other OIG products. Material weaknesses, internal control deficiencies, noncompliance, and/or management letter issues identified and reported in the financial statement audit will be tracked in the ICAF-TS in a similar manner as other OIG and GAO audit recommendations.

Corrective action plans should be submitted within 60 days of the date the recommendation was referred to the Bureau/Office (memoranda or other communication from PFM notifying the bureau of the referral by the OIG). Corrective actions for the Bureau/Office annual financial statement audit must be completed by June 30 of the subsequent fiscal year. For instance, FY 2009 Financial Statement recommendation should be implemented by June 30, 2010. If the corrective actions will not be completed by June 30 of the subsequent fiscal year, the Bureau/Office should contact PFM to obtain an extension. If the OIG referral is received after March 31 of the fiscal year, the corrective actions must be completed by December 31 of the following fiscal year, (e.g. Referral comes out in April 2009, implementation of the recommendations is due by December 31, 2009).

Bureaus/Offices must establish target implementation dates that are reasonable and achievable. Target dates should allow sufficient time for completion of all required actions so that slippage of implementation dates may be kept to a minimum. If it is necessary to establish long-term corrective action dates, an interim corrective action plan must be established and provided to PFM that describes continuing actions that will be taken so that the impact of a deficiency on affected programs and operations may be kept to a minimum.

Bureaus/Offices must notify PFM if the targeted implementation dates will not be met. Bureaus/Offices must actively monitor the implementation target dates and inform PFM of any slippage as soon as it is determined that a due date may not be achieved. In addition, the Bureaus/Offices must provide a written explanation for the delay, a revised target date, and the official responsible for implementation of the corrective actions.

5.5 Recommendation Status Reporting

Bureaus/Offices must provide monthly and quarterly updates to PFM on the status of corrective action plans. The corrective action plan template (Attachment 3) is the required reporting format. The first report on the status of a material weakness/noncompliance issue is due to PFM 30 calendar days after the OIG referral (and PFM acknowledgement) of the final audit report. Beginning on January 31 (or the last work day of the month) and at the end of each month thereafter, a report on the status of the CAP is due to PFM.

The status report should indicate if the CAP is on schedule, which milestones are completed, and which, if any, has been delayed. If delays have occurred in the completion of monthly milestones, a brief explanation for the delay, whether the delay impacts the bureau's/office's ability to meet the final deadline, how the bureau/office expects to get back on track, and the revised correction date should be noted.

Monthly Reporting

Status of the following items is required for monthly reporting:

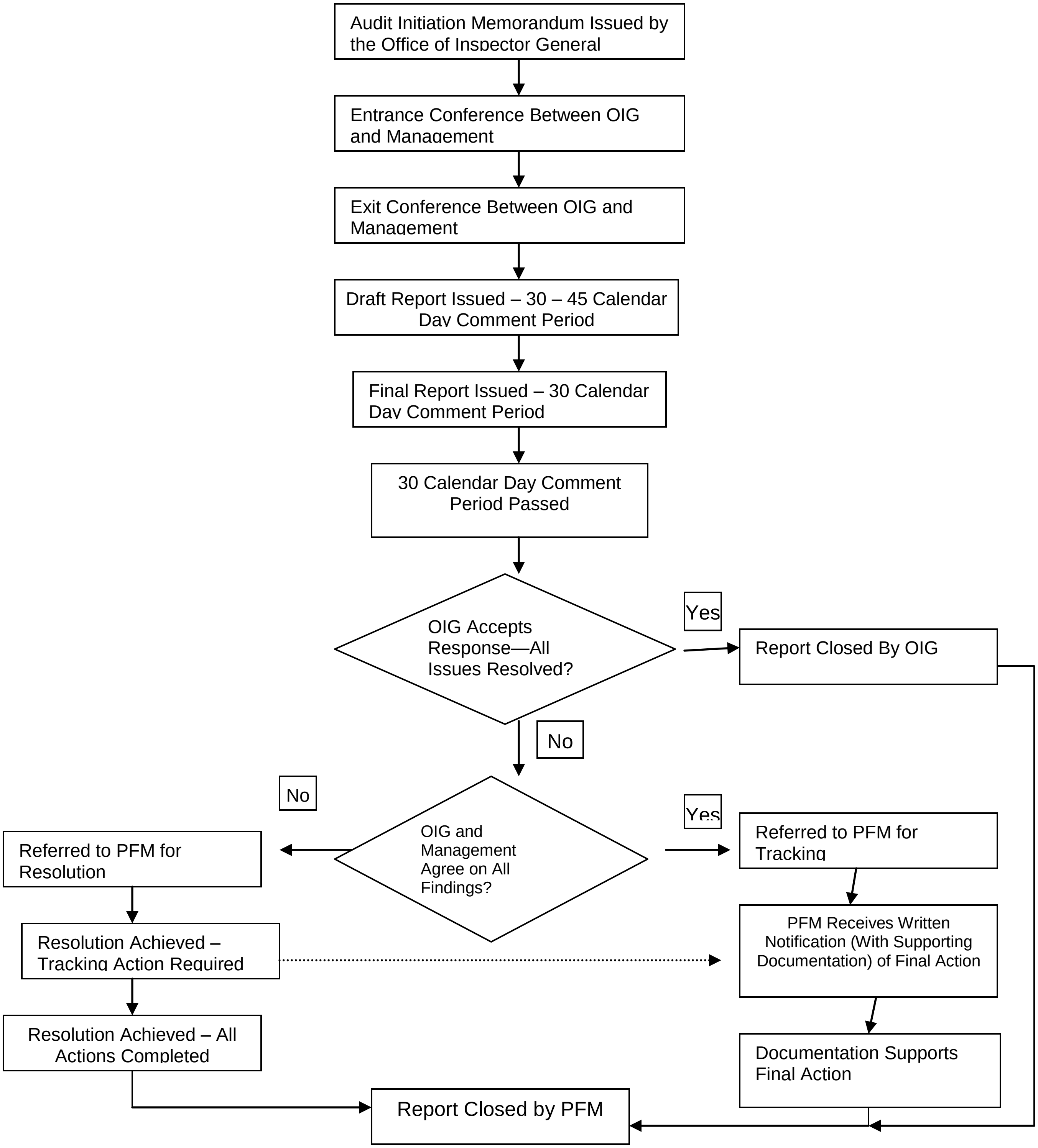
- Financial statement audit material weaknesses
- Financial statement audit noncompliance issues

Quarterly Reporting

An updated corrective action plan is to be provided within 15 days of the end of a quarter (expect for the 4th quarter, which must be submitted by the last day of the quarter) on the status of the following:

- Financial statement audit material weaknesses
- Financial statement audit noncompliance issues
- All other referred OIG and GAO recommendations
- Questioned cost in tracking
- Status of external audit reports with disallowed costs.

INTERNAL AUDIT PROCESS – OFFICE OF INSPECTOR GENERAL AUDIT REPORTS


Audit Initiation Memorandum Issued by the Office of Inspector General
Entrance Conference Between OIG and Management
Exit Conference Between OIG and Management
Draft Report Issued – 30 – 45 Calendar Day Comment Period
Final Report Issued – 30 Calendar Day Comment Period
30 Calendar Day Comment Period Passed
OIG Accepts Response—All Issues Resolved?
Yes
Report Closed By OIG
No
No
OIG and Management Agree on All Findings?
Yes
Referred to PFM for Resolution
Referred to PFM for Tracking
Resolution Achieved – Tracking Action Required
PFM Receives Written Notification (With Supporting Documentation) of Final Action
Resolution Achieved – All Actions Completed
Documentation Supports Final Action
Report Closed by PFM

Financial statement audit status is reported on a monthly basis for material weakness, noncompliance, and FMFIA recommendations. Significant deficiencies are reported on a quarterly basis.

