SECTION 1
CHAPTER 1
OVERVIEW

Legislative and regulatory requirements for federal agencies to establish and maintain adequate internal control programs are not new; they date back almost fifty years. The historical evolution of the internal control program is characterized by a number of key events that have had a significant influence on the current program as it operates today.

The Department's internal control organizational structure provides for the involvement and interaction of many personnel; their respective roles and responsibilities help contribute to a successful Departmental internal control program. Management recognizes the importance of internal controls to ensure efficient and effective programs and operations within their organizations.

BACKGROUND AND AUTHORITY

The Congress, the Office of Management and Budget (OMB), and the Government Accountability Office (GAO) have directed agencies to establish and maintain sound internal control systems as a primary means of improving accountability, effectiveness and efficiency in achieving program goals and objectives, and in preventing fraud, waste, and mismanagement. The Department promotes the continuous monitoring of internal controls as part of daily program and operations management to strengthen management accountability and enhance and improve program performance and operations.

The Federal Managers' Financial Integrity Act (FMFIA), OMB Circular A-123, "Management's Responsibility for Internal Control," which was revised December 21, 2004, requires agencies to conduct an ongoing review of internal controls and to report annually on the adequacy of agencies' program and operation internal control systems. Under authority provided by the Government Management Reform Act (GMRA), the Department's annual assurance statement on compliance with the FMFIA is incorporated into the Department's Annual Performance and Accountability Report (PAR). Appendix A to OMB Circular A-123 requires the submission of an additional assurance statement as of June 30 each year regarding financial reporting. The Chief Financial Officers (CFO) Act and Government Performance and Results Act (GPRA) reinforce the need for having effective internal controls. Department managers should establish environments where internal controls are understood, encouraged, practiced, and implemented.

The basic 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 FMFIA.

DEPARTMENT'S GPRA GOAL FOR INTERNAL CONTROL

The Department's overall GPRA goal for the Internal Control Program is twofold: (1) To ensure that a sound system of internal controls exists in all programs, organizations, and functions that meets the objectives and requirements of FMFIA and OMB Circular A-123, as revised; and, (2) To implement an effective, efficient, and systematic approach to assessing internal controls that integrates other management improvement initiatives within the Department. The Department's Management Excellence goal for improved accountability is to obtain an unqualified audit for DOI's eight bureaus, the Departmental offices, and the Department's consolidated financial statements. The timely correction of identified deficiencies is essential to improving the efficiency and effectiveness of DOI's programs and operations, and to achieving integrity and accountability goals. The current Departmental annual performance measure for internal control calls for correction of 100% of audited financial statement and FMFIA material weaknesses on schedule each year. Timely correction of material weaknesses will be accomplished through implementation of corrective action plans and more frequent monitoring of bureaus' progress by the Office of Financial Management (PFM), bureau senior management, the Senior Management Council, and internal control coordinators (ICCs).

Performance goals and measures are intended to enhance decision making and accountability; provide information on how a program is operating; and relate program results to organization or program mission, goals, and objectives. The Department's annual performance goal reflects these objectives and promotes management accountability as required by the GPRA.

ORGANIZATIONAL STRUCTURE

DOI has established an integrated organizational structure to implement the Internal Control Program. This structure starts with the Secretary, descends to the program assistant secretary, to the bureau director, and finally to the program manager. Roles and responsibilities of key components of the Internal Control Program are described below.

ROLES AND RESPONSIBILITIES

The Secretary - establishes internal policy direction for the Internal Control Program, issues an assurance statement on financial reporting in June of each year, which is updated in September, and submits the annual Performance and Accountability Report to the President and the Congress, which includes an annual assurance statement on FMFIA, in November of each year.

The Assistant Secretary-Policy, Management and Budget (Assistant Secretary-PMB) and Chief Financial Officer (CFO) - has operational responsibility for the Internal Control Program. The Chief Financial Officers Act of 1990 placed responsibility for internal controls with the agency CFO to ensure the Department's compliance with OMB Circulars A-123 and A-127, the FMFIA, the CFO Act, the FFMIA, and the GPRA.

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 and investigations, and reporting the results in its audit reports. In addition, the OIG annually reviews bureaus' administrative and accounting controls as part of its financial statement audits.

Program Assistant Secretaries/Solicitor – Program assistant secretaries and the Solicitor have responsibility over the various bureau programs within their purview, and are encouraged to establish internal control and audit follow-up councils or oversight groups in their respective organizations to coordinate and monitor the internal control and audit follow-up requirements for their bureaus' programs. Such councils or oversight groups may be used to implement the responsibilities for internal control which, at a minimum, are: (1) Institutionalizing the internal control process within their organizations; (2) Establishing priorities in identifying, correcting and reporting of internal control material weaknesses and accounting non-conformances; (3) Ensuring that funding to correct identified deficiencies is addressed in the budget formulation and execution process; and (4) 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. Program assistant secretaries also have Department-wide responsibilities for internal control as members of the Senior Management Council. Specific duties of the Council are defined in this section.

Bureau and Office Heads – Bureau heads and/or senior-level management officials 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 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 also includes determining that the systems of control are functioning as intended; 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 weakness and/or accounting systems non-conformance. Bureau heads are also responsible for:

- Determining on an annual basis 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 internal control guidelines issued by the Departmental Offices of Financial Management, Acquisition Management (PAM), Chief Information Officer (OCIO), and other Departmental offices are implemented;
- Allocating adequate resources to evaluate their systems of control;
- Developing procedures, documentation, training, and reporting requirement necessary to review, establish, maintain, test, improve, and report on control systems within their bureau programs and operations;
- Reporting to the Assistant Secretary-PMB and the Senior Management Council, in consultation with their Assistant Secretary, internal control deficiencies identified in audit reports, internal reviews, and from other sources;
- Specify employee accountability by including program specific internal control elements and standards in all managers' performance evaluations; and

- Ensuring timely correction and validation of all identified program and operational deficiencies whether material and/or nonmaterial;

Program Managers – Are responsible for insuring compliance with requirements for internal controls for their programs. Specifically, they must undertake within their programs, the duties listed above for bureau directors and office heads.

Senior Management Council (SMC) - within DOI, the responsibilities of the Senior Management Council are implemented by the DOI Internal Control and Audit Follow-up Council which is chaired by the Assistant Secretary-PMB and is comprised of all program assistant secretaries, the Solicitor, the Inspector General (ex officio), Deputy Assistant Secretary for Business Management and Wildland Fire, the Chief Information Officer, and Senior Procurement Executive. The Council provides senior-level oversight of the Internal Control and Audit Follow-Up programs, resolves issues related to both programs, and decides reporting issues for the Department's Annual Performance and Accountability Report. Specifically, the council will:

- Ensure DOI's commitment to an appropriate internal control environment;
- Approve DOI'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 effectiveness of internal controls over financial reporting;
- Recommend to the Assistant Secretary-PMB which control deficiencies are material to disclose in the annual FMFIA assurance statement and PAR;
- Oversee implementation of corrective actions related to material weaknesses; and
- Determine when sufficient action has been taken to declare a reportable condition or material weakness corrected.

Senior Assessment Team (SAT) – The duties of the Senior Assessment Team as defined in Circular A-123 are assigned to the DOI Management Initiatives Team (MIT) which is chaired by the Assistant Secretary-PMB and comprised primarily of Deputy Assistant Secretaries and Bureau Deputy Directors. Duties of the MIT in implementing the Circular are to:

- Ensure assessment objectives are clearly communicated throughout the agency;
- Ensure adequate funding and resources are made available to comply with the new requirements of the Circular;
- Ensure 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 new requirements of the revised Circular; and
- Determine or approve assessment design and methodology for each entity and the Department.

Office of Financial Management (PFM) is responsible for: (a) Providing staff assistance to the Assistant Secretary-PMB and the Senior Management Council; (b) Recommending internal control policies and procedures; (c) Providing oversight and guidance to the bureaus/offices concerning the review, evaluation, and maintenance of effective controls; (d) managing, directing, and evaluating the Department's reporting under OMB Circulars A-123 and A-127, the FMFIA, the FFMIA, and the CFO Act.

Office of Acquisition and Property Management (PAM) is responsible for developing and issuing control evaluation guidelines for the acquisition, Federal assistance and property management functional areas; assessing the results of bureau control evaluations in these areas; and providing to PFM annually a summary assessment of the adequacy of bureau controls in these functional areas. PAM is also responsible for overseeing, monitoring, and assessing and recommending for approval to PFM the completion of bureau corrective action plans addressing acquisition and property management material weaknesses, and advises PFM and Assistant Secretary-PMB regarding the closure of bureau/office recommendations.

Office of the Chief Information Officer (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 control evaluations in these areas; and providing to PFM annually a summary assessment of the adequacy of bureau controls in these areas. OCIO also reviews corrective action plans for identified IT deficiencies, and advises PFM and Assistant Secretary-PMB regarding the closure of bureau/office IT recommendations.

Department's Office of Environmental Policy and Compliance (OEP), Office of Human Resources (OHR), Office of Civil Rights, and Office of Budget (POB) are responsible for issuing guidance to assist bureaus in conducting control evaluations of their respective functional areas and correcting identified deficiencies.

Office of Planning and Performance Management (PPP) is responsible for developing and issuing guidelines on the preparation of strategic plans, annual performance plans, and annual performance reports. Guidelines include using internal control reviews to fulfill GPRA requirements for program evaluations and data verification and validation. PPP also is responsible for review and clearance of GPRA documents prior to publication, and collaboration with PFM on the selection of GPRA goals and measures for the Performance and Accountability Report.

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

See 340 DM 1 (pages 3 to 6) in Exhibit 1 for detailed information on the roles and responsibilities of the Assistant Secretary - PMB, Inspector General, Assistant Secretaries/Solicitor, Bureau Heads, PMB internal control coordinators and others in the Department's internal control process.

CALENDAR OF EVENTS

A generalized Department-wide calendar for each step of the internal control process is shown in Addendum A. Annual updates to this schedule providing specific due dates are prepared by PFM and transmitted in a yearly guidance memorandum to program assistant secretaries, heads of bureaus and offices, and internal control coordinators.

INTERNAL CONTROL PROCESS

The Internal Control Program consists of six major components.

1. Developing and Updating the Annual Internal Control Review Plan

The Internal Control Review Plan (ICRP) is an annual written plan which summarizes a bureau's components; identifies the relative priority ranking of each component (high, medium, or low risk activity); establishes the type of control evaluation to be conducted and the year in which the evaluation is to be completed; and fixes the responsibility for conducting the evaluation as planned. This plan provides a system for verifying and maintaining key controls in the Department's processes through careful planning, continued inspection, and corrective action where required.

2. Conducting Internal Control Assessments

An Internal Control Assessment is a systematic and comprehensive evaluation of a system to determine whether the internal controls are adequate to provide reasonable assurance of meeting the component's objectives efficiently and effectively while safeguarding government resources. All internal control assessments require testing to determine compliance with GAO control standards. The Department uses two types of control evaluation: the Internal Control Review (ICR) and the Alternative Internal Control Review (AICR). Emphasis should be placed upon using the type of review which best provides assurance that the control is in place and working effectively.

An Internal Control Review is an evaluation of key internal controls over <u>all</u> significant areas or activities of a component to determine if they are operating as intended. These evaluations must be supported by documentation, i.e., the individual(s) who conducted the testing and the date, the methods used to test the controls, controls tested, sample items, results, any deficiencies detected, and corrective action(s) taken.

An Alternative Internal Control Review provides the opportunity to narrow the scope of the review and focus attention on areas or activities of a component which have the highest potential for ineffective or inefficient operation or loss of government resources. Examples of an AICR include OIG and GAO audit reports, program evaluations, GPRA annual assessments, Congressional reports, bureau internal studies relating to operations, and reviews of financial systems and applications.

The Department's automated assessment tool can be a more efficient and less resource intensive alternative to a traditional internal control assessment. The automated approach utilizes standard assessment templates for common administrative programs and functions along with supplemental procedures, as necessary (see Chapter 2 for more information on the automated assessment approach).

3. Monitoring Quality Control Over Evaluations

The quality control process includes all internal control evaluations including AICRs, ICRs, and Departmental Functional Reviews (DFRs). This involves verifying and maintaining a desired level of quality by careful planning, continued inspection, and corrective action where required. Quality control can be accomplished through the use of the following tools:

a. Review Tracking System
b. Internal Control Review Committee
c. Peer Review
d. OIG/GAO Audit
e. Internal Control Coordinators

4. Developing and Implementing Corrective Actions

The determination of weakness materiality is at the discretion of Bureau management. Following the identification of weaknesses during the internal control assessment, material weakness corrective action plans must be developed and implemented. The culmination of the internal control process is not the preparation of evaluation reports; it is the improvement of program and functional services through the timely correction of control weaknesses. There are five types of control weaknesses:

> **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 misstatements on a timely basis.
>
> **Reportable Condition –** A control deficiency or combination of control deficiencies that in management's judgment should be communicated because they represent significant weaknesses in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives.
>
> While there is no requirement to report to the next higher management level, reportable conditions must be corrected and monitored. If the agency head determines the deficiency to be significant enough to be reported outside the agency, it shall be

considered a material weakness and must be reported and tracked.

Material weaknesses – 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. The two types of material weaknesses are:

- **FMFIA overall –** Reportable conditions in which the agency head determines to be significant enough to report outside of the agency.

- **Financial reporting –** 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.

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.

Non-material weaknesses - Control problems that can be corrected at the bureau level without the approval or attention of the next higher level of management.

The annual reporting of material weaknesses should comply with the format specified by PFM. Types of material weaknesses, at a minimum, to be included in the report are:

- Conditions which could lead to substantial damage or loss of a significant public asset or natural, biological, cultural or historical resource;
- Conditions which significantly impair the fulfillment of the Department's or Bureau's mission;
- Conditions which indicate systemic deficiencies across bureaus or in the Department's central support systems;
- Conditions that could lead to inaccurate or incomplete information being provided in areas of major importance to operations or policy;
- Conditions which result in an audit qualification on a financial statement;
- Waste, Fraud, and Abuse: An inherent program or administrative functional material weakness that makes the program or activity susceptible to fraud, waste and abuse;
- Inability to Carry Out Your Mission: A systemic deficiency caused by ineffective program or management support, financial systems, policies, and/or procedures established by a bureau or reporting entity to carry out a major program or administrative function;
- Health and Safety: A material weakness that is seriously detrimental to the public health or safety, a program or administrative activity, service delivery, national security, economic growth, privacy, or citizen's rights; and/or

- System Security: A material weakness that could result in significantly impaired service, program failure, significantly reduced program effectiveness or efficiency, public injury or loss of life, unreliable decision-making data, reduced confidence in government, and unauthorized disclosure, manipulation or misuse of sensitive information such as personal, financial management, or programmatic data maintained in computerized systems.

Bureaus must establish and maintain a follow-up system, record and track material and non-material weaknesses and non-conformance corrective actions, and monitor related progress against scheduled completion dates.

5. Reporting

Preparing and Issuing an Annual Assurance Statement on Financial Reporting

The Annual Assurance Statement for Internal Control over Financial Reporting is required beginning in fiscal year 2006. This assurance statement is a subset of the overall Statement of Assurance (item 6) and is based on the results of management's assessment as of June 30, conducted in accordance with the requirements of OMB's Circular A-123, Appendix A. Any changes to the conditions reported in the as of the June 30 Assurance Statement, whether positive (corrected weakness) or negative (additional identified weakness), is to be reported on an updated statement as of September 30.

Preparing and Issuing an Annual Assurance Statement on Compliance with FMFIA

The Annual Assurance Statement is required in the annual FMFIA reporting process. Bureau and office heads prepare an annual assurance statement that is submitted through their respective program Assistant Secretary to the Assistant Secretary – Policy, Management and Budget. Bureau assurance statements form the basis for the Secretary's Annual Assurance Statement which is submitted to the President and the Congress as part of the Department's Annual Report on Performance and Accountability (PAR). Annually, PFM will provide a sample assurance statement template.

6. Verifying and Certifying Corrective Actions

The final component in the Department's Internal Control Process involves verifying and certifying that corrective actions have been taken. For all non-material control deficiencies, reportable conditions, and material weaknesses, the responsible program official is accountable for ensuring that planned corrective action(s) are completed and that the identified weaknesses or non-conformances are resolved. This certification should be incorporated into the bureau internal Corrective Action Tracking System reporting process.

A more detailed explanation of these steps is provided in later chapters of the handbook.

SECTION 1
C H A P T E R 2
ANNUAL INTERNAL CONTROL REVIEW PLAN

The first step in the internal control process involves the preparation of an Internal Control Review Plan (ICRP). This plan helps institutionalize the internal control process within the bureau by involving all levels of management in its preparation and approval. The ICRP represents the bureau schedule for performing financial reporting and programmatic internal control assessments for the current fiscal year and/or later years (usually covering a five-year period, but some reviews are scheduled annually). This list includes not only the internal assessments described in this section, previously known as management control reviews, but also the list of financial statement-related internal controls that will be tested as well (as discussed in the next section).

An ICRP must summarize a bureau’s components; identify the relative priority ranking of each component as high, medium, or low risk activity; establish the type of control evaluation to be conducted and the year in which the evaluation is to be completed; and assign the responsibility for conducting the planned evaluation. The annual review plan may have reviews of key controls in the financial areas that do not result in an AICR-like deliverable that is surnamed and provided to PFM.

At a minimum, the plan should be updated annually. The update consists of adjusting the plan to accommodate Departmental Functional Reviews (DFRs); competitive sourcing; new components, programs, or reporting systems; changes in priority; the completion of control evaluations and corrective actions; and any additional information available on the status of controls. Annual updates should coordinate review activity to avoid redundancy by integrating, to the maximum extent possible, internal program, functional, and operational reviews, GPRA performance assessments, management studies, OIG and GAO audits, or any other independent review efforts.

The ICRP is a useful management tool for monitoring the Internal Control Program. Stages in developing the plan follow.

ESTABLISH AND MAINTAIN COMPONENT INVENTORY

The first stage in preparing the ICRP is to establish and maintain an inventory of bureau components. Internal controls should be designed to provide reasonable assurance regarding prevention or prompt detection of unauthorized use or disposition of assets. As a result, management is responsible for developing internal control components which provide an accurate reflection of financial reporting, program functions, and administrative activities of a specific bureau. Developing and maintaining an inventory of those components is the first stage in the review planning process.

Definition

A component is defined as a major program, administrative activity, organization, or functional subdivision of a bureau or office that requires one or more separate systems of internal controls. However, it is suggested that bureaus define their programs and administrative functions along budget and financial statement line items or other similar segmentation such as GPRA-defined activities for performance assessment and reporting purposes.

Scope and Size

Components should be properly sized to facilitate internal control assessments. Each component should:

- Contain sufficient information to support management's assertion;
- Include appropriate representations from officials and personnel responsible for monitoring, improving, and assessing internal controls; and
- Be documented appropriately.

Bureau component inventories should include a specified number of functional components. These components are functional activities generic to all bureaus and offices. They are defined by PFM as DFRs; however, the internal control assessment guidelines for the functional activities are issued by the responsible Assistant Secretary - Policy, Management and Budget (Assistant Secretary-PMB) office. Examples of DFRs include Acquisition Management, Information Technology Centers, Cash Management and Debt Collection, Property Management, and Travel.

Departmental and PMB offices should include as components only those programs or functions for which they have operational, as opposed to discretionary or policymaking, responsibilities.

Annual Update of Inventories

Component inventories should be updated annually before the ICRP is developed. This annual update is to ensure that the inventory:

- Includes all programs, organizations, or financial reporting functions which may encompass one or more systems of internal control;
- Addresses all automated data processing systems, either as a separate component or an integral part of a program component; and
- Breaks out components in such a way that each component could be reviewed in an efficient, reasonable, and logical manner.

Changes in budgetary resources assigned to a component or changes in mission may lead to consolidation or splitting of a component. Other items to consider when updating the inventory are new components, obsolete components, changes in the nature or scope of any components, and past experience in handling components.

Retention of Documentation

The ICC should maintain the current list of components as supporting documentation. This list should include a brief narrative description of each component's scope. This listing is the basis of the Plan.

REVIEW PRIORITY RATINGS (Risk Assessment)

The second stage of the review planning process is to evaluate the risk associated with individual components and assign each component an appropriate rating (high, medium, or low risk).

Definition

Risk is defined as the probability of an unwanted occurrence. Evaluation of risk is the judgmental review by bureau officials of the susceptibility of all the components to the occurrence of waste, loss, unauthorized use, and/or misappropriation. The bureau/office should evaluate management's processes for determining the level of risk related to internal controls over programs and financial reporting.

Scope

Ideally, assessments of risk should be completed for all components every year. Since the purpose of prioritizing components is to provide a basis for determining the appropriate nature, scope, and frequency of reviews, all components at least should be assessed in the established cycle.

Process

The review priority rating should be based on total organizational knowledge of the component and can be accomplished by gathering knowledgeable staff around a table for discussions about the components. Documentation of the process used and the conclusions reached should be retained for a minimum of five years for future reference by bureau officials, PFM, or OIG staff.

To assist in the priority rating process, the Department has designed the Priority Rating Worksheet. The worksheet, Exhibit 1 (or a comparable bureau-designed alternative), should be used in gathering relevant information prior to meeting with management officials as well as documenting decisions reached during roundtable discussions.

Appropriate consideration should be given to previous control assessments such as audit reports; internal control evaluations; the degree and timeliness of correcting known weaknesses; and institutional knowledge of the component. Other considerations in assigning priority rankings include factors that would:

- Prevent management from meeting program or financial reporting objectives and goals;

- Subject management to unwarranted potential loss of assets and revenues;
- Cause management to provide unreliable information and reports about the component;
- Encourage departures from established procedures; and/or
- Create adverse public opinion.

A component with a material weakness should be rated high until the weakness is corrected.

Items which may be considered when assessing risk and assigning the priority ratings are:

- **Control Environment -** The control environment is the organizational and structure and culture created by management attitude and employees to sustain organizational support for effective internal controls. An analysis of the control environment will provide an assessment of management's commitment to fostering an organizational tone that is conducive to providing a strong and effective control environment. The factors that influence the general control environment are: Define areas of authority and responsibility; appropriately delegate the authority and responsibility throughout the agency; establish a suitable hierarchy for reporting; support appropriate human capital policies for hiring, training, evaluating, counseling, advancing, compensating and disciplining personnel; and uphold the need for personnel to possess and maintain the proper knowledge and skills to perform assigned duties as well as understand the importance of maintaining effective internal controls within the bureau.

- **Risk Assessment -** Risk assessment is an entity's internal process for identifying, analyzing, and managing risk relevant to achieving the objectives of reliable financial reporting, safeguarding of assets, and compliance with budget and other laws and regulations. Management should make a thorough identification of all internal and external risks that may prevent the organization from meeting objectives. The major factors that affect the risks of a component are: Changes in the operating or statutory environment; new personnel who may have a different focus on internal control; new or significantly changed information systems; rapid growth of programs which can strain controls; new technology; new programs or activities which may introduce new control risks; restructurings or budget cutbacks; and adoption of new accounting principles which may have an impact on the financial statement. Identified risks should then be analyzed for their potential effect or impact on the agency. The various types of risks which may be identified are: inherent, control, combined, and/or fraud. See the Key Terms section of the handbook for a description of the various types of risk.

- **Control Activities -** Control activities include policies, procedures, and mechanisms in place to help ensure that agency objectives are met and that management’s assertions in financial reporting are valid. Due to frequent changes in information technology, human resources, and program functions, controls should be monitored and adjusted to remain effective.

- **Information and Communication -** Information should be communicated to relevant personnel at all levels within an organization. This communication should not only exist with the organization, but should also encompass communicating with external organizations, whether providing information or receiving it. Management should ensure that a system is in place to identify and record pertinent operation and financial information relating to internal and external events.

- **Monitoring -** Monitoring the effectiveness of internal controls should occur in the normal course of business. Periodic reviews and reconciliations of data should be conducted regularly. Management should ensure that: employees know their assigned responsibilities for internal control and control monitoring; procedures exist to ensure that all audit findings and other reviews are promptly evaluated; response decisions are made appropriately; and that corrective actions will resolve the issues promptly.

SCHEDULING INTERNAL CONTROL ASSESSMENTS

The third stage in preparing an ICRP is to schedule internal control assessments for each component. It is suggested that these assessments be scheduled over a cyclical number of years (unless required annually) to help assist bureaus with the review planning process. Scheduled internal control reviews that have been conducted should be documented.

Definition

An internal control assessment is a systematic assessment of a control system to determine if the controls in operation are adequate to provide reasonable assurance of meeting component objectives efficiently and effectively and safeguarding government resources. The two types of control evaluations are Internal Control Reviews (ICRs) and Alternative Internal Control Reviews (AICRs). Emphasis should be placed on using the type of review which is the most efficient and cost effective in assessing a component's system of control. ICRs are control evaluations which cover all significant areas or activities (event cycles) of a component. An AICR allows a bureau to narrow the scope of the review and focus attention on areas or activities of a component which have the highest potential for ineffective and inefficient operation or loss of government resources. Examples of AICRs include GAO and OIG audit reports, GPRA performance assessments, program evaluations and internal studies, reviews of financial systems and applications, Congressional reports, and the automated assessment approach. ICRs are control evaluations which cover all significant areas or activities (event cycles) of a component.

Scope and Frequency

The Department has decided that Internal Control Reviews (ICRs) are to be done on all controls or program areas considered to be of high risk. As discussed later in this handbook, since an ICR requires a description of all event cycles and analysis of control objectives and techniques, testing is normally very detailed and extensive. When the level of risk for controls or program areas is considered to be low, the Department has decided that an Alternative Internal Control Risk is appropriate because it is generally less paper intensive and more cost effective and efficient. For program areas considered to be medium risk, it is management's discretion as to whether the ICR or AICR is more appropriate; the decision to use the ICR or AICR should be based on the visibility of the program, the dollar impact of the program on outside entities (public or governmental), etc.

High risk activities should be given priority in the planning and scheduling of reviews. AICRs should be combined with existing bureau management review processes as much as possible. Bureaus are encouraged to consider reviewing all components ranked as high at least every three years; components with a medium or low priority ranking should be evaluated, at least every four or five years, respectively.

Retention of Documentation

The ICC is required to maintain current evaluation of risk assessments for each component for a minimum of five years, including documentation supporting the review priority ranking assigned. This documentation should demonstrate the basis for the priority rankings. It is suggested that each component's priority ranking be listed in the ICRP.

SECTION 1
CHAPTER 3
CONDUCTING INTERNAL CONTROL ASSESSMENTS

The second step in the Internal Control Process is conducting internal control assessments. All control evaluations require appropriate tests of controls in operation. There are two types of control evaluations: Alternative Internal Control Review (AICR) and Internal Control Review (ICR). Bureaus are encouraged to use the DOI automated assessment approach to review a component's controls; this approach is considered an AICR and is discussed further in the chapter (examples of an automated assessment approach and traditional AICR are included at the end of this chapter).

Differences Between AICRS and ICRS

AICRs are preferred over ICRs since they are generally less paper intensive and more cost effective and efficient; however, for high risk areas, an ICR must be used. The differences between an AICR and an ICR are in the focus of testing and documentation. Generally, the AICR documents only a specific subset of controls areas while the ICR documents controls in a component. Consequently, the AICR analysis focuses on documenting the control techniques in place for control of high risk components. Because of its limited scope, the AICR does not require a detailed description of a component's event cycles and analysis of the related control objectives. Since the ICR requires a description of all event cycles and analysis of control objectives and techniques, testing becomes much more involved. The differences can be seen by comparing the individual steps of AICRs and ICRs as shown in this chapter.

Similarities

AICRs and ICRs have the same goal: Assessing a component's control system effectiveness. Both types of reviews should answer the following questions.

- Does the component have clear objectives?
- Do the control systems provide reasonable assurance of meeting the objectives?
- Are there any control systems weaknesses?
- Have the weaknesses caused any problems?
- What actions, if any, are necessary to improve controls?

AICRs and ICRs also share common elements. Both types of reviews consist of the following steps:

1. Identifying what might go wrong (risk)
2. Comparing control systems to the GAO control standards
3. Testing control techniques
4. Documenting the evaluation
5. Planning corrective actions

6. Reporting the results

Identifying risk was discussed in Chapter 2. The remaining common elements will be discussed in Addendum A, "Conducting AICRs."

Departmental Functional Reviews (DFRs) are evaluations of function activities generic to bureaus and offices. Examples of DFRs include Acquisition Management, Security and Cash Management, etc. Evaluation guidelines are issued by the responsible PMB office after PFM review and are part of the Internal Control Plan for the bureau.

Automated Assessment Approach

The automated assessment approach is based on the results of an Internal Control Re-Engineering Laboratory conducted by the Department in 1996. The Laboratory developed a new automated, less resource-intensive approach for targeting and conducting internal control assessments. The automated assessment approach is built around eight management integrity measures that support the general and specific internal control standards outlined in OMB's Circular A-123, "Management Responsibility for Internal Control," and GAO's "Standards for Internal Control in the Federal Government." A unique feature of the automated assessment approach is that it provides for identifying areas of both potential material deficiencies and best practices. The assessment is performed electronically using an off-the-shelf surveying and analytical software tool (Survey Tracker) that provides diagnostic and executive-level reporting. The results of the survey questionnaire and responses are analyzed by the software and a graphical summary report known as a "spider diagram" is produced using MSExcel. The "spider diagram" presents the actual assessment against a Departmental standard for each management integrity measure. The eight integrity measures are:

> Organizational Control Environment**.** The objective of this measure is to ensure that an organization's goals, objectives, policies, and procedures are conducive to achieving sound internal controls, and that the organization places a high level of importance on management integrity and ethics. The organizational control environment sets the tone for and influences the internal control consciousness of its employees. It also provides the foundation for the internal control structure. Organizational control environment factors include the integrity, ethical values, and competence of employees; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; planning, budgeting, accounting and reporting; and the direction provided by senior management.
>
> Risk Management**.** The objective of the risk management measure is to ensure that an organization identifies, assesses, and considers the consequences of events that could prevent the achievement of its goals and objectives, and result in significant loss of resources. Every organization faces a variety of risks from external and internal sources and changes in its operating environment. These risks should be continuously monitored and assessed.

Fiscal Resources Stewardship**.** The objective of this measure is to ensure resources are safeguarded and managed in a manner consistent with the mission of the organization. Access to resources should be limited to authorized individuals, and accountability for the custody and use of resources should be assigned and maintained.

Program Effectiveness**.** The objective of this measure is to ensure that management plans and allocates sufficient resources to programs to achieve intended results. Further, the program effectiveness measure embraces the idea that organizations have strategic planning systems that employ performance measurement systems to provide for comparisons of planned outcomes and results against actual outcomes and results.

Regulatory Compliance**.** The objective of this measure is to ensure that laws and regulations are followed. Management and staff must be aware of and ensure that all programs, operations, obligations, and costs incurred comply with applicable laws, regulations, and executive orders.

Audit Resolution**.** The objective of the audit resolution measure is to ensure that organizations take prompt and responsive action on all audit findings and recommendations in order to improve program and organizational efficiency and effectiveness. Responsive action is that which corrects identified deficiencies within the agreed to timeframe. Where audit findings identify opportunities for improvement rather than cite deficiencies, responsive action is that which produces improvements.

Management Information**.** The objective of this measure is to ensure that reliable and timely information is obtained, maintained, reported, and used for decision-making at all levels. Information systems should produce reports containing program, operational, financial, and compliance related data, to effectively manage and control the programs and operations of an organization.

Financial Systems and Data Integrity**.** The objective of the financial systems and data integrity measure is to ensure that an organization's financial management system and related operations conform with Government-wide principles, standards and requirements, and that the process of managing information necessary to support program and financial managers, and assuring data captured and reported is complete, accurate, accessible, timely and usable.

For detailed information on the automated assessment approach, see Addendum A, and a sample "spider diagram" is included in Case Study No. 1 at the end of this chapter. Also, information on the integrity measures can be found in OMB Circular A-123 and GAO's "Standards for Internal Control in the Federal Government."

If a bureau wants to utilize the automated assessment approach, it should contact PFM which will work closely with the bureau in planning, conducting, analyzing, and reporting the results of the automated assessment approach. The automated assessment approach is a useful tool that can assist bureaus in planning and conducting more focused and cost-effective assessments and, for these reasons, the Department encourages its use.

CONDUCTING INTERNAL CONTROL ASSESSMENTS
COMPARISON OF AICR AND ICR ACTIVITIES

AICR	ICR
1. Start the Evaluation • planning • general control environment • IT	1. Start the Evaluation • planning • component survey • general control environment • IT
2. Define Control Systems • identify & document high risk cycles • identify and document control techniques •compare control systems to the GAO control standards	2. Define Control Systems • identify and document event cycles • identify and document all risks • identify and document control objectives • identify and document control techniques • compare control systems to the GAO control standards
	3. Review the System Design • adequacy of control objectives • adequacy of control techniques
3. Test the Control System • select controls to be tested • select test methods • determine amount of testing • plan data collection • conduct the tests • analyze test results, develop conclusions • develop plans for corrective actions	4. Test the Control System • select controls to be tested • select test methods • determine amount of testing • plan data collection • conduct the tests • analyze test results, develop conclusions • develop plans for corrective actions
4. Report the Results	5. Report the Results
5. Document the Evaluation	6. Document the Evaluation

SECTION 1
CHAPTER 4
MONITORING QUALITY CONTROL OVER EVALUATIONS

Quality control is the third step in DOI's Internal Control Process. Each bureau is to establish and maintain a quality control process to ensure that control techniques are properly defined, internal control assessments are properly performed, and results are accurately reported.

Definition

Quality control is a system for verifying and maintaining a desired level of quality in a process by careful planning, continued inspection, and corrective action, where required. The quality control process includes all internal control evaluations including AICRs, ICRs, and DFRs.

Quality Control Tools

Quality control can be accomplished through several tools.

> <u>Internal Control Review Committee</u>**.** The first quality control tool that can be used are bureau and Assistant Secretary Internal Control Review Committees. These committees can assure that all internal control assessments have been conducted in accordance with guidelines prior to submission to the Assistant Secretary-PMB. The Committees focus on the technical aspects of the evaluations as well as on the proper identification of the weaknesses and appropriateness of corrective actions.
>
> <u>Peer Review</u>**.** A second quality control tool is a peer review. Peer reviews on internal control assessments are another way of assuring that the assessment has been conducted in accordance with guidelines prior to submission to the Assistant Secretary-PMB. Peer reviews have the same focus as the Internal Control Review Committee, but may consist of program managers from a single bureau or from several bureaus.
>
> <u>Internal Control Coordinators</u>**.** A third quality control tool is internal control coordinators who have been designated by each program assistant secretary or bureau head to coordinate and facilitate compliance with Internal Control Program requirements.
>
> <u>Third Party</u>**.** Another tool for quality control is the third party. Third party reviews are another way of assuring that the evaluation has been conducted in accordance with guidelines prior to submission to the Assistant Secretary and/or PFM. Third party reviews have the same focus as the Internal Control Review Committee, but may consist of program managers from another agency with similar programs or an outside auditor.

SECTION 1
CHAPTER 5
DEVELOPING AND IMPLEMENTING CORRECTIVE ACTIONS

The fourth step of the Internal Control Process is correcting the weaknesses/deficiencies identified during the internal control assessments. The culmination of the internal control program is not the preparation of evaluation reports - it is the improvement of program and functional services through the timely correction of control weaknesses.

Definition

A nonmaterial weakness is a control problem which can be corrected at the bureau level without the approval or attention of the next higher level of management.

The overall FMFIA definition of material weaknesses are those control problems which are of significance to report outside of the bureau or agency. However, financial reporting material weaknesses/deficiencies are further defined as 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.

Correcting Material Weaknesses/Deficiencies

All weaknesses/deficiencies are to be corrected in a timely manner. An exception to this policy exists when a documented analysis demonstrates that the estimated costs of improved management control techniques exceed the potential benefits or when corrective actions are precluded by legislative actions. Responsible officials at all levels are expected to be actively involved in correcting material and nonmaterial weaknesses/deficiencies. The plans and schedules for correcting reported weaknesses/deficiencies include the following information:

1. **Summary Description of the Weakness/Deficiency**
2. **Year First Identified**
3. **Target Correction Date –** Unless adequately justified, all material weaknesses and noncompliance issues must be corrected within one year. To ensure that deficiencies are corrected prior to the beginning of the next year's audit process, final correction of the deficiency should end June 30 to allow sufficient time for testing to ensure that the material weakness/noncompliance issue has been corrected. Extensions beyond the June 30 deadline may be granted by PFM, but IT security weaknesses must be corrected by June 30. Programmatic recommendations may require longer lead time (legislative or regulatory changes) but justification is needed when submitting CAP to PFM.
4. **Accountable Official –** Senior manager(s) in charge of the program where the weakness or noncompliance issue was identified (including field office and/or headquarters, if applicable).
5. **Funding** -- Must be set aside (through budget allocations/allotments), and must be sufficient to completely correct the weakness or noncompliance issue. For deficiencies

requiring multi-year corrective action plans, costs for each year must be identified in the plan and in the bureau/office budget request to the Department. Funding may not be moved to other priorities until the material weakness prior to funds expiration.

6. **Summary of Corrective Actions –** List the critical path activities/milestones, target completion dates, and total resources committed to each milestone.
7. **Quarterly Corrective Action Milestones –** A comprehensive listing of specified actions/milestones and targeted completion dates by fiscal quarter, and the total resources associated with and committed to each action/milestone. As each specific milestone is completed, list the correction date, and where appropriate, the location of the supporting documentation for review upon request by PFM, the OIG, or the independent auditors.
8. **Metrics –** Two types of metrics should be developed: (a) The quantifiable target or otherwise qualitative characteristic that reports how resolution activities are progressing, <u>and</u> (b) the indicators, statistics, or metrics used to gauge resolution progress (in advance of audit follow-up) to validate the resolution of the deficiency.

NOTE: Corrective Action Plans for IT security issues must agree with what is submitted for the POA&M (discussed in another chapter). The same actions, funding, dates, etc., must be evident in both the Corrective Action Plan and the POA&M!

Bureau/office management is responsible for reviewing plans to ensure that sufficient time is available not only to complete the remediation, but also to ensure that retesting can be completed prior to September 30.

Monitoring Corrective Actions

Management at all levels is responsible for monitoring their programs and operations to insure adequate internal controls and prompt correction of identified weaknesses/deficiencies. Each bureau should develop a tracking system and reporting process for weaknesses/deficiencies identified during the management control assessments. The system should provide a complete record of actions taken to correct the weakness. The reporting system developed should be responsive to the needs of the bureau head, the program assistant secretary, the Assistant Secretary-PMB, the Senior Management Council, and OMB. Bureau tracking systems should include <u>all</u> weaknesses/deficiencies, not just the weaknesses/deficiencies identified as material at the Secretarial level and reported in the Department's Annual Performance and Accountability Report.

Bureau progress in correcting existing material weaknesses/deficiencies will be reported to PFM regularly in accordance with annual guidance, and at the mid-year and year-end ICAF progress meetings. PFM will report progress to the Assistant Secretary-PMB and the Senior Management Council. Bureaus also are encouraged to utilize a matrix as a tool to measure the progress of the corrective actions and which will assist managers and OMB in understanding the progress that has been made.

The Department currently requires bureaus to report progress in correcting material weaknesses/deficiencies on a monthly basis. However, after continuous progress of completing milestones without delays, consideration will be given to allowing quarterly reporting for a specified period. Due dates for the monthly and quarterly progress reports are provided by PFM in the annual internal control guidance.

Postponement in the remediation of a material weakness adversely impacts the achievement of the Department's GPRA goals. Delays in the resolution of any material weakness to a succeeding fiscal year must be approved by the responsible program assistant secretary and forwarded to PFM who will seek final approval from the Assistant Secretary-PMB.

NOTE: Per OMB Revised Circular A-123, if an agency cannot meet the deadlines outlined in the approved corrective action plan, OMB may, at its discretion, require the agency to obtain an independent audit opinion of their internal controls over financial reporting as part of their financial statement audit.

Completed Corrected Actions

Before reporting material weaknesses and financial non-conformance deficiencies as corrected, bureau ICCs need to verify that the corrective action was taken and that the weakness was corrected. Bureaus are required to document supporting verification that corrective actions have been implemented and that material weaknesses and non-conformances have been corrected as reported. Deficiencies will not be considered resolved and "closed" until resolution of a "deficiency" is reported to PFM and documentation is provided along with the bureau's request to close the recommendation. This process applies to OIG identified weaknesses/deficiencies, bureau identified weaknesses/deficiencies, GAO identified weaknesses/deficiencies, or weaknesses/deficiencies that may be identified by other sources.

Before removing reportable conditions and non-material weaknesses from the bureau internal Corrective Action Tracking System, the responsible program official must certify in writing that the planned corrective action was completed and that the action taken corrected the weakness. The certification should be written and incorporated into the bureau internal Corrective Action Tracking System.

For example, if the corrective action for a material weakness requires the issuance of policies and procedures, the ICC should verify that the policies and procedures were issued. If the corrective action requires the implementation of a system or process, the responsible program official needs to test the system or process and forward the test results to the ICC. After the ICC has verified that the corrective action was taken and reviewed the test results, bureaus may report a material weakness as corrected. Final approval of the completion of all required actions to correct a departmental material weakness is issued by PFM; financial statement material weakness correction is verified during the next fiscal year audit.

The responsible program officials(s) should conduct follow-up reviews to insure the weaknesses/deficiencies are resolved.

Linking the Correction of Weaknesses/Deficiencies to Budget Submission

Bureaus are encouraged to complete their scheduled internal control assessments to facilitate budget linkage of any newly identified material weaknesses/deficiencies. Once a weakness/deficiency is identified in a current evaluation, managers must initiate action to set aside the funding (through budget allocations/allotments) and staff resources needed to completely resolve the deficiency, even if it requires redirecting funds from previously planned activities. If redirection of funds is required, bureaus must follow bureau, departmental, and congressional reprogramming procedures. However, it is anticipated that most corrections of material weaknesses can be addressed without a formal congressional reprogramming request, given the broad purposes that funds are available. For weaknesses requiring multiple years to resolve, out-year funding requirements should be prioritized within base funding and included in the bureau and program assistant secretary budget submission(s) until the weakness is resolved. Except in extraordinary cases, funding needed to correct material weaknesses should be prioritized from available base resources, and not funded with new budgetary resources. These amounts must be identified and reported separately in bureau budget requests to the Department. The status of the request should be tracked throughout the budget review and appeals process, through budget enactment

SECTION 1
CHAPTER 6
REPORTING

The fifth step in the Internal Control Process is preparing the annual assurance statements from bureau/office heads and program assistant secretaries that support the Secretary's Assurance Statement and Annual Report to the President and the Congress.

Annual Reporting

DOI's annual reporting process is a vertical flow of information. Bureau/Office annual assurance statements must incorporate information regarding FMFIA Sections 2 and 4, information technology security, compliance with core accounting system requirements, and internal control over financial reporting, which is a subset of the overall FMFIA assurance statement. The bureaus'/offices' annual assurance statements form the basis for the Secretary's Statement to the President and the Congress which is included as part of the Department's Annual Performance and Accountability Report. The process is described below.

<u>Preparing and Issuing an Annual Assurance Statement on Financial Reporting</u>

The Annual Assurance Statement for Internal Control over Financial Reporting is required beginning in fiscal year 2006. This assurance statement is a subset of the overall Statement of Assurance and is based on the results of management's assessment as of June 30, conducted in accordance with the requirements of OMB's Circular A-123, Appendix A. Any changes to the conditions reported in the as of the June 30 Assurance Statement, whether positive (corrected weakness) or negative (additional identified weakness), is to be reported on an updated statement as of September 30.

<u>Preparing and Issuing an Annual Assurance Statement on Compliance with FMFIA</u>

The Annual Assurance Statement is required in the annual FMFIA reporting process. Bureau and office heads prepare an annual assurance statement that is submitted through their respective program Assistant Secretary. Bureau/Office assurance statements form the basis for the Secretary's Annual Assurance Statement which is submitted to the President and the Congress as part of the Department's Annual Performance and Accountability Report. Annually, PFM will provide a sample assurance statement template.

Bureau Reporting

To allow assistant secretaries to fulfill their reporting responsibilities to the Secretary, each bureau head is required to submit their annual assurance statements through their program assistant secretary to the Secretary. Assurance statements should be addressed to the Secretary and sent through the program assistant secretary to PFM. The annual assurances must include information on the following.

1. **Information on Bureau's System of Internal Controls (Section 2, FMFIA).** This statement is based on all available information, including scheduled internal control assessments, audits performed by OIG and GAO, GPRA performance assessments, management studies, and other reviews. These evaluations provide the basis for the bureau head's reasonable assurance, as explained below. The statement must include all open material weaknesses/deficiencies reported in the Secretary's previous assurance statement for which corrective actions have not been completed, and for all material weaknesses/deficiencies identified from the current year assessments, together with the plans and schedules for correcting such weaknesses/deficiencies. In addition, weaknesses/deficiencies reported in previous years that are no longer considered material, require a certification that the corrective actions were completed.

   Full compliance with Section 2 of the FMFIA includes having reasonable assurance that adequate review documentation exists with sufficient testing to support evaluation conclusions. Full compliance also includes the effective utilization of people and other resources, and the timely correction of weaknesses/deficiencies.

   Due to the differences in timing of the submission of the assessment of internal control over financial reporting and the reporting results in the PAR, there is a potential for a change to the status of the assessed effectiveness of internal controls. Changes in status should be reflected in the Annual Assurance statement as follows:

   - If a material weakness is discovered by June 30, but corrected before September 30, revise the assurance statement reported in the PAR to identify the material weakness, the corrective action taken, and that it has been resolved.

   - If a material weakness is discovered after June 30, but prior to the PAR issuance, revise the assurance statement to include the subsequently identified material weakness.

2. **Information on Bureaus' Information Technology System Security (OMB Circular A-130).** The information should describe whether adequate security exists in bureau automated information systems. It also describes information technology security material weaknesses/deficiencies identified during reviews or audits of sensitive applications and/or risk analyses of installations.

3. **Information on Bureau Accounting System Compliance Review (Section 4, FMFIA).** This information should be based on the results of the bureaus internal annual information systems assessments as well as the results of OIG and independent third party system reviews. The requirements contained in Section 3, Chapter 3, Information Technology Internal Control Reviews, of this handbook will be utilized as a guide in assessing system compliance. The requirements contained in this section are intended to serve as a tool to assist system owners and managers in conducting system reviews and to assist with the assessment of system compliance.

4. **Information on Bureau Core Accounting System Compliance.** This information should be based on the Core Compliance reviews, as required by the Chief Financial Officers Act of 1990 and the FFMIA Act of 1996 and other statutes, and, where appropriate, the results of the bureau financial statement audit reports.

5. **Basis for Assurance.** Bureau annual assurance statements must specifically list the management control assessments and OIG/GAO audits which were relied upon to reach assurance statement conclusions.

NOTE: PFM's annual internal control guidance to bureaus includes a sample assurance statement for bureaus to follow.

Secretary's Reporting

The Secretary, under FMFIA, has annual reporting responsibilities to the President and the Congress on: (1) The results of assessments made on the Department's controls including any identified material weaknesses (Section 2); and (2) whether the Department's financial management systems conform to the Federal Accounting Standards Advisory Board (FASAB) issued accounting standards and related requirements (Section 4).