SECTION 6
AUDIT REPORTS ISSUED BY THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO)

6.1 Overview

This chapter discusses Interior's responsibilities associated with audits or reviews conducted by GAO.

GAO will initiate work according to the following priorities:

1. Congressional mandates.
2. Senior congressional leader and committee leader requests.
3. Individual member requests, with additional consideration given to requests from members who are on a committee of jurisdiction.

.

6.2 Roles and Responsibilities

Department of the Interior - Interior is responsible for complying with GAO's request to undertake a proposed engagement or review and is required to cooperate fully with GAO as the review progresses by providing access to program experts and records.

Assistant Secretary - Policy, Management and Budget (A/S-PMB) - The Assistant Secretary serves as the Audit Followup Official for Interior and is responsible for the overall audit followup function, which includes audits issued by the GAO. The Assistant Secretary ensures that all GAO draft and final audit reports are acknowledged within Interior and that any recommendations agreed to by Interior are tracked through full implementation of the corrective action(s).

Office of Financial Management (PFM) - PFM has been delegated the responsibility for program management of the audit followup function. PFM is specifically responsible for:

➢ Receiving all correspondence from GAO initiating work within Interior.

➢ Transmitting GAO's correspondence which initiates the new engagement electronically within one day, when possible, to the affected program Assistant Secretary, the Assistant Secretary's Audit Liaison Officer (ALO), the Bureau ALO, the Department Budget Office (POB), and to Departmental Offices with program oversight.

➢ Scheduling entrance and exit conferences with GAO and appropriate program experts.

- Communicating the date and time of the entrance and exit conferences to all affected Bureau/Office ALOs and the appropriate Departmental Office(s) with program oversight.

- Monitoring the progress of ongoing audit activity on a semiannual basis.

- Ensuring that GAO concludes its audit activity with an exit conference attended by appropriate program officials.

- Receiving draft GAO reports for Interior; designating an organization to respond, transmitting the report, and establishing reasonable deadlines for the response.

- Ensuring that the Departmental responses to draft GAO reports state Interior's concurrence or non-concurrence with GAO's observations and any recommendations that are being proposed. Appropriate technical comments must be included as an enclosure to the response.

- Ensuring that the final signature is obtained and that the letter is e-mailed to GAO within the normal allotted time of 30 days (or as directed by GAO).

- Receiving the final GAO report for Interior; designating an organization to respond; transmitting the report; establishing reasonable deadlines for the Department's response, reviewing the proposed response for content, and ensuring that Interior is responsive to all recommendations contained in the report.

- Ensuring that the departmental response to the final GAO reports containing recommendations to the Department includes a corrective action plan prepared by the affected bureaus/offices.

- Ensuring that all Departmental Offices with program oversight have reviewed and surnamed the proposed response to draft and final GAO reports.

- Ensuring that the final signature is obtained and that the letters are mailed to the congressional staff, Office of Management and Budget, and the GAO within the allotted time of 60 days.

- Tracking the implementation of agreed to corrective actions and providing GAO with the information necessary to complete closure of the recommendation.

- Notifying the program and Bureau/Office ALOs of Departmental closure and GAO concurrence.

Program Assistant Secretary - The program Assistant Secretary is responsible for ensuring that a timely and appropriate response is provided to GAO and Congress on matters under their purview. The program Assistant Secretary is also responsible for designating a senior management official to function as the ALO at the Assistant Secretary level. It is preferable that the program Assistant Secretary ALO be a senior management official within the immediate office of the program Assistant Secretary.

Assistant Secretary Audit Liaison Officer - The ALO for the program Assistant Secretary's office has been delegated responsibility for program management of the audit followup function for the Assistant Secretary's office. The ALO is responsible for:

- Receiving all audit information pertaining to the program Assistant Secretary's area of responsibility;
- Keeping the Assistant Secretary and senior program management informed of audit issues related to their specific program area;
- Providing information and direction to bureau ALO's under their program area; and
- Ensuring that responses to both GAO draft and final reports are coordinated within the Assistant Secretary's office to ensure senior management concurrence with responses developed by program staff within established timeframes set by Interior.

Bureau/Office Director - The Bureau/Office Director is responsible for ensuring that the program Assistant Secretary is provided with a document for signature to ensure that a response to GAO and Congress are submitted within the timeframe allotted. The Bureau/Office director is also responsible for designating an official to function as the audit liaison officer at the Bureau/Office level.

Bureau/Office Audit Liaison Officer - The ALO is responsible for program management of the audit followup function at the Bureau/Office level. The Bureau/Office ALO is responsible for:

- Coordinating audit activity at the Bureau/Office and program office level;
- Scheduling entrance/exit conferences with GAO, when it involves a single Bureau/Office;
- Receiving both draft and final reports for the Bureau/Office;

- ➢ Coordinating internal Bureau/Office surnames;
- ➢ Providing the proposed response to the departmental GAO Audit Liaison and to the Assistant Secretary ALO;
- ➢ Maintaining a current status of corrective actions on open recommendations;
- ➢ Providing a monthly/quarterly status update to PFM on open recommendations, as appropriate; and,
- ➢ Providing implementation memoranda to PFM detailing corrective actions taken on recommendations.

6.3 GAO Audit Process

Notification Letter

Interior is notified by a letter addressed to the Office of Financial Management of the initiation of a new GAO review. The Departmental GAO Audit Liaison Officer notifies the program Assistant Secretary, the Assistant Secretary ALO, the Bureau/Office ALO, POB, and other Departmental Offices with program oversight, of the pending audit.

GAO's notification letter provides the scope and objectives of the proposed audit, the requester's name, additional information if the audit is mandated by legislation, and the name of the GAO team assigned to perform the audit. In addition, GAO's notification letter usually provides the name of the GAO Assistant Director and Analyst-in-Charge responsible for conducting the audit (see flow chart of the GAO audit process at the end of this chapter).

Entrance Conference

An entrance conference is a meeting that GAO holds with agency officials at the start of an engagement. Entrance conferences are held to formally acquaint Departmental staff with the GAO team assigned to conduct the audit.

At the entrance conference, GAO will:

(1) provide the source of the work;
(2) define the roles and responsibilities of the GAO staff;
(3) define information needs (e.g., data and access to agency officials);
(4) define key objectives (research questions);
(5) provide the sites where GAO expects to conduct its work, if known; and,

(6) determine the need for any precautions to protect the data and information (such as special clearances);
(7) provide an estimate of how long the work will take;
(8) request the designation of a key contact;
(9) request identification of knowledgeable agency personnel; and,
(10) discuss the kinds of information that would be useful to complete the work's objectives (such as available studies or electronic files).

Entrance conferences ensure that Interior staff fully understands the scope of the proposed audit.

Conduct of the GAO Audit

The GAO audit period usually lasts 12 – 16 months beginning with the GAO initiation letter, followed by an entrance conference, the survey phase (which is the work development stage), and the data collection and analysis stage. GAO concludes the assignment with an exit conference attended by the program staff prior to the issuance of the draft report.

Exit Conference

An exit conference is held between GAO and program staff at the conclusion of the work. GAO holds the exit conference (in person or by telephone**)** after completing the data collection and analysis. The purpose of the exit conference is to confirm that the critical facts and key information used to formulate GAO's analyses and findings are current, correct, and complete. GAO officials responsible for the completion of the engagement will participate in the meeting. Agency officials who have oversight of the issues related to the engagement's objectives are also expected to attend the meeting.

The exit conference is where the GAO Team provides Interior with a Statement of Facts which summarizes the findings and possible report recommendations, if any. Departmental officials have the opportunity at the exit conference to offer clarifying information or to provide GAO with updated information.

Departmental staff also has the opportunity after the exit conference to begin preparing for the issuance and response to the draft report. The ALO ensures that senior management is aware of the exit conference results and possible draft report recommendations, provides both management and program staff with the opportunity to discuss GAO's findings and recommendations, and concurs on possible corrective actions prior to the actual issuance of the draft report.

Issuance of the Draft Report for Agency Comment

As required by the generally accepted government auditing standards (GAAP), GAO provides Interior with an opportunity to review and comment on a draft of a report before it is issued. When the GAO draft report is issued to the agency, it is formally transmitted to Interior for review and comment. PFM receives all draft reports for Interior and transmits these reports to the Assistant Secretary-level ALO, the Bureau/Office ALO, POB, and departmental Offices with program oversight. Guidance for preparing the response is also provided at this time.

Interior has from 7 to 30 calendar days to comment on the draft report. Interior's policy is to provide written comments on all GAO products with recommendations unless otherwise requested by GAO. The amount of time available for the agency to comment is determined on a facts-and-circumstances basis. GAO, when determining the amount of time available for comment, will consider:

(1) the timing needs of the requester;
(2) the extent to which substantive discussions have already been held between GAO and the agency;
(3) the length of time spent on the engagement; and,
(4) the amount of resources GAO and the agency have expended to answer the engagement's objectives.

Draft reports without recommendations to Interior may be responded to via email stating Interior's position. However, a formal written response must be prepared and submitted to GAO, if any technical comments have been identified.

Responses to GAO draft reports are prepared by program staff for the program Assistant Secretary's signature and are transmitted to the Bureau/Office ALO for content review. Bureau/Office ALO's should ensure that each recommendation has been reviewed and concurred to or not. Interior's concurrence or non-concurrence to the recommendations must be clearly stated in the response to the draft report.

If a draft report involves more than one Bureau/Office within Interior, PFM will assign responsibility for coordinating each Bureau's comments into one consolidated departmental response to a specific Bureau/Office ALO.

Issuance of Final Report

After receiving comments from affected agencies, GAO revises the draft report, as appropriate, and issues the final report. GAO's final report is issued to the

Secretary of the Interior and received electronically in PFM on behalf of the Secretary. PFM provides electronic copies of the final report to the program Assistant Secretary ALO, the involved Bureau/Office ALO, POB, and all other Departmental Offices having program oversight.

If GAO’s final report contains recommendations to the Secretary, the Interior is required by 31 U.S.C. 720 to prepare, within 60 calendar days of receipt, a written statement of actions that have been or will be taken to implement GAO's recommendations. PFM assigns responsibility for the preparation of the response to the appropriate program Assistant Secretary. If the GAO Final Report involves more than one program Assistant Secretary area of responsibility, Interior’s response is prepared for the signature of the designated Agency Audit Followup official’s signature (Assistant Secretary – Policy, Management and Budget).

Response Template for Draft GAO Report Without Recommendations

Addressee should be the name of the GAO Director who heads the team performing the review. The email issuing the draft report would have been sent by this GAO Director.

David Wise
Acting Director, Physical Infrastructure Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Wise:

Thank you for providing the U.S. Department of the Interior, with the opportunity to review and comment on the draft Government Accountability Office Report entitled "Complete *Report Title,” (Report Number).*

We appreciate the diligent work of the team that prepared the report and the large amount of data collected. In general, we believe that this report is an informative and fair summation of the authorities, policies, and complex challenges associated with the disposal and transfer of lands and constructed assets.

If you have any questions or if you need additional information, please contact Program Expert at (xxx) xxx-xxxx.

Sincerely,

Rhea S. Suh
Assistant Secretary – Policy, Management
and Budget

The final signature will be by the Assistant Secretary for the particular Bureau/Office that the report is focused upon. If the report covers more than one Bureau/Office or Assistant Secretary, then it will be signed by Rhea S. Suh, Assistant Secretary – Policy, Management and Budget.

Response Template for Final GAO Report Without Recommendations

Addressee should be the name of the GAO Director who heads the team performing the review. Note: The email issuing the draft report would have been sent by this GAO Director

Robin M. Nazzaro
Director, Natural Resources and Environment
Government Accountability Office
441 G Street, N.W.
Washington, DC 20548-0001

Dear Ms. Nazzaro:

Thank you for the opportunity to review and comment on the Government Accountability Office draft report entitled, *"Complete Report Title,"* (Report Number).

The U.S. Department of the Interior concurs with the findings and recommendations for executive action and believes that these recommendations will help to improve the Wild Horses and Burro Program. The Bureau of Land Management will work to develop cost effective alternatives to long term holding. BLM will seek advice from the National Wild Horse and Burro Advisory Board and other partners and stakeholders to find acceptable solutions and will discuss any helpful legislative proposals with Congress.

The enclosure provides technical comments on the draft report (include only if there are enclosures).

If you have any questions, please contact subject matter experts (xxx) xxx-xxxx.

Sincerely,

Wilma Lewis
Assistant Secretary
Land and Minerals Management

The final signature will be by the Assistant Secretary for the particular Bureau/Office that the report is focused upon. If the report covers more than one Bureau/Office or Assistant Secretary, then it will be signed by Rhea S. Suh, Assistant Secretary – Policy, Management and Budget.

Enclosure

Sample Enclosure

Technical Comments (User this comment period provided by GAO to thoroughly review the draft report and to point out any technical comments in this format. Identify the exact location of the error)

Page 1; 1st paragraph: …only about 9,500 wild horses roamed America's …; Our Biannual reports to Congress indicate there were about 17,300 wild horses and 8,045 burros.

Page 14; 2nd to last line: ". . . is located in the Nevada . . ." should say: located in Nevada.

Page 23, Chart: Eliminate the row entitled Not reported by BLM. The 2 HMAs in this row are the Carracas Mesa which was set in 1995, and the Round Mountain/Devils Garden which was set in 1991.

Page 29, 5th to the last line: Change "4 to 5years" to "3 to 5 years". Insert a space and change 4 to 3. Rationale: The range in some AMLs from low end to high end is too narrow to allow a 4 to 5 year gather cycle without going over high end of AML. Wyoming and Oregon have 3 year cycle AML ranges and this situation may exist in other states as well.

Page 30, 1st paragraph 2nd sentence: Might be clearer if it said: ". . . may be overstated because for reporting purposes, BLM considers HMAs where the population is not more than 10 percent over the upper limit of AML to be at AML.

Page 39, Table 9: BLM Long-Term Holding Facilities, June 2008: The capacity for Pawhuska is 3,400 not 3,600 for a total of 22,100.

Page 41, 11 lines down from top: Change "reposed" to "repossessed"

Page 43, Chart: for 2006, 64/8081 is .79% not .25%, and 28/6944 is .40% not .79%.