Serving as the Secretary's key staff office on FMFIA, PFM prepares the Secretary's annual assurance statement. In addition to the Secretary's statements on Sections 2 and 4 of the FMFIA, the assurance statement includes: (1) Highlights of DOI's current fiscal year's Internal Control Program results; (2) actions taken to improve the program; (3) descriptions of material and mission critical weaknesses/deficiencies; and (4) schedules for corrective actions. This statement is based on all bureau assurance statements and is included in the Department's Annual Performance and Accountability Report.

SECTION 1
CHAPTER 7
VERIFYING AND CERTIFYING CORRECTIVE ACTIONS

Verifying and certifying completed corrective actions is the last step of DOI's Internal Control Program. This is an important step to determine if control weaknesses/deficiencies were corrected or still exist. Seemingly minor deficiencies can escalate to more serious problems. Diligence is required to ensure complete resolution.

Bureaus must establish and maintain a follow-up system to track the remediation of all identified weaknesses/deficiencies in internal controls. Responsible program officials have the discretion to determine how to track and validate correction of identified weaknesses/deficiencies and non-conformances. However, bureaus must maintain documentation to support the implementation of corrective actions and correction of the deficiency.

The responsible program official(s) should conduct follow-up reviews to insure the deficiency was resolved. These reviews may take the form of a follow-up internal control assessment, and/or continued monitoring of metrics previously established during the corrective action planning process. Follow-up reviews performed by the OIG or GAO also may be used for this purpose.

For all material weaknesses and financial non-conformance deficiencies, the bureau ICC should verify that corrective action was taken and that the weakness was corrected. Again, bureaus are required to document supporting verification that corrective actions have been implemented and that material weaknesses and non-conformances have been corrected as reported. Deficiencies will not be considered resolved and "closed" until resolution of these deficiencies is reported to PFM, and documentation is provided along with the bureau's request to close the recommendation. This process applies to OIG identified weaknesses/deficiencies, bureau identified weaknesses/deficiencies, GAO identified weaknesses/deficiencies, or weaknesses/deficiencies that may be identified by other sources.

For all reportable conditions and non-material weaknesses, the responsible program official should certify in writing that the planned corrective action was completed and that the action taken corrected the weakness. This certification should be written and incorporated into the bureau internal Corrective Action Tracking System reporting process.

SECTION 1
ADDENDUM A
Schedule of Key Actions
Internal Control and Audit Follow-up Programs

Action	Responsible Organization	Due Date
1. Issue Internal Control Program Guidance	PFM	October
2. OMB A-123 Test Plan (see Finance Section)	Bureaus/Offices	October
3. Finalize and publish the Department's internal control review priorities.	PFM	November
4. Advise bureaus and offices of FMFIA material weaknesses and OIG and GAO audit recommendations in GPRA Performance Goal Base.	PFM	November
5. Issue guidance on Departmental Functional Reviews (Property, Acquisition, Information Technology, etc.)	Various PMB Offices	November
6. Report internal control review priorities to PFM (all inclusive). (Priorities Plan)	Bureaus/Offices	December
7. Bureaus provide CAP's to PFM for audited financial statement material weakness and non-compliance issues	Bureau CFO's	December
8. Monthly Status Report on current year audited financial statement material weakness and non-compliance issue corrective actions to PFM	Bureaus	Monthly
9. Monthly Status Report to Assistant Secretary-PMB on current year audited financial statement material weakness and non-compliance issue corrective actions.	PFM	4^{th} Day of each month
10. Quarterly Status Report to PFM on FMFIA material weakness corrective action progress and OIG and GAO audit recommendation implementation.	Bureaus/Offices	December March June August

11. Quarterly Status Report on FMFIA Program to Assistant Secretary-PMB	PFM	January April July September
12. OMB A-123 Test Results Finalized PFM (FISMA and A-130)	Bureaus/Offices	April
13. Conduct mid-year ICAF progress meeting with bureaus, OIG, and PMB staff	Bureaus/Offices, OCIO, PAM, PFM, OIG	May
14. Complete all current fiscal year internal control reviews and Departmental functional reviews	Bureaus/Offices, OCIO, PAM, PFM, OIG	June
15. OMB Circular A-123 Appendix A Assurance Statement on financial reporting	Bureaus/Offices PFM	June
16. Complete all current fiscal year Financial, Internal control reviews, and Departmental functional reviews.	Bureaus/Offices, OCIO, PAM, PFM, OIG	August
17. Submit current year annual assurance statement to Assistant Secretary-PMB and PFM	Bureaus/Offices, OCIO, PAM, PFM, OIG	September
18. OMB A-123 Update (update to "as of June 30" statement combined with the program reviews)	Bureau/Offices PFM	September
19. Annual ICAF year end issue resolution meetings	Bureaus/Offices, OCIO, PAM, PFM, OIG	October
20. Complete final draft of Compliance with Laws and Regulations section of the current year Performance and Accountability Report.	PFM	October

SECTION 1
ADDENDUM B
CONDUCTING ALTERNATIVE INTERNAL CONTROL REVIEWS

Alternative Internal Control Reviews, used for programs determined to be low risk and some medium risk, are usually narrow in scope and focus attention on controls over areas or activities of a component which have the highest potential for ineffective or inefficient operation or loss of government resources. Such reviews may be combined with other review processes (such as internal control or technical reviews) or be conducted as a separate review. Where periodic reviews of programs, organizations, or functions are conducted by bureaus, PFM strongly encourages combining internal control reviews (financial and programmatic), GPRA/PART performance assessments, and other internal bureau reviews to avoid duplication of effort and to make them more acceptable to managers. **Bureaus are also encouraged to use the DOI automated assessment approach to review a component's controls. The automated assessment incorporates eight management integrity measures based on OMB's and GAO's objectives and standards for internal controls in federal programs and administrative functions (see page IC-33 in this appendix).** Additionally, combining reviews will help institutionalize the internal control processes within the Department.

The Department has decided that Internal Control Reviews (ICR) are to be done on all controls or program areas considered to be of high risk. Since an ICR requires a description of all event cycles and analysis of control objectives and techniques, testing is normally very detailed and extensive. When the level of risk for controls or program areas is considered to be low, the Department has decided that an Alternative Internal Control Risk is appropriate because it is generally less paper intensive and more cost effective and efficient. For program areas considered to be medium risk, it is management's discretion as to whether the ICR or AICR is more appropriate; the decision to use the ICR or AICR should be based on the visibility of the program, the dollar impact of the program on outside entities (public or governmental), etc.

Suggested steps for conducting AICRs are listed below.

START THE EVALUATION

Plan the Evaluation

The AICR should be carefully planned to gain managerial support and to ensure that the objectives are accomplished. The planning process should include the following tasks:

> **Determine scope and objectives**. Consider whether the purpose of the AICR is to perform a comprehensive review of controls over all the high risk areas or if it is to perform a limited review of one aspect of the component.
>
> **Assign staff.** The team members selected should be knowledgeable of the program area, have analytical skills, and be trained in conducting control evaluations. Ideally, team

members should be selected from within the responsible program office and from an independent "program-evaluation" function. The number of reviewers should be based on the complexity and scope of the review.

Allocate staff resources and establish timeframes. It is helpful to allocate the minimum and maximum amount of staff resources to be used for completing each task. The final planned completion date should be set with interim planned completion dates for each review task.

Analyze the General Control Environment

The purpose of analyzing the general control environment is to determine if management's attitude is conducive to a strong internal control system. The analysis of the general control environment will provide the reviewer with a preliminary opinion about the effectiveness of specific controls. If an analysis has been previously completed, check to see if it is still accurate and update, as necessary.

The factors that influence the general control environment are:

- Organization;
- Delegation of authority;
- Policies and procedures;
- Personnel;
- Planning, Budgeting and Accounting; and
- Reporting.

Exhibit 1 is a worksheet to use in analyzing the general control environment.

Analyze Information Technology

If the component contains an IT application, it should be analyzed to determine if IT application controls should be reviewed. This review of IT can be a separate review or part of the AICR. An IT application should be included if it contains any of the following characteristics:

- Processes information used for significant management decisions;
- Calculates or records amounts owed by or to the Government;
- Maintains balances or other records used to control government resources;
- Maintains or processes information necessary for effective and efficient program operation; or
- Maintains or processes sensitive information.

NOTE: Section 3, Chapter 3, Executing ICR for Information Systems and IT Programs, of this handbook provides additional details on this process.

DEFINE CONTROL SYSTEMS

Identify and Document High Risk Areas

The reviewer should identify those risks which are high for the component as a whole. High risks are potential unwarranted occurrences which, if they occur, would prevent a component from reaching its objectives or would result in a significant loss of government resources. When identifying high risk areas, the reviewer should also consider the probability of the unwanted occurrence and the severity of the consequences. Exhibit 1 is a worksheet for identifying and documenting high risks

Identify and Document Control Techniques

Control techniques are a series of carefully constructed checks and balances designed to provide reasonable assurance that the control objectives are met in an efficient and effective manner. Control techniques should be observable and cost effective. Examples of control techniques include passwords to limit access to databases, written delegations of authority, technical reports, documentation of processes and procedures for carrying out program and technical activities, periodic supervisory reviews, comparisons of actual results to planned results, and segregating sensitive duties among several individuals.

When developing control techniques, it is crucial to identify the relationship between the techniques and the risks within the event cycle. Control techniques are implemented to reduce risks and meet the control objectives.

Control techniques are the basis of testing. Testing verifies compliance with existing control techniques to determine if the controls are operating as intended and are sufficient to provide reasonable assurance of achieving the control objectives.

Compare Control Systems to the GAO Control Standards

The GAO control standards **(web site address www.gao.gov)** define the minimum level of quality acceptable for an internal control system. These standards apply to all operations and functions except development of legislation, rulemaking, or discretionary policymaking. The five GAO standards for internal control are: (1) Control environment; (2) risk assessment; (3) control activities; (4) information and communications; and (5) monitoring. These standards define the minimum level of quality acceptable for internal control in government programs and administrative operations and provide the basis against which internal control is to be evaluated. The standards apply to all aspects of an agency's operations—programmatic, financial, and compliance.

NOTE: The term internal control as used in the GAO standards is synonymous with the term management control as it was used in the prior version of OMB Circular A-123.

The GAO standards provide a general framework for internal controls. Agency/bureau management is responsible for developing the detailed policies, procedures, and practices to fit their operations, and ensuring that internal controls are built into and are an integral part of operations. A more detailed description of the standards follows.

- Control Environment**.** Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management.

- Risk Assessment**.** Internal control should provide for an assessment of the risks the agency faces from both external and internal sources. Risk assessment is the identification and analysis of relevant risks associated with achieving the objectives, such as those defined in strategic and annual performance plans developed under the GPRA, and forming a basis for determining how risks should be managed.

- Control Activities**.** Internal control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the Department's control objectives. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements for budget development and execution. They also help ensure actions are taken to address risks. Control activities include approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, and the creation and maintenance of related records which provide evidence of execution of these activities along with supporting documentation. Examples of control activities include:

    - Top level reviews of actual performance;
    - Reviews by management at the functional or activity level;
    - Management of human capital;
    - Controls over information processing;
    - Physical control over vulnerable assets;
    - Establishment and review of performance measures and indicators;
    - Segregation of duties;
    - Proper execution of transactions and events;
    - Accurate and timely recording of transactions and events;
    - Access restrictions to and accountability for resources and records; and
    - Appropriate documentation of transactions and internal control.

- Information and Communications**.** Information should be recorded and communicated to management and others within the entity who need it and in a form and within a timeframe that enables them to carry out their internal control and other responsibilities.

- Monitoring**.** Internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.

TEST THE CONTROL SYSTEM

Testing verifies the effectiveness of control techniques in operation by determining if they are, in fact, operating as intended, meeting the control objectives, and reducing risks. By testing, the responsible official can quickly validate whether: (1) Prescribed procedures are performed in accordance with instructions; (2) procedures are performed by personnel having no incompatible duties; (3) actual transactions processed in the operation are in fact those authorized for the group; and (4) actual operations are conducted in accordance with the control objectives and techniques which have been devised for the component.

The focus of testing should be upon the highest potential for ineffective or inefficient operation or loss of government resources and those areas of inadequate internal control system design. Testing consists of the following steps.

Select Controls to be Tested

It is both impractical and unnecessary to test all control techniques. The control techniques to be tested should be those that contribute most to achieving the control objectives or managing the risk. A control should be eliminated from testing when: (1) The technique does not meet the control objective or manage the risk because it is poorly designed, unnecessary, duplicative, or is not performed in a timely manner; and (2) The cost of testing exceeds the value of the technique being tested. If a technique is excluded from testing, the reasons supporting this decision should be recorded.

Select Test Methods

Testing methods include:

- Document analysis - reviewing existing records, completed forms, or other documentation;

- Transaction testing - entering and processing transaction data through the system or tracing transactions through the system;

- Observation - watching the performance of specific control techniques; and/or

- Interview - eliciting information from the personnel who perform the control technique.

Tests should not be limited to information obtained through interviews, but interviews should be used to supplement document analyses and/or observation. One or more methods of testing may be combined during the test.

As mentioned in Chapter 2, the Automated Assessment Approach is considered an AICR which can assist bureaus in reducing their costs for conducting reviews and reporting the results. The primary benefits of the automated assessment are that it provides: (a) A targeted and focused approach for control evaluations; (b) a concise and meaningful summary report for management; (c) an effective means of identifying and reporting best practices; (4) a view of assessment results (strengths and weaknesses) for all measurement areas at one glance; and (5) an effective means of tracking and reporting trend information over time. The assessment is performed electronically using an off-the-shelf surveying and analytical software tool (Survey Tracker) that provides diagnostic and executive-level reporting. Bureaus have the discretion to determine how many of the eight management integrity measures will be tested.

The survey assessment questionnaire is built around the eight integrity measures that support the general and specific internal control standards delineated in OMB Circular A-123 and incorporated in GAO's "Standards for Internal Control in the Federal Government." The eight management integrity measures follow.

- Organizational Control Environment. The objective of this measure is to ensure that an organization's goals, objectives, policies, and procedures are conducive to achieving sound internal controls, and that the organization places a high level of importance on management's integrity and ethics. The organizational control environment sets the tone for and influences the internal control consciousness of its employees. It also provides the foundation for the internal control structure. Organizational control environment factors include: employees integrity, ethical values, and competence; management's philosophy and operating style; management's methodology to assign authority and responsibility, and to organize and develop staff; management's planning, budgeting, accounting and reporting; and senior management direction.

- Risk Management**.** The objective of the risk management measure is to ensure that an organization identifies, assesses, and considers the consequences of events that could prevent the achievement of its goals and objectives, and/or result in significant loss of resources. Every organization faces a variety of risks from external and internal sources and changes in its operating environment. These risks should be continuously monitored and assessed.

- Program Effectiveness**.** The objective of this measure is to ensure that management plans and allocates sufficient resources to programs to achieve intended results. Further, the program effectiveness measure embraces the idea that organizations have strategic planning systems that employ performance measurement systems to provide for comparisons of planned outcomes and results against actual outcomes and results.

- Resource Stewardship. The objective of this measure is to ensure resources are safeguarded and managed in a manner consistent with the mission of the organization. Access to resources should be limited to authorized individuals, and accountability for the custody and use of resources should be assigned and maintained.

- Regulatory Compliance. The objective of this measure is to ensure that laws and regulations are followed. Management and staff must be aware of and ensure that all programs, operations, obligations, and costs incurred comply with applicable laws, regulations, and executive orders.

- Audit Resolution**.** The objective of the audit resolution measure is to ensure that organizations take prompt and responsive action on all audit findings and recommendations in order to improve program and organizational efficiency and effectiveness. Responsive action is that which corrects identified deficiencies. Where audit findings identify opportunities for improvement rather than cite deficiencies, responsive action is that which produces improvements.

- Management Information**.** The objective of this measure is to ensure that reliable and timely information is obtained, maintained, reported, and used for decision-making at all levels. Information systems should produce reports containing program, operational, financial, and compliance related data, to effectively manage and control the programs and operations of an organization.

- Financial Systems and Data Integrity**.** The objective of the financial systems and data integrity measure is to ensure that an organization's financial management system and related operations conform with Government-wide principles, standards, and requirements, and that the process of managing information necessary to support program and financial managers, and assuring data captured and reported is complete, accurate, accessible, timely, and usable.

NOTE: A sample survey assessment questionnaire is included as an Exhibit.

Determine Amount of Testing

It is unrealistic to observe every control used or review 100% of the records at each location. The reviewer must select the organizations and locations where the tests will be conducted and select a sample (using appropriate sampling techniques) for each control to be tested.

Plan Data Collection

Accurate recording of test results is an extremely important part of the testing process. A data collection plan assists in determining how to record the test results. For example, interview guides should be used to ensure that all areas of concern are covered.

Conduct the Tests

While conducting the tests, follow the sample plan unless a decision is made to review the scope or size of the sample based on the results of the initial sample. Increase the sample size if the initial tests provide mixed results. When possible, retain copies of authorizing documents or other physical evidence that control techniques are working.

A control is not effective when the assessment determines it is not adequately designed or when it is reviewed and determined that it is not functioning effectively. There is a control gap when a control does not exist for a given assertion, when a control does not adequately address a relevant assertion, or a control is not operating effectively. Reviewers should always determine that other compensating controls do not exist that would mitigate the risk.

NOTE: Watch for compensating controls. Sometimes a control technique will appear to be weak or not operating. In such a case, determine if personnel are compensating for the shortcomings by using informal control mechanisms. Control mechanisms being used need to be evaluated and documented during the testing.

Analyze Test Results and Develop Conclusions

The tests of specific control techniques must be analyzed to determine if the degree of compliance with control techniques is adequate. It is important to remember that several control techniques are usually utilized to meet a control objective or manage a risk. Accordingly, the failure to substantially comply with one individual control technique does not necessarily result in a failure to meet the control objective or manage a risk.

The test results should then be discussed with managers responsible for operating the control techniques at the location or organization that was reviewed. These discussions will: (1) Communicate the results of the tests and any conclusions drawn; (2) Seek agreement on those conclusions; and (3) Elicit recommendations from managers on any necessary corrective actions. Such discussions are best held as soon as the testing and related analyses of results are completed.

If you used the Automated Assessment Approach, the results of the survey questionnaire (questions based around the eight management integrity measures and other program or administrative policies and procedures) and responses are analyzed by the Survey Tracker software and a graphical summary report, known as a spider diagram, is produced. The summary report presents the actual assessment against a Department or bureau defined standard for each management integrity measure (as shown in the spider diagram contained in the Case Studies).   The closer the results of the actual assessment for each measure are to the defined minimum standard of each integrity measure or to the center of the spider diagram, sufficient internal controls for the program (or activity evaluated) are in place and working. The further from the center the minimum standard set for each integrity measure, the weaker the internal controls. Managers should use results to strengthen internal controls where needed in their areas of responsibility or do additional targeted testing.

Each internal integrity measure area is of equal importance and managers should use the spider diagram to determine the strong and weak internal control areas. Managers should work toward achieving balance between the areas to foster continuous improvement through benchmarking, training, and outreach programs with emphasis on accountability.

Develop Plans for Corrective Action

The primary purpose of the control evaluation process is to assist managers in identifying and correcting weaknesses. When a weakness is found, a decision must be made to institute new controls, improve existing controls, or accept the risk inherent with not correcting the weakness (unless the weakness surpasses established materiality thresholds). The decision must be documented in the evaluation's corrective action plan.

The following information should be completed while preparing corrective action plans (Refer to Chapter 4, Developing and Implementing Corrective Actions, for detailed requirements).

- Summary Description of the Weakness/Deficiency
- Year First Identified
- Target Correction Date
- Accountable Official
- Funding/Resources Required to Resolve the Weakness/Deficiency
- Summary of Corrective Actions
- Quarterly Corrective Actions
- Metrics

REPORT THE RESULTS

Control evaluation results for each component should be summarized in a report. The report should identify control weaknesses and describe plans for corrective action. Since the report forms the basis for the certification required by FMFIA, it must provide the bureau head and assistant secretary with sufficient assurance that the review was conscientiously performed and accurately reflects the condition of internal controls.

The report should contain all control weaknesses which are significant to the next higher organizational level, regardless of the process through which the weaknesses were identified. All sources of information on the status of controls, such as audit reports, management reviews, and routine management reports, are to be considered in identifying control weaknesses. The transmittal memorandum should describe: (1) The risks that the evaluation focused on; and (2) the testing conducted, locations, controls techniques tested, and type and amount of testing.

The report should be submitted to the official designated as the responsible official for component controls and their evaluation. After review by the responsible official, the report is to be transmitted to the bureau ICC for approval by the bureau head. The report must be approved by the bureau head and appropriate program assistant secretary and submitted to PFM with a copy to the OIG.

DOCUMENT THE EVALUATION

Documentation is written material explaining the operation of the control system and the conduct of an internal control assessment. GAO specific control standards require that all internal controls and all transactions and other significant events are to be clearly documented and the documentation is to be readily available for examination. In addition, responsible officials should prepare and maintain sufficient documentation to evidence the conduct of an internal control assessment and the basis for the results and conclusions reached. This documentation should include written evidence concerning:

- The officials participating in the review;
- The risks reviewed;
- The control examined;
- The extent and type of control tests performed;
- The analysis of the tests conducted;
- A description of any weaknesses found;
- The actions recommended to correct the weaknesses; and
- The responsible official.

System documentation provides a means of communicating information on the operation of the control system and serves as a standard to measure the operation of the control system. It further provides information necessary for supervisory or other review and serves as a basis for training new personnel. Assessment documentation provides evidence that an internal control assessment was performed and provides support for the reasonable assurance determination. It serves as the basis for supervisory review and quality control while assisting in subsequent assessments.

How much documentation is enough? Sufficient system documentation answers why the system was designed, what the system does, and how the system operates. Sufficient evaluation documentation answers who did what, what were the results, and why were actions taken?

NOTE: Sufficient documentation should not involve an inordinate amount of paper. However, when testing financial reporting internal controls sufficient documentation must be available to demonstrate the bureaus assessment.

SECTION 1
ADDENDUM C
CONDUCTING INTERNAL CONTROL REVIEWS

Internal Control Reviews include all high risk areas in each event cycle. They are usually much more time-consuming and paper-intensive than Alternative Internal Control Reviews. Therefore, they are to be used sparingly.

The Department has decided that Internal Control Reviews (ICR) are to be done on all controls or program areas considered to be of high risk. As discussed later in this handbook, since an ICR requires a description of all event cycles and analysis of control objectives and techniques, testing is normally very detailed and extensive. When the level of risk for controls or program areas is considered to be low, the Department has decided that an Alternative Internal Control Risk is appropriate because it is generally less paper intensive and more cost effective and efficient. For program areas considered to be medium risk, it is management's discretion as to whether the ICR or AICR is more appropriate; the decision to use the ICR or AICR should be based on the visibility of the program, the dollar impact of the program on outside entities (public or governmental), etc.

Suggested steps for conducting ICRs are listed below.

START THE EVALUATION

Plan the Evaluation

The ICR should be carefully planned to gain managerial support and to ensure that objectives are accomplished. The planning process should include the following tasks.

- **Determine scope and objectives**. Consider whether the purpose of the AICR is to perform a comprehensive review of controls over all the high risk areas or if it is to perform a limited review of one aspect of the component.

- **Assign staff**. The team members selected should be knowledgeable of the program area, have analytical skills, and be trained in conducting control evaluations. Ideally, team members should be selected from within the responsible program office or from an independent "program-evaluation" office. The number of reviewers should be based on the complexity and scope of the review.

- **Allocate staff resources and establish timeframes**. It is helpful to identify the minimum and maximum amount of staff resources to be used for completing each task. The final planned completion date should be set with interim planned completion dates for each review task.

Component Survey

The next step in the assessment process is to survey the component to be reviewed. The survey is primarily a fact-finding and data-gathering exercise to establish the framework in which the component operates. It includes reviewing authorizing legislation, implementing regulations, policies and procedures, planning and budget documents, organizational charts, and other pertinent documents and records. It also includes reviewing audit reports, results of internal reviews, and similar evaluations. The survey provides the input for the steps that follow. If a survey has been previously conducted, the reviewer should check to see if the survey is still accurate.

Analysis of the General Control Environment

The purpose of analyzing the general control environment is to determine if management's attitude is conducive to a strong internal control system. The analysis of the general control environment will provide the reviewer with a preliminary opinion about the effectiveness of specific controls. If an analysis has been previously completed, check to see if it is still accurate and update as necessary. (Use Worksheet in Exhibit 1 for this analysis).

The factors that influence the general control environment are:

- Organization;
- Delegation of authority;
- Policies and procedures;
- Personnel;
- Planning, Budgeting, and Accounting; and
- Reporting.

Analysis of Information Technology

If the component contains an IT application, it should be analyzed to determine if IT application controls should be reviewed. This review of IT can be a separate review. An IT application should be included if it contains any of the following characteristics.

- Processes information used for significant management decisions;
- Calculates or records amounts owed by or to the government;
- Maintains balances or other records used to control government resources;
- Maintains or processes information necessary for effective and efficient program operation; or
- Maintains or processes sensitive information.

NOTE: Section 3, Chapter 3, Executing ICR for Information Systems and IT Programs, of this handbook provides additional details on this process.

DEFINE CONTROL SYSTEMS

Identify and Document Event Cycles

An event cycle is a series of related steps that constitute a distinct and separate process or activity within a component. Each program or administrative component of a bureau contains one or more event cycles that help achieve the goals of the component.

In general, components can be comprised of either process-related sets of event cycles, as in administrative-type components, or program sets of event cycles. For example, the cash management administrative component of a bureau normally includes billing, collecting, depositing, procuring, and disbursing event cycles. By contrast, most program components normally include planning, budgeting, executing, reporting, and administrative event cycles.

Some components, such as concessions management, may be described as either an administrative or program component and, accordingly, may be segmented into administrative or program event cycles. It is up to the reviewer to determine which type best fits the component being reviewed.

An important step in the review process is to first identify and then list all the event cycles of the component. The next step is to develop a thorough understanding of how each event cycle functions. If a detailed description of the event cycle does not already exist, then documentation should be prepared using flowcharts and/or narrative descriptions. This detailed description should be retained as part of the ICR documentation.

Background information necessary for creating such documentation may be obtained through interview, observation, or existing records such as mission and function statements. Documentation of the event cycle should be sufficient to provide an in-depth understanding of the objectives and operations of every cycle.

Identify and Document All Risks

After listing the event cycles, the potential risks involved within each event cycle must be identified. The reviewer should categorize the identified risks within each cycle as high, medium, or low. The impact of each risk (the probability of its occurrence and the severity of its consequences) should be considered. High risks are those which could prevent the event cycle from achieving its objective or result in substantial loss of government resources.

The reviewer would then determine, based upon knowledge of the activity and the objective of the event cycle, which risks are high.

Identify and Document Control Objectives

Control objectives are what you want to achieve. Specifically, control objectives are the desired goals for a specific event cycle that reduce the potential for fraud, waste, and abuse or ensure the efficiency, effectiveness, and economy of operations within the event cycle. These objectives should correspond to the risks identified for the event cycle and set forth the specific goals the control system is to meet.

Setting control objectives involves turning the potential risk into a goal. To identify a control objective, ask what needs to happen in order to avoid a specific risk. The reviewer should state what the objective will achieve and how it will be determined whether the objective was achieved.

If the component being reviewed does not have control objectives, the reviewer should develop the control objectives during the review in order to proceed to identifying and documenting the control techniques.

Identify and Document Control Techniques

Control techniques are a series of carefully constructed checks and balances designed to provide reasonable assurance that the control objectives are met in an efficient and effective manner. Control techniques should be observable and cost effective. Examples of control techniques include passwords to limit access to databases, written delegations of authority, technical reports, documentation of processes and procedures for carrying out program and administrative activities, periodic supervisory reviews, comparisons of actual results to planned results, and segregating sensitive duties among several individuals.

When developing control techniques, it is crucial to identify the relationship between the techniques to determine if the controls are operating as planned and are sufficient to provide reasonable assurance of achieving the control objectives.

Compare Control Systems to the GAO Control Standards

The GAO control standards **(web site address www.gao.gov)** define the minimum level of quality acceptable for an internal control system. These standards apply to all operations and functions except development of legislation, rulemaking, or discretionary policymaking. The five GAO standards for internal control are: (1) Control environment; (2) risk assessment; (3) control activities; (4) information and communications; and (5) monitoring. These standards define the minimum level of quality acceptable for internal control in government programs and administrative operations and provide the basis against which internal control is to be evaluated. The standards apply to all aspects of an agency's operations—programmatic, financial, and compliance.

NOTE: The term internal control as used in the GAO standards is synonymous with the term management control as it was used in the prior version of OMB Circular A-123.

The GAO standards provide a general framework for internal controls. Agency/bureau management is responsible for developing the detailed policies, procedures, and practices to fit their operations, and ensuring that internal controls are built into and are an integral part of operations. A more detailed description of the standards follows.

- Control Environment**.** Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management.

- Risk Assessment**.** Internal control should provide for an assessment of the risks the agency faces from both external and internal sources. Risk assessment is the identification and analysis of relevant risks associated with achieving the objectives, such as those defined in strategic and annual performance plans developed under the GPRA, and forming a basis for determining how risks should be managed.

- Control Activities**.** Internal control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the Department's control objectives. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements for budget development and execution. They also help ensure actions are taken to address risks. Control activities include approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, and the creation and maintenance of related records which provide evidence of execution of these activities along with supporting documentation. Examples of control activities include:

    - Top level reviews of actual performance;
    - Reviews by management at the functional or activity level;
    - Management of human capital;
    - Controls over information processing;
    - Physical control over vulnerable assets;
    - Establishment and review of performance measures and indicators;
    - Segregation of duties;
    - Proper execution of transactions and events;
    - Accurate and timely recording of transactions and events;
    - Access restrictions to and accountability for resources and records; and
    - Appropriate documentation of transactions and internal control.

- Information and Communications**.** Information should be recorded and communicated to management and others within the entity who need it and in a form and within a timeframe that enables them to carry out their internal control and other responsibilities.

- Monitoring**.** Internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.

REVIEW THE SYSTEM DESIGN

An assessment of a system of internal controls is based on a documented understanding of the system. Information obtained during the survey of the component and documentation of the control system should be studied. This part of the ICR should focus on the adequacy of the control objectives and the design of the control techniques. During this process, the reviewer should answer at least the following questions.

Adequacy of control objectives: An agency must review sufficient controls to assure that systems and applications are designed to operate effectively, provide confidentiality, integrity, availability and protect information from loss, misuse and unauthorized access or modification.

Adequacy of control techniques: Control techniques must determine and gain a high level indication that the system and the information are adequately secured. Management, Operational and Technical controls should all be included in the assessment.

- Have complete, logical, and applicable control objectives been established?
- Do existing controls appear sufficient to manage the risks and satisfy the control objectives?
- Do existing controls appear excessive for the risks and control objectives specified?
- Can or should other controls be used to either reduce risk or improve the efficiency of the system?

The answers to these questions will lead the reviewer to a judgment about the system's theoretical strengths and weaknesses. This, in turn, enables the reviewer to focus on the appropriate areas to be examined during the testing phase.

TEST THE CONTROL SYSTEM

Testing verifies the effectiveness of control techniques in operation by determining if they are, in fact, operating as intended, meeting the control objectives, and reducing risks. By testing, the responsible official can quickly validate whether:

- Prescribed procedures are performed in accordance with instructions;
- Procedures are performed by personnel having no incompatible duties;
- Actual transactions processed in the operation are in fact those authorized for the group; and
- Actual operations are conducted in accordance with the control objectives and techniques which have been devised for the component.

The focus of testing should be upon high risk areas and those areas of inadequate internal control system design. Testing consists of the following steps.

Select Controls to be Tested

It is both impractical and unnecessary to test all control techniques. The control techniques to be tested should be those that contribute most to achieving the control objectives or managing the risk. A control should be eliminated from testing when: (1) The technique does not meet the control objective or manage the risk because it is poorly designed, unnecessary, duplicative, or is not performed in a timely manner; and (2) the cost of testing exceeds the value of the technique being tested. If a technique is excluded from testing, the reasons supporting this decision should be recorded.

Select Test Methods

Testing methods include:

- Document analysis – reviewing existing records, completed forms, or other documentation;
- Transaction testing – entering and processing transaction data through the system or by tracing transactions through the system;
- Observation – watching the performance of specific control technique; and/or
- Interview – eliciting information from the personnel who perform the control technique.

Tests should not be limited to information obtained through interviews, but interviews should be used to supplement document analyses and/or observation. One or more methods of testing may be combined during the test.

The Automated Assessment Approach discussed in detail in Addendum A may also be used here. Please refer to Addendum A for additional information.

Determine Amount of Testing

It is unrealistic to observe every time a control is used or review 100% of the records at all locations. The reviewer must select the organizations and locations where the tests will be conducted and select a sample for each control to be tested.

Plan Data Collection

Accurate recording of test results is an extremely important part of the testing process. A data collection plan assists in determining how to record the test results. For example, interview guides should be used to ensure that all areas of concerns are discussed.

Conduct the Tests

While conducting the tests, the sample plan should be followed unless it is determined that it is necessary to revise the scope or size of the sample based on the results of the initial sample. Consider increasing the sample size if the initial tests provide mixed results. When possible, retain copies of authorizing documents or other physical evidence that control techniques are working.

A control is not effective when the assessment determines it is not adequately designed or when it is reviewed and determined that it is not functioning effectively. There is a control gap when a control does not exist for a given assertion, when a control does not adequately address a relevant assertion, or a control is not operating effectively. Reviewers should always determine that other compensating controls do not exist that would mitigate the risk.

NOTE: Watch for compensating controls. Sometimes a control technique will appear to be weak or not operating. In such a case, determine if personnel are compensating for the shortcomings by using informal control mechanisms. If informal control mechanisms are being used, evaluate and document them during the testing.

Analyze Test Results and Develop Conclusions

The tests of specific control techniques must be analyzed to determine if the degree of compliance with control techniques is adequate. It is important to remember that usually several control techniques are utilized to meet a control objective or manage a risk. Accordingly, the failure to substantially comply with one individual control technique does not necessarily result in a failure to meet the control objective or manage a risk.

The test results should then be discussed with managers responsible for operating the control techniques at the location or organization that was reviewed. These discussions will: (1) Communicate the results of the tests and any conclusions drawn; (2) seek agreement on those conclusions, and (3) elicit recommendations from the managers on any necessary corrective actions. Such discussions are best held as soon as the testing and related analyses of results are completed.

Develop Plans for Corrective Action

The primary purpose of the control assessment process is to assist managers in identifying and correcting weaknesses. When a weakness is found, a decision must be made to institute new controls, improve existing controls, or accept the risk inherent in the weakness. In many cases the appropriate action is apparent but in other cases further analysis may be necessary before a plan for corrective action can be made. Selecting corrective actions involves creating a strategy for achieving the control objectives. The actions selected should use the least amount of dollar and personnel resources possible and ensure the achievement of the control objectives or results.

The following information should be completed while preparing corrective action plans (Refer to Chapter 4, Developing and Implementing Corrective Actions, for detailed requirements).

- Summary Description of the Weakness/Deficiency
- Year First Identified
- Target Correction Date
- Accountable Official
- Funding/Resources Required to Resolve the Weakness/Deficiency
- Summary of Corrective Actions
- Quarterly Corrective Actions
- Metrics

REPORT THE RESULTS

Control assessment results for each component should be summarized in a report. The report should identify control weaknesses and describe plans for corrective action. Since the report forms the basis for the certification required by FMFIA, it should provide the bureau head and program assistant secretary with sufficient assurance that the review was conscientiously performed and accurately reflects the condition of internal controls.

The report should contain all control weaknesses which are significant to the next higher organizational level, regardless of the process through which the weaknesses were identified. All sources of information on the status of controls, such as audit reports, management reviews, and routine management reports, are to be considered in identifying control weaknesses. The transmittal memorandum should describe: (1) Risks that the evaluation focused on; and (2) testing conducted, locations, controls techniques tested, and type and amount of testing.

The report should be submitted to the official designated as responsible for component controls and their evaluation. After review by the responsible official, the report is to be transmitted to the bureau ICC for approval by the bureau head. The report must be approved by the bureau head and appropriate program assistant secretary and submitted to PFM with a copy to the OIG.

DOCUMENT THE EVALUATION

Documentation is written material explaining the operation of the control system and the conduct of an internal control assessment. GAO specific control standards require that all internal controls and all transactions and other significant events are to be clearly documented, and the documentation is to be readily available for examination. In addition, responsible officials should prepare and maintain sufficient documentation to evidence the conduct of an internal control assessment and the basis for the results and conclusions reached. This documentation should include written evidence concerning:

- The officials participating in the review;
- The risks reviewed;
- The controls examined;
- The extent and type of control tests performed;
- The analysis of the tests conducted;
- A description of any weaknesses found;
- The actions recommended to correct the weaknesses; and
- The responsible official.

System documentation provides a means of communicating information on the operation of the control system and it serves as a standard to measure the operation of the control system. It further provides information necessary for supervisory or other review and serves as a basis for training new personnel. Evaluation documentation provides evidence that an internal control assessment was performed and provides support for the reasonable assurance determination. It serves as the basis for supervisory review and quality control while assisting in subsequent assessments.

How much documentation is enough? Sufficient system documentation answers why the system was designed, what the system does, and how the system operates. Sufficient evaluation documentation tells the reviewer who did what, what were the results, and why were actions taken.

NOTE: Sufficient documentation should not involve an inordinate amount of paper. However, when testing financial reporting internal controls, sufficient documentation must be available to demonstrate the bureau’s assessment.

SECTION 1
ADDENDUM D
REFERENCES FOR FEDERAL REGULATIONS

Information related to public laws, OMB Circulars, and regulatory authorities that govern the Department of the Interior's internal control program are included in this addendum. OMB circulars applicable to internal controls and referenced in this Handbook can be obtained from the OMB Web-site: **www.whitehouse.gov/OMB/Circulars**

Regulation	Title	Date
IG Act (P.L. 95-452)	Inspector General Act of 1978	Amended 10/18/88
GPRA	Government Performance & Results Act	1/5/93
FMFIA (P.L. 97-255)	Federal Managers Financial Integrity Act	9/8/82
CFO Act (P.L. 101-576)	Chief Financial Officer's Act of 1990	11/15/90
OMB Circular A-127	Financial Systems	Revised 12/1/04
GMRA (P.L. 103-356)	Government Management Reform Act	10/13/94
ITMRA Act of 1996 (P.L. 104-106)	Information Technology Management Reform Act (Clinger-Cohen Act)	8/8/96
FFMIA (P.L. 104-208)	Federal Financial Management Improvement Act	9/30/96
GPEA (P.L. 105-277, Title XVII)	Government Paperwork Elimination Act	10/21/98
OMB Circular A-130	Management of Federal Information Resources	Revised 11/30/00
IPIA (P.L. 107-300)	Improper Payments Information Act	11/26/02
FISMA (P.L.107-347 – Title III)	Federal Information Security Management Act	12/17/02
Sarbanes-Oxley Act (P.L.107-204 116 Stat. 745)	Sarbanes-Oxley Act of 2002	7/30/02
OMB Circular A-133 (P.L. 98-502 - 1984) (P.L. 104-156 – 1996)	Single Audit Act	Amended 6/27/03
OMB Circular A-123	Management's Responsibility for Internal Control	Revised 12/21/04
OMB Circular A-11	Preparation, Submission, and Execution of the Budget	6/21/05

Inspector General Act of 1978 (IG Act), as amended

The IG Act provides for independent reviews of agency programs and operations. IGs are required to submit semiannual reports to Congress on significant abuses and deficiencies identified during the reviews and the recommended actions to correct those deficiencies. IGs and/or external auditors are required by the Government Auditing Standards and OMB Bulletin No. 01-02 Audit Requirements of Federal Financial Statements, as amended to report material weaknesses in internal control related to financial reporting and noncompliance with laws and regulations as part of the financial statement audit. Auditors also provide recommendations for correcting the material weaknesses. Agency managers, who are required by the IG Act to follow up on audit recommendations, should use these reviews to identify and correct problems resulting from inadequate or poorly designed controls, and to build appropriate controls into new programs. Audit work planned by the IG should be coordinated with management's assessment requirements to ensure cost effectiveness and avoid duplication.

Government Performance and Results Act (GPRA) and Program Assessment Rating Tool (PART)

To support results-oriented management, GPRA requires agencies to develop strategic plans, set performance goals, and report annually on actual performance compared to goals. With the implementation of the revised Circular A-123 legislation, these plans and goals are integrated into the budget process, the operational management of agencies and programs, and accountability reporting to the public on performance results, and on the integrity, efficiency, and effectiveness with which they are achieved. Similarly, the Program Assessment Rating Tool (PART)'s primary purpose is to assess program effectiveness and improve program performance. The PART has also become an integral element of the budget process when making funding resource allocations or decisions.

Federal Managers Financial Integrity Act of 1982 (FMFIA)

The FMFIA requires agencies to establish and maintain internal control. The agency head must annually evaluate and report on the control and financial systems that protect the integrity of Federal programs; Section 2 and Section 4, respectively. 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.

Chief Financial Officers Act, as amended (CFO Act)

The CFO Act requires agencies to establish and assess internal control related to financial reporting. The Act requires the preparation and audit of financial statements. In this process, auditors report on internal control and compliance with laws and regulations related to financial reporting. Therefore, the agencies covered by the Act have a clear opportunity to improve internal control over their financial activities, and to evaluate the controls that are in place. The Accountability of Tax Dollars Act of 2002 amended the CFO Act to expand the types of Federal agencies that are required to prepare audited financial statements.

Meeting the accelerated financial statement reporting due date also provides incentive for agencies to have added discipline and effective internal control to routinely produce reliable financial information. Deficiencies in internal control need to be mitigated to ensure timely and accurate financial information.

OMB Circular A-127, Financial Systems

This circular prescribes policies and standards for executive Departments and agencies to follow in developing, operating, and reporting on financial management systems. A financial system is an information system (automated or manual) comprised of one or more applications, that is used for either: (a) collecting, processing, maintaining, transmitting, and reporting data about financial events; (b) supporting financial planning or budgeting activities; (c) accumulating and reporting cost information; or, (d) supporting the preparation of financial statements. OMB Circular A-127 was revised December 1, 1994, to include coordination among the operators of agency financial management systems, vendors of financial management software, E-Gov shared services, and the Department of Treasury. The revisions incorporate the transfer of responsibilities from the Joint Financial Management Improvement Program to the Chief Financial Officer's Council and the Office of Federal Financial Management.

Government Management Reform Act

The Government Management Reform Act was enacted to provide a more effective, efficient, and responsive Government. Included in this act: **Title I**, Limitation on Pay which amends the Legislative Reorganization Act of 1946 and other Federal law to limit annual cost of living adjustments for Members of Congress, the Vice President, senior Government officials; **Title II**, Human Resource Management amends Federal civil service law to eliminate unlimited accumulation of annual leave by members of the Senior Executive Service and sets a limit on excess leave of 90 days per year; **Title III**, Streamlining Management Control authorizes the Director of OMB to publish annually in the President's Budget any recommendations for the consolidation, elimination, or adjustment in frequency and due dates of statutorily required periodic reports to the Congress or its committees; and **Title IV**, Financial Management (Federal Financial Management Act of 1994, which amends Federal law to require direct deposit of Federal wage, salary, and retirement payments by electronic funds transfer for recipients who began receiving such payments on or after January 1, 1995.

Clinger-Cohen Act of 1996 (formerly known as the Information Technology Management Reform Act)

The Clinger-Cohen Act requires agencies to use a disciplined capital planning and investment control process to maximize the value and assess and manage the risks of the information technology acquisitions. The Act requires that agencies establish goals for improving the efficiency and effectiveness of agency operations and, as appropriate, the delivery of services to the public through the effective use of information technology; prepare an annual report . . . on the progress in achieving the goals; ensure that performance measurements are prescribed for information technology used by, or to be acquired for, the executive agency and that the performance measurements measure how well the information technology supports programs of the executive agency; where comparable processes and organizations in the public or private sectors exist, quantitatively, benchmark agency process performance against such processes in terms of cost, speed, productivity, and quality of outputs and outcomes; analyze the missions of the executive agency and, based on the analysis, revise the executive agency's mission-related processes and administrative processes as appropriate before making significant investments in information technology that is to be used in support of the performance of those missions; and ensure that the information security policies, procedures, and practices of the executive agency area adequate.

Federal Financial Management Improvement Act of 1996 (FFMIA)

The 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 (USSGL) at the transaction level. Financial management system shall have general and application controls in place in order to support management decisions by providing timely and reliable data. The agency head shall make a determination annually about whether the agency's financial management systems substantially comply with the FFMIA. If the systems are found not to be compliant, management shall develop a remediation plan to bring those systems into substantial compliance. Management shall determine whether non-compliances with FFMIA should also be reported as non-conformances with Section 4 of FMFIA.

Government Paperwork Elimination Act (GPEA)

GPEA was enacted to make government service delivery more efficient while ensuring baseline standards for electronic signatures across federal agencies.

OMB Circular A-130, Management of Federal Information Resources

This circular establishes uniform government-wide policies for the management of federal information resources required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995. The Paperwork Reduction Act mandates that agencies perform their information resources management activities in an efficient, effective, and economical manner. Agencies are to evaluate their information resources management practices to determine the adequacy and efficiency and compliance with information resources management policies, principles, standards, and guidelines promulgated by the Director, OMB.

In addition to the requirements of Circular A-130, the **Federal Information Security Management Act (FISMA) of 2002 (**part of the Electronic Government Act of 2002, Title III), assigned specific responsibilities to agencies to strengthen information system security. FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, Chief Information Officers, and Inspectors General to conduct annual reviews of the agency's information security program and report the results to OMB.

Improper Payments Information Act (IPIA) of 2002

The IPIA requires agencies to review and ". . . identify programs and activities that may be susceptible to significant improper payments." Agencies must annually submit estimates of improper payments, corrective actions to reduce the improper payments, and statements as to whether its current information systems and infrastructure can support the effort to reduce improper payments. The nature and incidence of improper payments shall be considered when assessing the effectiveness of internal control.

Federal Information Security Management Act (FISMA) of 2002

FISMA, part of the Electronic Government Act of 2002, Title III, assigned specific responsibilities to agencies to strengthen information system security. FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level.

Sarbanes-Oxley Act of 2002

Section 404 of the Public Company Accounting Reform and Investor Protection Act of 2002 (Sarbanes-Oxley Act), requires every annual report of public companies to include management's assessment on the effectiveness of the entity's internal controls.

OMB Circular A-133, Single Audit Act

The Single Audit Act, as amended June 21, 2005, requires financial statement audits of non-Federal entities that receive or administer grant awards of Federal monies. The financial statement audits include testing the effectiveness of internal control and determining whether the award monies have been spent in compliance with laws and regulations. Each Federal agency which provides Federal awards shall review audits of the recipients to determine whether corrective actions are implemented with respect to audit findings.

OMB Circular A-123, Management's Responsibility for Internal Control (formerly Management Accountability and Control)

Circular A-123 defines management's responsibility for internal control. The policy changes in this circular are intended to strengthen the requirements for conducting management's assessment of internal control over financial reporting and emphasize the need for agencies to integrate and coordinate internal control assessments with other internal control-related activities. This circular emphasizes the need for integrated and coordinated internal control assessments that synchronize all internal control-related activities. Agencies and individual Federal managers must take systematic and proactive measures to develop and implement appropriate, cost effective internal controls for results-oriented management; assess the adequacy of internal control in Federal programs and operations; separately assess and document internal control over financial reporting; identify needed improvements; take corresponding corrective action; and report annually on internal control through management assurance statements.