Response Template for Final GAO Report With Recommendations

Unlike GAO draft reports, Interior's response to a GAO Final report must have the Corrective Action Plan for each agreed to recommendation. Letters must be addressed to the requestors specified in the report.

The Honorable Joseph I. Lieberman
Chairman, Committee on Homeland Security
  and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Thank you for the opportunity to respond to the Government Accountability Office's recommendations as presented in the report entitled, "*Complete Report Name,"* (Report Number). The U.S. Department of the Interior concurs with the recommendation addressed to the heads of the 24 major agencies and has implemented the recommendation.

The enclosure describes the specific actions that have been taken by the Office of the Chief Information Officer that are in line with the one recommendation in the Report. A similar letter is being sent to the Full Senate Committee on Homeland Security and Governmental Affairs, the Full Senate and House Committees on Appropriations, the Senate and House Appropriations Subcommittees on Interior, Environment, and Related Agencies, the House Committee on Natural Resources, the House Committee on Government Reform, the Comptroller General of the Government Accountability Office, and the Director of the Office of Management and Budget.

If you have any questions or need additional information, please contact Program Expert at (xxx) xxx-xxxx.

Sincerely,

Rhea S. Suh
Assistant Secretary – Policy, Management
and Budget

The final signature will be by the Assistant Secretary for the particular Bureau/Office that the report is focused upon. If the report covers more than one Bureau/Office or Assistant Secretary, then it will be signed by Rhea S. Suh, Assistant Secretary – Policy, Management and Budget.

Sample Enclosure

U.S. Department of the Interior
Action Plan to Address Recommendations
INFORMATION TECHNOLOGY: Agencies Need to Establish Comprehensive Policies to Address Changes to Projects' Cost, Schedule, and Performance Goals
(GAO-08-925)

(1) Recommend each of the heads of the 24 major agencies direct the development of comprehensive rebaselining policies that address the weaknesses we identified.

In June 2008, Interior issued a policy defining our processes and standards for developing a new baseline and the requirement of validating the new baseline. The policy states that a change in (scope) performance requirements requires an updated project plan with recalculated cost and schedule for the (scope) performance requirements. There is special emphasis in “product scope” identification. It also requires an updated project plan with recalculated cost and schedule for the (scope) performance requirements, when management issues affect (scope) performance, cost and/or schedule.

This recommendation has been implemented.

If the actions taken to date does not account toward the implementation of a specific recommendation, then the following must be included for each unimplemented recommendation:

Target Date:

Responsible Official (name and title):

IDENTICAL LETTERS SENT TO:

Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510

Honorable Daniel K. Inouye
Chairman
Committee on Appropriations
United States Senate
Washington, D.C. 20510

Honorable Dianne Feinstein
Chairman
Subcommittee on Interior, Environment,
and Related Agencies
Committee on Appropriations
United States Senate
Washington, D.C. 20510

Honorable Nick J. Rahall II
Chairman
Committee on Natural Resources
House of Representatives
Washington, D.C. 20515

Honorable David R. Obey
Chairman
Committee on Appropriations
House of Representatives
Washington, D.C. 20515

Honorable Norman D. Dicks
Chairman
Subcommittee on Interior, Environment
and Related Agencies
Committee on Appropriations
House of Representatives
Washington, D.C. 20515

Honorable Susan M. Collins
Ranking Minority Member
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510

Honorable Thad Cochran
Ranking Minority Member
Committee on Appropriations
United States Senate
Washington, D.C. 20510

Honorable Lamar Alexander
Ranking Minority Member
Subcommittee on Interior, Environment,
and Related Agencies
Committee on Appropriations
United States Senate
Washington, D.C. 20510

Honorable Doc Hastings
Ranking Minority Member
Committee on Natural Resources
House of Representatives
Washington, D.C. 20515

Honorable Jerry Lewis
Ranking Minority Member
Committee on Appropriations
House of Representatives
Washington, D.C. 20515

Honorable Michael K. Simpson
Ranking Minority Member
Subcommittee on Interior, Environment,
and Related Agencies
Committee on Appropriations
House of Representatives
Washington, D.C. 20515

Honorable Edolphus Towns
Chairman
Committee on Oversight
and Government Reform
House of Representatives
Washington, D.C. 20515

Honorable Darrell Issa
Ranking Minority Member
Committee on Oversight
and Government Reform
House of Representatives
Washington, D.C. 20515

Honorable Gene L. Dodaro
Acting Comptroller General
United States Government
Accountability Office
Washington, D.C. 20548

Honorable Peter R. Orszag
Director
Office of Management and Budget
Executive Office of the President
Washington, D.C. 20503

SECTION 7
SINGLE AUDIT REPORTS

7.1 History

Prior to the implementation of the Single Audit Act of 1984, the federal government relied on numerous audits completed on individual federally-funded programs used by recipients to ensure that these funds were expended properly. Because the government had numerous agencies awarding monies to hundreds of different programs, the task of auditing all programs became increasingly difficult and time consuming. In an effort to improve this situation, Congress enacted the Single Audit Act of 1984 standardizing requirements for audits of States, local governments, Indian tribal governments, and Insular area governments that receive and use federal assistance funds.

In 1985, the Office of Management and Budget (OMB) issues OMB Circular A-128, "*Audits of State and Local Governments*," to provide guidance to recipients and auditors for implementing and carrying out the new Single Audit. In 1990, OMB administratively extended the Single Audit process to non-profit organizations by issuing OMB Circular A-133, "*Audits of Institutions of Higher Education and Other Non-Profit Organizations*" which superseded OMB A-128. With these new guidelines and provisions, the Single Audit was standardized to include any and all State, local governments, and non-profit organizations.

7.2 Purpose and Components

The federal government provides an extensive array of federal assistance to recipients of over $400 billion dollars annually. This assistance is provided through thousands of individual grants and awards for the purpose of benefiting the general public in the areas of education, health, public safety, welfare, public works, and others. However, as a condition of receiving this assistance, recipients must comply with applicable federal and state laws and regulations, as well as any particular provisions tied with the specific assistance. The single audit provides the federal government with assurance that these recipients comply with such directives by having an independent external source (a Certified Public Accounting firm) report on such compliance. However, it only applies to state and local government and nonprofit recipients that expend $500,000 or more of such assistance in one year.

7.3 Compliance Audit

High-Risk and Low-Risk Auditees

Before determining which federal programs the auditor will examine, the auditor must first study the recipient itself. This evaluation requires the auditor to interview recipient employees, observe the recipient in operations, obtain third-party references, and read the recipient's prior audit reports (as well as other procedures), in order to understand the recipient and to determine whether it is likely that it complies or does not comply with federal laws and regulations. This is performed because the recipient's operations, procedures, and work ethic directly affect the compliance of individual Federal programs with laws and regulations.

The evaluation concludes with the auditor's determining, based on the evaluation, whether the recipient is a high-risk auditee or a low-risk auditee. A high-risk auditee is a recipient who has a high risk of not complying with federal laws and regulations; a low-risk auditee is the opposite. For example, an auditor may judge a recipient to be a high-risk auditee because the audit reports of the past few years have numerous audit findings (e.g. specific situations of non-compliance with laws and regulations, serious deficiencies in internal controls, and/or acts of fraud). OMB Circular A-133 has set certain requirements a recipient must meet in order to be considered a low-risk recipient, which include the following:

- Single audits have been performed on an annual basis in prior years.
- The auditor's opinions on the financial statements and the Schedule of Federal Expenditures were unqualified (financial statements are reasonably correct).
- There were no significant deficiencies in internal control (also known as material weaknesses in internal controls) identified in prior year audits.
- None of the federal programs previously audited had audit findings in the last two years.