OMB Circular A-11, Preparation, Submission, and Execution of the Budget

This circular provides an overview of the budget process, including the basic laws that regulate the budget and the terms and concepts needed to understand the budget process. Circular A-11 provides instructions for preparing and submitting materials required for OMB and Presidential review of agency requests and for formulation of the fiscal year 2007 Budget, including development and submission of a performance budget, which replaces the annual performance plan required by the Government Performance and Results Act for fiscal year 2007. This circular also covers Federal credit programs, strategic plans and annual program performance reports, and provides an overview of the performance budget. Planning, budgeting, and acquisition of capital assets is discussed and instructions are provided for preparation and submission.

United States Department of the Interior

FISH AND WILDLIFE SERVICE
Washington, D.C. 20240

In Reply Refer To:
FWS/AMBS/DBHC/004416

Memorandum

To: Director, Office of Financial Management

Through: Assistant to the Assistant Secretary for Fish and Wildlife and Parks AUG 30 2001

From: FOR Acting Deputy Director AUG 29 2001

Subject: Management Control Assessment of Bird Habitat Conservation

A review of controls was conducted for the Bird Habitat Conservation (North American Wetlands Conservation Act) component during January-July 2001 in the Washington Office. The current Fiscal Year budget is $72 million and 19 FTEs. The review included an automated questionnaire covering the NAWCA grants process which is performed only in the Washington Office.

The automated assessment questionnaire was administered to ten staff within the Washington Office and ten were completed. The attached overall results exceed the Department minimum standards in each of the integrity measures: (1) Organizational Control and Environment; (2) Risk Management; (3) Program Effectiveness; (4) Regulatory Compliance; (5) Management Information; (6) Resource Stewardship; and (7) Audit Resolution.

The review focused on controls over the following risks:
(1) Program performance reviews not systematically conducted;
(2) Project monitoring site visits not systematically conducted;
(3) Division of labor between the Division of Contracting and General Services and the Division of Bird Habitat Conservation is unclear, inefficient, and often duplicative; and
(4) Intra-agency inconsistency in interpretation and application of laws and regulations.

Tests conducted during the evaluation were sufficient to provide reasonable assurance of detecting any significant control weaknesses. Testing methods used for this assessment were: questionnaire, interviews, observation, and document analysis. The attached Control Review Report describes the weaknesses found and the planned corrective actions to be undertaken and completed by December 2002.

Attachments
Control Review Report
Spider Diagram
DOI Integrity Measure Summary

CONTROL REVIEW REPORT

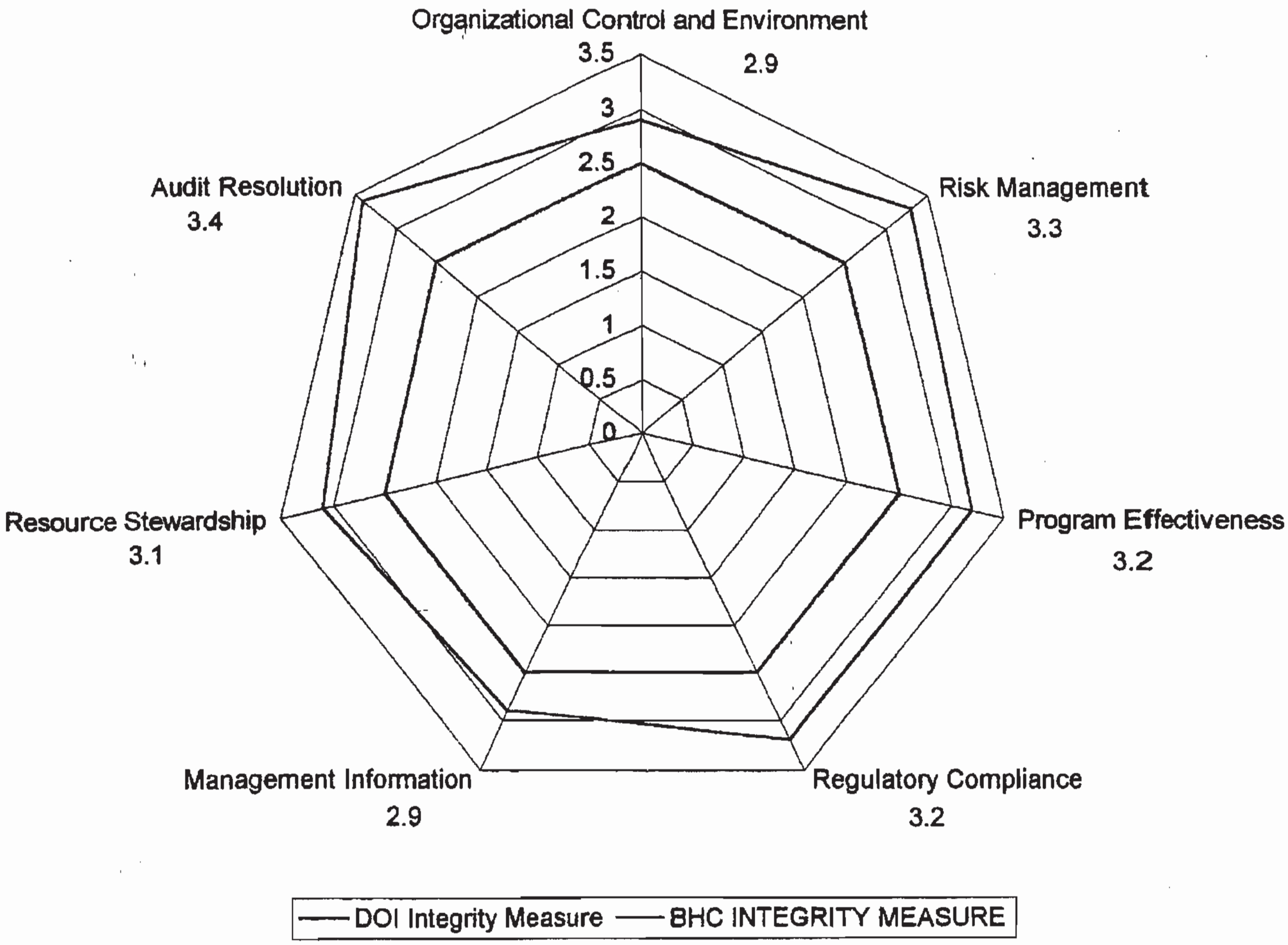
Bureau: U.S. Fish and Wildlife Service **Component:** Bird Habitat Conservation (NAWCA)

Responsible Official: Assistant Director-Migratory Birds & State Programs **Date:** August 7, 2001

NO.	IDENTIFIED CONTROL WEAKNESSES of the Division of Bird Habitat Conservation (North American Wetlands Conservation Act)	TYPE		NO.	PLANNED CORRECTIVE ACTION (PCA) (Assigned to/Certifying Offical)	PLANNED COMPLE-TION DATE
		S	C			
1	The status of program effectiveness is not known because program evaluations are not systematically conducted.	✔		1	A programmatic evaluation will be conducted; A procedure & plan for future evaluations will be developed and implemented (DBHC Program Analyst/ DBHC Division Chief).	2/02
2	The status of habitat acquired, enhanced or restored is not known because on-site monitoring and evaluation of projects are not systematically conducted.	✔		2	A systematic project monitoring and evaluation site-visit procedure and plan will be developed and implemented (DBHC Program Analyst/DBHC Division Chief).	6/02
3	Lack of Service policy or guidelines promotes inefficient division of labor between DCGS and DBHC which results in gaps in grants administration responsibilities.	✔		3	Procedures clarifying the division of labor between DCGS and DBHC will be developed for proposal to DCGS (DBHC Deputy Chief/Division Chief).	8/02
4	Intra-agency inconsistency in interpretation & application of laws and regulations may result in poor customer service and intra-agency conflicts.	✔		4	A NAWCA domestic grants administration policy will be developed and following rule-making procedures, will be published in the Federal Register (DBHC Deputy Chief/Division Chief).	12/02

1. **Indicate the type of weakness by checking the appropriate column.**
   S = A weakness in <u>system</u> design, i.e., necessary controls are lacking.
   C = A weakness in <u>complying</u> with established controls.
2. **Indicate whether a control weakness is a material weakness by inserting (MW) after the weakness.**
3. **Indicate position of person "Assigned to" complete each planned corrective action (PCA).**
4. **Indicate "Certifying Official" for each PCA; must be at least one level higher than person completing the action.**

BIRD HABITAT CONSERVATION



BIRD HABITAT CONSERVATION

	DOI Integrity Measure	BHC INTEGRITY MEASURE
Organizational Control and Environment	2.5	2.9
Risk Management	2.5	3.3
Program Effectiveness	2.5	3.2
Regulatory Compliance	2.5	3.2
Management Information	2.5	2.9
Resource Stewardship	2.5	3.1
Audit Resolution	2.5	3.4

Case Study No. 2

United States Department of the Interior

U.S. GEOLOGICAL SURVEY
Office of the Director
Reston, Virginia 22092

MEMORANDUM

JUL 1 1994

To: Director, Office of Financial Management

Through: for Elizabeth A. Rieke
Assistant Secretary--Water and Science

From: Gordon P. Eaton
Director, U.S. Geological Survey

Subject: Alternative Management Control Review--National Mapping Division Contractually Produced Digital Orthophoto Quadrangles

Attached is the completed Alternative Management Control Review for Contractually Produced Digital Orthophoto Quadrangles in the National Mapping Division. Extensive testing of the program was conducted by reviewing existing records, completed forms, or other documentation; by interviewing/eliciting information from the personnel who perform the control technique; or by observing the performance of a specific control technique. This testing was sufficient to provide reasonable assurance of detecting any significant control weaknesses. There were no identified control weaknesses.

Attachment

Copy to: Office of Inspector General

ALTERNATIVE MANAGEMENT CONTROL REVIEW

CONTRACTUALLY PRODUCED DIGITAL ORTHOPHOTO QUADRANGLES

GENERAL INFORMATION

MISSION OF THE NATIONAL MAPPING DIVISION (NMD)

The National Mapping Division (NMD) supports the U.S. Geological Survey's (USGS) mission to provide national earth science information in a variety of ways. The NMD provides current and accurate maps and other graphic products, as well as a variety of digital cartographic products to meet the needs of Federal and State governments and the private sector for multipurpose base information. The value of these digital cartographic data is increasing rapidly as computers become more readily available to a wider cross section of users. Additionally, new applications, such as those found in Geographic Information Systems (GIS), find their way into the decision making process at all levels. Advanced techniques for collecting, processing, and disseminating digital cartographic data are constantly evolving to meet the increasing demands. One of the newer products in high demand is the Digital Orthophoto Quadrangle (DOQ). Orthophotos. combine the image characteristics of an aerial photograph with the accuracy of a conventional map. When these data are combined with other earth science data, particularly in GIS systems, new levels of measurement and analysis are possible, providing increasingly high levels of support to the decision making process. These data are being used to support land use programs, resource management applications, transportation studies, and update of other products.

The NMD combines appropriated and reimbursable funds to produce these data. The annual appropriation is not sufficient to meet all of the high priority requirements of NMD and other activities. When joint requirements can be satisfied, the NMD enters into a variety of reimbursable work agreements with Federal, State, and local agencies, and some nongovernmental activities to fund the priority projects these organizations require.

LIMITS OF THIS ALTERNATIVE MANAGEMENT CONTROL REVIEW

A thorough Alternative Management Control Review of the entire Reimbursable Cartographic Program was completed in June of 1991 and all associated weaknesses have been corrected. Since then, the digital orthophoto program has expanded. The production procedures to generate the digital orthophoto product also have been refined. Additionally, the NMD is placing an increasing reliance on private contractors to provide the production capacity for a large part of this program. This AMCR is limited to the capabilities and procedures developed since the 1991 study. it focuses on the contract production process and examines the assignment of priorities, billing procedures, and quality control activities supporting contracted production.

FUNDING LIMITATIONS FOR COOPERATIVE CARTOGRAPHIC WORK

Cooperative cartographic work with other ***Federal*** agencies is generally performed under an appropriate agreement. There are no legal or regulatory requirements regarding the distribution of costs, therefore other-agency share of costs can be any percentage from full repay to no payment at all. Because this program produces a DOQ, which is a standard NMD product, the NMD goal is to share costs on a 50-percent-of-total basis whenever possible. Fixed prices based on average costs are used to compute the agreed funding levels.

Cooperative cartographic work with the ***States*** is subject to different regulations, evenwhen an NMD standard product results the process. Public law (43 U.S.C. 50) allows the USGS to enter into cooperative mapping projects with States, including counties and other municipal organizations. Language in the USGS's annual appropriation (P.L. 101-512), however, limits the amount of appropriated funds used for cooperative projects with States and municipalities to 50 percent of the actual cost. Estimated costs are provided to the cooperating agency as a planning tool but reimbursement to NMD is based on actual costs.

Historically the NMD has entered into ***private*** cooperative agreements for products with only service organizations such as the Boy Scouts of America, or academic institutions that are capable of providing unique insight into a technical investigation. To date there has been no opportunity to explore this funding option for the DOQ product.

The basis of reimbursement received by NMD can take several forms, direct payment of funds by the cooperator, work share where each agency performs a portion of the work and data exchange which provides for receipt of digital data of like value for that generated by NMD production processes. Supplemental funding is used to provide the incentive for a cooperating agency to add value or complete a product to NMD specifications. In this case, NMD transfers funds to the cooperating agency for the additional services.

ANALYSIS OF THE CONTROL ENVIRONMENT

The control environment is strong and dynamic due in large measure to the experience with a reimbursable program through the years. Management emphasizes a commitment to the existing directives and policies which delineate the procedures to be followed in this activity. Positive attitudes are evident from the personnel associated with the program. This is due largely to the successful implementation of tailored production software, systems, and procedures developed by NMD managerial and technical staff to pursue this activity. There is continuous interaction between the various offices associated with negotiating agreements with other organizations, and with completing the assignments. Because the program was developed within NMD, there is an exemplary sense of dedication to ensuring a quality outcome for each project. The shared responsibility for completion of this program institutes many checks and balances throughout the production process. Because of the control exercised at the various stages, an error made at one level would be quickly caught at the next before processing could continue.

See Attachment A, "Analysis of the General Control Environment" for a detailed summary of the General Control Environment.

DOCUMENTING AND ANALYZING THE PROCESS

The process was documented by delineating a high level event cycle for the process, (Attachment B). Using the event cycle for guidance, the risks associated with each event were identified in discussions with various headquarters and production personnel associated with the program. This step included analyzing the impact on the event, should the undesirable consequence occur. Once these were defined, it was possible in the next step to estimate the probability associated with each. Various production and staff personnel were interviewed to determine the probability of an undesirable event happening, and the management controls in place to mitigate each risk. The results are included as Attachment C, and a list of personnel and their contribution is at Attachment D.

TESTING

Testing was conducted at headquarters and at the Western Mapping Center in Menlo

Park California. Headquarter's elements are responsible for product standards, overall program direction, and final resolution of the financial agreements between USGS and cooperating agencies. Western Mapping Center (WMC) is in operational control of the program, with an organizational element dedicated to conducting the day-to-day activities of the program. In support of the contracting process, there are several WMC personnel serving as Contracting Officer's Technical Representatives (COTR); each is assigned primary responsibility for each contractor and a deputy is assigned back up duties. They have also established source evaluation, Quality Control, and product handling units.

Testing was conducted during April and May 1994 by review of existing documentation and record keeping procedures, interviews with staff and production personnel, and observation of production coordination activities. All information gathered is summarized and documented on the attachments included. in this AMCR report.

INVESTIGATIVE RESULTS

As a result of the investigation, the contracted DOQ production program was found to be functioning effectively and efficiently. The possibility of waste, fraud, and abuse is considered to be minimal. There are however some aspects of the process which would benefit from changes in the production procedures:

1. For all cooperative projects, there has always been a potential problem associated with cooperative funding agreements with States. USGS is limited by law to paying only 50% of the costs. Schedule or requirements changes can often result in unanticipated cost increases. The cooperating State then must provide additional funds to meet their hag of the increase. Problems are likely to occur when the State agency has a different fiscal year than the Federal Government, and is unable to readily acquire additional funding. NMD may be required to negotiate a decrease in the size of the project, accepting payment "in-kind" for products or data, or finding a different source of funding in order to avoid violating the 50% provision.

   Recommendation. Much of the uncertainty associated with this program would be eliminated if the source material such as aerial photography, field control, and map separates to be used for the project were to be collected and evaluated prior to making a resource estimate and giving it to the cooperator. A better feel for the quality and completeness of the source would eliminate schedule changes and the need for additional funds to acquire additional control or elevation models. NMD does not provide the resources for this "up front" evaluation, which has been described by several personnel interviewed as part of the cost of doing business. it is recommended that NMD evaluate the utility of available source material prior to entering into cooperative agreements.

2. Because the time required to collect and evaluate the source material (usually about 4 months) must be added to the time necessary to negotiate a contract, it is crucial that firm guidance as to the number of products which can be funded be provided as early as possible. The uncertainty in the level of funding greatly inhibits the ability of program managers to plan and allocate resources for the collection and evaluation of source material. There is a very real possibility that the obligation dates associated with the contracting process may preclude achieving the fiscal year's goals if final production requirements aren't known until near the end of the fiscal year.

Recommendation. To facilitate planning, production personnel have requested a periodic report, preferably monthly, showing the contract dollars remaining for projects. Given the lead times required to assemble and evaluate the source material to be used on a project, the limited number of personnel available, and the fact that the contractor can add another 11 weeks in evaluation and negotiation, this request seems reasonable.

ALTERNATIVE MANAGEMENT CONTROL REVIEW

CONTRACTUALLY PRODUCED DIGITAL ORTHOPHOTO QUADRANGLES

Although no control weaknesses were identified in the management review, two areas in which changes to management procedures or production process would strengthen the program were identified.

NUMBER	OPPORTUNITIES FOR STRENGTHENING PROGRAM	PROPOSED ACTION	COMPLETION SCHEDULE
1	Move source evaluation to an earlier point in the event cycle	Establish a process to facilitate earlier source collection and analysis	Details to be developed during a Government Furnished Materials Technical Exchange Meeting to be held in July 1994
2	Provide more frequent reports on the status of funds available for contract production	Initiate a more frequent reporting cycle to permit more detailed advance planning.	A more specific reporting program will be implemented beginning with the 4th quarter FY 1994

ANALYSIS OF THE GENERAL CONTROL ENVIRONMENT

	N/A	AGREE	UNCERTAIN	DISAGREE	COMMENT
POLICIES AND PROCEDURES					
Are policies and procedures clearly stated in writing and organized in manuals, handbooks, or other?		X			
Are they communicated throughout the assessable unit?		X			
Are they consistent with applicable laws, regulations, and policies prescribed by higher levels?		X			
Are they easy to locate at all times?		X			
PLANNING, BUDGETING, AND REPORTING					
Does the approved budget become the operating plan.		X			
Are plans and budgets effectively communicated throughout the assessable unit?		X			
Are financial reports available for comparison to the budget?		X			
do managers in the assessable unit make the comparison referred to above and initiate corrective action?		X			
Are expenditure reports accurate and timely?		X			
Are reports scanned by higher level management?			X		See note 1

[1] Many reports are provided but it was impossible to ascertain whether all the information reported was used by headquarters management, or just the data needed for a particular application. No activity receiving reports complained about too little data.

ATTACHMENT A

	N/A	AGREE	UNCERTAIN	DISAGREE	COMMENT
DELEGATION OF AUTHORITY AND RESPONSIBILITY					
Do delegations of authority exist in writing?		X			
Do they clearly outline duties, authority, and responsibilities (including any limitations thereof)?		X			
Do they prevent overlapping duplication, and conflicts of duties/authority/responsibility?		X			
Do they grant sufficient authority to carry out the responsibilities?		X			
PERSONNEL PRACTICES					
Is the Standards of Conduct for Federal Employees brought to employees' attention annually?		X			
Does each employee have an accurate up-to-date position description?		X			
Do performance standards include internal control considerations?		X			
In addition to the annual performance appraisal, are there interim appraisals/counseling sessions?		X			
Has there been training on internal controls for supervisor/managers of the assessable unit?			X		See note 2
Are there sufficient training opportunities to improve job competency and to update employees on new policies and procedures?		X			
Are employees held responsible for their performance?		X			

[2] There has been no recent formal training in management control at WMC and some supervisors have been promoted to supervisory roles since the last training session. Additionally several of the trained personnel took advantage of the "early out" window. All employees interviewed seemed to be familiar with the process and concepts. In addition, a brief tutorial was provided as part of the AMCR, to focus the review discussions and orientation. For practical purposes, the tutorial and participation in the review may suffice until a formal training course can be provided.

C:\DOCAMCR\ATCHMNT.A
June 14, 1994

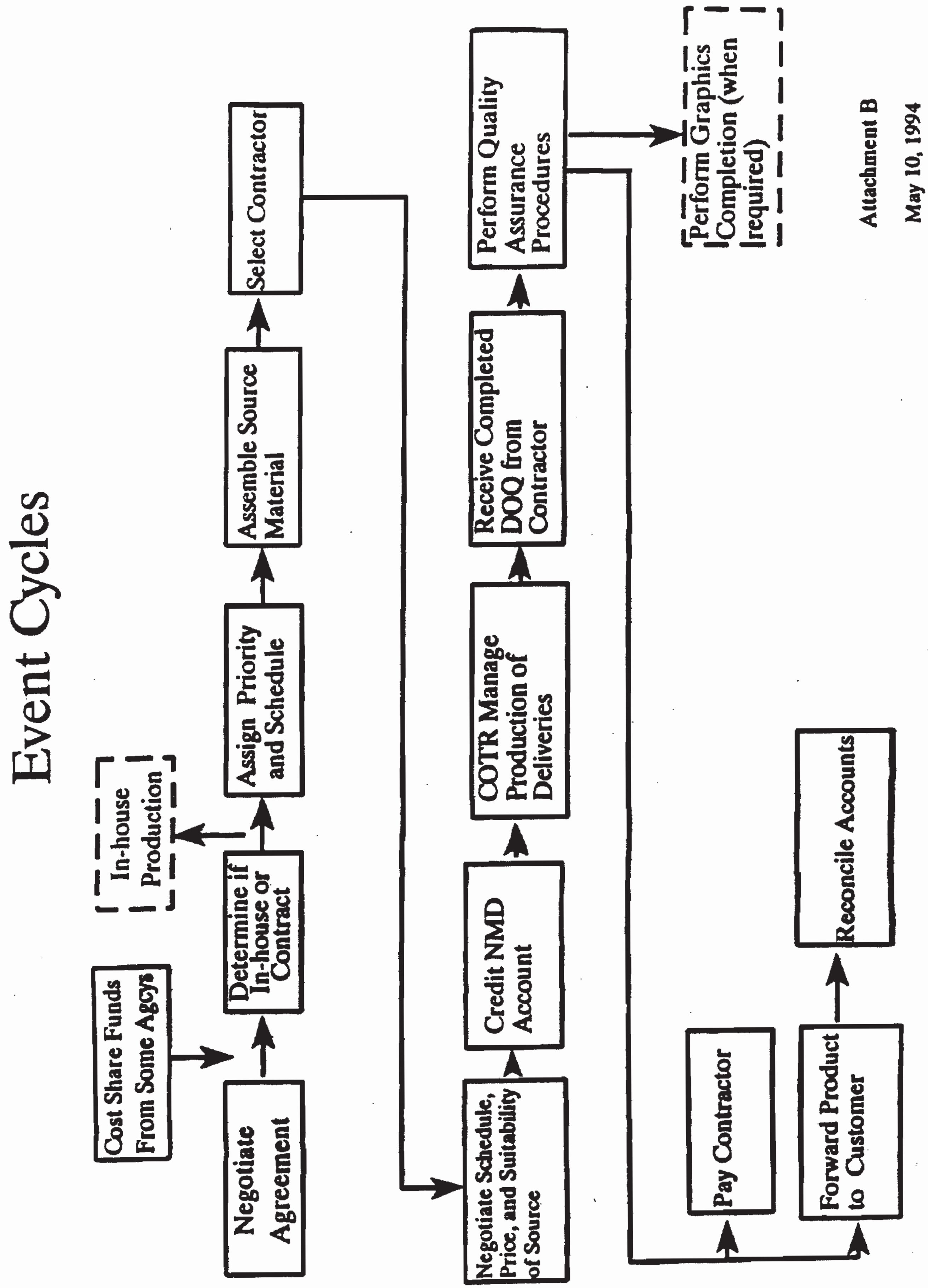
	N/A	AGREE	UNCERTAIN	DISAGREE	COMMENT
MANAGEMENT ATTITUDE AND COMMUNICATION					
Is management of this assessable unit aware of the importance of internal controls as they relate to this unit?		X			
Has management communicated that importance to employees in the assessable unit?		X			
In the past year has management specifically reviewed internal controls to assure they are working?		X			
Does unit management hold regular staff meetings?		X			
Is management receptive to suggestions for changes in operating procedures?		X			
ORGANIZATIONAL CHECK AND BALANCES					
Are contracts or cooperative agreements audited regularly by a third party?		X			
ADP CONSIDERATIONS					
Are security measures in effect which limits the use adp equipment to authorized personnel?	X				
Are published instructions and procedures available to the user or operator of this equipment?	X				
Are controls used to assure that only approved input is accepted in the system?	X				
Are output reports timely and reviewed for correctness?	X				
Are physical security measures present for the protection of the equipment during both office hours and non-office hours?	X				

C:\DOCAMCR\ATCHMNT.A
June 14, 1994

	N/A	AGREE	UNCERTAIN	DISAGREE	COMMENT
ORGANIZATIONAL STRUCTURE					Currently reorganizing
Does the assessable unit have clearly written goals and objectives?		X			
Does the assessable unit have necessary authority to meet those goals/objectives?		X			
Is the assessable unit sufficiently flexible to accommodate changes?		X			
Is the assessable unit held accountable for the results of this operation?		X			
Is the organizational chart current?		X			
Does the organizational structure provide for adequate separation of duties?		X			
Does the organizational structure provide for adequate supervision?		X			

Evaluation of factors derived from interviews and observations with personnel from various locations and levels within the Division, and review of documents and records.

C:\DOCAMCR\ATCHMNT.A
June 14, 1994


Event Cycles
Negotiate Agreement
Cost Share Funds From Some Agcys
Determine if In-house or Contract
In-house Production
Assign Priority and Schedule
Assemble Source Material
Select Contractor
Negotiate Schedule, Price, and Suitability of Source
Credit NMD Account
COTR Manage Production of Deliveries
Receive Completed DOQ from Contractor
Perform Quality Assurance Procedures
Perform Graphics Completion (when required)
Pay Contractor
Forward Product to Customer
Reconcile Accounts
Attachment B
May 10, 1994

ALTERNATIVE MANAGEMENT CONTROL REVIEW

WORKSHEET FOR DOCUMENTATION OR EVENT CYCLES, RISK, RISK SCALE IMPACT AUTHORITY, AND CONTROL TECHNIQUES

COMPONENT: NMD PRODUCTION OPERATIONS OFFICE

1. Agreement made with cooperating agency.

RISKS	RISK SCALE	IMPACT	TESTING*	CONTROL TECHNIQUES
A. Agreement over-extends production resources available to NMD.	Low	Deadlines not met or adversely impact another program's funding.	a. D/I b. D/I c. D/I d. D/I e. D/I	a. NMD Policy on State Joint funding Agreements (Jan 1989). b. NMD Policy on Funding of Reimbursable Production Programs/ Approval of Agreement (June 1991). c. Policy on Work Share Agreements (July 1992). d. Policies and Guidelines on Agreements (Feb 1993). e. Cost Estimates for Reimbursable and/or Work Share Agreements (May 1993).
B. Establishes unreasonable schedule or delivery requirements that cannot be logically met by NMD.	Low	NMD required to shift production priorities for other work or risk causing cooperator to miss scheduled deadlines.	a. D/I b. I	a. Documentation listed above plus several levels of management review of proposed agreement would forestall. b. Generally will not enter into the kind of arrangement calling for specific delivery dates.
C. Establishes inappropriate or unauthorized cost share or work share agreements.	Low	Violates statutory funding guideline. Slows process when discrepancy discovered.	a. D/I	a. Guidelines in place handle standard requirements. (A, a-e) Custom products or inaccurate estimates are adjusted after the true costs are known.
D. Establishes agreement that obligates cooperator to conditions that cannot be met because of subsequent budgetary cuts or cost overruns.	Medium	NMD share of costs goes up which violates statutory funding requirements. Alternatively State has to provide additional funds or agree to less work.	a. I b. I/O	a. NMD gaining experience with process and refining estimating procedures for costs involved with QA/QC and bringing new contractors up to acceptable productivity levels. b. Production process being subjected to more intensive standardization as experience is gained.

2. Assign priority and schedule

RISKS	RISK SCALE	IMPACT	TESTING*	CONTROL TECHNIQUES
A. Production schedule and priority do not reflect conditions necessary to meet delivery schedule.	Low	Early delivery wastes production resources which could be used for higher priority items. Late delivery may violate agreement or shift delivery into time frame where funds are no longer available from cooperator.	a. I/D	a. 14-18 month completion time used for estimates is realistic. Supported by production records.

3. Assemble Source Material

RISKS	RISK SCALE	IMPACT	TESTING*	CONTROL TECHNIQUES
A. Required source material not available.	Medium	Source Collection activity delays production and stretches out schedule. May result in higher cost than estimated if contractor has to provide additional work.	a. I b. I	a. Negotiations with contractors not started until source package complete. b. Higher costs, alternative delivery schedules or project areas negotiated with cooperator prior to starting work.
B. Previously scheduled source collection activities are not completed when expected.	Low - Medium	Production schedule delayed until source collection complete. May negate plans. Must negotiate new schedule with customer.	a. I/D	a. Condition usually occurs when weather precludes completion of serial photography or control. Either can delay completion of control analysis. To date, schedule adjustments have been possible to accommodate customer needs. Documented in Memo For Records "Factors that contribute to long turnaround time in the acquisition of Government Furnished Photography for the DOQ Contract", dated Apr 21, 1994.

C. Quality of existing or new source does not meet requirements.	Low	Use unsatisfactory material with quality of finished product suspect, or upgrade/recollect source. May impact schedule if prod. Ctr. has to upgrade or if contractor has to upgrade or replace.	a. I	a. Experience shows that except in rare cases source quality is satisfactory or there is enough time to modify existing or collect new source.
D. Poor quality source may result in unacceptable deliverable.	Low	May fail QC. May have to pay contractor for unacceptable product if use of source mandated by NMD	a. I	a. Quality of source established and documented prior to delivery to contractor. On rare occasions when questionable source must be used, the judgement as to whether the delivery schedule and estimated product quality takes priority over time to acquire additional source is made and approved by NMD management.

4. Select Contractor

RISKS	RISK SCALE	IMPACT	TESTING*	CONTROL TECHNIQUES
A. Signs inappropriate award under pre-negotiated contract.	Not considered possible	May not be able to hold contractor to delivery schedules or quality standards.	a. I	a. Given checks and balances currently employed, contractor is very closely scrutinized. In addition to forms 254 and 255 which contractor must keep current, the COTR periodically visits the production site and evaluates procedures and personnel.
B. Contractor overextended/ unrealistically optimistic about capabilities	Low	Delivery late due to scheduling conflicts.	a. I/D	a. Correspondence chain and record of past performances are used to monitor contractor capability.
C. Contractor does not have appropriately trained personnel or uses inappropriate technology	Low	Quality of product suffers or delivery late.	a. I	a. Contractor's facility and production procedures, including personnel are evaluated as part of certification process. Contractor then required by law to keep CO informed of changes by means of Forms 254 and 225 listing changes in equipment or personnel. COTR periodically evaluates to ensure that procedures are being followed. Change in performance or quality of product would also be noticed by COTR or QA personnel.

5. Negotiate schedule. Price and suitability of source.

RISKS	RISK SCALE	IMPACT	TESTING*	CONTROL TECHNIQUES
A. Can't reach accord with contractor.	Low-Medium	Affects schedule. May lose contract or COOP funds.	a. I/O	a. Source suitability is no longer an issue given recently developed evaluation techniques. Additionally the capabilities and costing standards for each process used by contractors are generally well known by the NMD staff.

6. Credit NMD account with estimated cost

RISKS	RISK SCALE	IMPACT	TESTING*	CONTROL TECHNIQUES
A. Amount billed is more or less than negotiated in agreement.	Low-Medium	Statutory requirements may be compromised. Funds may not be available for other projects.	a. I	a. With more data NMD personnel are developing better cost averages and estimating criteria, which will reduce risk. If procedures changed to allow source collection and evaluation prior to estimating cost much more accurate estimates and schedules could be provided.

7. Manage Production of Deliverables

RISKS	RISK SCALE	IMPACT	TESTING*	CONTROL TECHNIQUES
A. Possible incremental payment before production complete.	Not considered possible	Relives contractor of need for prompt delivery.	a. I/O	a. Given checks and balances currently employed, contractor is closely scrutinized by the COTR. Weekly production status reports are required and coordinated with other COTRs and the CO staff.
B. Schedule adjustments in response to changing requirements may not be effectively communicated.	Low	May require cost adjustments or cause conflicts in schedules.	a. I	a. Procedures require review of modified delivery schedules which would disclose problems. Cost changes must be negotiated before work is permitted to commence.
C. Response to technical questions from contractor late or incomplete.	Low - Medium	Wrong information may result in inaccurate or incomplete product.	a. I/O	a. All technical questions and responses are recorded and the response reviewed by Chief, Contractor Management Section. Also reviewed by COTR committee.

D. Negligent COTR does not maintain adequate records or insufficient contact with contractor	Low	Delivery schedule or quality of product suffers.	a. I/O/D	a. Weekly CO/COTR meeting would drive out discrepancy between expected performance and actual progress, and COTR's knowledge of current status.

8. Receive completed DOQ from contractor

RISKS	RISK SCALE	IMPACT	TESTING*	CONTROL TECHNIQUES
A. Completed DOQ late	Low	Schedule met. May influence availability of cooperators funds. Internal funds not available next FY	a. I	a. Schedule well defined monitored by COTR. b. Funds available in advance. Only problem may be if agreed cost exceeded and additional resources are not available form cooperator.
B. Job incomplete or damage in transit	Low	Schedule not met. May require rework.	a. I	a. If minor discrepancies on product are found, they are returned to contractor for correction. If major problems are found, products are formally rejected by letter from CO and must be completely reworked by contractor. Close attention by COTR precludes most problems.
C. Source material not returned or damaged	Low	Source material not available for subsequent QC activities. Delay while source solicited from contractor.	a. I/D	a. This has not happened to date but is considered a possibility. Each piece of source is valued prior to being forwarded to contractor. Part of contract is that contractor will replace lost or damaged source.

9. Preform quality assurance/quality control procedure

RISKS	RISK SCALE	IMPACT	TESTING*	CONTROL TECHNIQUES
A. Assigning the wrong level of QC with respect to the capabilities of the contractor.	Low	Too stringent QA/QC procedures may delay throughout and delivery to customer. Too lax control procedures may allow poor quality DOQ to be accepted and paid for.	a. I b. D	a. Each delivery individually evaluated for appropriate QA based on complexity of job and known capabilities of contractors. b. Draft QA procedures manual completed and disseminated for use.

10. Pay Contractor

RISKS	RISK SCALE	IMPACT	TESTING*	CONTROL TECHNIQUES
A. Contractor paid for work not done.	None to Low	Government has to initiate cost recovery activities when situation discovered.	a. I	a. COTR signs invoice only after work completed and passed through QC procedures. Many personnel looking at progress throughout production cycle and status reported at weekly CO/COTR meetings.
B. Contractor paid early or late.	Low	Government cost accounting procedures are disrupted. May incur penalty for late payment.	a. I	a. Early payment extremely unlikely, see above. Late payment also unlikely because COTR or designated alternate ensures that job leaves production area in a timely manner and invoices are accounted for.

11. Forward product to cooperator

RISKS	RISK SCALE	IMPACT	TESTING*	CONTROL TECHNIQUES
A. Shipped Late	Low	May adversely impact customer's schedule.	a. I	a. Mapping Center has established a special unit responsible for receiving products from contractor and shipping to customer when QC complete.
B. Lost or damaged in transit	Low	Product needs to be regenerated at cost of additional time and resources.	a. I	a. Has not happened in past although there is slight possibility. Back up of all digital data forwarded maintained in production center until customer acknowledges receipt. Most digital data also forwarded to MAC for inclusion in the NDCDB.

12. Reconcile accounts

RISKS	RISK SCALE	IMPACT	TESTING*	CONTROL TECHNIQUES
A. Accounts are not reconciled or funds are applied to inappropriate accounts	None to Low	May have to return funds for products not received.	a. I	a. Each contract draws on individual project account which is set up and approved at various levels throughout the mapping center and the headquarters organizations. No work is authorized or invoice paid without appropriate approvals and reference to established accounts.

B. Actual costs are less than estimated.	Low	Negotiated with customer for additional services or products to be provided by NMD to make up difference.	a. I	a. As estimating techniques have improved, the risk of this happening is reduced. In the event that it should occur, most tasks are parts of continuing projects to which the resources could be applied with the customers approval.
C. Actual costs exceed estimates Cooperator can provide difference	Medium	Negotiate with customer for additional funds	a. I	a. Changing requirements on the part of the customer or quality or availability of source material may require modification of the contract to increase the cost. In most cases details are known far enough in advance to preclude adverse consequences. In some cases the scope of the work can be reduced if additional funds from the cooperator are not expected to be available.
D. Actual costs exceed estimates. Cooperator may not have funds to pay 50 % of difference between estimated and actual costs.	Medium	NMD pays more than 50% statutory requirement for matching funds compromised. Funds taken from other in house programs to make up difference.	a. I	a. This happens only when cooperator is unable to produce additional funds which were expected to be available. Because much of the uncertainty derives from the quality of the source material which is projected to be available, the risk could be decreased significantly if the production process could be adjusted to allow the source material to be evaluated for accuracy and completeness before cost estimates are prepared.

*TESTING

D Document Analysis – reviewing existing records, completed forms, or other documentation.

O Observation – watching the performance of specific control techniques.

I Interview – eliciting information from the personnel who perform the control technique.

S A M P L E

PRIORITY RATING WORKSHEET

(UPDATING THE MANGEMENT CONTROL PLAN)

COMPONENT TITLE : ____

CURRENT REVIEW PRIORITY RATING: High _______ Medium _______ Low _______

LAST REVIEW: TYPE: MCR _______ AMCR _______ YEAR _______

REPORTED AS CURRENT MATERIAL WEAKNESS? YES _______ NO _______
(If yes, rating is high)

LIST ANY SIGNIFICANT WEAKNESSES CORRECTED SINCE LAST REVIEW.

LIST ANY SIGNIFICANT UNCORRECTED WEAKNESSES.

LIST ANY AUDITS/STUDIES CONDUCTED SINCE LAST REVIEW ALONG WITH ANY SIGNIFICANT RECOMMENDATIONS.

LIST ANY WEAKNESSES/PROBLEMS NOT PREVIOUSLY IDENTIFIED.

EXPLAIN ANY SIGNIFICANT INCREASE/DECREASE IN BUDGET.

EXPLAIN ANY SIGNIFICANT ORGANIZATIONAL CHANGES.

SUMMARY OF THE RATIONALE/DECISIONS SUPPORTING NEW PRIORITY RATING.

DATE, LOCATION, AND ATTENDEES OF MANAGEMENT CONTROL PLANNING MEETING.

NEW PRIORITY RISK RATING: HIGH _______ MEDIUM _______ LOW _______

PLANNED REVIEW: TYPE MCR _______ AMCR _______ YEAR _______

WORKSHEET FOR
ANALYSIS OF GENERAL CONTROL ENVIRONMENT
COMPONENT - ____________________
FY ______

FACTOR	QUESTIONS	RESPONSE		COMMENTS
		YES	NO	
A. Organization	1. Does/do the organizational unit(s) operating the component have a. clearly written goals and objectives? b. authority and responsibility to pursue the goals and objectives ?			
	2. Is/are the organization unit(s) operating the component a. sufficiently flexible to accommodate changes? b. held accountable for resources entrusted to it? c. held accountable for the results of its operations?			
B. Delegation of Authority	1. Do delegations of authority a. exist in writing? b. clearly delineate duties and responsibilities? c. prevent overlapping, duplication, and conflicts of duties and responsibilities? d. grant sufficient authority to officials to carry out their responsibilities? e. divide responsibility so that no single official controls all phases of a critical transaction?			

WORKSHEET FOR
ANALYSIS OF GENERAL CONTROL ENVIRONMENT
COMPONENT - ____________________
FY ______

C. Policies and Procedure	1. Are policies and procedures a. clearly stated in writing and systematically organized in manuals, handbooks or other publications? b. systematically communicated throughout the organization? c. consistent with applicable laws, regulations, and policies prescribed by higher levels? d. simple and easy to understand? e. structured to avoid overlap, confusion, conflict, or duplication? f. revised and updated as necessary? g. flexible enough to allow routine handling of unusual events? h. structured to provide for adequate separation of duties?		
D. Personnel	1. Do personnel practices include a. a code of conduct? b. provisions for conflict of interest disclosures? c. accurate and up-to-date position descriptions? d. periodic performance review (appraisal) of all employees? e. a reward system based on performance? f. sufficient training opportunities to improve competency and update employees on new policies and		

WORKSHEET FOR
ANALYSIS OF GENERAL CONTROL ENVIRONMENT
COMPONENT - ____________________
FY ______

	procedures?		
______ ______ ______ ______ ______ E. Planning, Budgeting and Accounting	1. Is there a long-range planning process? 2. Is the budgeting system integrated with the planning process? 3. Is the accounting system integrated with the budgeting system? 4. Are plans and budgets effectively communicated throughout the organization? 5. Does the approved budget become the operating plan and the standard against which performance can be measured? 6. Are there clearly established levels of operational and financial accountability?		
______ ______ ______ F. Reporting	1. Are reports made in accordance with assigned responsibilities? 2. Are individuals or units required to report only on those matters within their control? 3. Do progress or performance reports show comparisons with a. planned performance? b. budget allowances? c. past performance?		

WORKSHEET FOR
ANALYSIS OF GENERAL CONTROL ENVIRONMENT
COMPONENT - ____________________
FY ______

	4. Are reports a. relevant? b. timely? c. accurate? d. distributed to appropriate levels?		

SUMMARY OF
ANALYSIS OF GENERAL CONTROL ENVIRONMENT
COMPONENT - ____________________
FY ______

FACTORS	ANALYSIS SATISFACTORY	ANALYSIS UNSATISFACTORY	COMMENTS
A. Organization			
B. Delegation of Authority			
C. Policies and Procedures			
D. Personnel			
E. Planning, Budgeting, and Accounting			
F. Reporting			

IDENTIFYING RISKS
COMPONENT - ____________

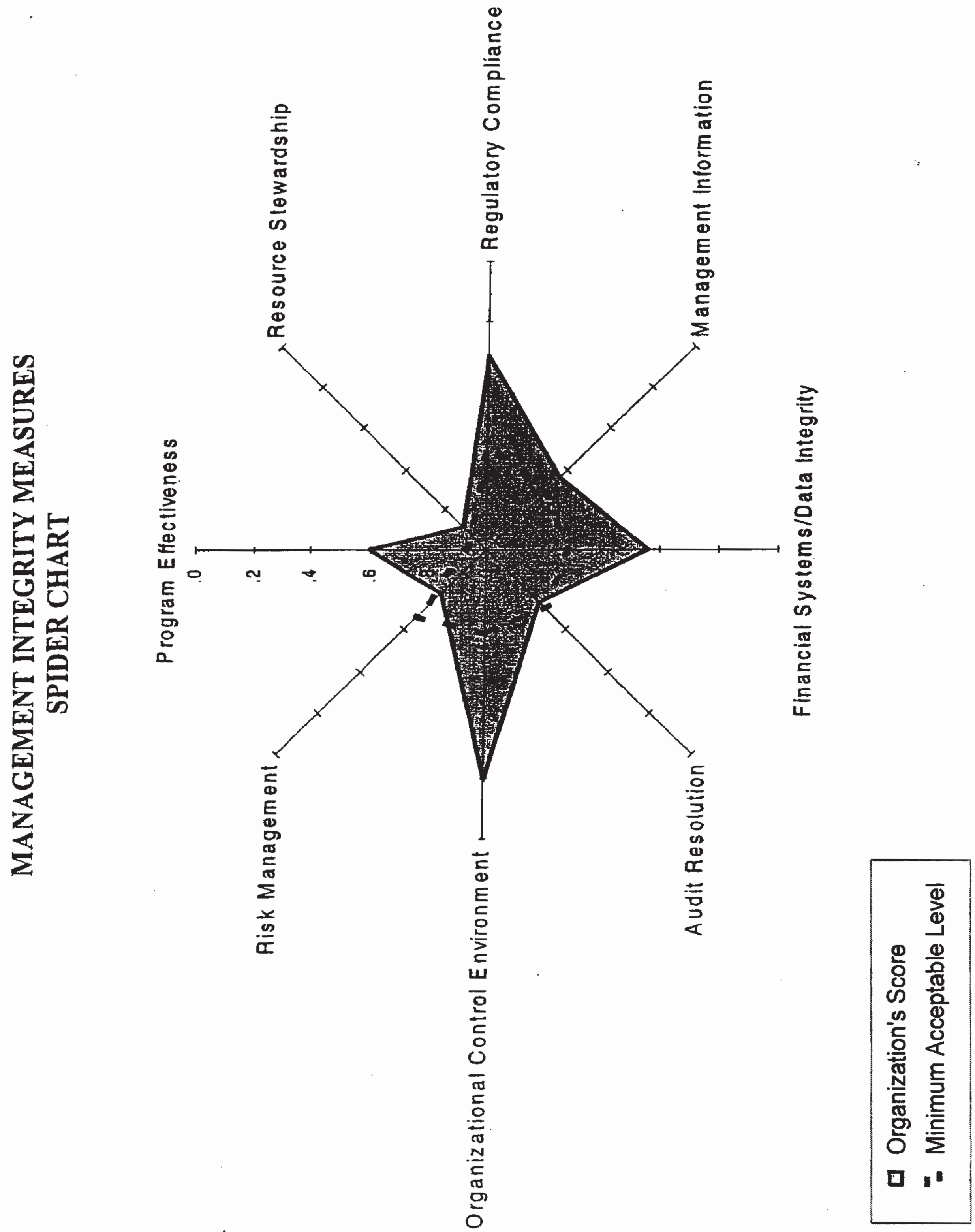
What is the component's objective?

	CHANCE			IMPACT		
WHAT COULD GO WRONG?	**HIGH**	**MED**	**LOW**	**HIGH**	**MED**	**LOW**
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						

ALTERNATIVE MANAGEMENT CONTROL REVIEW

WORKSHEET FOR DOCUMENTATION OF: RISKS, CONTROL OBJECTIVES, CONTROL TECHNIQUES, TESTING, AND FINDINGS

			TESTING					CONTROL			
RISK	CONTROL OBJECTIVE	CONTROL TECHNIQUES	DOCUMENT	TRANS. TEST'G	OBSERVATION	INTERVIEW	OTHER	ADEQUATE	WEAK	EXCESSIVE	FINDING/ COMMENTS


MANAGEMENT INTEGRITY MEASURES
SPIDER CHART
Program Effectiveness
Resource Stewardship
Regulatory Compliance
Management Information
Financial Systems/Data Integrity
Audit Resolution
Organizational Control Environment
Risk Management
0
.2
.4
.6
Organization's Score
Minimum Acceptable Level

OVERVIEW

FY 2000 Departmental Management Control Assessment – SMARTPAY (CHARGE CARD) PROGRAM

BACKGROUND

You have been selected by the Office of Acquisition and Property Management (PAM) and the Office of Financial Management (PFM) to participate in an automated management control assessment of the Department's SMARTPAY (Charge Card) Program. The sample of Departmental employees selected to participate in this assessment include Cardholders, Agency/Organization Program Coordinators (A/OPC's), Reviewing Officials, Finance Officers staff and Fleet Management staff. This automated assessment approach has been pilot tested for other management control assessments in all bureaus over the last 2 years. It has been found to be an efficient and easy to use assessment alternative.