OMB Circular A-133 uses the high and low risk determination in order to regulate the amount of auditing to be performed. Although the actual work necessary for a Single Audit is established by the auditor, OMB has set a limit for auditing high-risk and low-risk recipients. For high-risk recipients, the auditor is required to audit not less than 50% of all of the federal assistance received during the year. For low-risk recipients, that limit is decreased to 25%.

This determination also affects the entire Single Audit work process; the auditor will adjust the examination accordingly. Since the auditor must provide an opinion to the federal government on whether the recipient and its programs complied with laws and regulations, the auditor will perform sufficient tests and audit procedures (also known as audit work) in order to satisfy himself/herself that the opinion is correct. Normally, the auditor will greatly increase the amount of audit work for high-risk auditees to assure that his/her opinion is correct. For low-risk auditees, the auditor will not be as rigorous as with a high-risk; nevertheless the auditor must be aware that although a recipient is low-risk, it does not mean that it is fully complying with all laws and regulations (conversely, a high-risk determination does not necessarily mean that the recipient never complies with laws and regulations — just that it is more likely than not). When the audit is complete, the auditor provides a copy of the audit to the awarding entity.

7.4 Data Collection and Reporting Package

After the annual Single Audit is concluded, the recipient prepares two documents: a "Data Collection Form and a "Reporting Package".

The Data Collection Form, Form SF-SAC, is a standard form which is basically a summary of the Single Audit. It includes details of the auditor, a list of the federal programs audited, and a summary of any audit findings reported by the auditor. Form SF-SAC is available at http://harvester.census.gov/fac/.

The Reporting Package with all the auditor's final reports along with the recipient's financial statements includes:

- Auditor's reports;
- Management Discussion and Analysis (MD&A) – This serves as an introduction to the recipient's financial statements where the recipient's management (i.e., Governors, in case of States; Mayors, in case of cities; President, in case of non-profit organizations, etc.) discuss the results of operations and other financial information, offering insight and a detailed description about the recipient itself;
- Recipient's financial statements - This contains the financial statements required by the Governmental Accounting Standards Board (GASB), which includes the Governmentwide statements as well as the Fund Financial Statements;
- Recipient's notes to the financial statements – This includes any notes and disclosures for the financial statements as required by US Generally Accepted Accounting Principles (GAAP);
- Supplemental Information – This section includes both financial and non-financial information relative to the recipient which is not covered in the MD&A or the financial statements and their respective notes;
- Schedule of Federal Award Expenditures – This document details all federal assistance expenditures made by the recipient during the audit period, categorized by the federal program and federal agency;
- Schedule of Findings and Questioned Costs – If the auditor finds situations where the recipient did not comply with laws and regulations, where internal controls are deficient, or a situation of illegal acts or fraud,

the auditor is required to report such situations to the federal government in this section, as well as any questioned costs. Questioned costs are amounts that the recipient expended, but which the auditor had identified that they may require a determination by the Federal funding agency as to whether the identified cost are reasonable, allocable, or allowable.

- Schedule of Prior Audit Findings – In this section, the auditor is required to followup and report about the recipient's corrective action on any audit findings reported in prior years.
- Entities response or corrective action plans for the current audit.

Both the Data Collection and the Reporting Package are kept by the recipient with copies submitted to the Federal Audit Clearinghouse (FAC), and to any Federal agency who specifically requests it. Federal guidelines require recipients to submit the documents no more than 30 days after the auditor issues the report or 9 months after the final day of the audit period, whichever comes first.

7.5 Roles and Responsibilities

7.5.1 Office of Inspector General (OIG)

Secretarial Order No. 3254, dated June 24, 2004, transferred the Single Audit Act (the Act) report processing function from the OIG to the Office of Financial Management (PFM). The OIG has cognizant and oversight responsibilities cited by the Act. Therefore, the President's Council on Integrity and Efficiency desk review checklist is completed by the OIG and who will notify other Federal agencies of the acceptance or rejection of an audit report.

As a result of the Secretarial Order and the Act, the responsibilities cited below are delegated to the OIG. The OIG responsibilities are:

- Receives a copy of Report and Data Collection Form from FAC and provides a copy via E-mail or CD to PFM for its review and determination.
- Provides technical audit advice and liaison to auditees and auditors.
- Considers auditee requests for extensions to the report submission due date (Reports are required to be submitted nine months after the final day of the audit period). The agency cognizant for the audit may grant extensions for good cause.
- Obtains and conducts quality control reviews of selected audits made by non-Federal auditors, and provide the results, when appropriate, to other interested organizations.
- Informs other affected Federal agencies and appropriate Federal law enforcement officials promptly of any direct reporting by the auditee

or its auditor of irregularities or illegal acts, as required by Generally Accepted Government Auditing Standards (GAGAS) or laws and regulations.

- ➢ Advises the auditor and/or auditees of any deficiencies found in the audits when the deficiencies require corrective action. When advised of deficiencies, the auditee shall work with the auditor to take corrective action. If corrective action is not taken, the cognizant agency for the audit shall notify the auditor, auditee, and applicable Federal awarding agencies and pass-through entities of the findings and make recommendations for followup action. Major inadequacies or repetitive substandard performance by auditors shall be referred to appropriate State licensing agencies and professional entities for disciplinary action.
- ➢ Provides copies to PFM of technical comments related to the independent auditor's work. Copies are logged and filed with the completed single audit report package.
- ➢ Coordinates audits or reviews made by or for Federal agencies that are in addition to the audits made pursuant to this part, so that the additional audits or reviews build upon audits performed.
- ➢ Coordinates the audit work and reporting responsibilities among auditors to achieve the most cost-effective audit.
- ➢ Considers auditee requests to qualify as a low-risk auditee for permitted biennial audits.
- ➢ The National Single Audit Coordinator acts as the liaison with FAC to access, if appropriate, the FAC Image Management System.

7.5.2 Office of Financial Management – Internal Control and Audit Followup (ICAF)

As a result of the Secretarial Order, ICAF responsibilities are:

7.5.2.1 Tracking Single Audits

PFM tracks disallowed costs of $1,000 or more:

- ➢ That resulted from a violation or possible violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the use of federal funds, including funds used to match federal funds;
- ➢ Where the cost, at the time of the audit, is not supported by adequate documentation; or
- ➢ Where the costs incurred appear unreasonable.

Single Audit Reports and Data Collection Forms are received from the OIG via e-mail and/or CD. PFM reviews the single audit report to identify the oversight agency that provided the predominant amount of money in Federal awards.
Once this is determined, the reports are then disseminated to the analyst(s) responsible for that particular Bureau/Office.