This assessment questionnaire pertains to FINANCE OFFICE STAFF only. You will be asked to respond to a series of multiple-choice statements about management controls in several areas of the SMARTPAY Program. Your response to the assessment questionnaire should take approximately 1 hour or less to complete. You will also be given an option to provide any narrative comments you wish to offer about your experience with the SMARTPAY Program management controls.

By responding to this questionnaire, you will assist PAM and PFM in performing an initial assessment of the existence and effectiveness of management controls in the SMARTPAY Program, and whether the controls meet the objectives and guidelines prescribed by the Office of Management and Budget (OMB) in Circular A-123, Management Accountability and Control, and Department management control guidance. The results of this assessment will be used to improve management controls in the SMARTPAY Program and to support conclusions in the Department's FY 2000 Annual Management Control Assurance Statement. Therefore, it is important that you take sufficient time to provide accurate and complete responses. All participants will be expected to submit their response to the questionnaire no later than July 31, 2000.

The responses to the assessment questionnaire will be compiled, and diagnostic reports will be produced using an existing software tool designed specifically for the Department's management control program. The results are expected to identify any potential material deficiencies in the controls which will be subject to further review, analysis and validation by PFM and PAM. The summary results of this assessment will be posted on the PFM web-site for your review and inspection by the end of FY 2000.

PAM and PFM want to assure participants that their responses to the assessment questionnaire will be maintained on a confidential basis throughout the assessment process. At the completion of the assessment process, all participant responses will be deleted from the PFM/PAM assessment data base.

ABOUT THE QUESTIONNAIRE

You will be asked to respond to each question by selecting one (1) of six (6) possible multiple choice answers. The six multiple choices for your answer to each question are:

1. Strongly Disagree
2. Disagree
3. Agree
4. Strongly Agree
5. Don't Know; and
6. Not Applicable

Completing the questionnaire can be accomplished by an easy "Point and Click" response. Use your PC mouse to point and click the answer you select for each question. After you have responded to all of the questions (including any voluntary narrative comments you wish to add), please click on the "Submit" button at the end of the questionnaire to forward your response to PFM.

If you have any questions or concerns regarding this survey, please contact either Pete Horsley (PAM) at (202) 208-3347 or Wayne Howard (PFM) at (202) 208-4701.

Section 1 - Purchase Process

NOTE

Issuance of Charge Card with Purchase Authority

Written policies and procedures covering purchase card use (eligibility, use of card, record keeping, etc.) are in place.

- ❏ Strongly Disagree
- ❏ Disagree
- ❏ Agree
- ❏ Strongly Agree
- ❏ Don't Know
- ❏ Not Applicable

Cardholders report individually billed charges that should have been billed to a centrally billed account when they review their statement.

- ❏ Strongly Disagree
- ❏ Disagree
- ❏ Agree
- ❏ Strongly Agree
- ❏ Don't Know
- ❏ Not Applicable

Finance office reviews identify centrally billed charges that should have been individually billed.

- ❏ Strongly Disagree
- ❏ Disagree
- ❏ Agree
- ❏ Strongly Agree
- ❏ Don't Know
- ❏ Not Applicable

NOTE

Cardholder Usage

Finance office staff perform reviews of user purchase documentation to verify validity of purchases.

- ❏ Strongly Disagree
- ❏ Disagree
- ❏ Agree
- ❏ Strongly Agree
- ❏ Don't Know
- ❏ Not Applicable

The Finance office staff routinely select Bank of America statements to review for improper and unauthorized purchases.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Receipt of Transaction Files from Bank of America

An electronic edit is performed on bureau invoices to compare invoice total with detailed transaction total balance.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Payment of Bank of America Invoice

A post payment review is performed on an invoice payment to determine that the proper and correct amount is paid.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

A financial system status of funds, or equivalent report, is used to monitor purchase expenses.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Review of Transaction Data

Monthly card program reports are reviewed and adjustments, allocations, and reallocation of costs are performed.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

A policy is in place for reviewing card transactions for proper charges, misuse, accounting code, BOC, and comparing charges on statements with receipts maintained by user on a sample basis.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

There are written Bureau policies and procedures for identification and posting of adjustments between administrative and program offices.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

Timely action is taken to correct the erroroneous purchase transaction data.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

Section 2 - Convenience Check Process

NOTE

Issuance of Convenience Checks

There are written Bureau policies and procedures covering the issuance and use of convenience checks.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

All employees issued convenience checks are trained on related policies, procedures, and procurement regulations.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

The convenience check supply is located in a secure location.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Checkwriter Usage

A review of check documentation as outlined in written policies and procedures is performed to verify validity of check transactions.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

A periodic review of check supply, check register, documentation supporting issuance of the checks, and adherence to regulations is conducted.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Charge Billed to Bureau by Bank of America

A review of check transactions is done at a designated organizational level.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

An accounting system cardholder transaction report, or equivalent, is compared to selected cardholder transactions.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

An electronic edit is performed of bureau card program invoices to compare invoice total with detailed transaction total balance.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Receipt of Transactions File from Bank of America

There are written policies and procedures to control the completeness of transaction data.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Payment of Bank of America Invoice

There is a post payment review of card program invoice payments to determine that the proper and correct amount is paid.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

A financial system status of funds, or equivalent report, is reviewed to monitor convenience check expenses.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

There are written Bureau policies and procedures to control the timely processing of payments.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Review of Transaction Data

Monthly financial reports are reviewed, and adjustments, allocations, and reallocation of costs are made.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

Written policies and procedures include identification and posting of adjustments between administrative and program offices.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

Section 3 - Travel Process

NOTE

Issuance of Credit Card

The Bureau has written policies and procedures covering the government charge card for travel (eligibility for travel card, use of card, statement review, record maintenance, etc.).

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Cardholder Usage for Travel Related Expenses: Transportation, Rental Vehicles, Lodging Expenses, and ATM Withdrawal

User travel charges are reviewed to verify the validity of tickets purchased.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

There are travel policies and procedures established to require use of the government charge card to obtain tickets for official travel.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

Voucher examination can disclose use of other than government economy/coach class tickets.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

Card statements are reviewed for improper and unauthorized ticket purchases.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

Rental vehicle charges are validated by review officials.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

The traveler is required to use their Bank of America government charge card to obtain a rental vehicle for official travel.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

Card transactions are reviewed to ensure proper and authorized vehicle use.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

Cardholder transactions and receipts for rental vehicle and insurance charges are verified.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

The travel voucher is reviewed for rental vehicle receipts to verify rental dates and insurance charges.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

User lodging expenses are reviewed to verify the validity of the charges.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

The traveler is required to use a Bank of America government charge card to obtain lodging for official travel.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

EAGLS on-line transactions are reviewed for improper and unauthorized lodging charges.

- ☐ Strongly Disagree
- ☐ Disagree
- ☐ Agree
- ☐ Strongly Agree
- ☐ Don't Know
- ☐ Not Applicable

The travel voucher is reviewed for lodging receipts to verify lodging expenses and to identify unauthorized lodging charges.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

Travel charges are reviewed to verify validity of ATM withdrawals.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

EAGLS exception reports are used to monitor authorized ATM withdrawals.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Charge billed to Bureau by Bank of America

The accounting system review of reports of transactions is at a designated organizational level.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

An accounting system cardholder transaction report, or equivalent, is compared to selected cardholder statements.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

An electronic edit is performed of card invoices to compare invoice total with detailed transaction total balance.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Receipt of Transaction File from Bank of America

An electronic edit is performed of bureau centrally billed invoices to compare invoice totals with detailed transaction total balance.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

There are written policies and procedures for individuals to follow to assess the completeness of transaction data.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Payment of Bank of America Invoice

There is a post payment review of invoice payment to determine that the proper and correct amount is paid.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

A status of funds reports, or equivalent, is used to monitor travel expenses.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

There are written policies and procedures to control the timely processing of payments.
- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Review of Transaction Data

There are regular periodic reviews of travel transactions.
- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

Adjustments, allocations, and reallocation of costs are performed after the travel transaction review.
- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

There is a card transaction review for proper travel charges, misuse, accounting code, BOC, and charges comparing the statement with receipts maintained by users on a sample basis.
- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

Written policies and procedures include identification and posting of adjustments between administrative and program offices.
- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

Section 4 - Fleet Process

NOTE

Fleet Credit Card Usage

Random reviews of fleet purchase receipts are performed to verify the validity of purchases.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

Monthly reports are reviewed for transaction details.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Receipt of Transactions File from Bank of America

An electronic edit is performed of bureau centrally billed invoices to compare invoice totals with detailed transaction total balance.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

There are written policies and procedures to control the completeness of transaction data.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Payment of Bank of America for fleet transactions

There is a post payment review of invoice payments to determine that the proper and correct amount is paid.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

A financial system status of funds report, or equivalent is used to monitor fleet expenses.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

There are written policies and procedures to control the timely processing of payments.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

NOTE

Review of Transaction Data

There are regular periodic reviews of fleet transactions.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

After fleet transaction review, adjustments, allocations, and reallocations of costs are performed.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

There is a review of selected fleet credit card statements for proper charges, misuse, accounting code, BOC, and to compare charges on statements with receipts maintained by the user.

- ❑ Strongly Disagree
- ❑ Disagree
- ❑ Agree
- ❑ Strongly Agree
- ❑ Don't Know
- ❑ Not Applicable

Department of the Interior
Departmental Manual

Effective Date: 8/2/04
Series: Financial Management
Part 330: General
Chapter 1: Issuance of Instructions

Originating Office: Office of Financial Management

330 DM 1

1.1 **Purpose.** The Chief Financial Officers Act of 1990 requires that the Departmental Chief Financial Officer (CFO) issue financial policies and accounting standards for the Department of Interior (DOI). This chapter describes the objectives of the financial policies and accounting standards, provides references to the handbooks and documents that contain these guidelines, and establishes the responsibility for maintenance of this series.

1.2 **Objectives of Financial Policies and Accounting Standards.**

A. Standardize DOI financial data and provide for intra-bureau and office data interchange.

B. Streamline processes for recording financial events and reporting financial information.

C. Enable bureaus and offices to apply common standards while providing flexibility to satisfy unique needs.

D. Promote uniform accounting processes to aid entities in implementing the Department's accounting systems.

E. Increase the reliability and consistency of financial information in DOI.

1.3 **DOI Financial Policies and Accounting Standards.** DOI financial policies and accounting standards are contained in the following documents and can be accessed at www.doi.gov/pfm/policy.html**.**

A. Department of Interior Accounting Handbook is the official presentation and interpretation of the financial management-related laws, regulations, and policies issued by authoritative bodies to ensure their consistent application both in recording and reporting transactions throughout the Department. This Handbook provides bureaus and offices with a single, definitive source for Department-wide standards for financial policies and accounting standards.

B. Cash Management Handbook describes the regulations governing the administration of cash held outside the U.S. Treasury, i.e., cash under the direct control and custody of DOI employees. The objectives provide for uniformity in the administration and accountability of funds; lessen the vulnerability of loss or misuse of cash funds; and promote good cash management practices.

C. Credit and Debt Management Handbook provides guidance to bureaus and offices to ensure that consistent credit and debt management practices are established and followed throughout the Department.

D. Department of Interior Interagency Acquisitions Handbook applies to agreements between governmental departments (agencies) and between bureaus and offices within DOI. It assigns responsibilities and establishes general policies and procedures for the preparation, review, clearance, approval, monitoring, and closing of these agreements. This is issued in coordination with the Office of Acquisition and Property Management.

E. Department of Interior Guidance on Preparing Financial Statements provides Departmental guidance for preparing and publishing the bureau and offices and the Departmental Annual Reports on Performance and Accountability.

F. Travel Policy guidance is contained in 347 DM 1.

G. Department of Interior Real Property Financial Management Policy Guide provides the DOI real property accounting policies and procedures developed in accordance with Federal Property Management Regulations (FPMR) and Statements of Federal Financial Accounting Standards (SFFAS). These policies are provided to ensure effective financial control over DOI owned and leased real property. This is issued in coordination with the Office of Acquisition and Property Management.

H. Management Control and Audit Follow-up Handbook provides a reference tool to assist Department managers, management control coordinators, and audit liaison officers who are responsible for or carry out responsibilities in the Management Control Program and/or the Audit Follow-up Program.

I. Financial Administration Memoranda (FAM) are issued by the Department and implement regulatory agency directives of a routine or technical nature.

1.4 **Policy Development and Maintenance.** The Office of Financial Management (PFM) directs and leads a policy development and maintenance process. The process is inclusive of PFM; the Budget Office; and all bureau CFOs; and Finance, Budget and Program officers. It provides for regularly scheduled as well as unscheduled quick response policy decisions and maintenance. The process also allows for maintenance of a list of unresolved issues. The policy process is described below:

A. Policy Development Process. A collaborative team approach will be used to prioritize, research, and develop financial and accounting policy. Representatives from the bureaus and offices will comprise the teams. When the subject matter is program related, bureau and office program representatives will be consulted or incorporated into the policy development effort. Annually, in January, the Finance Officers Partnership (FOP) will identify policy issues, prioritize the issues, assign duties, and set due dates for development. PFM may identify additional policy issues throughout the year. The level of bureau and office involvement will depend upon the complexity, scope, and urgency of an issue and may require PFM to issue policy without using the collaborative team approach. When the circumstances and subject matter warrant, a formal team may be established to write the draft policy.

B. Review. The bureaus and offices will review the draft policy and comment within 30 days. At the end of the review period, a collaborative meeting of the FOP, if required, will be set to discuss the recommended changes and to finalize the policy document.

C. Issuance of Handbooks. The Director, PFM issues financial management handbooks as appropriate to supplement policy in the DM. The DOI financial management handbooks are on line on the Office of Financial Management website at www.doi.gov/pfm/policy.html**.** Amendments to the handbooks will be transmitted by email using a sequential transmittal number and current date and incorporated into the handbook. The last transmittal number will be referenced with the handbook.

8/2/04 #3635
Replaces 8/5/88 #2805

Department of the Interior
Departmental Manual

Effective Date: 8/2/04
Series: Financial Management
Part 340: Management Accountability and Control
Chapter 1: General Policy and Responsibilities

Originating Office: Office of Financial Management

---

340 DM 1

1.1 **Purpose**.

A. This Chapter provides Department of Interior (DOI) policy and responsibility for bureaus and offices in complying with the Federal Managers' Financial Integrity Act of 1982 (FMFIA) (P.L. 97-255 (31 U.S.C. Secs. 1105, 1106, 1108, 1113, 3512)) http://www.ustreas.gov/offices/management/dcfo/management-controls/fmfia-legislation.pdf. This policy is designed to assist bureaus and offices in improving the accountability and effectiveness of their programs and operations management controls. The major focus of the policy is the establishment, assessment, correction, and reporting on management controls. The procedure to implement this policy is contained in the Management Control and Audit Follow-up Handbook at http://www.doi.gov/pfm/mgmtcont.html. Bureaus have the discretion, where necessary, to supplement this policy guidance by developing additional bureau-specific instructions for use within the bureau.

B. Policy provided in this Chapter is intended to serve as a general framework for the Department's Management Control Program for which the Office of Financial Management (PFM) will periodically issue additional specific guidance.

1.2 **Scope.** All bureaus and offices with program and functional activities are to comply with this policy, except offices whose primary function is the issuance of policy. Instruction for administrative control of funds is contained 328 DM 1-3.

1.3 **Authority and Background.**

A. The Congress, Office of Management and Budget (OMB), and General Accounting Office (GAO) have directed attention to the need for agencies to establish and maintain sound management control systems as a primary means of providing greater accountability, effectiveness and efficiency in achieving program goals and objectives and in preventing fraud, waste, and mismanagement. As a part of daily program and operational management, the Department promotes the continuous monitoring of management controls. This monitoring will facilitate the strengthening of management accountability, as well as the enhancement and improvement of program performance and operations.

B. The FMFIA and OMB Circular A-123 at http://www.omb.gov require the agency head to conduct an ongoing review process of controls and to report annually on the adequacy of agency management and accounting control systems. Under authority provided by the Government Management Reform Act of 1994 (GMRA) (P.L. 103-356) (31 U.S.C. Sec 101, et seq.) http://www.thecre.com/fedlaw/legal1/s2170.htm, the Department's annual assurance on compliance with the FMFIA is incorporated into the Department's Performance and Accountability Report. The Chief Financial Officers (CFO) Act http://www.gao.gov/policy/12_19_4.pdf and Government Performance and Results Act (GPRA) http://www.whitehouse.gov/omb/mgmt-gpra/gplaw2m.html reinforce the need for effective management controls. These Acts also call for the development of program performance indicators to monitor management's success in reaching program goals and desired outcomes. Department managers are to establish environments where management controls are understood, encouraged, practiced, and implemented.

C. Authority. The basic authority for establishing and maintaining agency controls is vested in the Accounting and Auditing Act of 1950 (31 U.S.C. 3512), as amended by the FMFIA. Section 113 of the Accounting and Auditing Act of 1950) http://uscode.house.gov/title_31.htm requires the head of each agency to establish and maintain systems of management controls for all agency programs, organizations, and functions. The Act also stipulates that accounting systems should conform to Federal accounting standards and related requirements. The CFO Act identifies management control related activities as a primary responsibility of the Department's CFO. The following four statutes, two OMB Circulars, and GAO Internal Control Standards were used to prepare this policy:

(1) Federal Managers' Financial Integrity Act of 1982 (P.L. 97-255 (31 U.S.C. Secs. 1105, 1106, 1108, 1113, 3512)) at http://www.ustreas.gov/offices/management/dcfo/management-controls/fmfia-legislation.pdf.

(2) Chief Financial Officers Act of 1990, (P.L. 101-576 (31 U.S.C. Sec. 501; et seq.)) http://www.gao.gov/policy/12_19_4.pdf

(3) Government Performance and Results Act of 1993, (P.L. 103-62 (5 U.S.C. Sec. 306) (31 U.S.C. Secs 1115-1119) (39 U.S.C. 2801-2805) http://www.whitehouse.gov/omb/mgmt-gpra/gplaw2m.html

(4) Federal Financial Management Improvement Act of 1996 (FFMIA), (P.L. 104-208 (31 U.S.C. Sec. 801. et seq..)) http://www.dfas.mil/technology/pal/regs/ffmia.doc.

(5) OMB Circular A-123 Revised, Management Accountability and Control, http://www.whitehouse.gov/omb/circulars/a123/a123.html

(6) OMB Circular A-127 Financial Management Systems, http://www.whitehouse.gov/omb/circulars/a127/a127.html

1.4 **Policy.**

A. General. Bureaus will establish, maintain, evaluate, improve, and report on their systems of program and operational controls. These systems of control should constitute the full range of controls necessary to assist managers in reaching program goals and objectives, and in using Government resources efficiently and effectively. All levels of management will involve themselves in assuring the effectiveness and adequacy of controls. Also, all systems of management and accounting controls will be evaluated on an ongoing basis, and deficiencies, when detected, will be promptly corrected. The results of evaluations must be documented, maintained and made available upon request to the Office of Inspector General (OIG), GAO or the Office of Financial Management (PFM). The procedure to implement this policy is contained in the **Management Control and Audit Follow-up Handbook** available at www.doi.gov/pfm/mac/2003/mgmt_control_handbook.pdf.

B. Control Environment. Each bureau should establish a control-conscious environment. This environment should provide a disciplined atmosphere in which managers are aware of the need to establish systematic controls, monitor their application, and review periodically their effectiveness. The control environment should encourage employee awareness of the existence of controls and their individual responsibilities in the development and implementation of controls.

1.5 Responsibilities.

A. DOI Managers. All managers directing or controlling resources within the Department are responsible for establishing, maintaining, evaluating, improving, and reporting on controls for their assigned areas. Effective execution of management controls requires the utmost coordination and cooperation from all segments of the Department.

B. Management Control and Audit Follow-up Council.

(1) The Department's Management Control and Audit Follow-up Council (Council) comprised of the Assistant Secretary - Policy, Management and Budget/Chief Financial Officer (Chair), Inspector General (ex officio), Solicitor, and Program Assistant Secretaries, is responsible for the following:

(a) overseeing Departmental FMFIA policy and reporting processes,

(b) establishing priorities in the correction and reporting of program and operational material weaknesses and accounting material non-conformances (a material deviation in accounting system design or operation from accepted accounting standards).

(c) ensuring that appropriate funding for correction of the identified material weaknesses and material non-conformances is requested in the budget process, and

(d) emphasizing the early warning of potential management control deficiencies.

(2) The Council meets periodically (usually semiannually) with bureau and office heads to discuss their respective management control program and plans, identification and correction of program and operational material weaknesses and accounting non-conformances.

C. The Assistant Secretary - Policy, Management and Budget/CFO has the primary responsibility for managing the Department's compliance with OMB Circulars A-123 and A-127, the FMFIA, the CFO Act, the FFMIA, and the GPRA.

D. The Office of Financial Management (PFM) is responsible for: (a) providing staff assistance to the Council; (b) recommending management control policies and procedures; (c) providing oversight and guidance to the bureaus concerning the review, evaluation, and maintenance of effective controls; (d) managing, directing, and evaluating the Department's reporting under OMB Circulars A-123 and A-127, the FMFIA, the FFMIA, and the CFO Act.

E. The Office of Acquisition and Property Management (PAM) is responsible for developing and issuing control evaluation guidelines for the acquisition, Federal assistance and property management functional areas; assessing the results of bureau control evaluations in these areas; and providing to PFM annually a summary assessment of the adequacy of bureau controls in these functional areas. PAM is also responsible for overseeing, monitoring, and assessing and recommending for approval to PFM the completion of bureau corrective action plans addressing acquisition and property management material weaknesses.

F. The Office of the Chief Information Officer (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 control evaluations in these areas; and providing to PFM annually a summary assessment of the adequacy of bureau controls in these areas.

G. The Department's Office of Environmental Policy and Compliance, Office of Human Resources, Office of Civil Rights, Office of Budget, and PFM are responsible for issuing guidance to assist bureaus in conducting control evaluations of their respective functional areas.

H. The Office of Planning and Performance Management (PPP) is responsible for developing and issuing guidelines on the preparation of strategic plans, annual performance plans, and annual performance reports. Guidelines include using management control reviews to fulfill GPRA requirements for program evaluations and data verification and validation. PPP also is responsible for review and clearance of GPRA documents prior to publication, and collaborates with PFM on the selection of GPRA goals and measures for the accountability report.

I. The Office of Inspector General (OIG) is responsible for performing routine evaluations of management controls within the scope of internal audits, as part of the OIG overall program of audits and investigations, and reporting the results in its audit reports. In addition, the OIG annually reviews bureaus' administrative and accounting controls as part of its financial statement audits.

J. The Solicitor (SOL), Inspector General, and Program Assistant Secretaries. The Department's Council has proven to be an effective oversight forum for addressing and resolving management control and audit follow-up program issues. The SOL, OIG, and Program Assistant Secretaries are encouraged to establish similar management control and audit follow-up councils or oversight groups in their respective offices to coordinate and monitor the management control and audit follow-up programs. Such councils or oversight groups at a minimum should be responsible for: (1) institutionalizing the management control process within their organizations, (2) establishing priorities in identifying, correcting and reporting of management control material weaknesses and accounting non-conformances, (3) ensuring that funding to correct identified deficiencies is requested in the budget process, and (4) establishing a quality assurance process that permits the responsible official to provide reasonable assurance to the Secretary of the Interior (Secretary) that the objectives of the FMFIA are being achieved.

K. Bureau Heads. Bureau heads and/or senior-level management officials are responsible for establishing and maintaining the system of management control within their bureaus. This includes determining that the system of control is consistent with 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 also includes determining that the systems of control are functioning as intended; 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 management control weakness and/or accounting systems non-conformance. Bureau heads are also responsible for:

(1) determining on an annual basis which programs or administrative functions should be subject to a formal review in order to supplement management's judgment as to the adequacy of management controls;

(2) allocating adequate resources to evaluate their systems of control;

(3) developing detailed procedures, documentation, training, and reporting requirements necessary to review, establish, maintain, test, improve, and report on control systems within their bureau programs and operations;

(4) reporting to the Council, in consultation with their Assistant Secretary, management control deficiencies identified in audit reports, internal reviews, and from other sources that have the potential of meeting the Departmental material weakness criteria;

(5) ensuring timely correction and validation of all identified program and operational deficiencies whether material and/or nonmaterial; and

(6) ensuring management control guidelines issued by PAM, OCIO, and other Departmental offices are implemented.

Bureau heads should also specify employee accountability. Program specific management control elements and standards are to be included in all managers' performance evaluations.

L. Program and Other Managers. These management officials are responsible for the establishment and evaluation of management controls within their respective assigned program(s) or operational area(s).

M. Management Control Coordinators. Management control coordinators (MCCs) are the individuals designated by each bureau head or Assistant Secretary to coordinate and facilitate compliance with the FMFIA and relevant guidance issued by PFM, PAM and OCIO. Each bureau MCC or alternate is responsible for coordinating and directing the bureau control evaluation process, advising the bureau head on the operation of the bureau's management control program, the status of planned actions to correct deficiencies, and ensuring adherence to the Departmental management control program guidance. Bureau MCCs also have the discretion to develop any supplemental procedures required to evaluate the effectiveness of bureau control systems and to validate the completion of corrective actions through testing or other means.

1.6 **Dissemination of Information**. PFM's home-page for Management Accountability and Control includes (1) a current year schedule of management control program key action dates, (2) current year guidelines, and (3) management control summary information from the Department's Accountability Report such as a listing of open material weaknesses and material accounting non-conformances, and scheduled completion dates. This information is updated periodically. The web site address for accessing the PFM's home-page is www.doi.gov/pfm.

1.7 **Reporting**. Refer to the **Management Control and Audit Follow-Up Handbook,** Chapter 7 at http://www.doi.gov/pfm/mac/2003/mgmt_control_handbook.pdf for FMFIA and other reporting requirements.

8/2/04 #3638
Replaces 2/7/00 #3294

Department of the Interior
Departmental Manual

Effective Date: 8/2/04
Series: Audit
Part 361: Audit Follow-up
Chapter 1: General Audit Follow-up Responsibilities

Originating Office: Office of Financial Management

---

361 DM 1

1.1 **Purpose.** The purpose of this chapter is to provide policies and procedures for use by Departmental and bureau management when responding to and implementing recommendations in audit reports issued by the Office of Inspector General (OIG) and the General Accounting Office (GAO). Reference the Management Control and Audit Follow-up Handbook for procedures at http://www.doi.gov/pfm/mac/2003/mgmt_control_handbook.pdf. The audit follow-up program is an integral part of sound program management. Timely responses and implementation of corrective action in response to audit recommendations are essential to improving the effectiveness and efficiency of Departmental operations. This chapter identifies and implements pertinent statutes, regulations, and directives that apply to audit follow-up to OIG and GAO-issued reports and defines terms normally used in the audit follow-up process.

1.2 **Policy**. It is the policy of the Department that timely action is taken in response to audit findings and recommendations included in audit reports issued by the OIG and the GAO, or other outside parties conducting audits authorized by Federal government regulations.

1.3 **Definitions.**

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

B. Audit Initiation Memorandum means the OIG's or GAO's official notification of the initiation of an audit. The memorandum specifies the audit subject, scope, objective, and when the audit will start.

C. Audit Liaison Officer (ALO) means 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.

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

E. Corrective Action Plan means management's plan for addressing and implementing recommendations contained in audit reports and will include actions necessary to implement the recommendation, target completion dates, and officials responsible for completing required actions.

F. Disallowed Cost means a questioned cost that management, in a management decision, has sustained or agreed should not be charged to the Government.

G. External Audit means a grant audit, a preaward audit of contractor's proposed future costs, a concessions audit, a lease audit, or a contractor claim audit, or other federal awards administered by contractors, nonprofit entities, and other nongovernmental activities.

H. Financial Statement Audit means 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 and office are free of material misstatement. 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 and were not required to be included in the auditor's report on internal control, and other management issues.

(2) An entity shall be determined to be in compliance with Federal accounting standards as required by 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 Federal Financial Management Improvement Act of 1996 - 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 Determining Compliance section of the Federal Financial Management Improvement Act of 1996 - OMB Implementation Guidance issued January 4, 2001.

I. Final Action means the completion of all actions regarding a specific audit recommendation(s) that management, in a management decision, has concluded are necessary with respect to the findings and recommendations contained in an audit report.

J. Follow-up is the process of ensuring that audit recommendations are implemented and that disagreements between management and the OIG regarding corrective action are resolved.

K. GAO Audit means 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.

L. Internal Audit is 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.

M. Management means 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 cognizant program Assistant Secretary. 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.

N. Management Decision (Internal Audits) means the determination by management, with OIG concurrence, of action(s) required to implement audit recommendation.

O. Management Decision for single and external audits is 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.

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

Q. Performance Audit means 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.

R. Potential Additional, Lost or Underpaid Revenues represent 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.

S. Questioned Cost means 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; a finding that, at the time of the audit, the cost was not supported by adequate documentation; or a finding that the expenditure of funds for the intended purpose was unnecessary or unreasonable.

T. Reinstated Cost means 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.

U. Recommendations that Funds Be Put to Better Use (FBU) means 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

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

W. Single Audit means 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.

X. Time-barred means, the provision of the 1988 Amendments to the Indian Self-Determination and Education Assistance Act which precludes the government from recovering disallowed/sustained costs if notice of disallowance has not been given to the contractor/grantee within 365 days of the issuance of a single audit report.

Y. Sustained Cost means the same as Disallowed Cost (see paragraph 1.3F).

Z. Unsupported Cost means a cost that is questioned by the auditor because, at the time of the audit, such cost was not supported by adequate documentation.

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

1.4 **Roles and Responsibilities.**

A. Assistant Secretary - Policy, Management and Budget (A/S-PMB). The A/S-PMB is designated as audit follow-up official for the Department of the Interior. The designation is recorded in 109 DM 4. The A/S-PMB:

(1) Ensures that systems and procedures for audit follow-up are in place and properly documented and maintained.

(2) Makes the final determination regarding audit recommendations that have been referred to the audit follow-up official for resolution.

(3) Ensures that the Office of Financial Management carries out its delegated responsibilities regarding audit follow-up activities.

B. Office of Financial Management (PFM).

(1) Carries out audit follow-up responsibilities that were delegated by the Departmental audit follow-up official.

(2) Maintains the Departmental tracking system for audits referred to the A/S-PMB for tracking or resolution, and monitors implementation progress on a monthly or quarterly basis as necessary.

C. Audit Liaison Officers (ALO)

(1) Each program Assistant Secretary, and heads of bureaus and offices will appoint an ALO who serves as the point of contact for all Departmental audit activities.

(2) 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.

(3) Assistant Secretary level ALOs should monitor audit activity within bureaus reporting to the Assistant Secretary.

(4) Bureau level ALOs should keep the Assistant Secretary ALO apprised of significant audit issues/activities affecting the bureau.

(5) ALOs will ensure full cooperation with the OIG and GAO in the conduct of audits and with the audit follow-up official and PFM in all audit follow-up activities.

(6) ALOs will provide timely responses to auditors.

1.5 **Time Frames for Response**. As a convenience to readers, the appropriate response times for OIG and GAO audits are summarized below.

Time Frames for Comment

Organization	Draft Reports	Final Reports
GAO Reports	15-30 days (as directed)	60 days
OIG Reports:	45 days	30 days
Performance Audits	45 days	30 days
Financial Statement Audits		Refer to the DOI Guidance on Preparing Financial Statements at http://www.doi.gov/pfm/finstate.html
External Audits	N/A	90 days

8/2/04 #3640
Replaces 1/9/01 #3352

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

December 21, 2004

CIRCULAR NO. A-123
Revised

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

SUBJECT: Management's Responsibility for Internal Control

1. **Purpose.** This Circular provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal control. The attachment to this Circular defines management's responsibilities related to internal control and the process for assessing internal control effectiveness along with a summary of the significant changes. The Circular provides updated internal control standards and new specific requirements for conducting management's assessment of the effectiveness of internal control over financial reporting (Appendix A). This Circular emphasizes the need for integrated and coordinated internal control assessments that synchronize all internal control-related activities.

This revision to the Circular will become effective in Fiscal Year 2006 and supersede all previous versions. In the interim, OMB Circular No. A-123, "Management Accountability and Control," revised, June 21, 1995 should continue to be followed.

2. **Authority.** The Circular is issued under the authority of the Federal Managers' Financial Integrity Act of 1982 as codified in 31 U.S.C. 3512.

3. **Policy.** Management is responsible for establishing and maintaining internal control to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. Management shall consistently apply the internal control standards to meet each of the internal control objectives and to assess internal control effectiveness. When assessing the effectiveness of internal control over financial reporting and compliance with financial-related laws and regulations, management must follow the assessment process contained in Appendix A. Annually, management must provide assurances on internal control in its Performance and Accountability Report, including a separate assurance on internal control over financial reporting, along with a report on identified material weaknesses and corrective actions.

4. **Actions Required.** Agencies and individual Federal managers must 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.

5. **Effective Date.** This Circular is effective beginning with Fiscal Year 2006.

6. **Applicability.** This Circular is applicable to each executive agency, with the exception of the requirements in the appendix. The requirements of Appendix A are applicable to the 24 CFO Act agencies.

7. **Inquiries.** Further information concerning this Circular may be obtained from the Financial Standards and Grants Branch, Office of Federal Financial Management, Office of Management and Budget, Washington, DC 20503, 202/395-3993.

8. **Copies.** Copies of this Circular may be obtained from www.omb.gov.

Joshua B. Bolten
Director

Attachment

ATTACHMENT

Significant Revisions to OMB Circular A-123

Section	Revision to A-123	Purpose of Revision
Transmittal of Circular	Changed title from OMB Circular A-123, *Management Accountability and Control* to OMB Circular A-123, *Management's Responsibility for Internal Control*	Title changed to align better with the focus of the circular and current terminology.
Throughout Circular	Changed terminology from "management controls" to "internal control"	To better align with currently accepted standards for internal control and current terminology. The terms are intended to be synonymous.
Section II. Standards	Realigned section on the standards for internal control using the following categories: control environment, risk assessment, control activities, information and communication, and monitoring.	To better align with currently accepted standards for internal control.
Section III. Integrated Internal Control Framework	Provided a separate section on an integrated internal control framework. Provided a listing of statutes to consider when assessing internal control.	To highlight current legislative and regulatory requirements that should be coordinated and considered when assessing the effectiveness of internal control.
Section IV.B. Identification of Deficiencies	Introduced reportable condition as a category of deficiency.	To better align with current governmental terminology.

Significant Revisions to OMB Circular A-123

Section	Revision to A-123	Purpose of Revision
Section VI.A. Annual Assurance Statements	Require agencies subject to the CFO Act to include the FMFIA annual report in the PAR, under the heading "Management Assurances" and submit to OMB 45 days from the end of the fiscal year.	To consolidate assurance statements in one place within the PAR (Section 2, Section 4, and internal control over financial reporting). To accelerate the due date of the FMFIA reports to be consistent with the due date for the PAR.
Section VI.B. Reporting Pursuant to Section 2	Introduced a new assurance statement on the effectiveness of internal control over financial reporting. This statement will be a subset of the overall FMFIA assurance statement.	To emphasize management's responsibility for assessing and documenting internal control over financial reporting. To ensure Congress and the public that the Federal Government is committed to safeguarding its assets and providing reliable financial information.
Section VI. Reporting on Internal Control	Included a summary chart of definitions and reporting requirements for deficiency, reportable condition, material weakness, and nonconformance.	To provide a concise summary of reporting definitions.
Appendix A	To specifically address assessing, documenting, and reporting on the effectiveness of internal control over financial reporting.	To ensure Congress and the public that the Federal Government is committed to safeguarding its assets and providing reliable financial information.

New Requirements in Appendix A –
Internal Control over Financial Reporting

New Section	New Requirement
Transmittal of Circular	Requires the 24 CFO Act agencies to comply with Appendix A.
Section II. Scope	Defines the scope of assessing and documenting internal control over financial reporting to include the annual financial statements and other significant internal or external financial reports and compliance with laws and regulations that pertain to those financial reports.
Section II.C. Planning Materiality	Defines materiality for the purposes of assessing and documenting internal control over financial reporting.
Section III.A. Establish a Senior Assessment Team	Recommends the establishment of a senior assessment team, which at a minimum should oversee the assessment process.
Section III.B-E. Assessing Internal Control over Financial Reporting	Defines a process for assessing internal control over financial reporting at the entity level as well as at the process, transaction, or application level.
Section IV. Documentation	A. Requires that the controls over financial reporting be documented. B. Requires that the assessment process of the controls over financial reporting be documented.
Section V. Management's Assessment of Internal Control over Financial Reporting	Requires the assurance statement assert to the effectiveness of internal control "as of June 30." The assurance statement and corrective actions, if applicable, will be submitted in the PAR no later than 45 days after the end of each fiscal year.
Section V. Management's Assessment of Internal Control over Financial Reporting	Provides a sample assurance statement on the effectiveness of internal control over financial reporting.
Section V.A. Agencies Obtaining Audit Opinions on Internal Control	Agencies electing to receive a separate audit opinion on internal control over financial reporting may adjust the "as of" reporting date of June 30 to align better with the "as of" date of the audit opinion. This circular does not require a separate audit.
Section VI. Correcting Material Weaknesses in Internal Control over Financial Reporting	Provides a non-compliance clause that permits OMB to require an agency to obtain an audit opinion over the internal controls over financial reporting if the agreed upon deadlines for corrective actions are continuously not met.

TABLE OF CONTENTS

I. INTRODUCTION

Management has a fundamental responsibility to develop and maintain effective internal control. The proper stewardship of Federal resources is an essential responsibility of agency managers and staff. Federal employees must ensure that Federal programs operate and Federal resources are used efficiently and effectively to achieve desired objectives. Programs must operate and resources must be used consistent with agency missions, in compliance with laws and regulations, and with minimal potential for waste, fraud, and mismanagement.

Management is responsible for developing and maintaining effective internal control. Effective internal control provides assurance that significant weaknesses in the design or operation of internal control, that could adversely affect the agency's ability to meet its objectives, would be prevented or detected in a timely manner.

Internal Control -- organization, policies, and procedures – are tools to help program and financial managers achieve results and safeguard the integrity of their programs. This Circular provides guidance on using the range of tools at the disposal of agency managers to achieve desired program results and meet the requirements of the Federal Managers' Financial Integrity Act (FMFIA) of 1982. The FMFIA encompasses accounting and administrative controls. Such controls include program, operational, and administrative areas as well as accounting and financial management.

The importance of internal control is addressed in many statutes and executive documents. The FMFIA establishes overall requirements with regard to internal control. The agency head must establish controls that reasonably ensure that: "(i) obligations and costs are in compliance with applicable law; (ii) funds, property, and other assets are safeguarded against waste, loss, unauthorized use or misappropriation; and (iii) revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets."[1] In addition, the agency head annually must evaluate and report on the control and financial systems that protect the integrity of Federal programs (Section 2 and Section 4 of FMFIA respectively). The three objectives of internal control are to ensure the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. The safeguarding of assets is a subset of all of these objectives.

Instead of considering internal control as an isolated management tool, agencies should integrate their efforts to meet the requirements of the FMFIA with other efforts 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.

Federal managers must carefully consider the appropriate balance between controls and risk in their programs and operations. Too many controls can result in inefficient and ineffective government; agency managers must ensure an appropriate balance between the strength of controls and the relative risk associated with particular programs and operations. The benefits of controls should outweigh the cost. Agencies should consider both qualitative and quantitative factors when analyzing costs against benefits.

A. Agency Implementation. Internal control guarantees neither the success of agency programs, nor the absence of waste, fraud, and mismanagement, but is a means of managing the risk associated with Federal programs and operations. Managers should define the control environment (e.g., programs, operations, or financial reporting) and then perform risk assessments to identify the most significant areas within that environment in which to place or enhance internal control. The risk assessment is a critical step in the process to determine the extent of controls. Once significant areas have been identified, control activities should be implemented. Continuous monitoring and testing should help to identify poorly designed or ineffective controls and should be reported upon periodically. Management is then responsible for redesigning or improving upon those controls. Management is also responsible for communicating the objectives of internal control and ensuring the organization is committed to sustaining an effective internal control environment.

Appropriate internal control should be integrated into each system established by agency management to direct and guide its operations. As stated earlier in this document, internal control applies to program, operational, and administrative areas as well as accounting and financial management.

Generally, identifying and implementing the specific procedures necessary to ensure effective internal control, and determining how to assess the effectiveness of those controls, is left to the discretion of the agency head. While the procedures may vary from

[1] The quoted text is from the Federal Managers' Financial Integrity Act (FMFIA) of 1982.

agency to agency, management should have a clear, organized strategy with well-defined documentation processes that contain an audit trail, verifiable results, and specify document retention periods so that someone not connected with the procedures can understand the assessment process.

To ensure senior management involvement, many agencies have established their own senior management council, often chaired by the agency's lead management official, to address management accountability and related issues within the broader context of agency operations. Relevant issues for such a council include ensuring the agency's commitment to an appropriate system of internal control; actively overseeing the process of assessing internal controls, including non-financial as well as financial reporting objectives; recommending to the agency head which control deficiencies are material to disclose in the annual FMFIA report; and providing input for the level and priority of resource needs to correct these deficiencies. (See also Section IV.C. Role of a Senior Management Council.)

II. STANDARDS

Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.[2]

Internal control, in the broadest sense, includes the plan of organization, methods and procedures adopted by management to meet its goals. Internal control includes processes for planning, organizing, directing, controlling, and reporting on agency operations.

The three objectives of internal control are:

- Effectiveness and efficiency of operations,
- Reliability of financial reporting, and
- Compliance with applicable laws and regulations.

[2] Internal control standards and the definition of internal control are based on GAO, Standards for Internal Control in the Federal Government, November 1999, "Green Book".

The safeguarding of assets is a subset of all of these objectives. Internal control should be designed to provide reasonable assurance regarding prevention of or prompt detection of unauthorized acquisition, use or disposition of assets.

Management is responsible for developing and maintaining internal control activities that comply with the following standards to meet the above objectives:

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

A. Control Environment

The control environment is the organizational structure and culture created by management and employees to sustain organizational support for effective internal control. When designing, evaluating or modifying the organizational structure, management must clearly demonstrate its commitment to competence in the workplace. Within the organizational structure, management must clearly: define areas of authority and responsibility; appropriately delegate the authority and responsibility throughout the agency; establish a suitable hierarchy for reporting; support appropriate human capital policies for hiring, training, evaluating, counseling, advancing, compensating and disciplining personnel; and uphold the need for personnel to possess and maintain the proper knowledge and skills to perform their assigned duties as well as understand the importance of maintaining effective internal control within the organization.

The organizational culture is also crucial within this standard. The culture should be defined by management's leadership in setting values of integrity and ethical behavior but is also affected by the relationship between the organization and central oversight agencies and Congress. Management's philosophy and operational style will set the tone within the organization. Management's commitment to establishing and maintaining effective internal control should cascade down and permeate the organization's control environment which will aid in the successful implementation of internal control systems.

B. Risk Assessment

Management should identify internal and external risks that may prevent the organization from meeting its objectives. When identifying risks, management should take into account relevant interactions within the organization as well as with outside organizations. Management should also consider previous findings; e.g., auditor identified, internal management reviews, or noncompliance with laws and regulations when identifying risks. Identified risks should then be analyzed for their potential effect or impact on the agency.

C. Control Activities

Control activities include policies, procedures and mechanisms in place to help ensure that agency objectives are met. Several examples include: proper segregation of duties (separate personnel with authority to authorize a transaction, process the transaction, and review the transaction); physical controls over assets (limited access to inventories or equipment); proper authorization; and appropriate documentation and access to that documentation.

Internal control also needs to be in place over information systems – general and application control. General control applies to all information systems such as the mainframe, network and end-user environments, and includes agency-wide security program planning, management, control over data center operations, system software acquisition and maintenance. Application control should be designed to ensure that transactions are properly authorized and processed accurately and that the data is valid and complete. Controls should be established at an application's interfaces to verify inputs and outputs, such as edit checks. General and application control over information systems are interrelated, both are needed to ensure complete and accurate information processing. Due to the rapid changes in information technology, controls must also adjust to remain effective.

D. Information and Communications

Information should be communicated to relevant personnel at all levels within an organization. The information should be relevant, reliable, and timely. It is also crucial that an agency communicate with outside organizations as well, whether providing information or receiving it. Examples include: receiving updated guidance from central oversight agencies; management communicating requirements to the operational staff; operational staff communicating with the information systems staff to modify application software to extract data requested in the guidance.

E. Monitoring

Monitoring the effectiveness of internal control should occur in the normal course of business. In addition, periodic reviews, reconciliations or comparisons of data should be included as part of the regular assigned duties of personnel. Periodic assessments should be integrated as part of management's continuous monitoring of internal control, which should be ingrained in the agency's operations. If an effective continuous monitoring program is in place, it can level the resources needed to maintain effective internal controls throughout the year.

Deficiencies found in internal control should be reported to the appropriate personnel and management responsible for that area. Deficiencies identified, whether through internal review or by an external audit, should be evaluated and corrected. A systematic process should be in place for addressing deficiencies.

III. INTEGRATED INTERNAL CONTROL FRAMEWORK

Federal agencies are subject to numerous legislative and regulatory requirements that promote and support effective internal control. Effective internal control is a key factor in achieving agency missions and program results through improved accountability. Identifying internal control weaknesses and taking related corrective actions are critically important to creating and maintaining a strong internal control infrastructure that supports the achievement of agency objectives. Recent government-wide initiatives have been implemented to improve program management, as well as financial management, including tracking corrective actions for material weaknesses in internal control related to financial reporting, imposing accelerated reporting due dates for more timely financial information, and assessing the effectiveness and efficiency of program operations using the Program Assessment Rating Tool (PART). Activities conducted as part of these initiatives support an agency's overall internal control framework. Statutory requirements that should also be considered as part of an agency's internal control framework include:

Federal Managers Financial Integrity Act of 1982 (FMFIA)

The FMFIA requires agencies to establish and maintain internal control. The agency head must annually evaluate and report on the control and financial systems that protect the integrity of Federal programs; Section 2 and Section 4 respectively. 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.

Government Performance and Results Act (GPRA)

To support results-oriented management, GPRA requires agencies to develop strategic plans, set performance goals, and report annually on actual performance compared to goals. With the implementation of this legislation, these plans and goals are 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. Similarly, the PART's primary purpose is to assess program effectiveness and improve program performance. The PART has also become an integral part of the budget process when making funding resource allocations or decisions.

Chief Financial Officers Act, as amended (CFO Act)

The CFO Act requires agencies to both establish and assess internal control related to financial reporting. The Act requires the preparation and audit of financial statements. In this process, auditors report on internal control and compliance with laws and regulations related to financial reporting. Therefore, the agencies covered by the Act have a clear opportunity to improve internal control over their financial activities, and to evaluate the controls that are in place. The Accountability of Tax Dollars Act of 2002 amended the CFO Act to expand the types of Federal agencies that are required to prepare audited financial statements.

Meeting the accelerated financial statement reporting due date also provides incentive for agencies to have added discipline and effective internal control to routinely produce reliable financial information. Deficiencies in internal control need to be mitigated to ensure timely and accurate financial information.