Each PFM analyst with single audit responsibilities reviews the single audit report to:

- Determines the oversight or cognizant agency from the Data Collection Form.
- Ensures that all required components of the report are available for review (i.e. auditors' reports, schedule of Federal Assistance, schedule of current and prior year findings and/or questioned costs, and corrective action plan).
- Determines findings and/or questioned costs.
- Prepares memoranda for each bureau/office for which the audit identifies findings and/or questioned costs, as well as prior year(s) findings. The memoranda are standardized detailing the results of the review. If the respective bureau/office has a finding(s) and/or questioned costs, it is required to provide a response within 90 days of the PFM issuance date. (i.e., the date that is on PFM's memoranda to the Bureau/Office).
- E-mails memoranda and single audit reports to the Bureaus/Offices. The memoranda may also include an Attachment, when applicable (i.e., if the report contains a large number of findings and/or questioned costs, an Attachment will be provided which lists in detail each finding and questioned cost).
- Receives, reviews, and approves/denies requests for extensions from bureaus/offices of the response due date.
- Tracks audit findings in the PFM tracking system to ensure that information is accurate and up to date and that the recipient takes appropriate and timely corrective action.
- Receives and reviews resolution memoranda and to ensure adequacy.
- Determines that appropriate documentation to support the accomplishment for final action has been provided and that the audit may be closed.
- Followup on findings and/or questioned costs on responses that have not been received within the required 90 day period.

- Manages centralized library of files within PFM of all single audit reports that contain Interior findings and with all related correspondence.

7.5.3 DOI Bureaus and Offices

Although Interior does not track disallowed costs of less than $1,000, Bureaus/Offices are required to monitor, track, and collect all debts owed. Bureau/Office management is responsible for reviewing findings and auditee responses to determine whether the actions taken or planned will correct the findings reported. If the Bureaus/Offices determine that the actions will not correct the findings, the entity must be advised of the additional actions required to be taken. Bureau/office management also reviews all costs questioned by auditors and determines if the costs are sustained (management agrees with the auditors questioning of the costs and the costs must be repaid by the auditee) or if the costs may be reinstated (management determines that the costs is allowed and therefore does not have to be repaid). Awarding officials may also determine that a cost is not authorized under the terms of the contract, compact, or grant, even if the costs were not identified by the auditor as a questioned cost. When bureaus notify PFM of Single Audit final actions, management's notification to PFM must be specific and detailed, to document what action was required and what action was taken. Specific documentation must accompany management's notification of final action.

7.5.3.1 Referral of Audit Reports to the Department of the Treasury

The Debt Collection Improvement Act (DCIA) of 1966 makes the Department of the Treasury responsible for collecting delinquent debts Governmentwide. The DCIA requires agencies to transfer the delinquent, non-tax debt over 180 calendar days old to Treasury; the DCIA also applies to audit-related debts such as disallowed costs. In order to effectively collect the debts that agencies refer, Treasury issues demand letters, conducts telephone follow-up, refers debt for administrative offsets, and refers debts to private collection agencies. Audit-related debt in litigation or appeal by grantee is exempted from transfer to Treasury.

Final action on disallowed costs may include:

- Collection – which occurs when the auditee remits payment of disallowed costs to Interior;

- Offset – which means the collections of audit-related debt by means of offsets against other monies due to the entity from the federal government;
- Write-off – which means a decision by management that collection action is not in the best interest of the Federal Government;
- Reinstatement – which means a determination by an Awarding official that the auditee has, subsequent to the decision to disallow, provided sufficient documentation to support the expenditure of funds; and,
- Transfer – which means that the identified and sustained disallowed costs are transferred to the Treasury for collection action.

For disallowed costs that have been collected:

- A copy of a payment check;
- A copy of a bill for collection that has been annotated with information concerning payment (date and form of payment, check number, and the official accepting payment);
- A memorandum signed by an appropriate official (Assistant Secretary, Bureau/Office Director, or Awarding Official) certifying that payment has been made or that disallowed costs have been referred to Treasury for collection action.

For disallowed costs that have been offset or written-off;

- A memorandum signed by the appropriate official in accordance with Departmental Manual Chapter 344 (Debt Collection).

In order to ensure effective recovery of audit-related debt, bureaus and offices are expected to establish adequate accounting and collection controls and systems to ensure that audit-related debt is tracked, recovered, and reported. Disallowed costs should be collected in accordance with the Federal Claims Collection Standards, unless otherwise required by statute.

Collection of disallowed costs for grants issued under the authority of the Indian Self-Determination and Education Assistance Act, as amended (Public Law 93-638) is time-barred if an appealable notice of disallowance has not been provided to the grantee within 365 calendar days of receipt of the report by Interior (Section 106(f).) Awarding officials should be aware of this provision so that Indian Tribes are promptly notified of a decision to disallow questioned costs**.**

7.5.4 Audit Liaison Officer (ALO)

Bureaus are responsible for appointing an Audit Liaison Officer (ALO). ALOs are appointed by the program Assistant Secretaries or the Bureau Director and the Director of secretarial level offices, and serve as points of contact for all audit activity for their organizational component. The ALOs audit followup responsibilities are:

- Ensuring that any determination (findings and/or questioned costs) from PFM will be addressed in a timely manner;
- Ensuring that responses are sufficient for closure and received in PFM within the required timeframe;
- Ensuring that corrective actions agreed to be taken are completed;
- Ensuring that reconciliation is performed on the status of open and closed single audits;
- Reporting on the Status of External Audit Reports with Disallowed Costs on a quarterly basis (per PFM Annual Audit Followup Guidance; and,
- Designating a Single Audit Coordinator to conduct the day-to-day activities of the single audit program.

7.6. Time Frames for Responses to External Report (A-133) Findings and/or Questioned Costs

External Audits	90 calendar days from issuance of PFM letter

7.7. Internet References for OMB Circulars

OMB Circulars applicable to this program may be obtained from: www.whitehouse/omb/circulars.gov

- OMB Circular A-50*, Audit Followup* — This circular provides the policies and procedures for use by executive agencies when considering reports issued by the Inspector General, other executive branch audit organizations, the Government Accountability Office, and non-Federal auditors where follow-up is necessary.

- OMB Circular A-110***, Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and other Non-Profit Organizations*** — This circular sets forth standards for obtaining consistency and uniformity among federal agencies in the administration of grants to and agreements with institutions of higher education, hospitals, and other non-profit organizations.

- OMB Circular A-133*, Audits of States, Local Governments, and Non-Profit Organizations* — This Circular was issued pursuant to the Single Audit Act of 1984, Public Law 98-502, and the Single Audit Act Amendments, Public Law 104-156, to set forth standards for obtaining consistency and uniformity among federal agencies for the audit of states, local governments, and non-profit organizations expending federal awards.

7.8 Contacts

OIG, Single Audit Coordinator
703-487-5357
Fax: 703-487-5214

PFM
202 208-4701
Fax: 202-208-6940

SECTION 8
GRANT AUDIT REPORTS

8.1 Grant Audit Reports

A grant or a cooperative agreement is a legal instrument used by a Federal agency to enter into a relationship in which the principal purpose is financial assistance. When providing assistance, agencies must use grants when substantial involvement between the recipient and the Government is not contemplated and cooperative agreements when substantial involvement is contemplated.

The Office of Inspector General (OIG) is responsible for conducting audits of awards of funds expended under the authority of Office of Management and Budget (OMB) Circular A-110, "*Uniform Administrative Requirements of Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations*" as it applies to grants awarded by Interior to recipients and, through recipients, to sub-recipients.

Audit reports are addressed to the Cognizant Agency (Federal awarding agency that provides the predominant amount of direct funding to a recipient unless OMB makes a specific cognizant agency for audit assignment), and a copy is sent to the OIG. Bureau/Office management must respond to the audit report within 120 days of issuance. The response should address in detail all issues mentioned in the report and be sent to the OIG with a copy to PFM.

8.2 Grant Audits Referred for Resolution

When the bureau has not responded to the results of a grant audit within 120 days of issuance of the report, the report is referred to the Office of Financial Management (PFM) for resolution. Upon referral, PFM will:

- Contact the Bureau/Office and request a response to the audit report;
- Review the response for adequacy, once received; Request additional information if t he response is incomplete;
- Close the report if the response adequately addresses all findings and if all required corrective actions have been taken;
- Advise management, the Bureau/Audit Liaison Officer, and the OIG that the report is closed if all required corrective actions have been taken;
- Enter the report into the Departmental tracking system if one or more recommendations has not been implemented (all required corrective actions have not been taken); and,
- Track the audit until final action has been achieved and the report is closed by PFM.

8.3 Grant Audits Referred for Tracking

Grant audit reports are referred to PFM by the OIG for the tracking of implementation of recommendations contained in the audit report. Once the OIG has referred a grant audit report to PFM for tracking, the OIG continues to list the audit as open in the OIG database, but all tracking actions become the responsibility of PFM. PFM is responsible for determining that appropriate documentation to support the accomplishment of final action has been furnished and that an audit may be closed.

8.4 Closure of Grant Audit Reports in Tracking

PFM is responsible for making the determination that sufficient actions have been taken from documentation received from the Bureau/Office to close a grant audit report. The documentation received from management must be specific and detailed. The notification should include what actions were required and what actions were taken. Specific supporting documentation must accompany management's notification of final action.

8.5 Roles and Responsibilities

While the OIG conducts and issues audit reports, the Departmental Audit Followup Official (who has delegated day-to-day responsibility for the Audit Followup Program to PFM), resolves impasses between the OIG and management, and tracks, monitors, and reports on audits that have been referred by the OIG. The audit liaison officers and management work together to identify, respond, resolve, track, and close audit recommendations and reports. It is essential that all levels of the Department work cooperatively to ensure that the entire Audit process works efficiently which allows Interior to meet its Government Performance and Results Act (GPRA) performance goals.

Office of Inspector General

The Department of the Interior OIG reports directly to the Secretary of the Interior and the Congress on problems and deficiencies related to the administration of Interior programs and operations identified during audits/evaluations, including making recommendations to correct deficiencies.

The Assistant Inspector General for Audits, Evaluations, and Inspections is responsible for:

a) Developing policies, procedures, standards, and criteria relating to audit activities at all levels of Interior (see 361 DM 1.5);
b) Serving as the cognizant audit agency for grant programs, if appropriate; and,
c) Providing the required semi-annual report to Congress.

The OIG and PFM work cooperatively throughout the year to resolve, track, and monitor the impact of audit recommendations on the programs and operations of Interior and to report on the progress management is making to correct deficiencies cited in OIG audit report recommendations.

Assistant Secretary – Policy, Management and Budget (PMB)

The Assistant Secretary - PMB is designated as the audit followup official for the Department of the Interior (109 DM 4). The A/S-PMB is responsible for:

a) Ensuring that systems and procedures for audit followup are in place and properly documented and maintained;
b) Making the final determination regarding audit recommendations that have been referred to the audit followup official for resolution; and
c) Ensuring that the PFM accomplishes its delegated responsibilities regarding audit followup activities.

Office of Acquisition and Property Management (PAM)

a) Developing Departmental policies, procedures, and regulations for issuance in the Departmental Manual and other policy documents (as appropriate) which implement Governmentwide Federal assistance statutory or regulatory requirements;
b) Oversees the operation of the Interior Federal Assistance Working Group which is established to provide a focal point for coordinated Federal assistance activities of the Bureaus/Offices;
c) Providing an opportunity for representatives from Bureaus/Offices to take part in the formulation and implementation of policies; and,
d) Providing technical assistance and management oversight of Federal assistance activities in accordance with guidelines established under revised OMB Circular A-123, "*Internal Control Systems*."

Requests for technical assistance may need to be submitted in writing with appropriate documentation.

Office of Financial Management (PFM)

PFM assists the OIG in the preparation of the semi-annual reports to Congress by providing updated information on the status of audits that the OIG has referred to PFM for resolution and/or tracking. PFM is responsible for:

a) Accomplishing the audit followup responsibilities that were delegated by the Departmental Audit Followup Official;
b) Maintaining the Departmental tracking system for audits referred to the A/S-PMB for tracking and/or resolution; and,
c) Monitoring implementation progress on a monthly/quarterly basis, as necessary.

Interior Bureaus/Offices

a) Developing and issuing Bureau/Office policies, procedures, and regulations which will implement Departmental policies identified in DM 1.3A(1);
b) Overseeing the implementation of established policies at the regional and field levels;
c) Appointing one or more representatives to participate on the Interior Federal Assistance Working Group;
d) Appointing an Audit Liaison Officer to serve as the point of contact for all Departmental audit activities, including submission of responses to all audits within 120 days of issuance by each program Assistant Secretary, and heads of Bureaus/Offices;
e) Coordinating bureau/office responses to Departmental requests for comments on proposed policies and procedures; and,
f) Continuing review of Bureau/Office internal controls to ensure compliance with the control standards in 340 DM 2.3.

Bureau/Office Audit Liaison Officers (ALO)

The employee designated as ALO should be a senior level staff member who has sufficient access to management so that the ALO may keep senior management apprised of and involved with audit activities affecting the audited entity. The ALO may designate an audit liaison coordinator to assist in day-to-day activities. The Bureau/Office ALO is responsible for:

a) Serving as the point of contact for all Departmental audit activities;
b) Monitoring audit activity within bureaus reporting to the Assistant Secretary (Assistant Secretary designated ALO);
c) Keeping the Assistant Secretary ALO apprised of significant audit issues/activities affecting the bureau.

d) Ensuring full cooperation with the OIG and GAO in the conduct of audits, with the audit followup official and with PFM in all audit followup activities; and,

e) Providing timely responses to auditors.

Key Terms Related to Audit Reports

Audit Finding - the statement of problem(s) identified by the OIG or GAO during an audit.

Audit Followup - the process of ensuring that audit recommendations are implemented and that disagreements between management and the auditors regarding corrective action are resolved.

Audit Followup Official - the Assistant Secretary - Policy, Management and Budget (A/S-PMB).

Audit Initiation Memorandum - the OIG's/GAO's official notification of the initiation of an audit. The memorandum specifies the subject, scope, objective, and start date.

Audit Liaison Officer (ALO) - the person designated by management as the point of contact for all activities pertaining to the conduct of audits and audit follow-up in their organization.

Audit Recommendation - a course of action recommended by the auditors to correct an audit finding or set of findings.

Cognizant Agency - the Federal awarding agency that provides a predominant amount of direct funding to a recipient unless OMB determines the specific cognizant agency for audit assignment.

Corrective Action **-** measures taken to implement resolved audit findings and recommendations.

Corrective Action Plan - management's plan to address and implement recommendations contained in the audit report which includes appropriate corrective actions, target completion dates, and officials responsible for completing required actions.

Disallowed Costs - an incurred cost questioned by the auditors that management has agreed should not be charged to the Government.

Evaluation **-** an objective, independent study or appraisal conducted by the OIG, of a program's systems, records, and processes. The goal in conducting evaluations is to determine significance, value, and/or current operating condition of program elements and whether opportunities exist for improvements in program operation or effectiveness.

External Audit - an audit performed by an organization external to the Department, such as: grant audit, a preaward audit of contractor's proposed future costs, a concessions audit, a lease audit, a contractor claim audit, or another audit of federal awards administered by contractors, nonprofit entities, and other nongovernmental activities.