Inspector General Act of 1978, as amended (IG Act)

The IG Act provides for independent reviews of agency programs and operations. IGs are required to submit semiannual reports to Congress on significant abuses and deficiencies identified during the reviews and the recommended actions to correct those deficiencies. IGs and/or external auditors are required by the Government Auditing Standards[3] and OMB Bulletin No. 01-02, Audit Requirements of Federal Financial Statements, as amended[4] to report material weaknesses in internal control related to financial reporting and noncompliance with laws and regulations as part of the financial statement audit. Auditors also provide recommendations for correcting the material weaknesses. Agency managers, who are required by the IG Act to follow up on audit recommendations, should use these reviews to identify and correct problems resulting from inadequate or poorly designed controls, and to build appropriate controls into new programs. Audit work planned by the IG should be coordinated with management's assessment requirements to ensure cost effectiveness and avoid duplication.

Federal Financial Management Improvement Act of 1996 (FFMIA)

The 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 (USSGL) at the transaction level. Financial management systems shall have general and application controls in place in order to support management decisions by

[3] The Government Auditing Standards, June 2003 (GAO-03-673G) can be found on the GAO website at www.gao.gov. The Government Auditing Standards are commonly known as the "Yellow Book."
[4] The OMB Bulletin No. 01-02, Audit Requirements for Federal Financial Statements, as amended can be found on the OMB website at www.omb.gov.

providing timely and reliable data. The agency head shall make a determination annually about whether the agency's financial management systems substantially comply with the FFMIA. If the systems are found not to be compliant, management shall develop a remediation plan to bring those systems into substantial compliance. Management shall determine whether non-compliances with FFMIA should also be reported as non-conformances with Section 4 of FMFIA.

Federal Information Security Management Act of 2002 (FISMA)

The FISMA provides, "…a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets…" Agencies are required to provide information security controls proportionate with the risk and potential harm of not having those controls in place. Agency heads are required to annually report on the effectiveness of the agencies' security programs. "Significant deficiencies" found under FISMA must also be reported as material weaknesses under FMFIA.

Improper Payments Information Act of 2002 (IPIA)

The IPIA requires agencies to review and, "…identify programs and activities that may be susceptible to significant improper payments." Agencies must annually submit estimates of improper payments, corrective actions to reduce the improper payments, and statements as to whether its current information systems and infrastructure can support the effort to reduce improper payments. The nature and incidence of improper payments shall be considered when assessing the effectiveness of internal control.

Single Audit Act, as amended

The Single Audit Act, as amended requires financial statement audits of non-Federal entities that receive or administer grant awards of Federal monies. The financial statement audits include testing the effectiveness of internal control and determining whether the award monies have been spent in compliance with laws and regulations. Each Federal agency which provides Federal awards shall review the audits of the recipients to determine whether corrective actions are implemented with respect to audit findings.

Clinger-Cohen Act of 1996 (formerly known as the Information Technology Management Reform Act)

The Clinger-Cohen Act requires agencies to use a disciplined capital planning and investment control (CPIC) process to maximize the value of and assess and manage the risks of the information technology acquisitions. The Act requires that agencies "(1) establish goals for improving the efficiency and effectiveness of agency operations and, as appropriate, the delivery of services to the public

> through the effective use of information technology; (2) prepare an annual report…on the progress in achieving the goals; (3) ensure that performance measurements are prescribed for information technology used by, or to be acquired for, the executive agency and that the performance measurements measure how well the information technology supports programs of the executive agency; (4) where comparable processes and organizations in the public or private sectors exist, quantitatively benchmark agency process performance against such processes in terms of cost, speed, productivity, and quality of outputs and outcomes; (5) analyze the missions of the executive agency and, based on the analysis, revise the executive agency's mission-related processes and administrative processes as appropriate before making significant investments in information technology that is to be used in support of the performance of those missions; and (6) ensure that the information security policies, procedures, and practices of the executive agency are adequate."

A. Developing Internal Control. It is management's responsibility to develop and maintain effective internal control. As agencies develop and execute strategies for implementing or reengineering agency programs and operations, they should design management structures that help ensure accountability for results. As part of this process, agencies and individual Federal managers must take systematic and proactive measures to develop and implement appropriate, cost-effective internal control. The degree to which studies and analysis are performed will vary depending on the complexity and risk associated with a given program or operation. The expertise of the agency CFO can be valuable in developing appropriate control and the IG can be valuable in providing advice or consultation. Decisions made during this process should be documented and readily available for review.

IV. ASSESSING INTERNAL CONTROL

Agency managers should continuously monitor and improve the effectiveness of internal control associated with their programs. This continuous monitoring, and other periodic assessments, should provide the basis for the agency head's annual assessment of and report on internal control, as required by FMFIA.

Agency management should determine the appropriate level of documentation needed to support this assessment. Documentation should be appropriately detailed and organized and contain sufficient information to support management's assertion. Documentation should also include appropriate representations from officials and personnel responsible for monitoring, improving and assessing internal controls. Specific assessment and documentation requirements to support management's assurance statement on internal control over financial reporting are defined in Appendix A.

A. Sources of Information. The agency head's assessment of internal control can be performed using a variety of information sources. Management has primary responsibility for assessing and monitoring controls, and should use other sources as a supplement to -- not a replacement for -- its own judgment. Sources of information include:

- Management knowledge gained from the daily operation of agency programs and systems.
- Management reviews conducted (i) expressly for the purpose of assessing internal control, or (ii) for other purposes with an assessment of internal control as a by-product of the review.
- IG and GAO reports, including audits, inspections, reviews, investigations, outcome of hotline complaints, or other products.
- Program evaluations.
- Audits of financial statements conducted pursuant to the CFO Act, as amended, including: information revealed in preparing the financial statements; the auditor's reports on the financial statements, internal control, and compliance with laws and regulations; and any other materials prepared relating to the statements.
- Reviews of financial systems which consider whether the requirements of FFMIA and OMB Circular No. A-127, Financial Management Systems[5] are being met.
- Annual evaluations and reports pursuant to FISMA and OMB Circular No. A-130, Management of Federal Information Resources[6].
- Annual performance plans and reports pursuant to GPRA.
- PART assessments.
- Annual reviews and reports pursuant to IPIA.
- Single Audit reports for grant-making agencies.
- Reports and other information provided by the Congressional committees of jurisdiction.
- Other reviews or reports relating to agency operations, e.g. for the Department of Health and Human Services, quality control reviews of the Medicaid and Temporary Assistance for Needy Families programs.
- Results from tests of key controls performed as part of the assessment of internal control over financial reporting conducted in accordance with the requirements in Appendix A.

Use of a source of information should take into consideration whether the process included an evaluation of internal control. Agency management should avoid duplicating reviews which assess internal control, and should coordinate their efforts with other evaluations to the extent practicable.

[5] The OMB Circular No. A-127, Financial Management Systems can be found on the OMB website at www.omb.gov.

[6] The OMB Circular No. A-130, Management of Federal Information Resources can be found on the OMB website at www.omb.gov.

If a Federal manager determines that there is insufficient information available upon which to base an assessment of internal control, then appropriate reviews should be conducted which will provide such a basis.

B. Identification of Deficiencies. Agency managers and employees should identify deficiencies in internal control from the sources of information described above and the results of their assessment process. Agency employees and managers shall report control deficiencies to the next supervisory level, which will allow the chain of command structure to determine the relative importance of each deficiency.

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 internal control objectives is a reportable condition (internally tracked and monitored within the agency). A reportable condition that the agency head determines to be significant enough to be reported outside the agency shall be considered a material weakness[7] and included in the annual FMFIA assurance statement and reported in the agency's annual PAR. As it relates to financial reporting, agencies should also consider qualitative as well as quantitative measures to determine material items. This designation requires a judgment by agency managers as to the relative risk and significance of reportable conditions. In identifying and assessing the relative importance of reportable conditions, consideration should be given to the views of the agency's IG. Definitions of reportable conditions and material weaknesses for management's assessment of internal control over financial reporting are provided in Appendix A Section II. Scope. Additionally, definitions and reporting requirements are summarized in Exhibit 1. The "significant deficiencies" identified under FISMA must be reported as material weaknesses in the annual FMFIA report.

Agency managers and staff should be encouraged to identify control deficiencies, as this reflects positively on the agency's commitment to recognizing and addressing management problems. Failing to report a known reportable condition would reflect adversely on the agency and continue to place the agency's operations at risk. Agencies should carefully consider whether systemic weaknesses exist that adversely affect internal control across organizational or program lines.

C. Role of a Senior Management Council. Many agencies use a Senior Management Council to assess and monitor deficiencies in internal control. A Senior Management Council, which may include the Chief Financial Officer, the Senior Procurement Executive, the Chief Information Officer, and the managers of other functional offices, should be involved in identifying and ensuring correction of systemic weaknesses

---

[7] This Circular's use of the term "material weakness" is similar to the same term used by auditors to identify internal control weaknesses found during a financial statement audit (see OMB Bulletin 01-02 or GAO "Yellow Book"). This Circular's use of the same term encompasses not only financial reporting, but also encompasses weaknesses found in program operations and compliance with applicable laws and regulations. Material weaknesses for the purposes of this Circular are determined by management, whereas material weaknesses reported as part of a financial statement audit are determined by independent auditors.

relating to their respective functions. Consideration should be given to involving the IG in a consulting capacity but not to conduct management's assessment of internal controls. Such councils generally recommend to the agency head which reportable conditions are deemed to be material weaknesses to the agency as a whole, and should therefore be included in the annual FMFIA assurance statement and reported in the agency's PAR. This council should be responsible for overseeing the timely implementation of corrective actions related to material weaknesses. Such a council may also be useful in determining when sufficient action has been taken to declare that a reportable condition or material weakness has been corrected. While the establishment of such a council is not a requirement of this document, a Senior Management Council or similar construct is encouraged.

V. CORRECTING INTERNAL CONTROL DEFICIENCIES

Agency managers are responsible for taking timely and effective action to correct deficiencies identified by the variety of sources discussed in Section IV, Assessing Internal Control. Correcting deficiencies is an integral part of management accountability and must be considered a priority by the agency.

The extent to which corrective actions are tracked by the agency should be commensurate with the severity of the deficiency. Corrective action plans should be developed for all material weaknesses, and progress against plans should be periodically assessed and reported to agency management. Management should track progress to ensure timely and effective results. For reportable conditions that are not included in the FMFIA report, corrective action plans should be developed and tracked internally at the appropriate level.

A summary of the corrective action plans for material weaknesses shall be included in the agency's PAR. The summary discussion shall include a description of the material weakness, status of corrective actions, and timeline for resolution.

Management shall maintain more detailed corrective action plans internally which shall be available for OMB review. Management's process for resolution and corrective action of identified material weaknesses in internal control must:

- Provide for appointment of an overall corrective action accountability official from senior agency management. The corrective action accountability official should report to the agency's Senior Management Council, if applicable.
- Require prompt resolution and corrective actions.
- Maintain accurate records of the status of the identified material weaknesses through the entire process of resolution and corrective action.

- Assure that the corrective action plans are consistent with laws, regulations, and Administration policy.
- Assure that performance appraisals of appropriate officials reflect effectiveness in resolving or implementing corrective action for identified material weaknesses[8].

A determination that a reportable condition has been corrected should be made only when sufficient corrective actions have been taken and the desired results achieved. This determination should be in writing, and along with other appropriate documentation supporting the determination, should be available for review by appropriate officials. (See also Section IV.C. Role of a Senior Management Council.)

As managers consider IG and GAO audit reports in identifying and correcting internal control deficiencies, they must be mindful of the statutory requirements for audit follow-up included in the IG Act, as amended and OMB Circular A-50, Audit Followup. Management has a responsibility to complete action, in a timely manner, on audit recommendations on which agreement with the IG has been reached. Management must make a decision regarding IG audit recommendations within a six month period after issuance of the audit report and implement management's decision within one year to the extent practicable.

VI. REPORTING ON INTERNAL CONTROL

A. Annual Assurance Statements. The assurance statements and information related to Section 2, Section 4, and internal control over financial reporting should be provided in a single FMFIA report section of the annual PAR labeled "Management Assurances." The section should include the annual assurance statements, summary of material weaknesses and non-conformances, and summary of corrective action plans. Management's assurance statement relating to internal control over financial reporting and any related material weaknesses and corrective actions shall be separately identified.

B. Reporting Pursuant to Section 2. 31 U.S.C. 3512(d) (2) (commonly referred to as Section 2 of the FMFIA) requires that annually the head of each executive agency submit to the President and the Congress (i) a statement on whether there is reasonable assurance that the agency's controls are achieving their intended objectives; and (ii) a report on material weaknesses in the agency's controls.

- **Statement of Assurance.** The statement of assurance represents the agency head's informed judgment as to the overall adequacy and effectiveness of internal control within the agency. The statement must take one of the following forms:
  - Unqualified statement of assurance (no material weaknesses reported);

[8] Standards based upon OMB Circular A-50, Audit Followup.

  - Qualified statement of assurance, considering the exceptions explicitly noted (one or more material weaknesses reported); or
  - Statement of no assurance (no processes in place or pervasive material weaknesses).

  In deciding on the type of assurance to provide, the agency head should consider information from the sources described in Section III of this Circular, with input from senior program and administrative officials and the IG. The agency head must describe the analytical basis for the type of assurance being provided, and the extent to which agency activities were assessed. Management is precluded from concluding that the agency's internal control is effective (unqualified statement of assurance) if there are one or more material weaknesses. The statement of assurance must be signed by the agency head.

- **Statement of Assurance for Internal Control over Financial Reporting.** Management is required to provide a separate assurance over the effectiveness of the internal controls over financial reporting. This assurance is a subset of the overall Statement of Assurance and is based on the results of management's assessment conducted in accordance with the requirements in Appendix A. Refer to Appendix A Section V. Management's Assurance Statement on Internal Control over Financial Reporting for a further discussion.

C. Reporting Pursuant to Section 4. 31 U.S.C. 3512(d) (2) (B) (commonly referred to as Section 4 of the FMFIA) requires an annual statement on whether the agency's financial management systems conform to government-wide requirements. These financial systems requirements are mandated by the FFMIA and OMB Circular No. A-127, Financial Management Systems, section 7. If the agency's systems do not substantially conform to financial systems requirements, the statement must list the nonconformances and discuss the agency's plans for bringing its systems into substantial compliance. Financial management systems include both financial and financially-related (or mixed) systems.

D. Government Corporations. For government corporations**,** Section 306 of the Chief Financial Officers Act established a reporting requirement related to the internal controls for corporations covered by the Government Corporation and Control Act. These corporations must submit an annual management report to the Congress. This report must include, among other items, a statement on control systems by the head of the management of the corporation consistent with the requirements of the FMFIA. The corporation is required to provide the President, the Director of OMB, and the Comptroller General a copy of the management report when it is submitted to Congress.

Exhibit 1: Summary of A-123 reporting requirements

	Definition[9]	**Reporting**
Control Deficiency (FMFIA Section 2 and internal control over financial reporting)	Control deficiencies exist when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A design deficiency exists when a control necessary to meet the control objective is missing or an existing control is not properly designed, so that even if the control operates as designed the control objective is not always met. An operation deficiency exists when a properly designed control does not operate as designed or when the person performing the control is not qualified or properly skilled to perform the control effectively.	Internal to the organization and not reported externally. Progress against corrective action plans should be periodically assessed and reported to agency management.
Reportable Condition (FMFIA Section 2 and internal control over financial reporting)	**FMFIA overall** – A control deficiency, or combination of control deficiencies, that in management's judgment, should be communicated because they represent significant weaknesses in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives. **Financial reporting** - A control deficiency, or combination of control 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[10] likelihood that a misstatement of the entity's financial statements, or other significant financial reports, that is more than inconsequential will not be prevented or detected.	Internal to the organization and not reported externally. Progress against corrective action plans should be periodically assessed and reported to agency management.

[9] The definition of control deficiency and definitions of reportable condition and material weakness relative to financial reporting are based upon the definitions provided in Auditing Standard No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements issued by the Public Company Accounting Oversight Board (PCAOB).
[10] The term "remote" is defined in SFFAS No. 5, Accounting for Liabilities of the Federal Government, as the chance of the future event, or events, occurring is slight.

	Definition[9]	Reporting
Material Weakness (FMFIA Section 2 and internal control over financial reporting)	**FMFIA overall** - Reportable conditions in which the agency head determines to be significant enough to report outside of the agency. **Financial reporting** - Reportable condition, or combination of reportable conditions, that results in more than a remote[11] likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected.	Material weaknesses and a summary of corrective actions shall be reported to OMB and Congress through the PAR (Management Report for Government Corporations). Progress against corrective action plans should be periodically assessed and reported to agency management.
Non-conformance (FMFIA Section 4)	Instances 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.	Non-conformances and a summary of corrective actions to bring systems into conformance shall be reported to OMB and Congress through the PAR (Management Report for Government Corporations). Progress against corrective action plans should be periodically assessed and reported to agency management.

[11] The term "remote" is defined in SFFAS No. 5, Accounting for Liabilities of the Federal Government, as the chance of the future event, or events, occurring is slight.

APPENDIX A: INTERNAL CONTROL OVER FINANCIAL REPORTING

TABLE OF CONTENTS

I. INTRODUCTION

This Appendix provides a methodology for agency management to assess, document, and report on the internal controls over financial reporting. This document also encourages an integrated approach to assessing the internal controls over financial reporting considering the current legislative and regulatory environment in which Federal entities operate.

> *Effective internal control over financial reporting provides reasonable assurance that misstatements, losses, or noncompliance with applicable laws and regulations, material in relation to financial reports, would be prevented or detected.*[12]

The Sarbanes-Oxley Act of 2002 required that management of publicly-traded companies strengthen their processes for assessing and reporting on the internal controls over financial reporting. The passage of the Sarbanes-Oxley Act served as an impetus for the Federal government to reevaluate its current policies relating to internal control over financial reporting and management's related responsibilities. While the Sarbanes-Oxley Act created a new requirement for managers of publicly-traded companies to report on

[12] The definition of effective internal control is based on the GAO/PCIE, Financial Audit Manual.

the internal controls over financial reporting, Federal managers have been subject to similar internal control reporting requirements for many years.

Federal agencies are subject to numerous legislative and regulatory requirements that promote and support effective internal control. The Federal Managers' Financial Integrity Act (FMFIA) of 1982 provides the statutory basis for management's responsibility for and assessment of internal control. In addition, the Chief Financial Officers Act (CFO Act) of 1990 requires agency CFOs to, "develop and maintain an integrated agency accounting and financial management system, including financial reporting and internal controls, which … complies with applicable … internal control standards…" The Federal Financial Management Improvement Act (FFMIA) of 1996 and OMB Circular No. A-127, Financial Management Systems also instruct agencies to maintain an integrated financial management system that complies with Federal system requirements, FASAB Standards, and the USSGL at the transaction level. The Inspector General Act (IG Act) of 1978, as amended requires that IGs submit semiannual reports to the Congress on significant abuses and deficiencies identified during these reviews and the recommended actions to correct those deficiencies. The GAO Government Auditing Standards (Yellow Book) and OMB Bulletin No. 01-02, Audit Requirements for Federal Financial Statements, as amended require auditors to test and report on internal control as part of a Federal agency financial statement audit, including a description of reportable conditions and material weaknesses in internal control over financial reporting.

Recent government-wide initiatives have also contributed to improvements in financial management and placed greater emphasis on implementing and maintaining effective internal control over financial reporting. These initiatives include aggressive OMB quarterly tracking of corrective actions for material weaknesses in internal control related to financial reporting, accelerated financial reporting due dates, and the emphasis on demonstrating the availability of timely and accurate financial management information for management decisions.

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

II. SCOPE

A. Objectives of Internal Control over Financial Reporting

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

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

B. Definition of Financial Reporting

Internal control over financial reporting should assure the safeguarding of assets from waste, loss, unauthorized use, or misappropriation as well as assure compliance with laws and regulations pertaining to financial reporting. Financial reporting includes annual financial statements of an agency as well as other significant internal or external financial reports. Other significant financial reports are defined as any financial reports that could have a material effect on a significant spending, budgetary or other financial decision of the agency or that is used to determine compliance with laws and regulations on the part of the agency. An agency needs to determine the scope of financial reports that are significant, i.e., which reports are included in the assessment of internal control over financial reporting. In addition to the annual financial statements, significant reports might include: quarterly financial statements; financial statements at the operating division or program level; budget execution reports; reports used to monitor specific activities such as specific revenues, receivables, or liabilities; reports used to monitor compliance with laws and regulations such as the Anti-Deficiency Act, etc.

C. Planning Materiality

Materiality for financial reporting is the risk of error or misstatement that could occur in a financial report that would impact management's or users' decisions or conclusions based on such report. The planning materiality for the assessment should be designed as to ensure that items required to be reported will be detected. Therefore, the planning materiality should be at a lower threshold than the reporting materiality as defined below. Materiality should be determined for each financial report included in the scope of the assessment. Materiality may differ from report to report. Materiality shall be considered when determining the extent of testing or work required to assess internal control over financial reporting as well as what deficiencies should be reported. Management must determine whether the internal controls over a financial report is sufficient to prevent or detect errors or misstatements that would be considered material for a specific financial report. Therefore, the extent of work performed and reporting threshold for control deficiencies must be determined on a report by report basis. Additionally, agencies should consider qualitative as well as quantitative measures to determine material items.

D. Definition of Deficiencies[13]

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

A reportable condition is a control deficiency, or combination of control 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[14] likelihood that a misstatement of the entity's financial statements, or other significant financial reports, that is more than inconsequential will not be prevented or detected.

A material weakness in internal control is a reportable condition, or combination of reportable conditions, that results in more than a remote[15] likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected. Material weaknesses in internal control over financial reporting shall be included in the annual FMFIA report, but separately identified.

---

[13] The definition of control deficiency and definitions of reportable condition and material weakness relative to financial reporting are based upon the definitions provided in Auditing Standard No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements issued by the Public Company Accounting Oversight Board (PCAOB).

[14] The term "remote" is defined in SFFAS No. 5, Accounting for Liabilities of the Federal Government, as the chance of the future event, or events, occurring is slight.

[15] Ibid.

A summary of the above definitions and corresponding reporting requirements are summarized in Exhibit 1.

III. ASSESSING INTERNAL CONTROL OVER FINANCIAL REPORTING

A. Establish a Senior Assessment Team

The success of an agency's assessment will depend in large part on who will be responsible to carry out or direct the assessment. Given the significance and breadth of the assessment, a senior assessment team should be established that includes senior executives and derives its authority and support from the head of the agency or the Chief Financial Officer. The senior assessment team could be a subset of the Senior Management Council. The senior assessment team could take many forms, such as a financial management improvement committee. The senior assessment team, at a minimum, should provide oversight of the assessment process and is responsible for:

- Ensuring that assessment objectives are clearly communicated throughout the agency;
- Ensuring that the assessment is carried out in a thorough, effective, and timely manner;
- Identifying and ensuring adequate funding and resources are made available;
- Identifying staff and/or securing contractors to perform the assessment;
- Determining the scope of the assessment, i.e., those financial reports covered by the assessment; and
- Determining the assessment design and methodology.

B. Evaluate Internal Control at the Entity Level

Internal control at the entity level refers to those elements of the five components of internal control that have an overarching or pervasive effect on the agency. Specific elements of internal control that should be evaluated at this level are discussed below.

1. Control Environment

The assessment should include obtaining a sufficient knowledge of the control environment to understand management's attitude, awareness, and actions concerning the control environment. The assessment should consider the collective effect on the control environment, since management's strengths and weaknesses can have a pervasive effect on internal control. Specific elements of the control environment that should be considered include:

- Integrity and ethical standards
- Commitment to competence
- Management philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human resource policies and practices

2. Risk Assessment

The assessment should include obtaining sufficient knowledge of the agency's process on how management considers risks relevant to financial reporting objectives and decides about actions to address those risks. The assessment should determine how management identifies risks, estimates the significance of risks, assesses the existence of risks in the current environment, and relates them to financial reporting. The results of this assessment at the agency-wide level will drive the extent of testing and review performed at the process, transaction, or application level. Some significant circumstances or events that can affect risk include:

- Complexity or magnitude of programs, operations, transactions, etc;
- Accounting estimates;
- Related party transactions;
- Extent of manual processes or applications;
- Decentralized versus centralized accounting and reporting functions;
- Changes in operating environment;
- New personnel or significant personnel changes;
- New or revamped information systems;
- Significant new or changed programs or operations;
- New technology; and
- New or amended laws, regulations, or accounting standards.

3. Control Activities

Control activities are the policies and procedures that help ensure that management directives are carried out and that management's assertions in its financial reporting are valid. The assessment should include obtaining an understanding of the control activities applicable at the entity level, such as:

- Policies and procedures;
- Management objectives (clearly written and communicated throughout the agency);
- Planning and reporting systems;
- Analytical review and analysis;
- Segregation of duties;
- Safeguarding of records; and

- Physical and access controls.

4. Information and Communication

The assessment should include obtaining an understanding of the information system(s) relevant to financial reporting. Such an understanding should include:

- The type and sufficiency of reports produced;
- The manner in which information systems development is managed;
- Disaster recovery;
- Communication of employees' control related duties and responsibilities; and
- How incoming external communication is handled.

5. Monitoring

The assessment should include obtaining an understanding of the major types of activities the agency uses to monitor internal control over financial reporting, including the source of the information related to those activities, and how those activities are used to initiate corrective actions. Several examples include:

- Self assessments by management;
- Evaluations by the IG or external auditor; and
- Direct testing.

C. Evaluate Internal Control at the Process, Transaction, or Application Level

1. Determine Significant Accounts or Groups of Accounts

For each financial report identified in the scope of the assessment, identify those accounts or groups of accounts that individually or collectively could have a material effect on the financial report. Agencies should consider qualitative as well as quantitative measures to determine material items.

2. Identify and Evaluate the Major Classes of Transactions

For each significant account or group of accounts, identify the major classes of transactions that materially affect those accounts. In identifying transactions, specifically consider whether a class of transactions is routine, non-routine, or represents an accounting estimate. This type of classification can help the senior assessment team identify the inherent risk and the controls necessary to adequately mitigate such risks. The assessment should include obtaining an understanding of the specific processes and document flow involved in each class of transactions. Thoroughly understanding the processes and document flow will help in understanding where errors could occur and what control objectives and techniques may prevent or detect those errors.

3. Understand the Financial Reporting Process

Obtaining an understanding of the process and workflow that links the accounting system to the financial report(s). Often times, financial information is not directly transferable from the accounting system to the financial report, but requires intervening calculations, summarizations, etc. This represents another point where errors can be introduced into the financial report, and it is important to understand where such errors could occur and what control objectives and control techniques can prevent or detect these errors.

4. Gain an Understanding of Control Design to Achieve Management's Assertions

Prepare a control evaluation(s) for each significant account or group of accounts that aligns specific controls with management's assertions for each account or group of accounts. An individual assessment of the potential effectiveness of the design of the controls for each account or group of accounts should be made considering the risk of error and the controls that are designed and in place to prevent or detect such errors. Assessing the effectiveness of the design of a control is concerned with whether the control is suitably designed to prevent or detect a material error related to an account or group of accounts. Procedures to obtain such evidential matter ordinarily include inquiries of appropriate agency personnel; inspection of documents, reports, or electronic files; and observation of the application of specific controls. This is sometimes referred to as a "walk-through" and helps the senior assessment team ensure its understanding of the controls. An assessment of the control design should identify controls as effective, moderately effective, or not effective.

5. Controls Not Adequately Designed

If a control over a significant account or group of accounts is missing or its design is determined to be not effective considering the associated risk of error, the senior assessment team does not need to test this control for the purpose of concluding on control effectiveness. This instance should be noted in the report of deficiencies and suggestions for improvement. However, management may nevertheless seek to further test affected transactions to determine if there was any actual loss, fraud, error, improper payment, or noncompliance resulting from those ineffective controls.

6. Test Controls and Assess Compliance to Support Management's Assertions

For those controls whose design is deemed effective or moderately effectively, the senior assessment team should test those controls to determine the extent to which the controls were applied, the consistency of their application, and who applied them. Tests of controls ordinarily include procedures such as inquiries of appropriate agency personnel; inspection of documents, reports, or electronic files, indicating performance of the control; observation of the application of specific control; and reperformance of the application of the control by the senior assessment team. If testing indicates that a significant control is not operating as designed, it should be reported as a deficiency.

D. Overall Assessment of the Design and Operation of Internal Control over Financial Reporting

The final step in the assessment is an overall conclusion as to the design and operation of the internal controls over financial reporting based on the assessments at the entity level and the process, transaction, or application level. The overall assessment should conclude whether the internal controls over financial reporting are operating effectively or whether material weaknesses exist in the design or operation. A template for the Statement of Assurance can be found in Exhibit 2.

E. Reliance on Other Work to Accomplish Assessment

The assessment of internal control over financial reporting should be coordinated with other activities to avoid duplication of efforts with similar activities. For example, agencies are required to perform reviews of financial systems under FFMIA or information security under FISMA. Reviews performed by management, or at management's direction, may be used to help accomplish this assessment. Management may consult with the agency IG to plan and coordinate related work. The IG may be involved in a consulting capacity but shall not conduct management's assessment of internal controls over financial reporting.

Control weaknesses at a service organization could have a material impact on the controls of the customer organization. Therefore, management of cross-servicing agencies will need to provide an annual assurance statement to its customer agencies in advance to allow its customer agencies to rely upon that assurance statement. Management of cross-servicing agencies shall test the controls over the activities for which it performs for others on a yearly basis. These controls shall be highlighted in management's assurance statement that is provided to its customers. Cross-servicing and customer agencies will need to coordinate the timing of the assurance statements.

IV. DOCUMENTATION

A. Documenting Internal Control over Financial Reporting

The senior assessment team should document its understanding of the agency's internal control over financial reporting. The form and extent of documentation depends in part on the nature and complexity of the agency's controls, the more extensive and complex the controls, the more extensive the documentation. Documentation may be electronic, hard copy format, or both and be readily available for examination. Documentation could include organizational charts, flow charts, questionnaires, decision tables, or memoranda. Documentation may already exist as part of normal agency policy or procedure; however, the senior assessment team should separately identify, verify, and maintain the documentation it uses in making its assessment. The documentation prepared by internal or external auditors may also be used, but again, the senior assessment team must take responsibility and verify and maintain that documentation. Documentation should also include appropriate representations from officials and personnel responsible for monitoring, improving and assessing internal controls. After an initial assessment, subsequent assessments may focus on updating existing documentation. All documentation and records shall be properly managed and maintained; therefore, agencies will need to establish, or review existing retention policies for documentation (paper and electronic media).

B. Documenting the Assessment of Effectiveness

The senior assessment team must also document the assessment process of internal control over financial reporting, including:

- The establishment of the senior assessment team, its authority and members;
- Contracting actions if contractors are used to perform or assist in the assessment;
- Communications with agency management and employees regarding the assessment;
- Key decisions of the senior assessment team;
- The assessment methodology and guide;
- The assessment of internal control at the entity level;
- The assessment of internal control at the process, transaction, or application level;
- The testing of controls and related results; and
- Identified deficiencies and suggestions for improvement.

The documentation may be electronic, hard copy format, or both, and should be available for review. Documentation should also include appropriate representations from officials and personnel responsible for monitoring, improving and assessing internal controls.

V. MANAGEMENT'S ASSURANCE STATEMENT ON INTERNAL CONTROL OVER FINANCIAL REPORTING

An agency's management is required to include an assurance statement on the internal controls over financial reporting in its annual Performance and Accountability Report as described in Section VI. Reporting on Internal Control. This statement is management's assessment of the effectiveness of the agency's internal control over financial reporting as of June 30 of that fiscal year (see Exhibit 2). This assurance statement is required to include the following:

- A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the agency.
- A statement identifying the OMB Circular A-123, Management's Responsibility for Internal Control as the framework used by management to conduct the assessment of the effectiveness of the agency's internal control over financial reporting.
- An assessment of the effectiveness of the agency's internal control over financial reporting as of June 30, including an explicit conclusion as to whether the internal controls over financial reporting are effective.
- 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.
- If a material weakness is discovered after June 30, but prior to September 30, the statement identifying the material weaknesses should be updated to include the subsequently identified material weakness.

In its assurance statement on the internal controls over financial reporting, management is required to state a direct conclusion about whether the agency's internal controls over financial reporting are effective. The statement must take one of the following forms:

- Unqualified statement of assurance (no material weaknesses reported);
- Qualified statement of assurance, considering the exceptions explicitly noted (one or more material weaknesses reported); or
- Statement of no assurance (no processes in place or pervasive material weaknesses).

Management is precluded from concluding that the agency's internal control over financial reporting is effective if there are one or more material weaknesses. Management must make the final determination with regard to what constitutes a material weakness. Management is required to disclose all material weaknesses that exist as of June 30 of the current fiscal year.

Management may be able to accurately represent that internal control over financial reporting, as of June 30 of the agency's current fiscal year, is effective even if one or more material weaknesses existed during the period. To make this representation, management must have implemented improvements in internal control over financial reporting to mitigate the material weaknesses and have satisfactorily tested the effectiveness over a period of time that is adequate for it to determine whether, as of June 30 of the current fiscal year, the design and operation of the internal controls over financial reporting are effective.

A. Agencies Obtaining Audit Opinions on Internal Control

This Circular does not require a separate audit opinion on internal control over financial reporting. Agencies may at their discretion elect to receive an audit opinion on internal control over financial reporting. Agencies electing to receive an audit opinion on internal control over financial reporting may adjust the "as of" reporting date of June 30 to coincide with the "as of" date of the audit opinion on internal control. Refer to Appendix A Section VI. Correcting Material Weakness in Internal Control over Financial Reporting for special circumstances requiring an opinion level of assurance.

VI. CORRECTING MATERIAL WEAKNESSESS IN INTERNAL CONTROL OVER FINANCIAL REPORTING

Each agency shall establish systems to assure the prompt and proper resolution and implementation of corrective action on identified material weaknesses. These systems shall provide for a complete record of action taken on the material weaknesses identified. Management's process for resolution and corrective action of the identified material weaknesses in the internal controls over financial reporting must also meet the standards listed in Section V. Correcting Internal Control Deficiencies.

If the agency cannot meet the deadlines outlined in the approved corrective action plan, OMB may, at its discretion, require the agency to obtain an independent audit opinion of their internal control over financial reporting as part of their financial statement audit.

Exhibit 2: Sample Annual Assurance Statement on Internal Control over Financial Reporting

Fiscal Year 2xxx

Annual Assurance Statement on Internal Control over Financial Reporting

The [Agency's] management is responsible for establishing and maintaining effective internal control over financial reporting, which includes safeguarding of assets and compliance with applicable laws and regulations. The [Agency] conducted its assessment of the effectiveness of the [Agency's] internal control over financial reporting in accordance with OMB Circular A-123, Management's Responsibility for Internal Control. Based on the results of this evaluation, the [Agency] can provide reasonable assurance that internal control over financial reporting as of June 30, 2xxx was operating effectively and no material weaknesses were found in the design or operation of the internal controls over financial reporting.

____

Head of the Agency

SECTION 2
CHAPTER 1
GUIDELINES TO EVALUATE
INTERNAL CONTROL OVER FINANCIAL REPORTING

BACKGROUND AND AUTHORITY

Developing a comprehensive assessment plan to evaluate internal control over financial reporting is essential to effective implementation of revised OMB Circular A-123. Management is responsible for establishing and maintaining the operational effectiveness and design of the Department's internal control environment. This requires evaluating, testing, and correcting internal controls independent of auditors, including the OIG.

The revised OMB Circular A-123, *Management's Responsibility for Internal Control*, provides updated internal control standards and new specific requirements for conducting management's assessment of the effectiveness of internal control over financial reporting. (See OMB Circular A-123--Appendix A.).

The Department's framework for the assessment is *Standards for Internal Control in the Federal Government*, issued by the GAO in November 1999 (and outlined in 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; (3) and 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 controls. COSO uses a matrix to illustrate the direct relationship between objectives, control components. The third dimension of the matrix is those units or activities that relate to internal control.

In conducting an evaluation of internal control over financial reporting, personnel should first plan and scope the evaluation. Effective planning is critical. Then, reviewers should document the significant controls, evaluate design and operating effectiveness of control over financial reporting, and document evaluation results. Management must identify and correct deficiencies and report on internal controls in management's written assertion.

SECTION 2
CHAPTER 2
PLAN AND SCOPE OF THE EVALUATION

The key organizing and planning steps are:

- Establish the process
- Significant financial reports
- Materiality thresholds
- Significant accounts
- Relevant financial report assertions
- Major transaction cycles
- Link accounts and transaction cycles
- Establish overall organizational approach

ESTABLISH THE PROCESS

There is a difference between the overall Federal Managers' Financial Integrity Act of 1982 (FMFIA) assurance statement that the Department has been issuing since 1983 and will continue to issue and the assessment of internal controls for financial reporting required by the 2004 revision to OMB Circular A-123. The overall FMFIA assurance statement addresses the three overall objectives of internal control: effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. The assurance statement on internal control is a subset of the existing FMFIA assurance statement. It requires management to specifically document the process and methodology used to evaluate the operating effectiveness of internal control.

Determine the Overall Approach: A Top-Down Focus. Under 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, the Department will meet the strengthened monitoring requirements through a top-down approach focusing on the assurance at the Departmentwide level. This approach begins with the Department's significant consolidated financial reports and works back to the key processes, controls, and supporting documentation. This approach also focuses resources on the items most material and most at risk to the Department's financial reporting.

Organizational Structure. DOI has established an integrated organizational structure to implement the Internal Control Program. This structure starts with the Secretary descends to the program assistant secretary, to the bureau director, and finally to the program manager. Roles and responsibilities of key components of the Internal Control Program are described below.

Roles and Responsibilities.

Senior Management Council (SMC) - within DOI, the responsibilities of the Senior Management Council are implemented by the DOI Internal Control and Audit Follow-up Council which is chaired by the Assistant Secretary-Policy, Management and Budget and is comprised of all program assistant secretaries, the Solicitor, the Inspector General (ex officio), Deputy Assistant Secretary for Business Management and Wildland Fire, the Chief Information Officer, and Senior Procurement Executive. The Council provides senior-level oversight of the Internal

Control and Audit Follow-Up programs, resolves issues related to both programs, and decides reporting issues for the Department's Annual Performance and Accountability Report (PAR). Specifically, the council will:

- Ensure DOI's commitment to an appropriate internal control environment;
- Approve DOI'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 effectiveness of internal controls over financial reporting;
- Recommend to the Assistant Secretary-Policy, Management and Budget which control deficiencies are material to disclose in the annual FMFIA assurance statement and PAR;
- Oversee implementation of corrective actions related to material weaknesses; and
- Determine when sufficient action has been taken to declare a reportable condition or material weakness corrected.

<u>Senior Assessment Team (SAT)</u> – The duties of the Senior Assessment Team as defined in Circular A-123 are assigned to the DOI Management Initiatives Team (MIT) which is chaired by the Assistant Secretary Policy, Management and Budget and comprised primarily of Deputy Assistant Secretaries and Bureau Deputy Directors. Duties of the MIT in implementing the Circular are to:

- Ensure assessment objectives are clearly communicated throughout Interior;
- Ensure adequate funding and resources are made available to comply with the new requirements of the revised Circular;
- Ensure 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 the revised Circular; and
- Determine or approve assessment design and methodology for each entity and the Department.

<u>Office of Financial Management (PFM)</u> is responsible for: (a) Providing staff assistance to the AS/PMB and the Senior Management Council; (b) Recommending internal control policies and procedures; (c) Providing oversight and guidance to the bureaus/offices concerning the review, evaluation, and maintenance of effective controls; (d) managing, directing, and evaluating the Department'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). PFM annually issues *Guidelines for Internal Control and Audit Follow-up Programs* providing that year's schedule of key actions.

<u>DOI Assessment Teams</u> – composed of bureau staff from each bureau assigned to test other bureau key controls and provide independent review. PFM is the project manager.

Provide training. Training should be developed and tailored to the level and type of involvement expected from participants in the process. Management, process owners, and those carrying out transaction cycles will need training applicable to their area of responsibility.

Appropriate training should be given to personnel whether involved in planning at a high level, preparing documentation, or testing controls.

Development of standard templates for documentation. Use standard templates, workpapers, and forms for documentation of all processes, testing, and conclusions to expedite the review and allow comparability of findings across the Department.

Document the Plan and Methodology for the assessment. The assessment of internal control over financial reporting should be documented as follows. This documentation should be readily available for review and should include appropriate representations from officials and personnel responsible for monitoring, improving, and assessing internal control.[1]

- The establishment of the senior assessment team, its authority and members
- Contracting actions if contractors are used to perform or assist in the assessment
- Communications with Interior's management and employees regarding the assessment
- Key decisions of the SAT
- The assessment methodology and guide, including:
    - The understanding obtained and the evaluation of the design of each component of the entity's internal control over financial reporting
    - The process used to determine significant accounts and disclosures and major classes of transactions, including determination of the locations or agency components at which testing was performed
    - The process and decisions supporting a test plan which forms the approach for evaluating all controls and possible contingencies for completing testing related to internal control over financial reporting (e.g., rotational testing schedule)
    - The reliance on the work of others, such as for cross-servicing entities or service organizations, and how the sufficiency of such work was determined
    - Other information that could affect management's certification of its internal control over financial reporting
- The assessment of internal control at the entity level (Refer to Addendum D)
- The assessment of internal control at the process, transaction, or application level (Refer to Exhibit 2 and Exhibit 3)
- The testing of controls and related results
- Identified deficiencies and their classifications
- The remediation plans and actions taken to correct identified deficiencies

Establish a process to communicate and coordinate with the OIG. The OIG is responsible for the audit of the Department's financial statements. Even if the OIG and any hired CPA firm are not performing an audit of Interior's internal control assessment, the OIG and the CPA firm are still required to evaluate and report on Interior's compliance with laws and regulations that include compliance with Circular A-123 and FMFIA. The auditor may rely in part on management's testing of internal control over financial reporting, so obtaining and incorporating the OIG and CPA firm's views of management's assessment plan provides the opportunity to design the evaluation in a way that enables the auditor to conduct a more efficient audit. In that same vein, it is prudent to integrate other control-related activities and determine internal assessments that may impact control objectives related to financial reporting.

[1] Circular A-123, Appendix A, Section IV.B.

Though not a requirement, Interior's management may ask the auditor to provide an audit opinion on internal control over financial reporting. In that case, the auditor should be involved in key aspects of the process, starting in the planning phase. Also, access to the project calendar allows the auditor to maximize the efficiency of interviews and testing processes by attending those significant to their opinion. If Interior's management elects to receive such an audit opinion, Interior may adjust the "as of" reporting date of June 30 to coincide with the "as of" date of the audit opinion.[2]

Establish standards for contract support personnel. Ensure that any contractors used to perform any aspect of the assessment, such as preparing the assessment plan, documentation, or performing testing have the appropriate qualifications. It is best for such contracts to clearly define the scope of performance so the contractor's work may be reviewed before it is included in management's final assessment.

Establish a basis to communicate, review, remedy, and obtain management concurrence. Management is responsible for documenting the internal control over financial reporting even if documentation has been prepared by the senior assessment team or others. Establish a process for management to review and comment on the documentation, those conducting assessments to respond to management's comments, and management to indicate its final decision on the effectiveness of internal control over financial reporting based on the evidence. The senior assessment team should retain evidence of the review and approvals through signatures or electronic postings.

Prepare a calendar. Interviews and meetings with Department and bureau management and personnel should be scheduled as early as is feasible and then posted to a calendar that is maintained and accessible. This allows process owners adequate time to plan the interviews and meetings, and it enables delays in the assessment to be identified and corrected before affecting deadlines. Testing of monthly and quarterly financial reporting should be scheduled throughout the year to balance workloads. Refer to the memo *Guidelines for Internal Control and Audit Follow-up Programs* issued annually by PFM for a schedule of key actions.

Establish a status reporting process. Status reports identify the status of all tasks relating to the assessment's critical paths, and ensure those affected by the assessment are kept informed of the assessment's progress, the upcoming steps, and any issues that need to be resolved. Status reports should be scheduled and issued on a regular basis which is posted in the calendar.

SIGNIFICANT FINANCIAL REPORTS

The Department has identified the following principal financial reports as "significant" and subject to Circular requirements[3]:

1. Annual/Quarterly Financial Statements
2. Year-end Financial Statement information supporting the Financial Report of the U.S. Government
3. SF-133, Report on Budget Execution and Budgetary Resources
4. SF-132, Apportionment and Reapportionment Schedule
5. SF-224, Statement of Transactions

---

[2] Circular A-123, Appendix A, Section V.A.
[3] Circular A-123, Appendix A, Section II.B.

6. FMS Form 2108, Year-End Closing Statement

Other reports may be subject to the Circular requirements based on qualitative and other criteria.

MATERIALITY THRESHOLDS

The Department should set materiality sufficiently low for the assessments to ensure that controls are in place to prevent and detect material internal control weaknesses, with goals to ensure timely, current, accurate, and accessible financial information. 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.

Planning Materiality. The Department should estimate 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 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.[4] Materiality should be reconsidered at least immediately prior to concluding on the assessment and determining what control weaknesses must be reported.[5] Refer to Addendum A for discussion on financial reporting items not covered by the financial statement materiality definition.

Interior's planning materiality for financial statement line items, based on net cost to the government (appropriations), is specified as 1% of Net Outlays for the prior fiscal year's Combined Statement of Budgetary Resources (the materiality base).

Testing Materiality. Interior's testing materiality is the same as planning materiality. Reviewers will assess material items. Management's materiality is well below the financial statement auditor's materiality defined by GAO as 1% of the larger of Assets or Expenditures.

Report Materiality. Report materiality is a function of management judgment, and it serves as a threshold of reporting control weakness as reportable or material, impacting whether an unqualified statement of assurance can be issued. In the reporting phase, the Department considers whether misstatements are quantitatively or qualitatively material. If considered to be

[4] Revised Circular A-123, Appendix A, Section II.C.

[5] Page 17 in CFO Council's *Implementation Guide for OMB Circular A-123, Management's Responsibility for Internal Control, Appendix A*

material, the Department is precluded from issuing an unqualified statement of assurance over financial reporting. Report materiality generally should be 3% of the materiality base.

SIGNIFICANT ACCOUNTS

For each applicable financial report, apply the materiality threshold to identify accounts or groups of accounts that may have a material effect on the respective financial report. Consider whether there is more than a remote likelihood that the account may contain misstatements (either an overstatement or understatement) that individually or in the aggregate may have a material effect on the financial report. Then, identify significant transactions that affect those accounts. Refer to Exhibit 1 for an example Internal Control Matrix with significant accounts.

Qualitative characteristics to consider include:

- Political sensitivity of a program or balance
- 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)
- Likelihood of significant contingent liabilities arising from the underlying activities
- Changes in account characteristics.

RELEVANT FINANCIAL REPORT ASSERTIONS

Map the financial report assertions to each of the significant accounts. Not all assertions will be relevant or significant to all accounts. The following are the types of assertions that may be inherent in the significant accounts[6]:

1. <u>Existence and Occurrence</u> – All reported transactions actually occurred during the reporting period and all assets and liabilities exist as of the report date.
2. <u>Completeness</u> – All assets, liabilities, and transactions that should be reported have been included, and no unauthorized transactions or balances are included.
3. <u>Rights of Ownership and Obligations</u> – The Department legally owns all assets, and all liabilities are its legal obligation.
4. <u>Valuation and Allocation</u> – All assets and liabilities have been properly valued and where applicable, all costs properly allocated.
5. <u>Presentation and Disclosure</u> – The financial report is presented in proper form with required disclosures.
6. <u>Compliance</u> – The transactions are in compliance with applicable laws and regulations.
7. <u>Safeguarding</u> – All assets have been safeguarded against fraud and abuse.
8. <u>Documentation</u> – Documentation for internal control, all transactions, and other significant events is readily available for examination.