Financial Statement Audit - an audit conducted by the OIG or an independent public accounting firm in accordance with the Chief Financial Officers Act (CFO) of 1990, the purpose of which is to obtain reasonable assurance that the financial statements of a bureau/ office are free of material misstatements. A financial statement audit also means an Indian Trust Funds audit that is required by the CFO Act and that is contracted to an independent public accounting firm.

(1) A financial statement audit report consists of: a) an opinion as to whether the financial statements are fairly presented, in all material respects, in conformity with generally accepted accounting principles; b) a report on internal controls; and c) a report on compliance with laws and regulations. In addition to an audit report, a management letter may be issued. A management letter is a letter prepared by the auditor that discusses findings and recommendations for improvements in internal control, which were identified during the audit, but were not required to be included in the auditor's report on internal control, or other management issues.

(2) An entity shall be determined to be in compliance with Federal accounting standards as required by Federal Financial Management Improvement Act of 1996 (FFMIA) Section 803 requirements if they have implemented and maintain financial management systems that comply substantially with: a) Federal financial management requirements; b) applicable Federal accounting standards; and, c) the United States Government Standard General Ledger at the transactional level. Refer to the FFMIA- OMB Implementation Guidance issued January 4, 2001. For additional guidance refer to the following OMB website: http://www.whitehouse.gov/omb/financial/ffmia_implementation_guidance.pdf. Indicators that entities have achieved substantial compliance in meeting these standards include:

(a) An unqualified opinion on the bureau, office and agency's financial statements. For a qualified opinion, a review of the underlying reasons for the qualified opinion is needed to determine whether or not the entity is in substantial compliance with this requirement. In limited circumstances, a qualified opinion on the agency's financial statements may indicate substantial compliance with this requirement when it is solely due to reasons other than the agency's ability to prepare auditable financial statements. Further, a disclaimer of opinion may not indicate substantial noncompliance with this requirement when it results from a material uncertainty, such as resolution of litigation.

(b) No material weaknesses in internal controls that affect the entity's ability to prepare auditable financial statements and related disclosures.

(c) Compliance with laws or regulations, which have a direct and material effect on the financial statements being audited.

(d) In situations where an entity receives an unqualified opinion but material weaknesses and/or noncompliance with laws and regulations are reported, the nature and extent of the material weaknesses and/or noncompliance should be considered in determining whether the agency is in substantial compliance with the Federal Managers Financial Integrity Act (FMFIA), as outlined in the charts found under the *Factors to Consider in DeterminingCompliance* section of the Federal Financial Management Improvement Act of 1996 – OMB Implementation Guidance issued January 4, 2001.

Final Action - the completion of all actions regarding one or more specific audit recommendations that management, in a management decision, has concluded are necessary with respect to the findings and recommendations contained in an audit report.

Flash Report **-** means a report issued when a problem that the OIG determined merited immediate attention and resolution, is identified in an audit, evaluation, or inspection.

GAO Audit - an audit or review conducted by the GAO at the request of Congress or for other purposes determined by GAO to be in the best interest of the Federal government.

Government Performance Results Act (GPRA) Performance Goal - the annual audit follow-up performance goal based on the GPRA and established by the Department to ensure the implementation of at least a minimum percentage (e.g., at least 85%) of the OIG and GAO audit recommendations within one year of the referral of those recommendations for tracking of implementation.

Inspection **-** means an independent, objective examination of various program elements (such as documents, facilities, records, and other assets). The goal in conducting inspections is to determine if a program is following specific regulations or criteria.

Internal Audit - an audit that adds credibility to reports produced and used within an organization; internal auditors examine record keeping processes, assess whether managers are following established operating procedures, and evaluate the efficiency of operating procedures.

Management - the agency official to whom an audit report, or the OIG memorandum which transmits an audit report, is addressed. For internal audits, the agency official is usually the Assistant Secretary of the cognizant program. For external audits, the agency official is usually the contracting officer or grants awarding official within whose purview the subject matter of the audit falls.

Management Decision for Internal Audits - the determination by management of action(s) required to implement audit recommendation.

Management Decision for Single and External Audits - management's assessment of the adequacy of the audited entity's response to each audit recommendation and/or questioned costs included in a single or external audit report.

Material Weakness - a significant deficiency, or combination of significant deficiencies, that results in a more than remote likelihood that a material misstatement of the financial statements (or other subject matter) will not be prevented or detected. This material weakness definition aligns with the material weakness definition used by management to prepare an agency's FMFIA assurance statement.

Offset - the collection of audit-related debt from other monies due from the United States government.

Performance Audit - an audit of an organization, program, activity, or function of the Department or an insular area government. Performance audits include economy and efficiency audits and program audits that evaluate the achievement of desired results, effectiveness, and compliance with laws and regulations.

Potential Additional, Lost or Underpaid Revenues - monetary amounts from revenue generating functions such as rent, leases, mineral royalties, or fees that were underpaid or not realized because policies, procedures, agreements, or requirements were lacking or were not followed. For example, this category may be used in audit reports involving concessions, grants, royalties, reimbursable services, and fees.

Questioned Cost - a cost that is questioned by the OIG or another audit entity because of an alleged violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the expenditure of funds; cost at the time of the audit was not supported by adequate documentation; or a finding that the expenditure of funds for the intended purpose was unnecessary or unreasonable.

Reinstated Cost - a cost questioned by auditors that management, in a management decision, has agreed should be charged to the Government and is, therefore, not owed by the audited entity.

Recommendations that Funds Be Put to Better Use (FBU) - a recommendation by the OIG that quantifies a specific dollar value of funds that would be generated if management took actions to implement and complete the audit recommendations, including reductions in outlays; deobligation of funds from programs or operations; withdrawal of interest subsidy costs on loans or loan guarantees, insurance or bonds; costs not incurred by implementing recommended improvements related to the operations of the establishment, a contractor or grantee; avoidance of unnecessary expenditures noted in preaward reviews of contract or grant agreements; or any other savings which are specifically identified, i.e., the opportunity cost associated with an audit finding.

Resolution - the process of reaching a management decision or, in the case of external audits, resolution means responding to audit recommendations within established timeframes.

Response to Audit Report **-** comments written by agency officials indicating agreement or disagreement on reported findings and recommendations. Comments indicating agreement on final reports shall include planned corrective actions and, where appropriate, dates for achieving actions. Comments indicating disagreement shall explain fully the reasons for disagreement.

Significant Deficiency - a deficiency in internal control, or combination of deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report data reliably in accordance with the applicable criteria or framework (e.g., Generally Accepted Accounting Principles) such that there is more than a remote likelihood that a misstatement of the subject matter that is more than inconsequential will not be prevented or detected.

Single Audit - an audit completed by an independent audit organization in accordance with OMB Circular A-133, "Audits of States, Local Governments, and Non-Profit Organizations," specifically, an audit which includes both the audited entity's financial statements and Federal awards.

Time-barred **-** the government is precluded from recovering disallowed/sustained costs if a notice of disallowance has not been given to the contractor/grantee within 365 days of the issuance of a single audit report based on relevant provisions of the 1988 Amendments to the Indian Self-Determination and Education Assistance Act.

Sustained Cost - the same as Disallowed Cost.

Unsupported Cost – a cost that is questioned by the auditor because, at the time of the audit, the cost was not supported by adequate documentation. See also Questioned Costs.

Written Off - a decision by management that collection action is not in the best interest of the Federal government.