Risks are associated with each type of assertion, so the team should review each significant account and determine the type of material error or misstatement that may occur for each assertion. This step is critical. The results of the evaluation of these assertions and identification

[6] Circular A-123, Appendix A, Section II.A.

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 Document Controls and the Evaluate Design and Operating Effectiveness phases.

MAJOR TRANSACTION CYCLES

Identify the major transaction cycles or classes of transactions that materially affect each of the significant accounts or groups of accounts. A major transaction cycle is a business process for which the quantity and dollar volume of transactions is so great that if a material error occurred in the process, it would affect the Department or bureau's decision-making process. For example, disbursement of funds is a major transaction cycle since a material error may affect several accounts, including Fund Balance with Treasury. Another consideration when identifying major transaction cycles and financial systems is whether the transactions are routine, non-routine, or represent an accounting estimate. Refer to Attachment 2 for transaction cycles that should be considered for testing.

LINK ACCOUNTS AND TRANSACTION CYCLES

Use mapping and link significant accounts to the transaction cycles and processes that provide the source data. List all significant accounts and ensure that each has the requisite transaction cycle(s) mapped to it.

ESTABLISH OVERALL ORGANIZATIONAL APPROACH

Interior is using a Departmentwide approach whereby analysis of the Departmentwide financial statements and identification of the significant line items helps determine which components, programs, or administrative functions contribute to those line items. Only those controls needed to provide sufficient evidence to provide assurance on the internal control over the Department's financial reporting are evaluated. This process will be repeated for all significant reports and all material line items included in the Department's assessment.

SECTION 2
CHAPTER 3
DOCUMENTING CONTROLS

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

Steps required:

- Document the assessment of effectiveness
- Document the major transaction cycles
- Assess the control environment
- Assess the risk assessment process
- Assess the control activities
- Assess the information and communication processes
- Assess the monitoring processes
- Obtain process owner's concurrence with the documentation of controls

DOCUMENT THE ASSESSMENT OF EFFECTIVENESS

The senior assessment team must document the assessment process of internal control over financial reporting, including[7]:

- The establishment of the senior assessment team, its authority and members;
- Contracting actions if contractors are used to perform or assist in the assessment;
- Communications with agency management and employees regarding the assessment;
- Key decisions of the senior assessment team;
- The assessment methodology and guide;
- The assessment of internal control at the entity level;
- The assessment of internal control at the process, transaction, or application level;
- The testing of controls and related results; and
- Identified deficiencies and suggestions for improvement.

The documentation may be electronic, hard copy format, or both, and should be available for review. Documentation should also include appropriate representations from officials and personnel responsible for monitoring, improving and assessing internal controls.

DOCUMENT THE MAJOR TRANSACTION CYCLES

Documentation is overseen by the Senior Assessment Team and managed by the Office of Financial Management. Documentation may include narratives, organizational charts, flow charts, questionnaires, decision tables, and memoranda. The first step is documenting the transaction cycles used for each of the significant accounts, groups of accounts, and transactions at bureaus and developing an understanding, from beginning to end, of the underlying processes and document flows involved in each transaction cycle. These are the processes for initiating,

---

[7] Circular A-123, Appendix A, Section IV.B.

authorizing, recording, processing, and reconciling accounts and transactions that affect the financial reports. The documentation process helps identify the controls that support the assertions made by management related to those accounts or transactions. And it will identify the places in the processes where an error or a misstatement due to error or fraud may occur. Consider multiple controls within the transaction cycle as a single control within a transaction cycle is normally not considered sufficient. Examples of controls that may be identified by management are listed in Addendum B.

To document the Department and bureau's major transaction cycles, gain an understanding of institutional knowledge; examine policy and procedures manuals; gather existing forms and documents; and develop transaction cycle memos (TCMs), process flowcharts, and control matrices. Use the process narrative or the flowchart to document the assessment team's understanding, and then summarize its understanding using the control matrices.

Institutional knowledge. Interviews should be conducted with personnel who have knowledge of the Department and bureau's operations to obtain an understanding of financial and operational business processes. Policy and procedures manuals define the way controls are supposed to function, but interviews with the personnel performing the processes are likely to reveal the way the controls actually operate. Moreover, interviewing the owners of the major classes of transactions may help to identify the controls in place.

Existing policy and procedure manuals. Existing policy and procedure manuals should be reviewed and referred to in the documentation. This is more effective than creating new documentation. If the manuals are obsolete or insufficient, management will be requested by the senior assessment team to update the manuals.

Existing forms and documents. The documentation process includes obtaining examples of the forms and other documents used by the bureau and then highlighting the evidence of controls on each documented example. For example, a person performing a reconciliation usually initials and dates a reconciliation form when he or she completes the reconciliation. Obtain a copy of the form, highlight the evidence of the control activity (e.g., initials and date), and include the form with the documentation. This process will enable the testing of controls, reviewing of project workpapers, and recurring annual assessments to be significantly more efficient.

Some level of documentation of internal controls over financial reporting should be maintained for all locations, including those not considered to be significant either individually or in aggregate. The extent of this documentation may vary across locations, and often is based on the financial significance of each location. This documentation may take many forms, including: policy manuals, accounting manuals, memoranda, flow charts, job descriptions, documents, decision tables, procedural write-ups, self-assessment reports, and other documentation as appropriate. The form and extent of documentation will vary depending on the bureau and office's size, complexity, and documentation approach. However, simply having manuals and policies without demonstration of any reconciliation to the assessment process is not sufficient.

Transaction cycle memos. TCMs provide a written summary describing each transaction's starting point, processing, and completion point. The TCM identifies significant or key controls in the process designed to meet the Department's control objectives and cover management's financial statement assertions. Management relies upon these key controls to prevent and detect material errors and misstatements. Write TCMs ensuring that a reader familiar with internal controls over financial reporting will understand the process. Since most cycles have many controls, number the controls and identify them by control type. The process owners should review TCMs and ensure that the key controls identified are appropriate and completely address identified risks.

Transaction cycle flowchart. Transaction cycle flowcharts are an efficient way to document key controls in a process, provide basis to confirm the TCMs' accuracy with the process owners, and help identify if more than one control accomplishes the same objective of reducing the risk of an error or misstatement within a process. A flowchart marking key controls with control numbers assigned in the TCM allows comparability with the narrative.

Internal control matrices. Control matrices are an efficient approach to documenting and understanding the key controls and specific risks. A control matrix 1) lists the risks and assertions for an account or line item and the control characteristics that cover the assertions; 2) cross-references the controls to the risks they address; and 3) notes the effectiveness of the process design and operation. It also provides information about the type, level, frequency, objectives, and significance of the controls. This information enables quick determination of an identified risk for which there is no key control. If the risk is determined valid by the process owners, a related control must be present, or there is a gap in internal controls that must be remedied. Refer to Exhibit 1 for a sample internal control matrix.

ASSESS THE CONTROL ENVIRONMENT

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.

Conduct interviews and surveys to document management's leadership style and the tools management uses to achieve control environment objectives. Automated surveys may help gain a sense of the control environment and point to areas needing additional focus. This serves as evidence of due diligence in assessing the general control environment. A conclusion should indicate whether each of the following aspects of the general control environment is adequate:

- Integrity and Ethical Standards [Integrity, Competence, Attitude, Compliance with Laws]
- Commitment to Competence [Integrity, Competence, and Attitude]
- Management's Relationship with Oversight (Congress, OMB, Etc.)
- Management's Philosophy and Operating Style [Integrity, Competence, and Attitude]
- Organizational Structure [Delegation of Authority and Responsibility]
- Assignment of Authority and Responsibility [Delegation of Authority and Responsibility]
- Human Resource Policies and Practices [Integrity, Competence, Attitude, and Compliance with Laws]
- Compliance with other applicable laws (FMFIA, FFMIA, CFO Act, Inspector General Act of 1978, as amended (IG Act), Financial Information Security Management Act of 2002 (FISMA), Improper Payments Information Act of 2002 (IPIA), Government Performance and Results Act (GPRA), Single Audit Act, as amended, and Clinger-Cohen Act of 1996)

ASSESS THE RISK ASSESSMENT PROCESS

Identify Risk Factors for Financial Reporting. Risk assessment relates to how management considers risks relevant to financial reporting objectives and decides about actions to address those risks. Evaluate management's processes for determining the level of risk related to internal controls over financial reporting and determine actions to address those risks. Starting with the Department's process for complying with GPRA, this includes determining how organization objectives are established, identifies risks that would prevent achievement of the objectives, estimates the significance of the risks in relation to financial reporting, assesses the possible existence of the risks in the current environment, and continues to monitor changes to the environment that may increase or reduce the risks. The results of this assessment at the Departmentwide level will drive the extent of testing and review that needs to be performed at the process, transaction, and application levels.

Consider the following circumstances or events affecting risk:

- Complexity or size of programs, operations, transactions, etc.
- Decentralized versus centralized operations, accounting, and reporting functions
- Extent of manual or automated processes or applications
- New or amended laws, regulations, or accounting standards
- Changes in the operating environment
- Significant new or changed programs or operations
- Restructurings or budget cutbacks which may include downsizing and changes in supervision and segregation of duties
- New personnel or significant personnel changes
- New or revamped information systems
- New technology
- Existence of related party transactions
- Accounting estimates

Prepare a summary of specific risks of misstatement for each significant line item, which will be used to determine the testing plan. The summary should include a list of the significant line items or accounts, related balances and financial statement assertions, and the related risks. Assess the control or combined risk for each assertion, document the assessment, and prepare the testing plan. Refer to Addendum 3 and Exhibit 1 and 2 for additional information and sample templates of the summary of risks.[8]

The types of risks identified may be adapted in determining the testing plan for internal control over financial reporting.

- <u>Inherent risk</u> – the susceptibility of an assertion to misstatement, assuming there are not related specific control activities. Inherent risk factors include: the nature of the Department or bureaus' programs, transactions and accounts and whether the Department had significant audit findings.
- <u>Control risk</u> – the risk that misstatements will not be prevented or detected by the Department or bureaus' internal control (assess separately for each significant financial statement assertion in each significant cycle or accounting application).

[8] Page 19 in CFO Council's *Implementation Guide for OMB Circular A-123, Management's Responsibility for Internal Control, Appendix A*

- Combined risk – the likelihood that a material misstatement would occur (inherent risk) and not be prevented or detected on a timely basis by the Department or bureaus' 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.
- Detection risk – the risk that management will not detect a material misstatement that exists in an assertion.

Identify Control Objectives that Reduce or Eliminate Identified Financial Reporting Risks. Control objectives should address financial processes at each bureau or office. Control objectives are the positive effects that management tries to attain or an adverse condition or negative effect that management seeks to avoid. Controls should provide reasonable, but not absolute assurance of deterring or detecting misuse of resources, failure to achieve program objectives, noncompliance with laws, regulations, and management policies. Controls should be reasonable and weighed against their cost and potential gain. Some control objectives and/or activities that may eliminate or reduce financial reporting risks are:

- Personal integrity and trustworthiness;
- Background investigations and favorable screening;
- Management team that provides continuity and stability;
- Sufficient resources to perform the various job functions;
- Staff possess the requisite knowledge, competencies, and experience;
- Safeguarding of assets and compliance with laws and regulations;
- Physical security/access;
- Segregation of duties;
- Restricted access to resources, records, systems, etc;
- Authorization and approval (supervision) over information and systems;
- Review and reconciliation of financial transactions;
- Transactions and other significant events are well documented in policies and procedures;
- Transactions and events are promptly recorded by authorized persons;
- Adequate internal controls over third party systems or activities;
- Sufficient internal controls in areas that could result in personal gain;
- Adequate training (continuing education) exists that provides staff with technical and ethical training to ensure current knowledge of new rules, regulations, and practices;
- Monitoring of the above control activities to ensure processes, systems and controls are updated and being followed; and
- Sufficient testing to determine whether controls are adequate and consistently applied.

ASSESS THE CONTROL ACTIVITIES

Control activities are policies, procedures, and mechanisms that help ensure the control objectives are met and that management's assertions in the financial reporting are valid. Control activities include preventative or detective controls and may be either manual or automated.

Control activities that may be present include[9]:

- Policies and procedures

[9] Pages 12-16 in GAO's *Standards for Internal Control in the Federal Government* (report AIMD-00-21.3.1), issued November 1999.

- Management objectives
- Top-level reviews of actual performance
- Review and analysis by management at the functional or actual level
- Management of human capital
- Controls over information processing (planning and reporting systems)
- Physical controls over vulnerable assets
- Establishment and review of performance measures and indicators
- Segregation of duties
- Proper execution of transactions and events
- Accurate and timely recording of transactions and events
- Access restrictions to and accountability for resources and records
- Appropriate documentation of transactions and internal control

Reviews by management should be coupled with another control technique to sufficiently mitigate risk. As part of the evaluation, identify any manual controls that are either redundant or secondary to a primary automated control. Redundant and secondary controls that are not effective or not providing the desired level of risk mitigation may be eliminated.

There are three unique elements of control activities that need to be evaluated: information technology controls, third-party service providers, and fraud.

Information technology controls. Interior relies on information technology (IT) controls to perform its missions, manage processes, and report financial information. Evidence that IT system components are operating effectively supports the assessment of internal controls over financial reporting. Applicable system components (e.g. calculations, accumulations, interfaces, and reports) are those affecting significant accounts or disclosures and other relevant financial assertions. Evaluate the following elements of IT controls:

- General IT policies and procedures. General IT policies and procedures are controls relating to key areas like IT strategic planning, budgeting, roles and responsibilities, segregation of duties, resource management, and third-party providers. The Department is integrating the assessment of IT controls as part of the evaluation of internal controls over financial reporting. Compliance with FFMIA and FISMA serve as a foundation for documenting and evaluating the IT controls over financial reporting.
- IT general controls:
    - Systems development and change management. Ensure that IT systems perform their intended functions in an unimpaired manner, free from unauthorized or inadvertent manipulation, and are able to achieve data completeness, accuracy, and timeliness.
    - Availability. Key financial systems subject to outage would adversely affect internal controls because the capability to process, retrieve, and protect data is vital to the Department's ability to accomplish its mission. Key elements related to data availability that need to be considered are business continuity, contingency plans, and environmental and hardware maintenance controls.
    - Information security. The Departmentwide IT security program develops policies, assigns responsibilities, monitors security-related controls, and otherwise manages security risks. Access controls for general support systems and applications should provide reasonable assurance that computer resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized alteration, disclosure, loss, or impairment.

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

Refer to Section 3 for more in-depth information on Interior's IT systems and programs.

Multiple Locations. Interior and its bureaus are comprised of many locations. Stratifying[10] these locations into groups that are expected to behave similarly with respect to audit measures can improve efficiency and the sample results. The stratification should be based on the relative size or qualitative factors such as inherent risk or control risk. If exact information is not available, then estimates may be used. Locations may be stratified into a top, intermediate, and bottom stratum. Criteria for stratifying may include the following factors:

- Amount of assets
- Amounts of revenue or expenses incurred or processed at the location
- Number of personnel, where payroll costs are significant
- Amount of appropriations
- Concentration of specific items (e.g., inventory storage locations)
- Inherent and control risk, including fraud risk and management turnover
- Special reporting requirements (e.g., separate reports, special disclosures)

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

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

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

- Type I Report: A Type I report covers the design of a service provider's controls.

[10] GAO's *Financial Audit Manual*, Section 295

- Type II Report: A Type II report covers both the design and the operating effectiveness of the service provider's controls.

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

- Type of opinion. If the opinion is not unqualified, obtain an understanding of the nature of the auditor's findings and how these findings may affect the operating effectiveness of Interior's internal controls over financial reporting.
- Period of time covered. The report should cover a sufficient portion of the assessment period to provide evidence of the operating effectiveness for the entire assessment period. If a significant period of time has passed between the end of the time period covered by the service auditor's test of controls and the date of assessment, perform procedures to determine any information in the SAS 70 Type II report in need of update to reflect significant changes in the service organization's controls.
- Scope of the report. Evaluate the report to ensuring coverage of all key controls that need to be tested to provide evidence of the operating effectiveness of internal controls over financial reporting over the functions performed by the service provider.
- Consistency of results with management's review of the service provider. Determine if the results listed in the Type II report are consistent with the results from management's day-to-day review of the accuracy of the service provider.

Fraud. Controls needed to prevent, detect, and correct fraudulent financial reporting should be identified and documented. Normally, these are controls related to estimates and assets that are liquid and more susceptible to misappropriation or theft. Independent verification of and concurrence with the estimating methodology and the data elements of the estimating assumptions are likely to prevent fraudulent financial reporting. Safeguard controls such as restriction of access, requirements for authorizations, and separation of duties may also prevent fraudulent reporting resulting from misappropriation or theft of liquid assets.

Three conditions are generally present when fraud occurs[11]:

- Incentive/Pressure. Management, other employees, or external parties have an incentive or are under pressure, which provides a motive to commit fraud.
- Opportunity. Circumstances exist, such as ineffective or absent controls or the ability of management to override controls that provide an opportunity to commit fraud.
- Attitude/Rationalization. Individuals involved are able to rationalize committing fraud. Some individuals possess an attitude, character, or ethical values that allow them to knowingly and intentionally commit a dishonest act.

ASSESS THE INFORMATION AND COMMUNICATION PROCESSES

Relevant, reliable, and timely information related to financial reporting should be communicated to relevant personnel at all levels within the Department. To that end, evaluate and document the Department's financial reporting processes to determine what information is based upon

[11] GAO's *Financial Audit Manual*, Section 260

integrated systems or the same source information; whether the information is recorded and communicated in a form and within a time frame that enables managers, operating personnel, and others within the Department who require the information to carry out their internal control, operational, and other responsibilities; and whether the information is made available outside the Department, as appropriate. Documentation should include the evidence reviewed, inquiries performed, and the conclusion as to whether the process is effective. Any aspects of the process found ineffective in the conclusion should be remedied by management. Evaluate the notification to employees of their control-related duties and responsibilities and the manner in which incoming external communications are handled. These responsibilities are usually documented in position descriptions, policy and procedures manuals, written memos and letters that identify and confirm actions taken, meeting agendas, meeting minutes, and oral communications.

ASSESS THE MONITORING PROCESSES

Monitoring the effectiveness of internal control should occur as the normal course of business. Evaluate in what manner the Department and bureaus are monitoring and evaluating the internal control environment and identifying and correcting deficiencies in a timely fashion throughout the year. Consider:

- Ongoing monitoring activities. Look for regular management and supervisory review, comparisons between planned and actual performance, and reconciliations between systems as a part of the regular assigned duties of personnel who affect the Department's financial reporting.
- Performing separate evaluations. Determine processes and resources in place to perform ongoing testing to monitor the operating effectiveness of internal control over financial reporting. Look for inquiries of unusual matters, detail testing of selected transactions, and periodic analysis of trends.
- Reporting deficiencies. Evaluate the process for reporting deficiencies in operating effectiveness to the appropriate level of management, undertaking corrective action in a timely fashion, and tracking the status of corrective actions.

OBTAIN PROCESS OWNER'S CONCURRENCE WITH THE DOCUMENTATION OF CONTROLS

All TCMs, flowcharts, and control matrices should be reviewed and approved by personnel responsible for the respective business processes, transaction cycles, or contract activity. All process owners' comments should be retained and marked to indicate how the comments were resolved. Each comment should result in either a change to the documentation or, if no change occurs, acknowledgement by the process owner that, after further explanation, the comment is not relevant. After addressing the comments, the process owner should sign and date the documentation to show that management has accepted the documentation as a correct representation of the process and controls.

SECTION 2
CHAPTER 4
EVALUATING DESIGN AND OPERATING EFFECTIVENESS

Evaluating the design and operating effectiveness of internal controls involves three steps that are used to test all key controls needed to support management's assurance statement on internal control over financial reporting:

- Assess the design of key controls
- Define and document the testing approach
- Test the key controls

EVALUATE THE DESIGN OF KEY CONTROLS

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. The design of key controls may be evaluated through interview, inquiry, 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[12]:

- 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?

The reviewer should document the results of the evaluation of design in a memorandum that includes 1) the name and contact number of any person interviewed, the specific items selected for evaluation, the results of the evaluation, and his or her conclusion regarding whether the control is designed properly and 2) was it effective, moderately effective, or not effective. The documentation memorandum should note an identifying number, amount, and date for each transaction reviewed, and be written in sufficient detail to enable someone of similar knowledge to reperform the evaluation using the same items.

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 a list of deficiencies and suggested for improvement with enough space to note the nature of the deficiencies. Further testing of transactions subject to such controls help determine if any actual loss, fraud, error, improper payment, or noncompliance occurred.

DEFINE AND DOCUMENT THE TESTING APPROACH

Test if key controls that were deemed effective or moderately effective function as they were designed. The test determines 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, use a testing approach that defines the nature, timing, and extent of testing necessary to provide sufficient evidence to support management's assertion. This requires that the TCMs, flowcharts, and internal control matrices be reviewed; the controls to be tested be listed in a test program with

[12] Page 28 in CFO Council's *Implementation Guide for OMB Circular A-123, Management's Responsibility for Internal Control, Appendix A*

the nature, timing, and extent of testing for each control defined; and the controls in the test program be cross-referenced with the memos, flowcharts, and control matrices to ensure all are tested. The testing should address both manual and automated controls. When the IT control environment is considered effective, greater reliance with less testing may be appropriate for those automated controls as compared to manual controls.

Nature of testing. An acceptable testing procedure should be developed for each key control. Acceptable tests include:

- Inspection of documents, reports, or electronic files demonstrating control performance
- Reperforming the application of specific controls
- Observing the application of specific controls in operation
- Inquiry of appropriate personnel
- A walkthrough tracing a transaction from origination through the information system until the transaction is reflected in the financial reports. A walkthrough encompasses the entire process of initiating, authorizing, recording, processing, and reporting individual transactions and controls for each significant process.

Evaluation at the Departmentwide 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. Questionnaires and checklists are most useful at this level. Adapt the Department's automated survey and assessment tool based on the GAO Assessment Tool for evaluation of internal control to assist in assessing internal control at the entity-wide level.

Tests of design at the process level are usually performed by inquiry and observation; or inspection of documents, such as reports and completed forms; or through on-screen prompts, such as errors or warnings. Tests of design typically address the:

- Type of control, including configuration, management review, and authorization
- Nature of the control (i.e., automated or manual, preventive or detective)
- Frequency of the control (e.g., daily, weekly, monthly)
- Experience and competence of the individual performing the control
- Error investigation and correction procedures, including the timeliness of such procedures. It is important to note that inquiry alone ordinarily is not sufficient to support design effectiveness.

Timing of testing. Testing should be schedule throughout the year or quarterly for those controls that coincide with preparation of quarterly financial statements to OMB. Certain financial reporting controls have 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.

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, and signed off by the affected process owners. The extent of testing also depends on the risk of failure of the control defined as the risk of a material misstatement arising from the failure of a control. If it is believed there is a high risk of failure, expand the extent of testing for that control. Factors that affect whether the control may represent a higher risk of failure include:

- Changes in the volume or nature of transactions
- Changes in the design of controls

- The degree to which the control relies on the effectiveness of other controls
- Changes in key personnel who perform the control or monitor its performance
- Degree to which the control relies an individual's performance rather than automation
- The complexity of the control

Statistical and judgmental sampling may be used to limit the number of transactions and other items tested, yet ensure the testing is adequate for the conclusions to be drawn and provide sufficient evidence to support management's assurance statement. Statistical sampling may be the most efficient approach for tests of complex controls (e.g. several locations, many samples throughout the year). The GAO and AICPA offer statistical sampling approaches for financial statement audit purposes that may be used alone or in combination with judgmental sampling.

To determine the sample size for controls at various locations, the auditor uses judgment to determine three factors: the confidence level, the tolerable rate (maximum rate of deviations from the prescribed control acceptable without altering the preliminary assessment of control effectiveness), and the expected population deviation rate (expected error rate). Once these factors are determined, software such as Interactive Data Extraction and Analysis (IDEA) or tables are used to determine sample size and how many deviations may be found without having to change the control risk assessment. Developing a representative sampling plan may require the use of a qualified statistician to define expected error rates and the level of confidence obtained from actual error rates.

TEST THE KEY CONTROLS

Test the controls are operating effectively and the assertions valid compared to the acceptable level of error documented in the testing plan. 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 reperformance of transactions or controls will determine if the controls perform as designed and allow others to duplicate the reperformance if needed.

SECTION 2
CHAPTER 5
IDENTIFYING AND CORRECTING DEFICIENCIES

Identifying and correcting deficiencies involves four steps:
- Interpret the results
- Categorize the types of control deficiencies
- Attempt to remedy deficiencies and test remedied controls
- Changes in status between June 30 and September 30

INTERPRET THE RESULTS

Analyze the results and determine if the error rate on each control exceeded the acceptable error rate as written in the plan or was high enough to allow material errors or misstatements to occur without detection. Beyond just dollar amounts, consider whether a control that is not executed properly or consistently would allow a material error or misstatement to occur and not be detected and the control's importance or significance. Process owners should review and validate detected errors and determine if compensating controls may mitigate the problem. A compensating control is a technique or other effort(s) designed to mitigate the absence of a control or to mitigate a deficiency in control design or operating effectiveness. The sampling plan should allow for the expansion of the sample to determine if the initial error rate is correct when it appears the original smaller sample was not representative of the function of the controls. If, after additional testing, the control is still considered to be not functioning, it should be documented as deficient (i.e., a control that is not functioning nor is mitigated by other controls).

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

CATEGORIZE THE TYPES OF CONTROL DEFICIENCIES

An internal control deficiency[13] 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 errors or misstatements on a timely basis. A deficiency in design keeps the control objective from being met even when the control functions as designed. A deficiency in operation is a properly designed control does not operate as designed or is performed by an unqualified or improperly skilled person. Deficiencies are categorized as follows:[14]
- <u>Simple deficiency</u> - generally an anomaly and creates minimal exposure for management (e.g. missing initials indicating a supervisor's review on 1 of 26 reconciliations sampled).

[13] Control deficiency and related reportable condition and material weakness are based on the definitions provided in <u>Auditing Standard No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements</u> issued by the Public Company Accounting Oversight Board (PCAOB) and referred to in the <u>Implementation Guide for OMB Circular A-123, Management's Responsibility for Internal Control, Appendix A</u>

[14] Page 38 in CFO Council's *Implementation Guide for OMB Circular A-123, Management's Responsibility for Internal Control, Appendix A*

- Significant deficiency - indicates a history of internal control deficiencies that when consolidated equate to a reportable condition (e.g. only 8 months of reconciliations were performed for the year).
- Reportable condition - significant internal control deficiency, or combination of control deficiencies, that adversely affects Interior's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles to such a degree that there is more than a remote[15] likelihood that a misstatement in the financial statements, or other significant financial reports, that is more than inconsequential[16] 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 (e.g. reconciliation of several key accounts were not performed throughout the year, only at year-end).

List each control deficiency and note whether it is mitigated by a compensating control. If it is not mitigated or can not be tested then decide if the deficiency is significant enough to report outside Interior. Weaknesses significant enough to report outside Interior must be included in Interior's assurance statement that is included in the PAR. Significant deficiencies identified under FISMA should also be considered material weaknesses to be included in the assurance statement if they might cause a material misstatement to the Department's financial reports included in the assurance statement.

OMB requires that a corrective action plan (CAP) be developed for each material weakness, reportable condition, other control deficiency, and "non-conformances" with the financial system requirements. Refer to Section I Chapter 4 for additional information on CAPs.

ATTEMPT TO REMEDY DEFICIENCIES AND TEST REMEDIED CONTROLS

Attempting to correct control deficiencies as they are identified benefits the Department by improving the controls in the current fiscal year and allowing 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. Review the Department's plan for correcting deficiencies to ensure that sufficient time is available to both complete the remediation and retest the controls prior to either the assessment date (June 30) or the fiscal year-end (September 30). 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.

This testing should be tracked on the assessment calendar to ensure that it covers transactions in the proper period. Any 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.

---

[15] The term "remote" is defined in the Statement of Federal Financial Accounting Standards (SFFAS) No. 5, Accounting for Liabilities of the Federal Government. as the chance of the future event(s) occurring is slight.

[16] The PCAOB Auditing Standard No. 2 specifies that a misstatement is inconsequential if a reasonable person would conclude, after considering the possibility of further undetected misstatements, that the misstatement, either individually or when combined with other misstatements, would clearly be immaterial to the financial statements. If a reasonable person could not reach such a conclusion regarding a particular misstatement, that misstatement would be more that inconsequential.

CHANGES IN STATUS BETWEEN JUNE 30 AND SEPTEMBER 30

Evaluate internal controls from June 30 to the fiscal year-end to determine areas needing update by considering any weaknesses disclosed at June 30, whether those weaknesses have been corrected, or whether any new weaknesses have been identified. Consider the effects and update the Department's initial report to include all errors constituting a material weakness at year-end.

The 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
  - Major changes in the Department's mission or programs
  - Reorganizations or other changes to the Department's organizational structure
  - Significant increases or decreases in staffing levels
  - 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

SECTION 2
CHAPTER 6
REPORTING ON INTERNAL CONTROL

The Secretary of the Interior reports on the effectiveness of internal controls over financial reporting. This involves two steps:

- Arriving at the overall conclusion
- Preparing management's assurance statement

ARRIVING AT THE OVERALL CONCLUSION

Management's conclusion as to the operating effectiveness of internal controls is based on the results of the assessment performed at the Departmentwide level and of assessments made at the component, process, transaction, application, and other subordinate levels. Bureau heads will provide assurance to the Secretary by signing the statement of assurance and submitting it through the bureau's assistant secretary. Refer to Exhibit 4 for a sample assurance letter.

Management should state its conclusion in one of the following ways:

- Unqualified statement of assurance (no material weaknesses to report)
- Qualified statement of assurance (one or more noted material weaknesses)
- Statement of no assurance (pervasive material weaknesses or no processes in place)

PREPARING MANAGEMENT'S ASSURANCE STATEMENT

The final step in reporting is for management to prepare an assurance statement on internal controls over financial reporting to be included in the PAR. Refer to Exhibit 5A, 5B, and 5C for sample assurance letters. The purpose of the statement is to report the results of management's assessment of the effectiveness of internal controls over financial reporting as of June 30 of that fiscal year. The assurance statement must include the following:

- A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the Department
- A statement identifying OMB Circular A-123, *Management's Responsibility for Internal Control*, as the framework used by management to conduct the assessment
- An assessment of the effectiveness of the Department's internal controls over financial reporting as of June 30, including an explicit conclusion as to whether internal controls over financial reporting are effective

Include additional information in the assurance statement if one of the following has happened:

- If a material weakness is discovered by June 30, but corrected by September 30, revise the assurance statement reported in the PAR to identify the material weakness, state the corrective action taken, and indicate that it has been resolved. This resolution may be reported only if the control is in place for an adequate amount of time to be properly tested as in the testing plan.
- If a material weakness is discovered after June 30, but prior to September 30; the assurance statement should be updated to include the subsequently identified material weakness.

The assurance statement should be accompanied by a summary of the CAPs for the material weaknesses and system "non-conformances." The summaries should include a description of the material weaknesses, the status of corrective actions, and the timelines for completion. CAPs need not be reported for reportable conditions not included in the FMFIA report.

ADDENDUM A
DOI A-123 IMPLEMENTATION PROJECT -
FINANCIAL REPORTING ITEMS NOT COVERED BY THE MATERIALITY DEFINITION

BACKGROUND

The scope of financial reporting subject to A-123 requirements covers required supplementary information (RSI) and required supplementary stewardship information (RSSI) as well as the principal financial statements and accompanying notes. The statement of Federal Financial Accounting Standards No. 6 "Accounting for Property , Plant and Equipment," requires annual disclosure of the estimated cost to remedy accumulated deferred maintenance on Interior's Plant, Property, and Equipment (PP&E) for both general and stewardship PP&E. However, the planning materiality threshold does not apply to all items presented in the RSI and RSSI sections of the DOI financial report. The quantitative data in some of these sections does not have a direct relationship to the information in the financial statements, and in many cases are presented in units of measure other than dollars.

Following is a list of items in the RSI and RSSI sections for which a separate materiality threshold is required:

Item	Units of Measure
Deferred Maintenance: • Roads, bridges, and trails • Irrigation, dams, and other water structures • Buildings • Other structures (e.g., recreation sites, hatcheries)	Dollars
Stewardship Lands	Acres / Square miles
Non-Collectible Cultural Resources	Number of sites
Museum collections	Number of collections / objects
Library Collectible Heritage Assets	Number of books/periodicals
Intra-Governmental Transactions	Dollars
Investment in Research and Development	Dollars
Investment in Human Capital	Dollars
Investment in non-Federal Physical Property	Dollars

ACTION REQUIRED

A separate materiality analysis needs to be performed on each of these items to determine at what level a misstatement of an item would impact management's or users' conclusions or decisions.

ADDENDUM B
TRANSACTION CYCLES THAT SHOULD BE CONSIDERED FOR TESTING

Financial Reporting
- Budget and Management Reporting
- General Ledger Maintenance
- Accounting Policies and Procedures
- Account Analysis and Reconciliation
- CFO Reporting
- External Financial Reporting

Revenue Management
- Recording Budget Authority
- Services Provided
- Collect Advances
- Interagency Agreements
- Reconcile Unfilled Customer Orders

Funds Management
- Fund Balance with Treasury
- Cash Receipts and Disbursements
- Investments

Grants Management
- Requests and Awards
- Monitoring
- Closeouts

Inventory Management
- Acquisition Requests/Purchases
- Distribution/Sales
- Consumption of Inventory

Environmental Management
- Evaluation and Reporting of Exposure
- Mitigation
- Prevention

Custodial Collections
- Plan and Conduct Lease Sales
- Approve and Enter Into Leases
- Receive Bonuses
- Maintain Long Term Bonuses
- Receive and Process Royalty Reports
- Process Royalty Reports
- Receive Royalty Payments
- Perform Matching Process
- Perform Exception Reporting
- Maintain Royalty Accounts Receivable
- Calculate Royalty Accrual
- Perform Royalty Compliance Requirements

Custodial Distributions
- Identify Payee
- Generate Payables
- Identify and Process Payments Exceptions
- Generate Vouchers
- Perform Pay-cycle
- Pay Late Payment Interest
- Reconcile Change in Untransferred Revenue

Human Capital Management
- Personnel
- Time and Attendance
- Processing Payroll
- Pension and Postretirement Benefits

Procurement
- Credit Cards
- Requisition
- Award and Obligate
- Receive and Pay Invoices
- Invoicing
- Contract Monitoring
- Contract Closeouts

Credit Program Management
- Extending Credit
- Loan Servicing
- Estimate Modeling

Real Property Management
- Stewardship and Heritage Assets
- Capital Acquisition Requests
- Manage and Maintain Capital Assets
  - Inventory
  - Maintenance
  - Depreciation
- Dispose of Assets
- Leases (Operating or Capital)

Information Technology
- Overall Control Environment
- Program Development
- Program Changes
- Access and Security
- System Support and Operation

ADDENDUM C
RISK FACTORS FOR FINANCIAL REPORTING

Financial categories that have political, public impact, or cause embarrassment to the administration [e.g. hazardous waste sites (environmental clean-up), prison conditions, poor education at Indian schools, inadequate safeguarding of stewardship and heritage assets, etc.]

Diverse, decentralized, and remote (12 Regions throughout the United States including Alaska) operations ranging from law enforcement and hospitals to power and irrigation projects.

Lack of technology (internet)

- Impedes accuracy and timeliness of financial reporting to Treasury and OMB
- Impacts compliance or ability to transition to internet based only systems
- Forces manual work processes and the use of applications that affect accuracy and timeliness of data

Existence/reliance of third party data

- National Business Center
- Environmental Clean-Up estimates from Regions
- Contingent Liabilities
- Stewardship and Heritage Assets

Antiquated accounting/information systems

- Lack sufficient interfaces with FFS to minimize errors
- Reliance on data from independent/off-line systems [Loans (LOMAS), Trust systems]

ADDENDUM D
ENTITY LEVEL INTERNAL CONTROL ASSESSMENT

The example entity level internal control assessment[17] is based on the five components of internal control and the GAO checklist used in the financial statement audit. Detail is entered into the template.

Entity Level Internal Control Assessment

Date	Name	Telephone Number	Email Address

Purpose: To document and evaluate internal controls operating at the entity level

Definitions:

Internal control at the entity level refers to those elements of the five components of internal control that have an overarching or pervasive effect on the agency. The five components are:

i. Control Environment
The control environment relates to management's attitude, awareness, and actions concerning the control environment.

- Integrity and ethical standards
- Commitment to competence
- Management philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human resource policies and practices

ii. Risk Assessment
Risk assessment relates to how management considers risks relevant to financial reporting objectives and decides about actions to address those risks.

- Complexity or size of programs, operations, transactions, etc.
- Decentralized versus centralized operations, accounting, and reporting functions
- Extent of manual or automated processes or applications
- New or amended laws, regulations, or accounting standards
- Changes in the operating environment
- Significant new or changed programs or operations
- Restructurings or budget cutbacks which may include downsizing and changes in supervision and segregation of duties
- New personnel or significant personnel changes
- New or revamped information systems
- New technology
- Existence of related party transactions
- Accounting estimates

[17] Circular A-123, Appendix A, Section III.B.

iii. Control Activities

Control activities relate to the policies and procedures that help ensure that management directives are carried out and that management's assertions in its financial reporting are valid. The Control activities section of the Entity Level Internal Control Assessment will include subsections describing:

- Policies and procedures
- Management objectives
- Planning and reporting systems
- Analytical review and analysis
- Segregation of duties
- Safeguarding of records
- Physical and access controls

iv. Information and Communication

- Type and sufficiency of reports produced
- Management of IT system development
- Disaster recovery
- Communication of employees control related duties and responsibilities
- How incoming external communication is handled

v. Monitoring

- Self assessments by management
- Evaluations by the OIG or external auditor
- Direct Testing

Entity level evaluation of the Control Environment

CONTROL ENVIRONMENT	
Integrity and Ethical Values Comments/Descriptions	
1. The agency has established and uses a formal code or codes of conduct and other policies communicating appropriate ethical and moral behavioral standards and addressing acceptable operational practices and conflicts of interest.	**Yes** ☐ **No** ☐ **N/A** ☐
2. An ethical tone has been established at the top of the organization and has been communicated throughout the agency.	**Yes** ☐ **No** ☐ **N/A** ☐
3. Management appropriately addresses intervention or overriding internal control.	**Yes** ☐ **No** ☐ **N/A** ☐
Commitment to Competence Comments/Descriptions	

1. Management has identified and defined the tasks required to accomplish particular jobs and fill the various positions.	**Yes** ☐	**No** ☐	**N/A** ☐
2. The agency provides training and counseling in order to help employees maintain and improve their competence for their jobs.	**Yes** ☐	**No** ☐	**N/A** ☐
Management's Philosophy and Operating Style Comments/Descriptions			
1. Management has a positive and supportive attitude toward the functions of accounting, information management systems, personnel operations, monitoring, and internal and external audits and evaluations.	**Yes** ☐	**No** ☐	**N/A** ☐
2. Valuable assets and information are safeguarded from unauthorized access or use.	**Yes** ☐	**No** ☐	**N/A** ☐
3. Management has an appropriate attitude toward financial, budgetary, and operational/programmatic reporting.	**Yes** ☐	**No** ☐	**N/A** ☐
Organizational Structure Comments/Descriptions			
1. Key areas of authority and responsibility are defined and communicated throughout the organization.	**Yes** ☐	**No** ☐	**N/A** ☐
2. Appropriate and clear internal reporting relationships have been established.	**Yes** ☐	**No** ☐	**N/A** ☐
3. Management periodically evaluates the organizational structure and makes changes as necessary in response to changing conditions.	**Yes** ☐	**No** ☐	**N/A** ☐
Assignment of Authority and Responsibility Comments/Descriptions			
1. The agency appropriately assigns authority and delegates responsibility to the proper personnel to deal with organizational goals and objectives.	**Yes** ☐	**No** ☐	**N/A** ☐
2. Each employee knows (1) how his or her actions interrelate to others considering the way in which authority and responsibilities are assigned, and (2) is aware of the related duties concerning internal control.	**Yes** ☐	**No** ☐	**N/A** ☐
3. The delegation of authority is appropriate in relation to the assignment of responsibility.	**Yes** ☐	**No** ☐	**N/A** ☐
Human Resource Policies and Practices Comments/Descriptions			
1. Policies and procedures are in place for hiring, orienting, training, evaluating, counseling, promoting, compensating, disciplining, and terminating employees.	**Yes** ☐	**No** ☐	**N/A** ☐
2. Employees are provided a proper amount of supervision.	**Yes** ☐	**No** ☐	**N/A** ☐
Oversight Groups Comments/Descriptions			

	Yes	No	N/A
1. Within the agency, there are mechanisms in place to monitor and review operations and programs.	☐	☐	☐
RISK ASSESSMENT			
Establishment of Entity-wide Objectives Comments/Descriptions			
1. The agency has established entity-wide objectives that provide sufficiently broad statements and guidance about what the agency is supposed to achieve, yet are specific enough to relate directly to the agency.	**Yes** ☐	**No** ☐	**N/A** ☐
2. Entity-wide objectives are clearly communicated to all employees, and management obtains feedback signifying that the communication has been effective.	**Yes** ☐	**No** ☐	**N/A** ☐
3. The agency has an integrated management strategy and risk assessment plan that considers the entity-wide objectives and relevant sources of risk from internal management factors and external sources and establishes a control structure to address those risks.	**Yes** ☐	**No** ☐	**N/A** ☐
Establishment of Activity-Level Objectives Comments/Descriptions			
1. Activity-level (program or mission-level) objectives flow from and are linked with the agency's entity-wide objectives and strategic plans.	**Yes** ☐	**No** ☐	**N/A** ☐
2. The activity-level objectives are relevant to all significant agency processes.	**Yes** ☐	**No** ☐	**N/A** ☐
3. Activity-level objectives include measurement criteria.	**Yes** ☐	**No** ☐	**N/A** ☐
4. Management has identified those activity-level objectives that are critical to the success of the overall entity-wide objectives.	**Yes** ☐	**No** ☐	**N/A** ☐
Risk Identification Comments/Descriptions			
1. Management comprehensively identifies risk using various methodologies as appropriate.	**Yes** ☐	**No** ☐	**N/A** ☐
2. Adequate mechanisms exist to identify risks to the agency arising from external factors.	**Yes** ☐	**No** ☐	**N/A** ☐
3. Adequate mechanisms exist to identify risks to the agency arising from internal factors.	**Yes** ☐	**No** ☐	**N/A** ☐
4. In identifying risk, management assesses other factors that may contribute to or increase the risk to which the agency is exposed.	**Yes** ☐	**No** ☐	**N/A** ☐
5. Management identifies risks both entity-wide and for each significant activity-level of the agency.	**Yes** ☐	**No** ☐	**N/A** ☐
Risk Analysis Comments/Descriptions			

1. After the risks to the agency have been identified, management undertakes a thorough and complete analysis of their possible effect.	**Yes** ☐ **No** ☐ **N/A** ☐
2. Management has developed an approach for risk management and control based on how much risk can be prudently accepted.	**Yes** ☐ **No** ☐ **N/A** ☐
Managing Risk During Change Comments/Descriptions	
1. The agency has mechanisms in place to anticipate, identify, and react to risks presented by changes in governmental, economic, industry, regulatory, operating, or other conditions that can affect the achievement of entity-wide or activity-level goals and objectives.	**Yes** ☐ **No** ☐ **N/A** ☐
CONTROL ACTIVITIES	
General Application Comments/Descriptions	
1. Appropriate policies, procedures, techniques, and mechanisms exist with respect to each of the agency's activities.	**Yes** ☐ **No** ☐ **N/A** ☐
2. The control activities identified as necessary are in place and being applied.	**Yes** ☐ **No** ☐ **N/A** ☐
3. Control activities are regularly evaluated to ensure that they are still appropriate and working as intended. (This point is closely related to the functions, and points included in the "Monitoring" section. See that section for more specific information on monitoring and periodic evaluation of control activities)	**Yes** ☐ **No** ☐ **N/A** ☐
Common Categories of Control Activities Comments/Descriptions	
1. Top-Level Reviews. Management tracks major agency achievements in relation to its plans.	**Yes** ☐ **No** ☐ **N/A** ☐
2. Management Reviews at the Functional or Activity Level. Agency managers review actual performance against targets.	**Yes** ☐ **No** ☐ **N/A** ☐
3. Information Processing. The agency employs a variety of control activities suited to information processing systems to ensure accuracy and completeness. (Further guidance on control activities for information processing is provided in the following section under "Control Activities Specific for Information Systems." In addition, see GAO's Federal Information System Controls Audit Manual (FISCAM) and OMB Circular A-130, Management of Federal Information Resources)	**Yes** ☐ **No** ☐ **N/A** ☐
4. Physical Control Over Vulnerable Assets. The agency employs physical control to secure and safeguard vulnerable assets.	**Yes** ☐ **No** ☐ **N/A** ☐
5. Performance Measures and Indicators. The agency has established and monitors performance measures and indicators.	**Yes** ☐ **No** ☐ **N/A** ☐
6. Segregation of Duties. Key duties and responsibilities are divided or segregated among different people to reduce the risk of error, waste, or fraud.	**Yes** ☐ **No** ☐ **N/A** ☐
7. Execution of Transactions and Events. Transactions and other significant events are authorized and performed by the appropriate personnel.	**Yes** ☐ **No** ☐ **N/A** ☐

8. Recording of Transactions and Events. Transactions and other significant events are properly classified and promptly recorded.	**Yes** ☐ **No** ☐ **N/A** ☐
9. Access Restrictions to and Accountability for Resources and Records. Access to resources and records is limited and accountability for their custody is assigned.	**Yes** ☐ **No** ☐ **N/A** ☐
10. Documentation. Internal Control and all transactions and other significant events are clearly documented.	**Yes** ☐ **No** ☐ **N/A** ☐
Control Activities Specific for Information Systems General Control	
Entity-wide Security Management Program Comments/Descriptions	
1. The agency periodically performs a comprehensive, high-level assessment of risks to its information systems.	**Yes** ☐ **No** ☐ **N/A** ☐
2. Senior management has established a structure to implement and manage the security program throughout the agency and security responsibilities are clearly defined.	**Yes** ☐ **No** ☐ **N/A** ☐
3. The agency monitors the security program's effectiveness and makes changes as needed.	**Yes** ☐ **No** ☐ **N/A** ☐
Access Control Comments/Descriptions	
1. Resource owners have identified authorized users, and their access to the information has been formally authorized.	**Yes** ☐ **No** ☐ **N/A** ☐
2. The agency has established physical and logical controls to prevent or detect unauthorized access.	**Yes** ☐ **No** ☐ **N/A** ☐
3. The agency monitors information systems access, investigates apparent violations, and takes appropriate remedial and disciplinary action.	**Yes** ☐ **No** ☐ **N/A** ☐
Application Software Development and Change Control Comments/Descriptions	
1. Information system processing features and program modifications are properly authorized.	**Yes** ☐ **No** ☐ **N/A** ☐
2. All new or revised software is thoroughly tested and approved.	**Yes** ☐ **No** ☐ **N/A** ☐
3. The agency has established procedures to ensure control of its software libraries, including labeling, access restrictions, and use of inventories and separate libraries.	**Yes** ☐ **No** ☐ **N/A** ☐
System Software Control Comments/Descriptions	
1. The agency limits access to system software based on job responsibilities, and access authorization is documented.	**Yes** ☐ **No** ☐ **N/A** ☐
2. Access to and use of system software is controlled and monitored.	**Yes** ☐ **No** ☐ **N/A** ☐

3. The agency controls changes made to the system software.	**Yes** ☐ **No** ☐ **N/A** ☐
Segregation of Duties Comments/Descriptions	
1. Incompatible duties have been identified and policies implemented to segregate those duties.	**Yes** ☐ **No** ☐ **N/A** ☐
2. Access controls have been established to enforce segregation of duties.	**Yes** ☐ **No** ☐ **N/A** ☐
3. The agency exercises control over personnel activities through the use of formal operating procedures, supervision, and review.	**Yes** ☐ **No** ☐ **N/A** ☐
Service Continuity Comments/Descriptions	
1. The agency has taken steps to prevent and minimize potential damage and interruption through the use of data and program backup procedures including off- site storage of backup data as well as environmental controls, staff training, and hardware maintenance and management.	**Yes** ☐ **No** ☐ **N/A** ☐
Control Activities Specific for Information Systems Application Control	
Authorization Control Comments/Descriptions	
1. Source documents are controlled and require authorization.	**Yes** ☐ **No** ☐ **N/A** ☐
2. Data entry terminals have restricted access.	**Yes** ☐ **No** ☐ **N/A** ☐
3. Master files and exception reporting are used to ensure that all data processed are authorized.	**Yes** ☐ **No** ☐ **N/A** ☐
Completeness Control Comments/Descriptions	
1. All authorized transactions are entered into and processed by the computer.	**Yes** ☐ **No** ☐ **N/A** ☐
2. Reconciliations are performed to verify data completeness.	**Yes** ☐ **No** ☐ **N/A** ☐
Accuracy Control Comments/Descriptions	
1. The agency's data entry design features contribute to data accuracy.	**Yes** ☐ **No** ☐ **N/A** ☐
2. Data validation and editing are performed to identify erroneous data.	**Yes** ☐ **No** ☐ **N/A** ☐
3. Erroneous data are captured, reported, investigated, and promptly corrected.	**Yes** ☐ **No** ☐ **N/A** ☐
4. Output reports are reviewed to help maintain data accuracy and validity.	**Yes** ☐ **No** ☐ **N/A** ☐

Control Over Integrity of Processing and Data Files Comments/Descriptions	
1. Procedures ensure that the current versions of production programs and data files are used during processing.	**Yes** ☐ **No** ☐ **N/A** ☐
2. Programs include routines to verify that the proper version of the computer file is used during processing.	**Yes** ☐ **No** ☐ **N/A** ☐
3. The application protects against concurrent file updates.	**Yes** ☐ **No** ☐ **N/A** ☐
INFORMATION AND COMMUNICATIONS	
Information Comments/Descriptions	
1. Information from internal and external sources is obtained and provided to management as a part of the agency's reporting on operational performance relative to established objectives.	**Yes** ☐ **No** ☐ **N/A** ☐
2. Pertinent information is identified, captured, and distributed to the right people in sufficient detail, in the right form, and at the appropriate time to enable them to carry out their duties and responsibilities efficiently and effectively.	**Yes** ☐ **No** ☐ **N/A** ☐
Communications Comments/Descriptions	
1. Management ensures that effective internal communications occur.	**Yes** ☐ **No** ☐ **N/A** ☐
2. Management ensures that effective external communications occur with groups that can have a serious impact on programs, projects, operations, and other activities, including budgeting and financing.	**Yes** ☐ **No** ☐ **N/A** ☐
MONITORING	
Ongoing Monitoring Comments/Descriptions	
1. Management has a strategy to ensure that ongoing monitoring is effective and will trigger separate evaluations where problems are identified or systems are critical and testing is periodically desirable.	**Yes** ☐ **No** ☐ **N/A** ☐
2. In the process of carrying out their regular activities, agency personnel obtain information about whether internal control is functioning properly.	**Yes** ☐ **No** ☐ **N/A** ☐
3. Communications from external parties should corroborate internally generated data or indicate problems with internal control.	**Yes** ☐ **No** ☐ **N/A** ☐
4. Data recorded by information and financial systems are periodically compared with physical assets and discrepancies are examined.	**Yes** ☐ **No** ☐ **N/A** ☐
5. The Inspector General and other auditors and evaluators regularly provide recommendations for improvements in internal control with management taking appropriate follow-up action.	**Yes** ☐ **No** ☐ **N/A** ☐
Separate Evaluations Comments/Descriptions	
1. The scope and frequency of separate evaluations of internal control are appropriate for the agency.	**Yes** ☐ **No** ☐ **N/A** ☐

2. The methodology for evaluating the agency's internal control is logical and appropriate.	**Yes** ☐ **No** ☐ **N/A** ☐
3. Deficiencies found during separate evaluations are promptly resolved.	**Yes** ☐ **No** ☐ **N/A** ☐
Audit Resolution. Comments/Descriptions (Audit Resolution includes the resolution of findings and recommendations not just from formal audits, but also resulting from informal reviews, internal separate evaluations, management studies, and assessments made pursuant to the requirements of the Federal Managers' Financial Integrity Act (FMFIA) of 1982 and the Federal Financial Management Improvement Act (FFMIA) of 1996)	
1. The agency has a mechanism to ensure the prompt resolution of findings from audits and other reviews.	**Yes** ☐ **No** ☐ **N/A** ☐
2. Agency management is responsive to the findings and recommendations of audits and other reviews aimed at strengthening internal control.	**Yes** ☐ **No** ☐ **N/A** ☐

Department of the Interior

____

Agency

________________________________ ______________

Chief Financial Officer (signature) Date

____

Chief Financial Officer (printed)

SECTION 2
EXHIBIT 1
INTERNAL CONTROL MATRIX

The Internal Control Matrix identifies significant accounts and groups of accounts (financial statement line items) and links to a process. Complete the matrix to identify accounts over the testing materiality and those with qualitative or risk factors.

						Assertions						Control Characteristics					Effectiveness	
Process / Sub-Process	Activity	Control Objective	Risk	Line Item	GL Accounts	Presentation & Disclosure	Existence & Occurrence	Rights & Obligations	Completeness	Valuation	Control #	Control Description	Preventative / Detective	Automated / Manual	Frequency	Categories	Design	Operation
I.A. Financial Reporting																		
Budget and Management Reporting																		
General Ledger Maintenance																		
Accounting Policies and Procedures																		
Account Analysis and Reconciliation	Treasury Report on Receivables (TROR - quarterly) - reconcile w/ SGL debt due from public																	
CFO Reporting																		
External Financial Reporting																		
I.B. Revenue Management																		
Recording Budget Authority																		
Services Provided																		
Collect Advances																		
Interagency Agreements	Biennial Review of User Charges (CFO Act of 1990 requirement). There is an annual cost recovery review requirement but that was imposed by DOI (Accounting Handbook, OMB Circ. A-25 & former DM 346).																	
Reconcile Unfilled Customer Orders																		
I.C. Funds Management																		
Fund Balance with Treasury																		
Cash Receipts and Disbursements	Improper Payment Information Act																	
	Recovery Audits (DOD Authorization Act 2002 Sec. 831)																	
	Government Freight Bills prepayment audits (Travel and Transportation Act of 1998)																	
	Automatic late payment interest and timely payment (Prompt Payment Act of 1982 et seq. & Travel and Transportation Reform Act of 1998)																	
	Required payment via EFT, collection of TINs for all vendor/misc. payment transactions (Debt Collection Improvement Act of 1996)																	
Investments																		

SECTION 2
EXHIBIT 2
ACCOUNT RISK ANALYSIS

Account Risk Analysis (adapted from the GAO/PCIE Financial Audit Manual as described in the CFO Council Guide)

ENTITY: *XYZ Agency (XYZ)*

ACCOUNT RISK ANALYSIS FORM

PREPARER:____________
DATE OF FINANCIAL STATEMENTS: *9/30/XX* REGION: ____________

FILE: ___________ DATE: ____________

LINE ITEM: Accounts Receivable - Net

Page ____ of ____

PLANNING PHASE					INTERNAL CONTROL PHASE			TESTING PHASE		
Account		Financial Statement Assertions/Risks	Inherent, Fraud, and Control Risk Factors	Cycle/ Accounting Application	Effectiveness of Control Activities	Control Risk	Combined Risk	Timing I/F	Nature & Extent	W/P Ref.& Audit Step
Name	Balance									
Accounts Receivable, Net	*$876,000,000*	***Existence or Occurrence:*** *Recorded accounts receivable do not exist.*	*No significant inherent, fraud, or control risk factors identified.*	*Sales/ Billing* *Sales Returns* *Cash Receipts* *Accounts Receivable*	*Effective* *Effective* *Effective* *Effective*	*Low*	*Low*	*F*	*Confirm balances and test reconciliation of subsidiary ledger to the general ledger.*	*III-5 to III7*

Account Risk Analysis (cont.)

ENTITY: *XYZ Agency (XYZ)*

ACCOUNT RISK ANALYSIS FORM

PREPARER:____________

DATE OF FINANCIAL STATEMENTS: *9/30/XX* REGION: ____________

FILE: ____________ DATE: ____________

LINE ITEM: Accounts Receivable - Net

Page ____ of ____

PLANNING PHASE					INTERNAL CONTROL PHASE			TESTING PHASE		
Account		Financial Statement Assertions/Risks	Inherent, Fraud, and Control Risk Factors	Cycle/ Accounting Application	Effectiveness of Control Activities	Control Risk	Combined Risk	Timing I/F	Nature & Extent	W/P Ref.& Audit Step
Name	Balance									
		Completeness: *Accounts receivable are not recorded in a timely manner so as to be included in the financial statements.*	*No significant inherent, fraud, or control risk factors identified.*	*Sales/ Billing* *Sales Returns* *Cash Receipts* *Accounts Receivable*	*Effective* *Effective* *Effective* *Effective*	*Low*	*Low*	*F*	*Perform analytical procedures. Test cut-off.*	*III-8 to III-12*

Account Risk Analysis (cont.)

ENTITY: *XYZ Agency (XYZ)*

ACCOUNT RISK ANALYSIS FORM

PREPARER:____________
DATE OF FINANCIAL STATEMENTS: *9/30/XX*

REGION: ____________

FILE: ____________

DATE: ____________

LINE ITEM: Accounts Receivable - Net

Page ____ of ____

PLANNING PHASE					INTERNAL CONTROL PHASE			TESTING PHASE		
Account		Financial Statement Assertions/Risks	Inherent, Fraud, and Control Risk Factors	Cycle/ Accounting Application	Effectiveness of Control Activities	Control Risk	Combined Risk	Timing I/F	Nature & Extent	W/P Ref.& Audit Step
Name	Balance									
		Valuation or Allocation: *Accounts receivable are not valued accurately or on an appropriate basis in the financial statements.*	*The bankruptcy filing by a major debtor and the financial difficulties of several other debtors in the current economic environment give rise to an inherent risk. No significant fraud or control risk factors identified. .*	*Sales/ Billing* *Sales Return* *Cash Receipts* *Accounts Receivable*	*Effective* *Effective* *Effective* *Effective*	*Low*	*Moderate*	*F*	*Confirm balances (see existence), test the accuracy of the aging, analytically review bad debts and allowance, and examine evidence of collectibility for selected accounts receivable. Discuss with management collectibility from troubled debtors.*	*III-13 to III18*

Account Risk Analysis (cont.)

ENTITY: *XYZ Agency (XYZ)*

ACCOUNT RISK ANALYSIS FORM

PREPARER:____________
DATE OF FINANCIAL STATEMENTS: *9/30/XX* REGION: ____________

FILE: ___________ DATE: ____________

LINE ITEM: Accounts Receivable - Net

Page ____ of ____

PLANNING PHASE					INTERNAL CONTROL PHASE			TESTING PHASE		
Account		Financial Statement Assertions/Risks	Inherent, Fraud, and Control Risk Factors	Cycle/ Accounting Application	Effectiveness of Control Activities	Control Risk	Combined Risk	Timing I/F	Nature & Extent	W/P Ref.& Audit Step
Name	Balance									
		Rights and Obligations: *XYZ does not own unencumbered rights to recorded accounts receivable.*	*No significant inherent, fraud, or control risk factors identified.*	*Accounts Receivable*	*Effective*	*Low*	*Low*	*F*	*Identify accounts receivable from related parties or major debtors. Review confirmations for indication of guarantees or encumbrances.*	*III-19 to III-22*

Account Risk Analysis (cont.)

ENTITY: *XYZ Agency (XYZ)*

ACCOUNT RISK ANALYSIS FORM

PREPARER:____________
DATE OF FINANCIAL STATEMENTS: *9/30/XX* REGION: ____________

FILE: ___________ DATE: ____________

LINE ITEM: Accounts Receivable - Net

Page ____ of ____

PLANNING PHASE					INTERNAL CONTROL PHASE			TESTING PHASE		
Account		Financial Statement Assertions/Risks	Inherent, Fraud, and Control Risk Factors	Cycle/ Accounting Application	Effectiveness of Control Activities	Control Risk	Combined Risk	Timing I/F	Nature & Extent	W/P Ref.& Audit Step
Name	Balance									
		Presentation and Disclosure: *Accounts receivable are not properly classified or disclosed in the financial statements, nor are they based on a consistent application of accounting principles.*	*No significant inherent, fraud, or control risk factors identified.*	*Accounts Receivable*	*Effective*	*Low*	*Low*	*F*	*Determine appropriateness of footnote disclosures. Summarize and test credit risk disclosures. Review accounting principles used.*	*III-23 to III-25, IV-16*
Line Item Total	*$876,000,000*									

SECTION 2
EXHIBIT 3
SPECIFIC CONTROL EVALUATION WORKSHEET

Specific Control Evaluation Worksheet (adapted from the GAO/PCIE Financial Audit Manual) (obtained from the Specific Control Evaluation Worksheet (SCE) from the GAO/PCIE Financial Audit Manual as described in the CFO Council Guide)

ENTITY: *XYZ Agency (XYZ)*

SPECIFIC CONTROL EVALUATION

PREPARER:____________
DATE OF FINANCIAL STATEMENTS: *9/30/XX* REGION: ____________

FILE: ___________ DATE: ____________

LINE ITEM: Accounts Receivable - Net

Page ____ of ____

ACCOUNTING APPLICATION: CASH RECEIPTS

ACCOUNTING APPLICATION ASSERTION	RELEVANT ASSERTIONS IN RELATED GROUPS OF ACCOUNTS		POTENTIAL MISSTATEMENT IN ACCOUNTING APPLICATION ASSERTIONS	CONTROL OBJECTIVES	INTERNAL CONTROL ACTIVITIES	IS (Y/N)	EFFECTIVE NESS OF CONTROL ACTIVITIES	W/P REF. & CONTROL TESTING PROGRAM STEP
	Cash	*Accts. Rec.*						

Existence or Occurrence	*Existence or Occurrence*	*Completeness*	*Validity:* *1. Receipt is recorded, but cash is not received.*	*1a. Recorded cash receipts and cash receipt processing procedures should be authorized by federal laws, regulations, and management's policy.* *1b. Recorded receipts should be approved by appropriate individuals in accordance with management's general or specific criteria.* *1c. Recorded receipts should represent amounts actually received by the entity and should be properly classified.*	*1a. Receipts processing is governed by documented procedures for accepting, obtaining, reviewing, and approving receipts.* *1b. Supervisory review is made of receipts processing to provide reasonable assurance that procedures are followed.* *1c1. Recorded cash receipts are matched with the appropriate supporting documentation.* *1c2. Entries to the accounting records are reviewed and approved by supervisory personnel.*	*N* *N* *N* *N*	*Effective*		[In this column, the manager would indicate, by cross-referencing, the procedures in the detailed control testing program that were designed to test each effective control determined to be relevant. Such tests will involve inquiry, observation, inspection, or a combination thereof.]

Specific Control Evaluation Worksheet (cont.)

ENTITY: *XYZ Agency (XYZ)*

SPECIFIC CONTROL EVALUATION

PREPARER:____________
DATE OF FINANCIAL STATEMENTS: *9/30/XX*

REGION: ____________

FILE: ____________

DATE: ____________

LINE ITEM: Accounts Receivable - Net

Page ____ of ____

ACCOUNTING APPLICATION: CASH RECEIPTS

ACCOUNTING APPLICATION ASSERTION	RELEVANT ASSERTIONS IN RELATED GROUPS OF ACCOUNTS		POTENTIAL MISSTATEMENT IN ACCOUNTING APPLICATION ASSERTIONS	CONTROL OBJECTIVES	INTERNAL CONTROL ACTIVITIES	IS (Y/N)	EFFECTIVE NESS OF CONTROL ACTIVITIES	W/P REF. & CONTROL TESTING PROGRAM STEP
	Cash	*Accts. Rec.*						
			Cutoff: *2. Receipt is recorded in this period, but the cash is received in a different period.*	*2. Cash receipts recorded in the period should be actually received in the period.*	*2. Recorded receipts are reconciled to cash receipts listings and bank deposits reports before posting.*	*Y*	*Effective*	
			Summarization: *3. Receipt transactions are overstated due to improper summarization.*	*3. The summarization of receipt transactions should not be overstated.*	*3a. Receipt data in the general ledger is reconciled to subsidiary cash ledgers and records.*	*Y*	*Effective*	
					3b. Batch totals of input documents are reconciled to output registered, journals, reports, or file updates.	*Y*		

Specific Control Evaluation Worksheet (cont.)

ENTITY: *XYZ Agency (XYZ)*

SPECIFIC CONTROL EVALUATION

PREPARER:____________
DATE OF FINANCIAL STATEMENTS: *9/30/XX* REGION: ____________

FILE: ____________ DATE: ____________

LINE ITEM: Accounts Receivable - Net

Page ____ of ____

ACCOUNTING APPLICATION: CASH RECEIPTS

ACCOUNTING APPLICATION ASSERTION	RELEVANT ASSERTIONS IN RELATED GROUPS OF ACCOUNTS		POTENTIAL MISSTATEMENT IN ACCOUNTING APPLICATION ASSERTIONS	CONTROL OBJECTIVES	INTERNAL CONTROL ACTIVITIES	IS (Y/N)	EFFECTIVE NESS OF CONTROL ACTIVITIES	W/P REF. & CONTROL TESTING PROGRAM STEP
	Cash	*Accts. Rec.*						
Completeness	*Completeness*	*Existence or Occurrence*	*Transaction Completeness:* *4. Cash is received, but receipt is not recorded.*	*4. All receipts of cash should be promptly recorded and properly classified.*	*4a. Cash receipts are listed by the central mailroom staff and independently reconciled to deposits and accounting summaries, providing adequate segregation of duties. Collections and complaints are handled by others.*	*N*	*Effective*	
					4b. Supervisory reviews of the processing of cash receipts.	*N*		
			Cutoff: *5. Cash is received in this period, but receipt is recorded in a different period.*	*5. Cash receipts actually received in the period should be recorded in the period.*	*5. Same as procedure 2 above.*	*Y*	*Effective*	
			Summarization: *6. Receipt transactions are understated as a result of improper summarization.*	*6. The summarization of cash receipt transactions should not be understated.*	*6. Same as procedure 3a and 3b above.*	*Y*	*Effective*	

Specific Control Evaluation Worksheet (cont.)

ENTITY: *XYZ Agency (XYZ)*

SPECIFIC CONTROL EVALUATION

PREPARER:____________
DATE OF FINANCIAL STATEMENTS: *9/30/XX* REGION: ____________

FILE: ___________ DATE: ____________

LINE ITEM: Accounts Receivable - Net

Page ____ of ____

ACCOUNTING APPLICATION: CASH RECEIPTS

ACCOUNTING APPLICATION ASSERTION	RELEVANT ASSERTIONS IN RELATED GROUPS OF ACCOUNTS		POTENTIAL MISSTATEMENT IN ACCOUNTING APPLICATION ASSERTIONS	CONTROL OBJECTIVES	INTERNAL CONTROL ACTIVITIES	IS (Y/N)	EFFECTIVE NESS OF CONTROL ACTIVITIES	W/P REF. & CONTROL TESTING PROGRAM STEP
	Cash	*Accts. Rec.*						
Valuation	*Valuation*	*Valuation*	*Accuracy:* *7. Receipt transactions are recorded at incorrect amounts.*	*7. Receipt transactions should be recorded accurately*	*7a. Recorded receipts are compared with bank statements by persons who have no other receipts processing responsibilities.* *7b. Supervisor reviews and approves reconciliations of recorded receipts to bank statements.*	*Y* *N*	*Effective*	
Segregation of Duties	*Various*	*Various*	*Segregation:* *8. The entity is exposed to loss of cash receipts and various misstatements as the result of inadequate segregation of duties.*	*8. Persons should be prevented from having uncontrolled access to both cash receipts and records.*	*8a. No individual has uncontrolled access (direct or indirect) to both cash receipts and records.*	*N*	*Effective*	

Preparation Notes:
1. The third column is for use where the effects of the accounting application on the line items are different. For example, misstatements in the existence or occurrence assertion for cash receipts typically result in misstatements in the existence or occurrence assertion for cash and in the completeness assertion for accounts receivable.

2. If there is inadequate segregation of duties, the manager should identify the specific affected account assertions in columns 2 and 3.

SECTION 2
EXHIBIT 4
ILLUSTRATIVE TEMPLATE FOR A DESIGNATED SENIOR OFFICIAL TO THE AGENCY HEAD

Memorandum

To: Assistant Secretary - Policy, Management and Budget
Attention: Director, Office of Financial Management

Through: Assistant Secretary

From: Bureau/Office Head

Subject: FY 200X Annual Assurance Statement on Internal Control over Financial Reporting

In accordance with your delegation of responsibilities to me, I have directed an evaluation of the internal control over financial reporting of [bureau/office] in effect during the year ended June 30, 200X. This evaluation was conducted in accordance with departmental guidance and OMB Circular A-123, *Management's Responsibility for Internal Control*, dated December 21, 2004.

In evaluating internal control over financial reporting at [bureau/office], I directed my staff to:

- Identify the financial reports that have a material effect on [bureau/office's] financial decisions
- Identify the accounts in each selected report that are material to the report
- Identify the transaction cycles that generate the information for these accounts
- Document and obtain an understanding of those transaction cycles
- Evaluate the agency's control environment, risk assessment process, information and communication processes, and monitoring process
- Identify the control activities in each transaction cycle
- Assess the design of the controls to determine whether they would prevent or detect errors or misstatements in the selected financial statements
- Test the controls that are considered suitably designed and assess whether they are functioning as designed.

Based on the results of this evaluation, the [bureau/office] may provide reasonable assurance that internal control over financial reporting as of June 30, 2xxx, was operating effectively, **with the exception of the following material weakness(es) that was (were) found in the design or operation of the internal controls over financial reporting.**

- **Insert title(s) and description(s) of material weakness(es)**

[Or, if an unqualified assurance statement may be made, replace the bolded statement above with the following: "and no material weaknesses were found in the design or operation of the internal controls over financial reporting."]

Name of Designated Senior Official

SECTION 2
EXHIBIT 5A
ILLUSTRATIVE TEMPLATE FOR A STATEMENT OF ASSURANCE

Memorandum

To: Assistant Secretary - Policy, Management and Budget
Attention: Director, Office of Financial Management

Through: Assistant Secretary

From: Bureau/Office Head

Subject: FY 200X Annual Assurance Statement on Internal Control

The [bureau/office] management is responsible for establishing and maintaining effective internal control and financial management systems that meet the objectives of the Federal Managers' Financial Integrity Act (FMFIA). The [bureau/office] conducted its assessment of the effectiveness of internal control over the effectiveness and efficiency of operations and compliance with applicable laws and regulations in accordance with departmental guidance and OMB Circular A-123, *Management's Responsibility for Internal Control*, dated December 21, 2004. The objectives of this assessment are to ensure that:

- Programs achieve their intended results;
- Resources are used consistent with agency mission;
- Resources are protected from waste, fraud, and mismanagement;
- Laws and regulations are followed; and
- Reliable and timely information is maintained, reported, and used for decision-making.

In performing this assessment, the [bureau/office] relied on the knowledge and experience management has gained from the daily operation of its programs and systems of accounting and administrative controls, and information obtained from sources such as internal control assessments, OIG and GAO audits, program evaluations and studies, audits of financial statements, and performance plans and reports. The following specific internal control assessments conducted by the bureau, and audits and/or reviews conducted by the OIG and/or GAO were relied upon to support the conclusions expressed herein.

Assessment /Audit	Date Completed	Results (Material Weakness or Best Practice)
(List or attach list)		

Name of Designated Senior Official

Statement of Unqualified Assurance (con't)

Based on the results of the evaluation, the [bureau/office] can provide reasonable assurance that its internal control over the effectiveness and efficiency of operations and compliance with applicable laws and regulations as of September 30, 200X was operating effectively and no material weaknesses were found in the design or operation of the internal controls.

In addition, the [bureau/office] conducted its assessment of the effectiveness of internal control over financial reporting, which includes safeguarding of assets and compliance with applicable laws and regulations, in accordance with the requirements of Appendix A of OMB Circular A-123. Based on the results of this evaluation, the [bureau/office] can provide reasonable assurance that its internal control over financial reporting as of June 30, 200X was operating effectively and no material weaknesses were found in the design or operation of the internal control over financial reporting.

The corrective action reports for material weaknesses and/or accounting system non-conformances identified in the FY 200X assessment, or carried over from the prior fiscal year, are attached. These reports identify the nature of the weakness or non-conformance, its cause and effect, appropriate interim milestones in the corrective action plan, progress to date, metrics used to measure progress and insure correction, the funds set aside to correct the weakness, and the individuals, including field officials, accountable for the timely completion of stated corrective actions. (If any material weakness corrective action plan targeted for completion in FY 200X was not completed as planned, please report the reasons for the slippage and a summary of what actions remain.) The existence of these material weaknesses or accounting system non-conformances does/does not prevent the [bureau/office] from providing reasonable assurance on the effectiveness of its internal control taken as a whole.

I also conclude that the [bureau/office's] information technology systems generally comply/do not generally comply with the requirements of the Federal Information Security Management Act (FISMA), and Appendix III of OMB Circular A-130, Management of Federal Information Resources.

Further, I conclude that the [bureau/office] substantially complies/does not substantially comply with the three components of the Federal Financial Management Improvement Act (FFMIA): Financial system requirements, Federal accounting standards, and the U.S. Standard General Ledger at the transaction level.

Attachments

SECTION 2
EXHIBIT 5B
ILLUSTRATIVE TEMPLATE FOR A QUALIFIED STATEMENT OF ASSURANCE

Memorandum

To: Assistant Secretary - Policy, Management and Budget
Attention: Director, Office of Financial Management

Through: Assistant Secretary

From: Bureau/Office Director

Subject: FY 200X Annual Assurance Statement on Internal Control

The [bureau/office] management is responsible for establishing and maintaining effective internal control and financial management systems that meet the objectives of the Federal Managers' Financial Integrity Act (FMFIA). The [bureau/office] is able to provide a qualified statement of assurance that the internal controls and financial management systems meet the objectives of FMFIA, with the exception of [number] material weakness(es) and [number] non-conformance(s). The details of the exception(s) are provided in Exhibit [xx].

The [bureau/office] conducted its assessment of the effectiveness of internal control over the effectiveness and efficiency of operations and compliance with applicable laws and regulations in accordance with departmental guidance and OMB Circular A-123, *Management's Responsibility for Internal Control*, dated December 21, 2004. The objectives of this assessment are to ensure that:

- Programs achieve their intended results;
- Resources are used consistent with agency mission;
- Resources are protected from waste, fraud, and mismanagement;
- Laws and regulations are followed; and
- Reliable and timely information is maintained, reported, and used for decision-making.

In performing this assessment, the [bureau/office] relied on the knowledge and experience management has gained from the daily operation of its programs and systems of accounting and administrative controls, and information obtained from sources such as internal control assessments, OIG and GAO audits, program evaluations and studies, audits of financial statements, and performance plans and reports. The following specific internal control assessments conducted by the bureau, and audits and/or reviews conducted by the OIG and/or GAO were relied upon to support the conclusions expressed herein.

Assessment /Audit (List or attach list)	Date Completed	Results (Material Weakness or Best Practice)

Statement of Qualified Assurance (con't)

Based on the results of the evaluation, the [bureau/office] identified [number] material weakness(es) in its control over the effectiveness and efficiency of operations and compliance with applicable laws and regulations as of September 30, 200X. Other than the exceptions noted in Exhibit [xx], the internal controls were operating effectively and no other material weaknesses were found in the design or operation of the internal controls.

In addition, the [bureau/office] conducted its assessment of the effectiveness of internal control over financial reporting, which includes safeguarding of assets and compliance with applicable laws and regulations, in accordance with the requirements of Appendix A of OMB Circular A-123. Based on the results of this evaluation, the [bureau/office] can provide reasonable assurance that its internal control over financial reporting as of June 30, 200X was operating effectively and no material weaknesses were found in the design or operation of the internal control over financial reporting.

The corrective action reports for material weaknesses and/or accounting system non-conformances identified in the FY 200X assessment, or carried over from the prior fiscal year, are attached. These reports identify the nature of the weakness or non-conformance, its cause and effect, appropriate interim milestones in the corrective action plan, progress to date, metrics used to measure progress and insure correction, the funds set aside to correct the weakness, and the individuals, including field officials, accountable for the timely completion of stated corrective actions. (If any material weakness corrective action plan targeted for completion in FY 2005 was not completed as planned, please report the reasons for the slippage and a summary of what actions remain.) The existence of these material weaknesses or accounting system non-conformances does/does not prevent the [bureau/office] from providing reasonable assurance on the effectiveness of its internal control taken as a whole.

I also conclude that the [bureau/office's] information technology systems generally comply/do not generally comply with the requirements of the Federal Information Security Management Act (FISMA, and Appendix III of OMB Circular A-130, Management of Federal Information Resources.

Further, I conclude that the [bureau/office] substantially complies/does not substantially comply with the three components of the Federal Financial Management Improvement Act (FFMIA): Financial system requirements, Federal accounting standards, and the U.S. Standard General Ledger at the transaction level.

Attachments

SECTION 2
EXHIBIT 5C
ILLUSTRATIVE TEMPLATE WHEN CANNOT PROVIDE A STATEMENT OF ASSURANCE

Memorandum

To: Assistant Secretary - Policy, Management and Budget
Attention: Director, Office of Financial Management

Through: Assistant Secretary

From: Bureau/Office Director

Subject: FY 2006 Annual Assurance Statement on Internal Control

The [bureau/office] management is responsible for establishing and maintaining effective internal control and financial management systems that meet the objectives of the Federal Managers' Financial Integrity Act (FMFIA). The [bureau/office] is unable to provide a qualified statement of assurance that the internal controls and financial management systems meet the objectives of FMFIA, due to the [number] material weakness(es) and [number] non-conformance(s) listed in Exhibit [xx].

The [bureau/office] conducted its assessment of the effectiveness of internal control over the effectiveness and efficiency of operations and compliance with applicable laws and regulations in accordance with departmental guidance and OMB Circular A-123, *Management's Responsibility for Internal Control*, dated December 21, 2004. The objectives of this assessment are to ensure that:

- Programs achieve their intended results;
- Resources are used consistent with agency mission;
- Resources are protected from waste, fraud, and mismanagement;
- Laws and regulations are followed; and
- Reliable and timely information is maintained, reported, and used for decision-making.

In performing this assessment, the [bureau/office] relied on the knowledge and experience management has gained from the daily operation of its programs and systems of accounting and administrative controls, and information obtained from sources such as internal control assessments, OIG and GAO audits, program evaluations and studies, audits of financial statements, and performance plans and reports. The following specific internal control assessments conducted by the bureau, and audits and/or reviews conducted by the OIG and/or GAO were relied upon to support the conclusions expressed herein.

Assessment /Audit	Date Completed	Results (Material Weakness or Best Practice)
(List or attach list)		

Statement of No Assurance (con't)

Based on the results of the evaluation, the [bureau/office] identified [number] material weakness(es) in its control over the effectiveness and efficiency of operations and compliance with applicable laws and regulations as of September 30, 200X. Other than the exceptions noted in Exhibit [xx], the internal controls were operating effectively and no other material weaknesses were found in the design or operation of the internal controls.

In addition, the [bureau/office] conducted its assessment of the effectiveness of internal control over financial reporting, which includes safeguarding of assets and compliance with applicable laws and regulations, in accordance with the requirements of Appendix A of OMB Circular A-123. The [bureau/office] did not fully implement the requirements included in OMB Circular A-123 and therefore cannot provide assurance that it's internal control over financial reporting as of June 30, 2xxx was operating effectively. A summary of actions the [bureau/office] will take to comply with the Circular A-123 requirements is included in Exhibit [xx].

The corrective action reports for material weaknesses and/or accounting system non-conformances identified in the FY 2005 assessment, or carried over from the prior fiscal year, are attached. These reports identify the nature of the weakness or non-conformance, its cause and effect, appropriate interim milestones in the corrective action plan, progress to date, metrics used to measure progress and insure correction, the funds set aside to correct the weakness, and the individuals, including field officials, accountable for the timely completion of stated corrective actions. (If any material weakness corrective action plan targeted for completion in FY 2005 was not completed as planned, please report the reasons for the slippage and a summary of what actions remain.) The existence of these material weaknesses or accounting system non-conformances does/does not prevent the [bureau/office] from providing reasonable assurance on the effectiveness of its internal control taken as a whole.

I also conclude that the [bureau/office's] information technology systems generally comply/do not generally comply with the requirements of the Federal Information Security Management Act (FISMA), and Appendix III of OMB Circular A-130, Management of Federal Information Resources.

Further, I conclude that the [bureau/office] substantially complies/does not substantially comply with the three components of the Federal Financial Management Improvement Act (FFMIA): Financial system requirements, Federal accounting standards, and the U.S. Standard General Ledger at the transaction level.

Attachments

SECTION 3
CHAPTER 1
OVERVIEW

In accordance with 340 DM §1.5.F, this section of the Internal Control and Audit Follow-up Handbook is designed to provide guidance and establish policy and process procedures for the information technology and information security community, within the Department of the Interior, for conducting the necessary Internal Control Reviews (ICRs) for information systems and Information Technology (IT) programs.

As identified in the Federal Regulations and OMB circulars, referenced in Addendum B, the Department of the Interior is required to conduct an ongoing review of internal controls and report annually on the adequacy of the department's program and operation internal control 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 identified herein. The ICR of information systems and IT programs directly supports and substantiates the annual assurance statement signed by the Secretary of the Interior.

It is paramount that bureaus and offices streamline their ICRs with their system and reporting requirements to facilitate more efficient reporting and use of their financial and human resources. Internal review processes and reporting requirements shall be evaluated to identify overlap and to facilitate eliminating or streamlining of those reviews that can satisfy multiple requirements.

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

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

I. <u>OCIO</u> – Office of the Chief Information Officer, an organization under the Office of the Secretary.
II. <u>CSD</u> – Cyber Security Division, an organization under the Office of the Chief Information Officer.
III. <u>OCIO ICR Coordinator</u> – A designated "ICR" official in the Cyber Security Division of the OCIO.

SECTION 3
CHAPTER 2
ROLES AND RESPONSIBILITIES POLICY

Bureau and Office Directors have the overall responsibility to monitor bureau 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 follow-up program to ensure that Departmental Management is advised of impending problems and recommended solutions that shall ensure that the bureau 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 IT programs:

A. Departmental Chief Information Officer - Responsible for the overall ICR program of information systems and IT programs for the department. Provides the department level assurance statement to the Secretary of the Interior.

B. OCIO ICR Coordinator - Responsible for the annual guidance, support, compliance, and Department level reporting relating to ICRs of information systems and IT programs for the Department. This position is designated to a member of the Cyber Security Division in the Office of the Chief Information Officer.

C. Bureau and Office Chief Information Officers - Responsible for the overall ICRs of information systems and IT programs within their respective bureau or office.

D. Bureau and Office IT Security Managers - Responsible for the integrity and quality of ICRs of information systems and IT programs within their respective bureau or office. Responsible for ensuring that weaknesses are tracked and managed in accordance with regulation, policy, and the POA&M process.

E. System Owners - Responsible for certifying the results of ICRs for their assigned information systems and IT programs.

F. System Managers - Responsible for approving the results of ICRs for their assigned information systems and IT programs.

G. System Security Officers - Responsible for planning and conducting ICRs of their assigned information systems and IT programs.

SECTION 3
CHAPTER 3
EXECUTING INTERNAL CONTROL REVIEWS FOR INFORMATION SYSTEMS & IT PROGRAMS

1. Policy: Internal Control Reviews (ICRs) of all information systems and Information Technology (IT) 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, NIST Special Publications 800-26, 800-37, and 800-53.

2. Scope: All Department information systems and IT programs.

3. Definitions:

3.1. 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 Special Publication 800-37).

3.1.1. 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 application should be provided by security of the system in which they operate (either a major application or general support system). Source: OMB A-130 Appendix III

3.1.2. 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 A-130 Appendix III

3.1.3. 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

3.1.4. 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)

3.1.5. 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 relate (or mixed) systems. The OIG often terms this as a NONCompliance issue. (IC-8)

3.1.6. Nonmaterial 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)

4. Policy & Process:

* Note: If the dates provided in the policy and process do not fall on a business day, the next business day should be used.

4.1. The OCIO ICR Coordinator shall distribute the revised assessment template and guidance document for completing the template; and shall issue a complete listing of information systems to all bureaus and offices for reconciling and baselining the information systems to be reviewed. This shall be completed during the month of January.

4.1.1. Any discrepancies between the distributed list and bureau and office lists shall be immediately resolved, and any necessary updates completed.

4.2. The Bureau and Office Chief Information Officers shall immediately begin formalizing and executing plans to review all of the information systems and IT program(s) under their responsibility. Plans shall be submitted by each Bureau and Office Chief Information Officer to the OCIO ICR Coordinator by March 1st.

4.2.1. The plans shall include all information systems and IT program(s) for the bureau or office.

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

4.2.3. The plans shall demonstrate a schedule that meets the date requirements for delivery of the reports to the department.

4.3. ICRs for all Information Systems and IT programs shall be completed and submitted to the OCIO ICR Coordinator by June 1st.

4.3.1. The ICR of each Information System shall include:

4.3.2. a completed NIST Special Publication 800-26, or a revised 800-26 self assessment questionnaire;

4.3.2.1. The guidance and instructions in NIST Special Publication shall be followed to ascertain and conclude the maturity level of the program and information systems for each control area.

4.3.3. A statement letter of "No Weaknesses" or "Weaknesses Found." Statement letters shall be addressed to the Departmental CIO and OCIO ICR Coordinator. A separate statement letter shall be completed for each individual Information System and IT program.

4.3.3.1. All Material Weaknesses, Non-conformance, and Nonmaterial Weaknesses found shall be recorded in the statement letter and recorded in the respective Information System or IT program Plan of Actions and Milestone (POA&M) report.

4.3.3.1.1. A POA&M is used to identify, prioritize, and manage corrective efforts associated with the mitigation of security weaknesses identified in a system or program. It is also used to report the status of security weakness remediation efforts to OMB and Congress.

4.3.3.1.2. A POA&M entry shall be made for each weakness and shall include the related corrective actions, the scheduled completion date for correcting each weakness, and the status for correcting each weakness.

4.4. The OCIO ICR Coordinator shall validate that ICRs have been submitted for each system identified in the list completed in §4.1. <u>This shall be completed by June 5th.</u> Any missing ICRs shall be announced to the respective Bureau or Office IT Security Manager and Bureau or Office Chief Information Officer.

4.5. The OCIO ICR Coordinator shall assess all ICRs for quality and completeness with the respective System Security Officers, System Managers, Systems Owners, and Bureau and Office IT Security Managers. <u>This quality review shall be completed by July 1st.</u> <u>Within 7 business days, a letter from the OCIO ICR Coordinator, addressed to the Departmental Chief Information Officer, shall attest that all ICRs have been completed for information systems and IT programs, and all ICRs shall be included in the transmittal.</u>

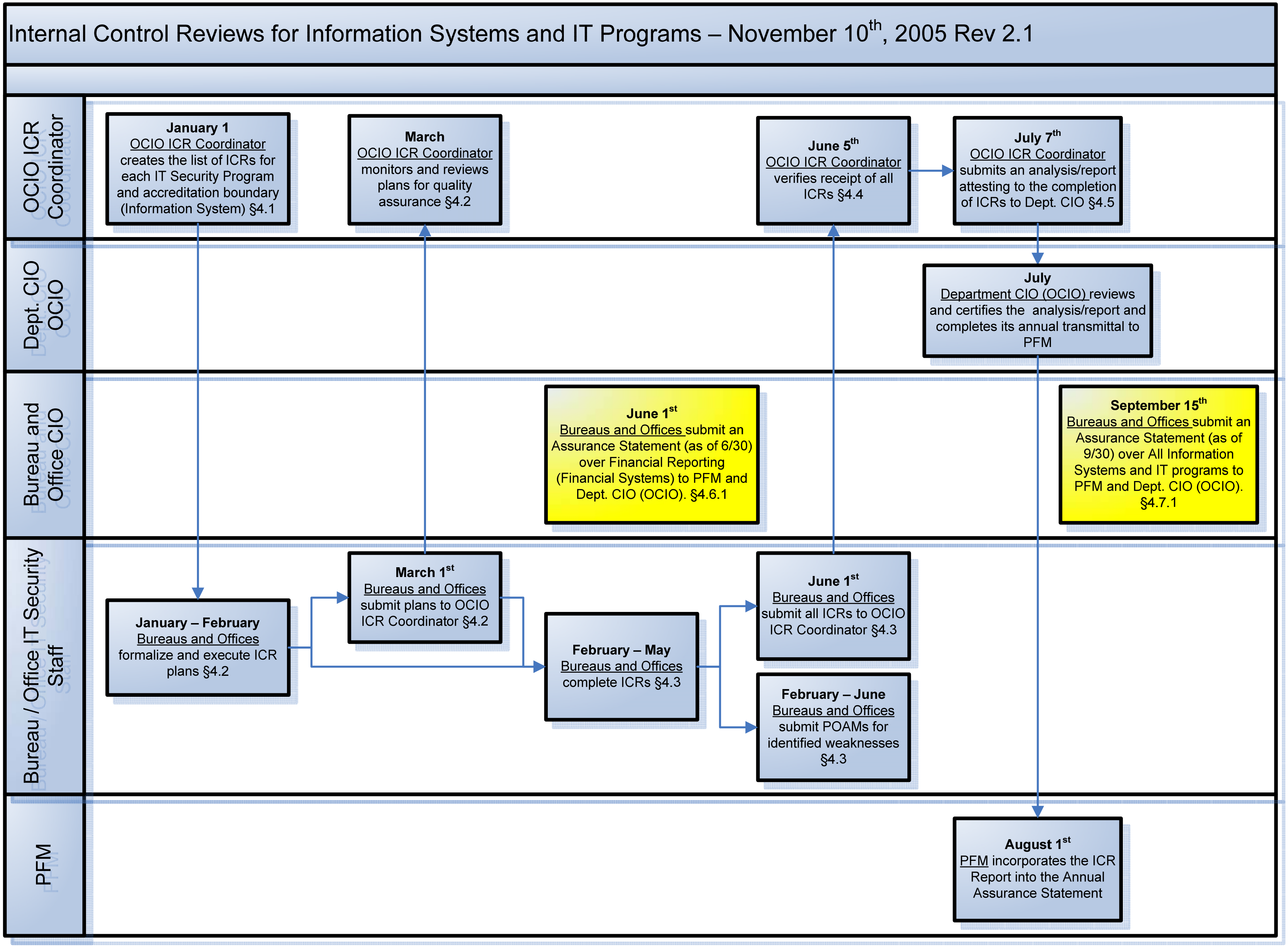
<u>Bureau and Office Assurance Statements</u>

4.6. All bureau and office ICRs over financial reporting shall be completed on or before June 1st. This includes required reviews for financial information systems. Bureaus' and offices' assurance statements over financial reporting as of June 30th must be submitted to PFM on or before June 1. The assurance statement must address compliance with FFMIA for financial Information Systems. (PFM Guidance)

4.6.1. POLICY: On or before June 1st, bureau and office CIOs shall sign the bureau/office assurance statement or submit a separate assurance statement. The assurance statement shall include the results of the ICR(s) and any weaknesses found for financial information systems.

4.7. All reviews of non-financial programs or operations planned shall be completed on or before August 31st. Bureaus' and offices' annual assurance statement over all programs and operations, including Information Systems, as of September 30th, must be submitted to PFM on or before September 15th. This statement should include an update to the June 30th assurance statement over financial reporting which verifies that key financial reporting controls either have no reportable changes between June 30th, and September 30th, or reportable material weaknesses have been corrected. (PFM Guidance)

4.7.1. POLICY: On or before September 15th, bureau and office CIOs shall sign the bureau/office assurance statement or submit a separate assurance statement. The assurance statement shall include the results of the ICR(s) and any weaknesses found for all Information Systems and IT programs reviewed, and any updates from the June 30th assurance statement.



IT – Addendum A

SECTION 3
Addendum B -
Statutory and OMB Requirements Outline

Federal Regulations

1. FISMA (Federal Information Security Management Act of 2002)

The E-Government Act (Public Law 107-347) passed by the one hundred and seventh 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 agencywide 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

(6) ***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

(7) ***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.

2. 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.

3. GISRA (Government Information Security Reform Act of 2000)
FISMA replaced GISRA.

4. CSA (Computer Security Act of 1987)
FISMA repealed CSA.

5. 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.

6. OMB Circular A-11, Preparation, Submission, and Execution of the Budget

OMB 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. PRA (Paperwork Reduction Act)
Amended by GPEA.

12. 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.

13. 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

<u>National Institute of Standards and Technology</u>

14. **800-16** Information Technology Security Training Requirements: A Role and Performance-Based Model
15. **800-18** Guide for Developing Security Plans for Information Technology Systems
16. **800-23** Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
17. **800-26** Self-Assessment Guide for Information Technology Systems
18. **800-30** Risk Management Guide for Information Technology Systems

19. **800-34** Contingency Planning Guide for Information Technology Systems
20. **800-37** Guide for the Security Certification and Accreditation of Federal Information Systems
21. **800-47** Security Guide for Interconnecting Information Technology Systems
22. **800-50** Building an Information Technology Security Awareness and Training Program
23. **800-53** Recommended Security Controls for Federal Information Systems
24. **800-55** Security Metrics Guide for Information Technology Systems
25. **800-60** Guide for Mapping Types of Information and Information Systems to Security Categories
26. **800-61** Computer Security Incident Handling Guide
27. **800-64** Security Considerations in the Information System Development Life Cycle
28. **800-65** Integrating Security into the Capital Planning and Investment Control Process

S E C T I O N 3

Addendum C - REPORTING REQUIREMENTS

1. FISMA

a. What: Annual reporting defined in OMB memorandum (2005: M-05-15)

b. Who: OMB M-05-15
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 (2005: October 7, 2005)

d. How: Using the OMB Guidance and Excel template, completed and transmitted (hard copy and electronic). Tools used to gather inputs for section B include DEAR, Command Center C&A module, DOI CIRC, Department policy, online training reports, and data calls using various office automation tools include Word and Excel.

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) 2005: August 30, 2005 [?]

d. How: 1)
2)
3)

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
1) 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 Congress regarding implementation of FFMIA
b. Who: (a) Agency Director
(b) Inspector General
(c) Comptroller General
c. When: (a) Annually, by March 311
(b) [?]

(c) Annually, by October 1

d. How: [?]

Statutory and OMB Requirements Traceability Matrix

Replaced /Notes	1. FISMA	Applies to all Federal Systems 2. A-130	Replaced by FISMA 3. GISRA	Repealed by FISMA 4. CSA	5. ITMRA /CCA	6. A-11	Internal Control Reviews 7. FMFIA	FMFIA Guidance 8. A-123	Pursuant to FMFIA / Financial Mgmt Systems 9. A-127	External Audits 10. FFMIA	11. PRA	Amends to PRA 12. GPEA	13. GPRA
1. FISMA													
2. OMB A-130				REQ	REQ	REF	REF	REF			REQ	REQ	REQ
2e. M-05-15	REQ	REF			REF			REF					
5. ITMRA/CCA													
6. A-11	REF	REF			REQ						REF	REF	REF
7. FMFIA													
8. A-123							REQ						
9. A-127		REF					REQ						
10. FFMIA													
14. 800-16		REQ		REQ									
15. 800-18		REQ		REQ									
16. 800-23		REQ		REQ									
17. 800-26	REQ	REQ	REQ	REQ	REC	REQ	MCR						
18. 800-30	REQ	REQ	REQ	REQ	REQ								
19. 800-34		REQ		REQ	REQ								
20. 800-37	REQ	REQ			REF						REF		
21. 800-47		REQ		REQ	REQ								
22. 800-50	REQ	REQ											
23. 800-53	REQ	REQ											
24. 800-55	REQ	REQ	REQ		REQ	REQ	MCR					REQ	REQ
25. 800-60	REQ	REQ											
26. 800-61	REQ	REQ											
27. 800-64	REQ	REQ			REF								
28. 800-65	REQ	REQ			REF	REC							

REQ	Required by LAW
REQ	Required
REC	Recommended
REF	Referenced
PREREQ	Prerequisite to X
OPT	Optional;

NIST Requirements Traceability Matrix – Continued

	800-16	800-18	800-23	800-26	800-30	800-34	800-37	800-47	800-50	800-53	800-55	800-60	800-61
14. 800-16													
15. 800-18													
16. 800-23													
17. 800-26		PREREQ		REF									
18. 800-30		REF											
19. 800-34					REF								
20. 800-37		REF				REF		REF	REF				REF
21. 800-47		REF							REF				
22. 800-50	REF												
23. 800-53		REF		REF	REF		REF					REF	
24. 800-55				REF									
25. 800-60		PREREQ		PREREQ	PREREQ		PREREQ			PREREQ			
26. 800-61					REF								
27. 800-64					REF								
28. 800-65				REF	REF					REF	REF		

	800-64	800-65	800-70	FIPS	FIPS 87	FIPS 199	FIPS 200	FIPS 201	FPC 65	PDD	PDD 67	PDD 63	FEMA/ FRP
14. 800-16													
15. 800-18													
16. 800-23													
17. 800-26													
18. 800-30				REF									
19. 800-34					OPT				OPT		OPT	OPT	OPT
20. 800-37			REF					REF					
21. 800-47													
22. 800-50													
23. 800-53						REF	REF						
24. 800-55				REF						REF			
25. 800-60						REF	REF					OPT	
26. 800-61													
27. 800-64													
28. 800-65													

REQ	Required by LAW
REQ	Required
REC	Recommended
REF	Referenced
PREREQ	Prerequisite to X
OPT	Optional;

SECTION 4
CHAPTER 1
OVERVIEW

Audit Follow-Up 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 Follow-Up," (see Addendum A) directs each federal agency to "establish systems to assure the prompt and proper resolution and implementation of audit recommendations."

The Department 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, the Department has established goals for meeting the requirements of 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 Department has established a comprehensive audit follow-up program to ensure that policy and direction regarding the resolution and implementation of audit recommendations is promulgated for the Department's managers, that audit recommendations are implemented in a timely and cost-effective manner, and that audit-related debt and other funds due the federal government from contractors and grantees are collected, offset, or written-off, as appropriate.

This section of the handbook discusses the roles and responsibilities of all components of the audit follow-up process, procedures for responding to audit reports, the Department's audit follow-up tracking system, reporting, and references to key OMB, GAO, and Departmental guidance pertaining to the Audit Follow-Up Program.

ROLES AND RESPONSIBILITIES

The Department's Audit Follow-Up program provides for the clear responsibility of all components involved in reviewing, responding to, and implementing of 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

The OIG, under the general supervision of the Secretary, is responsible for conducting, supervising, and issuing audit reports of programs, operations, activities and functions conducted by the Department as well as programs funded by the Department. The OIG is also responsible for conducting or supervising audits of insular area governments' programs and operations. It determines when audits can be carried out by organizations outside the OIG, such as state and local auditors. In addition, the OIG issues audit reports that it has conducted or that have been conducted by other audit organizations.

Government Accountability Office

GAO is the investigative arm of Congress that supports the Congress in meeting its Constitutional responsibilities and assists in improving the performance and accountability of the federal government.

Assistant Secretary - Policy, Management and Budget

The Assistant Secretary - Policy, Management and Budget (AS/PMB) is the Department's Chief Financial Officer (CFO), and, as such, discharges the authority of the Secretary for all phases of management and administrative activities and serves as a principal policy advisor to the Secretary. The AS/PMB is also the Chair, Internal Control and Audit Follow-Up (ICAF) Council and Audit Follow-Up Official. In this capacity, the Assistant Secretary is responsible for overseeing the Department's Audit Follow-Up Program, including the resolution of disputed audit recommendations and corrective actions.

Office of Financial Management

The Assistant Secretary - Policy, Management and Budget has delegated day-to-day responsibility for carrying out the responsibilities of the Audit Follow-Up Program to the Office of Financial Management (PFM). PFM is responsible for establishing Departmental policy regarding the Departmental Audit Follow-Up Program, for assisting the Audit Follow-Up Official in resolving disputed audit recommendations, for establishing and maintaining the Departmental audit follow-up tracking system, and for providing training and technical assistance to bureaus and offices regarding the Department's Audit Follow-Up Program.

Departmental Management (Program Assistant Secretaries and Bureau and 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 to be responsible for day-to-day audit and audit follow-up functions, and for ensuring that systems are in place that provide for the prompt and thorough response to audit recommendations and for the 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 for their organizational component.

Senior Management Council/Internal Control and Audit Follow-up Council

The Council is chaired by the AS/PMB and is comprised of all program assistant secretaries, the Solicitor, and the Inspector General (ex officio), Deputy Assistant Secretary – Business Management and Wildland Fire, Chief Information Officer, and 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 effectiveness of internal controls over financial reporting;
- Recommend to the AS/PMB which control deficiencies are material to disclose in the annual Federal Managers Financial Integrity Act (FMFIA) assurance statement and PAR;
- Oversee implementation of corrective actions related to material weaknesses; and
- Determine when sufficient action has been taken to declare a reportable condition or material weakness corrected.

Senior Assessment Team/Management Initiatives Team

The team is responsible to:

- Ensure assessment objectives are clearly communicated throughout the agency;
- Ensure adequate funding and resources are made available to comply with the requirements of OMB A-123, as revised;
- Ensure 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 A-123, as revised; and
- Determine or approve assessment design and methodology for each entity and the Department.

SECTION 4
CHAPTER 2
ACCOUNTABILITY AND REPORTING

The Department places a high priority on improving and promoting accountability and integrity in the Departmental Audit Follow-Up Program and in achieving GPRA performance goals. To evaluate the effectiveness of (1) the Audit Follow-Up Program and (2) the Department managers and program officers in implementing audit recommendations, PFM works in partnership with bureaus, PMB 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, periodic reporting, and progress meetings provide opportunities to monitor the effectiveness of the Audit Follow-Up Program.

Corrective Action Plans

The development of corrective action plans and target implementation dates precedes periodic reporting; however, it is integral to the Department's Audit Follow-up Program. Per OMB Circular A-50, responses indicating agreement on final reports shall include planned corrective actions and, where appropriate, dates for achieving actions. To facilitate prompt implementation of recommendations and to reduce slippage, bureaus and offices must make every effort to:

- Provide responses to recommendations that include target implementation 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 quarterly milestones are achieved.

Monthly Audited Financial Statement Status Reports and Audit Recommendation Implementation Progress

To facilitate the prompt resolution of audited financial statement recommendations and implementation of other audit recommendations, bureaus/offices are required to provide monthly status reports on all financial statement material weaknesses and non-compliance issue corrective actions and open audit recommendations at the end of each calendar month. Information from these reports is included in PFM's monthly scorecard reports to senior management. Bureau/office status reports formats should adhere to the PFM fiscal year guidance regarding material weaknesses and noncompliance reporting and open audit recommendations.

To prevent/reduce backlogs of unimplemented audit recommendations, to ensure the accuracy of the Departmental Audit Follow-Up Tracking System, and to achieve the annual GPRA performance goal for the Audit Follow-Up Program, bureaus and offices are required to provide detailed status reports on implementation progress for each pending OIG, GAO, and financial statement audit. Appropriate closure documentation should be forwarded to PFM at the same time. Where targeted implementation dates for pending audit recommendations have slipped, a concise statement of the reasons for the slippage and the revised target dates should be included. 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). Information from these reports will also be included in PFM's monthly scorecard reports to senior management

Bureaus/Offices may be advised that they may report on a quarterly basis if monthly reports are consistently submitted on time and a green status on achievement is indicated each month.

Quarterly Status Reports

Quarterly Status Reports contain the same information as that provided during the monthly cycle (status of material weakness, non compliance, and open audit recommendation correction) with the addition of a summary of audits closed and recommendations implemented during the reporting period and the disposition of disallowed costs. Appropriate closure documentation should be forwarded to PFM at the same time. Where targeted implementation dates for pending audit recommendations have slipped, a concise statement of the reasons for the slippage and the revised target dates should be included. 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.

Note: Bureaus/offices are not confined to providing notice of implementation of audit reports/recommendations via monthly reports; bureaus are encouraged to notify PFM of implementation along with the submission of appropriate documentation throughout the year. PFM provides their decision on the closure of OIG recommendations/audits to the appropriate bureaus/offices and the OIG.

Mid-Year and Year-End Progress Meetings

Bureaus/offices are required to participate in a mid-year and year-end progress meeting with PFM, PMB, and OIG; these meetings are usually held in May and September, respectively. The purpose of the meetings is to review program status and discuss and resolve other pertinent audit follow-up 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.

Internal Control and Audit Follow-Up Council Meetings (Senior Management Council)

If issues arise at the mid-year progress meetings that cannot be resolved during the meetings, 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 Assistant Secretary – PMB and the ICAF Council, PFM will prepare a list of the issues for which agreement/resolution could not be achieved at the mid-year and year-end issue resolution meetings and will schedule the ICAF Council meeting.

Annual Performance and Accountability 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 GMRA also authorized the OMB to implement a pilot program to streamline and consolidate certain statutory financial management and performance reports into a single, annual accountability report.

The objective of the Annual Performance and Accountability Report (PAR) is to provide complete and concise financial and performance information concerning the effectiveness of the Department in achieving its financial program objectives. The information previously reported in the Secretary's FMFIA Annual Report, the Secretary's Semi-Annual Report on Audit Follow-Up, the CFO Act Annual Report, and Civil Monetary Penalties and Prompt Payment Act Reports are condensed into the Accountability Report. A component of the PAR is a compliance section that discusses the ICAF and provides performance data and statistics regarding the effectiveness of bureaus and offices in meeting the requirements of pertinent laws and regulations pertaining to the ICAF and Audit Follow-Up Programs.

The PAR also includes key performance measurement data in accordance with the Government Performance and Results Act (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. In accordance with the GPRA, the Department has established an objective to resolve audit findings in a timely manner. The PAR now includes both the Appendix A as of June 30 assurance statement, as well as the FMFIA required September 30 assurance statement.

Tools such as the monthly and quarterly updates, the issue resolution meetings, ICAF Council meetings, the PAR, as well as the departmental audit follow-up tracking system, provide tools to measure the Department's effectiveness in meeting the GPRA goals for the Audit Follow-Up Program.

Time Frames for Audit Responses

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

	Draft Reports	Final Reports

OIG Reports	30 to 45 calendar days for draft reports	30 calendar days
Financial Statement Audits	14 calendar days	30 calendar days
GAO Reports	7-30 calendar days (as directed by GAO)	60 calendar days
External Audits	N/A	90 calendar days

SECTION 4
ADDENDUM A
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 Follow-Up

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
CHAPTER 1
OFFICE OF INSPECTOR GENERAL AUDIT REPORTS

A PARTNERSHIP: THE OFFICE OF INSPECTOR GENERAL AND AND THE OFFICE OF FINANCIAL MANAGEMENT

The Inspector General Act of 1978 established the OIG in federal departments and agencies. The objective of the Act was to create independent and objective offices to provide policy direction for conducting, supervising, and coordinating audits, investigations, and other activities to promote economy, efficiency, and effectiveness and to prevent and detect fraud, waste, abuse and mismanagement in programs and operations. The Department of the Interior OIG reports directly to the Secretary of the Interior and the Congress on problems and deficiencies relating to the administration of Departmental programs and operations identified during audits including making recommendations to correct deficiencies.

The Inspector General Act requires the OIG to report semiannually (no later than April 30 and October 31) to the Secretary and the Congress on significant problems, abuses, and deficiencies found in programs and operations during each reporting period. The reporting periods cover the periods from October 1 to March 31 and from April 1 to September 30. The Office of Financial Management (PFM) assists the OIG in the preparation of its semi-annual reports by providing updated information on the status of audits that the OIG has referred to PFM for resolution and/or tracking.

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 the Department and to report on the progress Departmental management is making to correct deficiencies cited in OIG audit report recommendations.

While the OIG conducts and issues audit reports, the Departmental Audit Follow-Up Official, who has delegated day-to-day responsibility for the Audit Follow-Up Program to the PFM, resolves impasses between the OIG and management, and tracks, monitors, and reports on the audits that have been referred to it by the OIG. The smooth transition from audits under the purview of the OIG to audits that have been referred by the OIG to PFM, enables the Departmental Audit/Audit Follow-Up Programs to operate efficiently and effectively. The additional components of audit liaison officers and management, working together to identify, respond to, resolve, track, and close audit recommendations and reports ensures that all levels of the Department are working cooperatively to make the entire Audit/Audit Follow-Up Programs work for maximum efficiency and also allows the Department to meet its GPRA goals.

SECTION 5
CHAPTER 2
INTERNAL AUDIT REPORTS

The objectives of an internal audit (also referred to as a program audit) include determining: (1) The extent to which the desired results or benefits established by the legislature or other authorizing body are being achieved; (2) The effectiveness of organizations, programs, activities, or functions; and, (3) Whether the audited entity has complied with laws and regulations applicable to the program. The OIG conducts and issues internal audits and evaluations of a Departmental, bureau, or office program or operation, or an audit of an insular area or tribal government.

The internal audit process (see flowchart at the end of the chapter) 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 Department-wide or bureau/office specific. The entrance conferences' purpose is for the OIG to discuss the scope and objectives of the new audit start. The OIG can also choose to provide only general information and state that after the audit survey phase, specific audit scope and objectives will be defined. Generally, after the entrance conference audit work will begin.

After the audit work has been completed, the OIG holds an exit conference with program officials. It is during the exit conference that the OIG discusses preliminary audit findings and can ask for additional information prior to the issuance of a draft audit report. Management and program officials are encouraged to use the exit conference as an opportunity to thoroughly review and discuss preliminary findings with the auditors, 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.

Factors that impact the implementation of audit recommendations should be taken into consideration when establishing target implementation dates. Management should establish target implementation dates that are both <u>reasonable</u> and <u>achievable</u>. Target dates should allow sufficient time for completion of all required actions so that delays 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 should 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.

After all audit work has been completed, the OIG will issue a draft audit report to which management normally has 30 – 45 calendar days to respond. Draft reports allow management the opportunity to review audit findings and provide comments that are incorporated into the final report. If, after management has responded to the recommendations in the final internal audit report, the OIG and management cannot agree on management's proposed corrective actions, or if management disagrees with the OIG's findings, the OIG will refer the report to PFM (through the Assistant Secretary - PMB) for resolution within 90 calendar days of the report's issuance. OMB Circular A-50, "Audit Follow-Up," directs that resolution should be made within a maximum of six months after issuance of a final report.

Internal Audit Reports Referred for Resolution

Because the audit follow-up official has delegated responsibility to PFM, the OIG refers internal reports directly to PFM for resolution action (see flow chart at the end of the chapter). Upon receipt of the referral, PFM enters the report and its recommendations into Departmental tracking and notifies management and the appropriate audit liaison officer of the referral.

PFM will review the issues in dispute and discuss these issues with management and the OIG in an informal attempt to reach agreement on audit findings and/or corrective actions. If PFM is unable to achieve resolution at this point, PFM will present the disputed issues to the Assistant Secretary - PMB with a suggested resolution plan. Upon the Assistant Secretary-PMB's determination of the resolution of the recommendations (known as the management decision), management and the OIG are notified and the report is closed unless there are open corrective actions which must be tracked through final action.

The OIG also refers to PFM for resolution, audit reports for which management has not responded within the specified time frame (30 calendar days for a final internal report). PFM then assumes responsibility for requesting and receiving management's response and making the final determination of the adequacy of the response. If all corrective actions have been taken when management responds, PFM closes the report and notifies management, the Audit Liaison Official, and the OIG of closure. If all corrective actions have not been taken, the report is entered into Departmental tracking through final action.

Internal Audit Reports Referred for Tracking

After management officials have reviewed the recommendations contained in an internal audit report and all corrective actions have been taken at this point, the audit report is closed by the OIG. If, however, there are any incomplete or unimplemented corrective actions, the OIG refers the report to PFM for departmental tracking (see flowchart at the end of the chapter). The date of the referral of the report to PFM for tracking is considered the date of the management decision. **Once the OIG has referred a report to PFM for tracking, the OIG closes the audit out in its tracking system and all tracking action becomes the responsibility of PFM.** All correspondence pertaining to the referred report should be provided to the Focus Leader, Internal Control and Audit Follow-up, PFM.

Upon receipt of a referral for tracking, PFM enters the report into departmental tracking and notifies the appropriate management official and audit liaison officer of the referral. PFM will continue to track unimplemented recommendations until sufficient documentation has been provided by management that all recommendations have been implemented and PFM makes a determination that the report may be closed.

Delays of Target Implementation Dates

Delays of target implementation dates occur when final implementation action has not been accomplished by the target date established by management. The Department considers delays of target dates to have a negative impact on programs and operations affected by the OIG recommendation. An indication of the importance the Department places on the timely implementation of audit recommendations is the establishment of an annual GPRA performance measure for timely completion of recommendations on schedule.

As soon as management becomes aware that an unimplemented recommendation will not be completed by the established target**,** PFM must be notified. Management's notification should provide an explanation for the delay, a new target date, and the name(s) of the official(s) responsible for implementation. Audit liaison officers should stay abreast of target dates so that they may notify the appropriate officials of the impending date and should coordinate with PFM, new information regarding corrective action target dates. It is imperative that PFM is informed of delay and revised target dates so that the Departmental audit follow-up tracking system is current and up to date.

Closure of Audit Reports and Documentation of Final Action

An internal audit report that has been referred to PFM for tracking may be closed when all unimplemented recommendations have been completed and accepted by PFM. Management is responsible for notifying PFM of the implementation of each recommendation until all recommendations have been completed. Management's notification must be complete, i.e., the notification should describe the OIG's recommendation and should discuss, in detail, all actions that were taken to implement the recommendation, how the implementation actions relate to the audit recommendation, and provide appropriate documentation of those actions.

The determination by PFM to close a recommendation is based upon the content of the OIG's recommendation and management's description and support for the actions that have been taken in response to the recommendation. For example, if the recommendation was for management to hire a computer analyst, the notification of implementation of the recommendation must provide the employee's name, date of hire, and, if appropriate, a copy of the position description. If the recommendation was to issue a specific directive, the notification of final action must state when the directive was issued and a copy of the directive must be provided. If the OIG recommends that a specific rule be developed and management provides documentation, in the form of a copy of the proposed rule, this action meets the intent of the recommendation and should be closed. If, however, the OIG recommends that a rule be published in the Federal Register, the recommendation cannot be closed until the rule has, in fact, been published in the Federal Register, either as a proposed or finale rule. In that example, management's notification to PFM must include a copy of the proposed or final rule.

Examples of appropriate supporting documentation include, but are not limited to:

- Bureau/office manual chapters
- Departmental Manual chapters

- New or revised policies and/or operating procedures
- Code of Federal Regulation or Federal Register chapters

In those instances where supporting documentation may be too voluminous to reasonably provide to PFM, such as bureau policy manuals, an appropriate citation or reference or website is acceptable as long as the original documentation is available upon request by PFM.

There may be occasions where PFM closed an audit recommendation/report but the OIG does not concur and can ask for additional information or request the recommendation/audit be reopened.

The OIG often performs follow-up audits of issues that were previously reported. Follow-up audit reports will usually discuss recommendations made in previous reports and whether, during the follow-up audit process, the OIG has determined that recommendations made in earlier reports have been implemented. PFM will close those recommendations made in earlier reports that the OIG says have been implemented. All other recommendations will remain unimplemented until management requests closure from PFM.

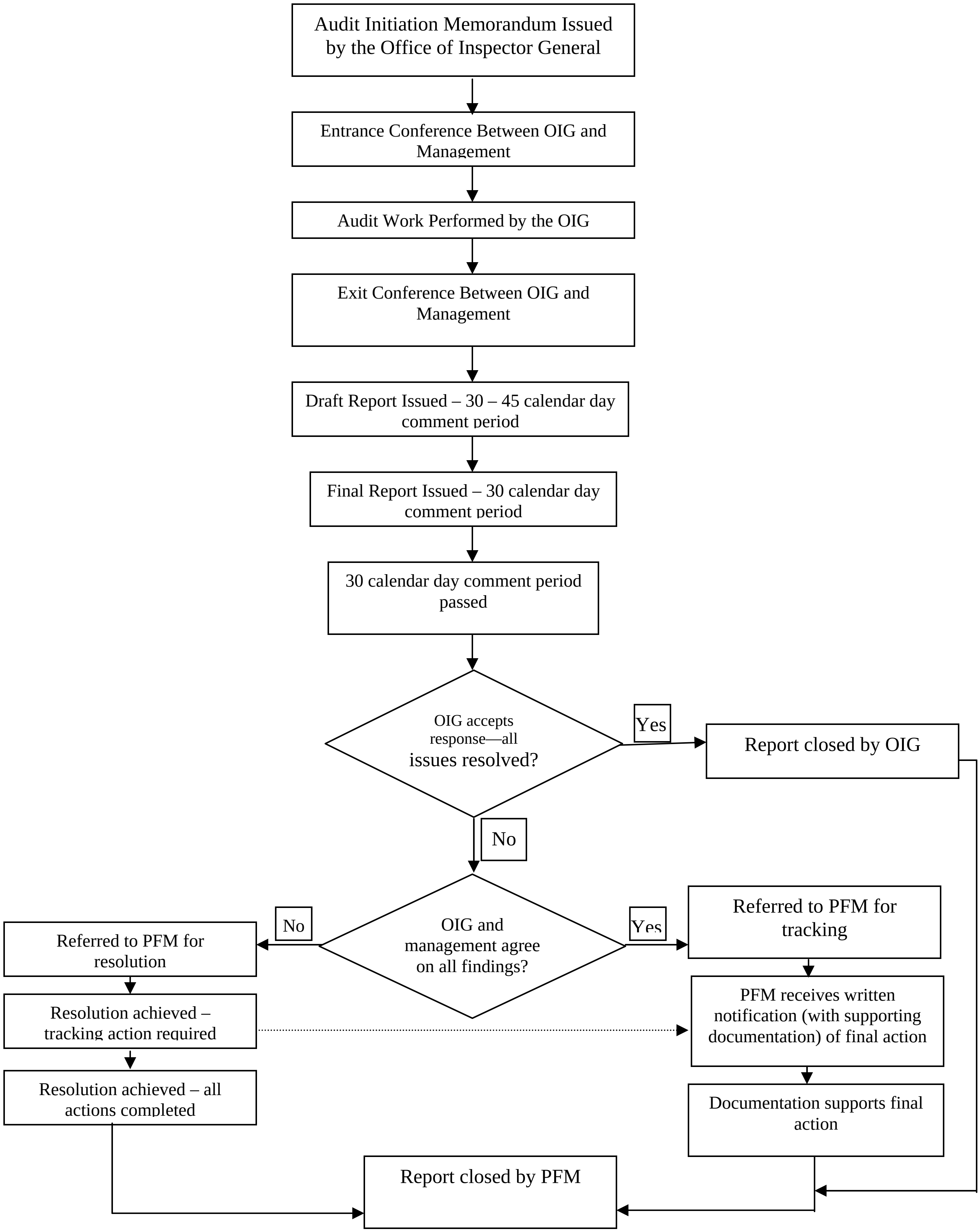
Internal Audits with Monetary Findings

For internal audit reports that contain OIG's assessment of the monetary impact of findings, such as funds to be put to better use, or potential additional or unpaid revenue, management is expected to indicate agreement or disagreement with the OIG's assessment of the monetary impact of the findings in its response to the audit report. If management has not indicated agreement with the monetary impact findings at the time of referral, the monetary finding(s) will not be entered into the Departmental tracking system.

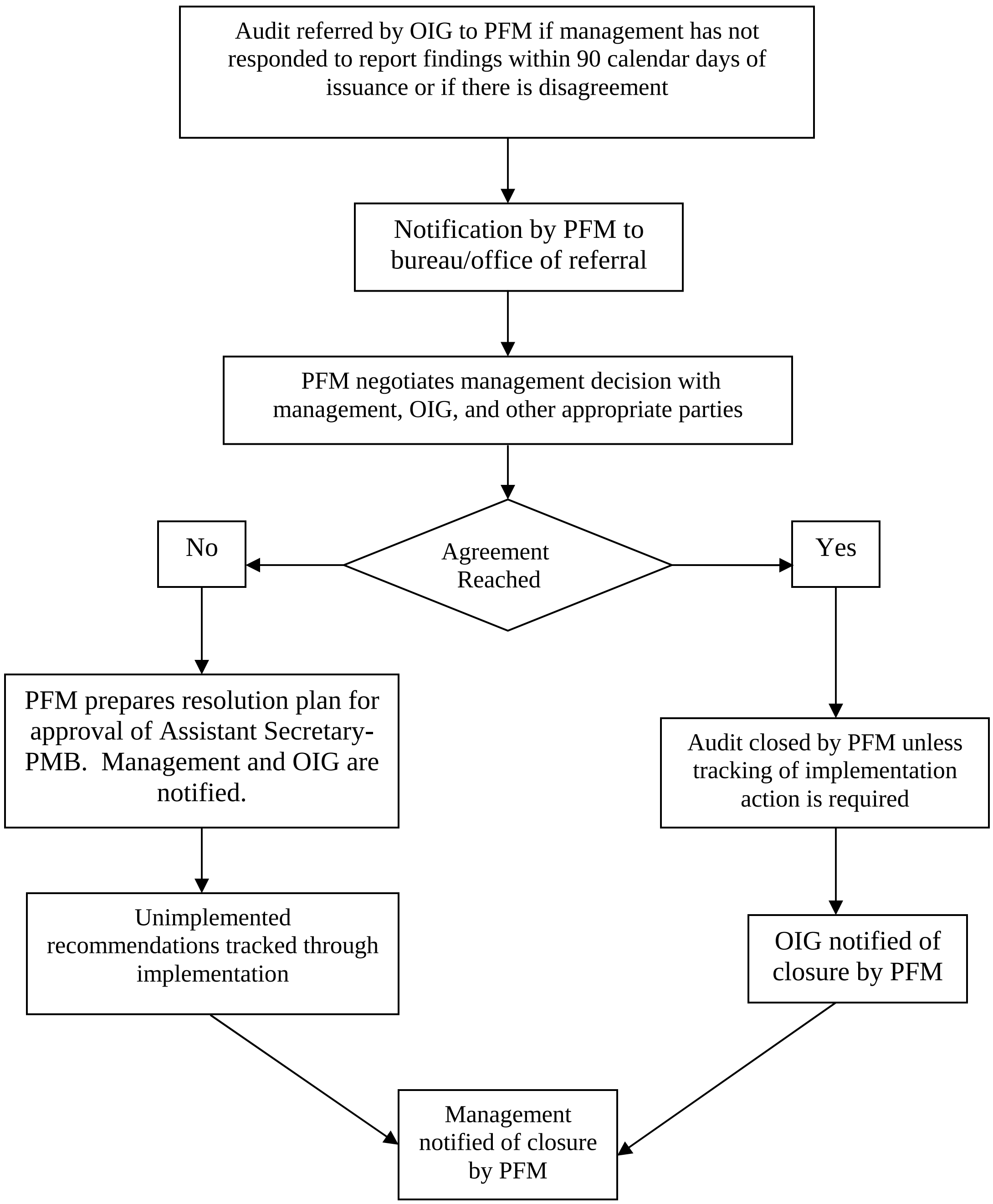
Insular Area Audits

The Department has administrative responsibility for coordinating federal policy in the territories of American Samoa, Guam, the U.S. Virgin Islands and the Commonwealth of the Northern Mariana Islands, and oversight of federal program funds in the freely associated states of the Federated States of Micronesia, the Republic of the Marshall Islands, and the Republic of Palau. The OIG has responsibility for conducting audits of insular area governments. The scope of the audits of insular areas conducted by the OIG include federal funds received by insular area governments and of local funds and issues. The OIG refers and PFM tracks, however, only those audits of insular area governments that involve federal funds and programs.

INTERNAL AUDIT PROCESS – OFFICE OF INSPECTOR GENERAL AUDIT REPORTS



RESOLUTION OF INTERNAL AUDITS ISSUED BY THE OFFICE OF INSPECTOR GENERAL



PROCESS FOR TRACKING INTERNAL AUDIT REPORTS REFERRED BY THE OFFICE OF INSPECTOR GENERAL

Audit referred by OIG to PFM for tracking/resolution of unimplemented recommendations

↓

PFM enters recommendations into Departmental Audit Follow-up Tracking System and notifies bureau/office ALO of referral.

↓

PFM tracks recommendations until notification of final action – requests quarterly updates *

↓

PFM is notified by management that final action has been taken (supporting documentation provided by management)

↓

PFM determines that supporting documentation supports final action for recommendation (audit report will be closed when all referred recommendations have been implemented and officially closed by PFM)

↓

PFM notifies management and OIG that recommendation or audit report, as appropriate, has been officially closed (no further action is required) and updates the tracking system

* Financial statement audits status is reported on a monthly basis

SECTION 5
C H A P T E R 3
EXTERNAL AUDIT REPORT

An external audit is defined as a single audit, a grant audit, a pre-award audit of contractor proposed future costs, a concessions audit, or a contractor claim audit. External audits may be conducted by the OIG, a state or local auditor, or the Defense Contract Agency. Grant audits are the most frequent type audit reports referred to the Audit Follow-up Official for action by the OIG.

Single Audits

The Single Audit Act of 1984 (Public Law 98-502), authorizes the conduct of single audits of state and local governments that are recipients of federal funds. OMB Circular A-133, "Audits of States, Local Governments, and Non-Profit Organizations," provides policies and procedures for federal agencies to use when conducting or supervising single audits. Audits performed under the Single Audit Act are intended to satisfy all federal agencies providing assistance to the entity. Non-federal organizations that expend $500,000 ($300,000 or more in fiscal years ending prior to December 31, 2003) or more in federal awards are subject to the requirements of the Single Audit Act and OMB Circular A-133. Single audits are conducted by auditors that are usually local certified public accounts. Non-federal auditors retained by state and local governments follow federal guidelines in performing single audits.

Grants Administration

Bureau/office programs are responsible for administrating grant agreements or cooperative agreements awarded which reflect the cooperative effort and the respective interests, investments, and rights of the parties of the agreement. Bureau/office programs are responsible for accessing the Federal Audit Clearinghouse website (http://harvester.census.gov/sac) to determine when audit reports have been submitted. If audit reports have not been submitted, bureau/office programs shall request follow-up action by the Clearinghouse. At their discretion, and in accordance with guidance at 43 CFR 12, programs may consider the imposition of sanctions, e.g. award no new grants in cases of continued inability or unwillingness of applicable financial assistance awardees to have to have audits conducted in accordance with the requirements of the Single Audit Act of 1984 and OMB Circular A-123.

A-133 assigns the Federal Awarding Agency with the responsibility of ensuring that single audit reports are received in a timely manner. While BIA has a sanction policy, the Common Rule is applicable to 638 contracts only to the extent negotiated in the contract.

Tracking Single Audits

Secretarial Order 3254, dated June 24, 2005, transferred the report processing function from the OIG to PFM. PFM issues single audit reports and tracks the status of recommendations and questioned costs in its management tracking system to final action.

During the audit, an auditor will question a cost:

- 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.

PFM tracks disallowed costs of $1,000 or more. Although the Department does not track disallowed costs less than $1,000, bureaus and offices continue to have the to monitor, track, and collect all debts owed the Department authority and are encouraged to do so.

Management is responsible for reviewing auditee responses and all costs questioned by auditors and determining if the costs are sustained (management agrees with the auditors questioning of the costs and costs must be repaid by the auditee) or if the costs may be reinstated (management determines that the costs is allowed and 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, PFM is responsible for determining that appropriate documentation to support the accomplishment for final action has been furnished and that an audit may be closed.

Final action on disallowed costs may include:

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

- Offset – which means the collection of audit-related debt by means of offsets against other monies due 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 of disallowed costs to the Department of the Treasury for collection action.

Closure of External Audit Reports in Tracking

PFM is responsible for making the determination that sufficient actions have been taken and documented to close an external report in tracking. Management's notification to PFM must be specific and detailed, to evidence what action was required and what action has been taken. Specific documentation must accompany management's notification of final action. Documentation may include, but is not limited to the following:

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 the Department of the 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 the Department (Section 106(f)). Awarding officials should be aware of this provision so that tribes are promptly notified of a decision to disallow questioned costs.

Referral of Audit Reports to the Department of the Treasury

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

Contract/Grant Audits

The OIG is responsible for conducting audits of awards of funds expended under the authority of OMB Circular A-110, “Uniform Administrative Requirements of Grants and Agreement With Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations,” as it applies to grants and contracts awarded by the Department to recipients and, through recipients, to sub-recipients. A contract audit is an audit of a government contract for goods and services with profit as well as non-profit organizations**.**

Contract/Grant Audits Referred for Resolution

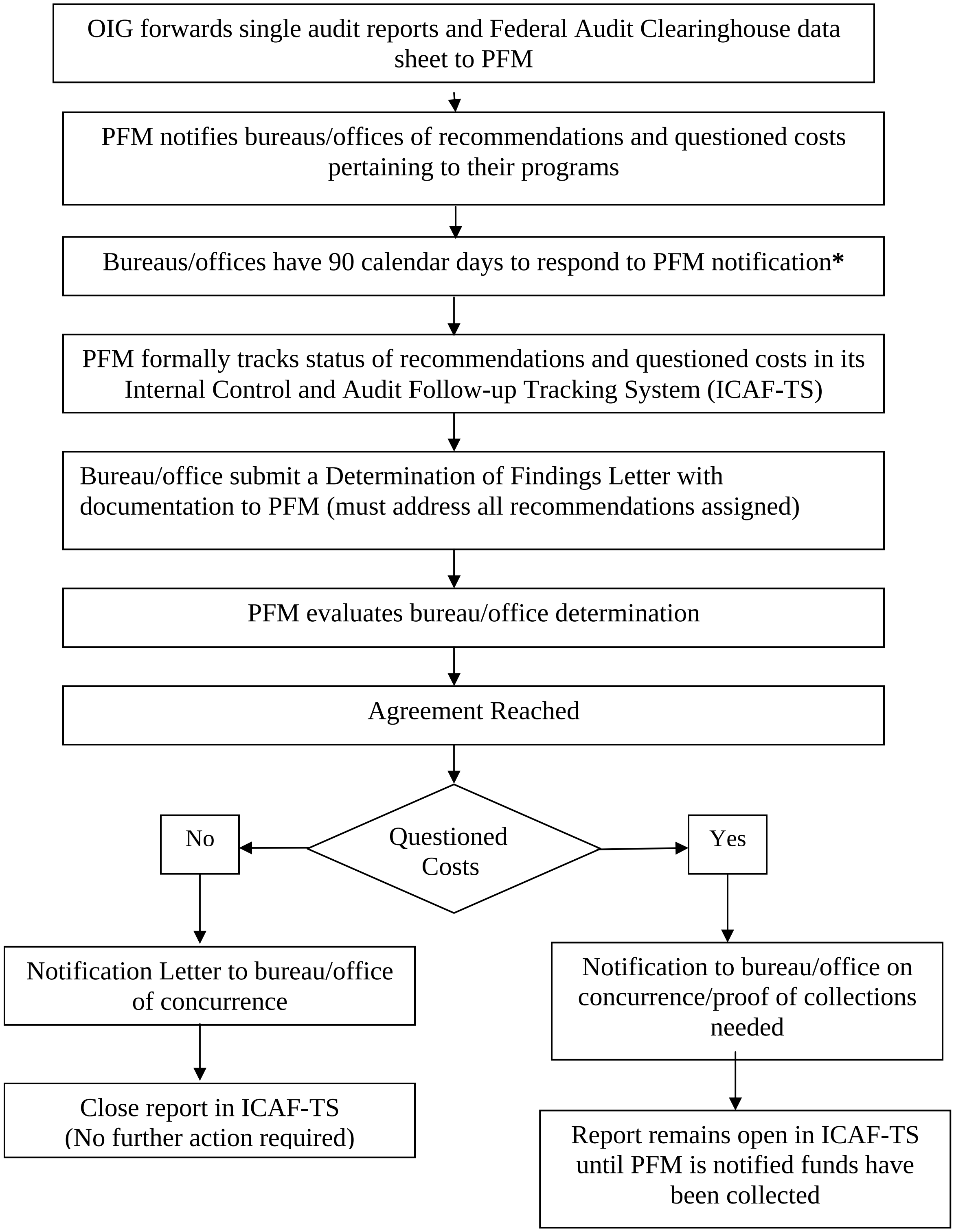
When management has not responded to a contract or grant audit within 120 calendar days of issuance of the report, the report is referred to PFM for resolution. When PFM has received a referral for resolution, PFM will contact management and request their response to the audit report. Once the response has been received, PFM will review the response for adequacy (i.e., the response adequately address all findings). If the response is incomplete, PFM will request additional information. If the response adequately addresses all findings and if all required corrective actions have been taken, the report is closed by PFM and management, the Audit Liaison Official, and the OIG are notified. If the response adequately address all findings but one or more recommendations have not been implemented, for instance if there are disallowed costs that have not been collected, PFM enters the report into the Department tracking system and tracks the audit until final action has been achieved and the report is closed by PFM.

Audits on Official Appeal

As previously stated, once an external audit report has been issued, management officials are responsible for reviewing the auditee response to determine the adequacy of the response. In cases where management has made a finding of disallowance of questioned costs, and has requested that the costs be repaid, an auditee has the right to appeal the finding of disallowance. An official appeal must be filed with the Interior Board of Contract Appeals or, in some instances, with a local or state court; Indian Tribes may also appeal to federal courts under the regulations in Public Law 93-638. PFM must be notified by management when an auditee has appealed any aspect of management’s findings; PFM continues to track audits on appeal until it has been notified by management of an official determination on the merits of the appeal. The notification to PFM should include what body is viewing the appeal, a docket number in the case of appeals filed with the Interior Board of Contract Appeals, or a case number for an appeal filed with another body. When the appeal has been resolved, PFM is to be notified of the disposition of the finding and whether further tracking is required.

In cases where a contractor has submitted a claim for reimbursement for services render, or if the contractor requests additional funds, an awarding official may request that the OIG perform an audit of the contractor’s claim. If OIG questions a submitted claim and management agrees with the OIG’s finding, a contractor may file an appeal of the finding of disallowance. In these situations, PFM will track the audit through disposition of the appeal. If all issues have been resolved at this point, PFM will close the audit; if there are incomplete issues, they will be tracked by PFM though final action. The report will remain open until PFM has been notified by management that all issues on appeal have been addresses and will continue to be reported by PFM to the OIG as open even though management cannot take action to close the report until the appeal is decided.

PROCESS FOR ISSUING SINGLE AUDIT REPORTS



*** If no response within 90 calendar days PFM contacts bureaus/offices Audit Liaison Officer.**

PROCESS FOR TRACKING CONTRACT/GRANT AUDIT REPORTS
REFERRED BY THE OFFICE OF INSPECTOR GENERAL

Audit referred by OIG to PFM for tracking of implementation of unimplemented recommendations

↓

PFM enters recommendation into ICAF and notifies bureau/0ffice of referral

↓

PFM tracks recommendations until notification of final action – request quarterly updates

↓

PFM is notified by management that final action has been taken (supporting documented provided by management)

↓

PFM determines that supporting documentation supports final action for recommendation (audit report will be closed when all referred recommendations have been implemented and officially closed by PFM)

↓

PFM notifies management that recommendation or audit report, as appropriate, has been officially closed
(No further action is required)

SECTION 5
CHAPTER 4
FINANCIAL STATEMENT AUDITS

The CFO Act of 1990 (Public Law 101-576), directs that each federal agency shall prepare and submit to the OMB, a financial statement for the preceding fiscal year, covering:

- Each revolving fund and trust fund of the agency; and,
- To the extent practicable, the accounts of each office, bureau, and activity of the agency which performed substantial commercial functions during the preceding fiscal year.

The CFO Act further specifies that each financial statement of an executive agency shall reflect:

(1) The overall financial position of the revolving funds, trust funds, offices, bureaus, and activities covered by the statement, including assets and liabilities thereof;
(2) Results of operations of those revolving funds, trust funds, offices, bureaus, and activities;
(3) Cash flows or changes in financial position of those revolving funds, trust funds, offices, bureaus, and activities; and
(4) A reconciliation to budget reports of the executive agency for those revolving funds, trust funds, offices, bureaus, and activities.

Preparation of Financial Statements

Financial statements for the Department and the bureaus will be prepared and audited on an annual basis. Final financial statements, including the auditor's opinion on the financial statements, will be issued within 45 days of year end (November 15). If the financial statements for the Department cannot be completed by the statutory due date, the Department will provide OMB with a written explanation of the reason for the delay and the expected date of completion.

The financial statements will be prepared in compliance with OMB's "Form and Content of Agency Financial Statements" (OMB Bulletin No. 01-09 or its successor documents).

Audit Opinion on Financial Statements

The audit opinions will be issued in compliance with OMB Circular A-136, Financial Reporting Requirements." The audit opinion will include the following:

(1) An opinion as to whether the reporting entity's Principal Statements and Required Supplementary Information is fairly presented in all material respects, in conformity with Federal Accounting Standards;
(2) A report on internal controls; and
(3) A report on the reporting entities compliance with applicable laws, regulations, and governmentwide policy requirements.

Reporting Entity Responses to Audit Opinion Findings

As required by OMB's audit guidance, the reporting entity shall provide comments on the auditor's findings and recommendations included in the audit report, including corrective actions taken or planned and comments on the status of corrective actions taken or planned and comments on the status of corrective action taken on prior findings. To the extent practical, these comments shall be included in the audit report on internal controls or report on compliance. Departmental response to audit findings shall be provided to the Office of Inspector General within 14 calendar days of the issuance of the draft report to allow for the timely publication of the audited financial statements, but no later than December (specific dates provided in Annual Guidance document).

Correction of Material Weaknesses and Reportable Conditions

Material weaknesses, reportable conditions reported in the auditors opinion, internal control deficiencies, and/or noncompliance issues audit recommendations will be tracked in the Department Audit Follow-Up Tracking system in a similar manner as other OIG and GAO audit recommendations. Corrective action plans with appropriate interim milestones and target dates will be developed by Bureau Chief Financial Officers, ALOs and other cognizant offices, and updated on a regular basis. The audited entity should seek to complete corrective action plans before the next annual financial statement audit. The Department will monitor implementation progress to ensure completion of corrective actions by original target dates.

Specific requirements for corrective action plans are detailed in "Corrective Action Plan Contents."

Non-Compliance with Federal Financial Management Improvement Act (FFMIA)

The Department will comply with policies and guidance on reporting of FFMIA non-compliance. Required corrective action plans related to FFMIA non-compliance will be provided to OMB, as required. The Department will use the Audit Follow-Up Tracking System and implementation progress information to monitor corrective action plans to bring the Department or individual bureaus into compliance with the FFMIA.

Corrective Action Plans Contents

To ensure results, corrective action plans must adhere to the following framework:

1. Summary Description of the Deficiency – Provides a summary description of the deficiency.
2. Year First Identified – Lists the first year that the deficiency was identified.
3. Target Correction Date – Unless adequately justified, all material weaknesses and noncompliance issues must be corrected within one year. To ensure that deficiencies are corrected prior to the beginning of the next year's audit process, final correction of the deficiency should end June 30 to allow sufficient time for testing to ensure that the material weakness/noncompliance issue has been

corrected. Extensions beyond the June 30 deadline may be granted by PFM, but IT security weaknesses must be completed by June 30.

4. Accountable Official – Senior manager(s) in charge of the program where the weakness or noncompliance issue was identified (including field office and/or headquarters, if applicable);
5. Summary of Corrective Actions – Lists specific actions/milestones and targeted dates by fiscal quarter in ascending order, and total resources associated with and committed to each milestone. As each specific milestone is completed, list the correction date, and where appropriate, the location of the supporting documentation for review upon request by PFM, OIG, or the independent auditor.
6. Funding – Must be set aside (tied to the budget), and must be sufficient to completely correct the weakness or noncompliance issue. For deficiencies requiring multi-year corrective action plans, costs for each year must be identified in the plan and in the bureau/office budget. Funding may not be moved to other priorities.
7. Quarterly Corrective Action Milestones – A comprehensive listing of specified actions/milestones and targeted completion dates by fiscal quarter in ascending order, and the total resources associated with and committed to each action/milestone. As each specific milestone is completed, list the correction date, and where appropriate, the location of the supporting documentation for review upon request by PFM, the OIG, or the independent auditors.
8. Metrics – Should be developed to measure the progress in completing the corrective action. Metrics should also be developed that demonstrate that the actions taken actually remedied the weakness/noncompliance.

The required format for submission of the Corrective Action Plan is Addendum A.

NOTE: Corrective Action Plans for IT security issues must agree with what is submitted for the POA&Ms (discussed in section 3). The same actions, funding, dates, etc., must be evident in both the Corrective Action Plan and the POA&M!

Reporting on Material Weaknesses and Noncompliance Issues

The PFM currently requires monthly status reports on the correction of all material weakness and noncompliance issues identified in the financial statement audit. If a bureau/office reports consistently on time and is achieving a green status, PFM may approve quarterly reporting.

The first report on the status of the material/noncompliance issue is due to PFM 30 calendar days after the issuance of the final audit report. Beginning in January 30 (or the last work day of the month) and each end of 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, have been delayed. If delays have occurred in the completion of monthly milestones, a brief explanation for the delay, whether the delay impacts the bureau/office ability to meet the final deadline, how the bureau/office expects to get back on track, and the revised correction date should be noted.

PFM will summarize the CAP information in a scorecard format and provide an advance copy for comment to each bureau CFO. Bureaus have one day to offer any comments. The scorecard will then be forwarded to the Assistant Secretary – PMB.

Status Reports on OIG and GAO Audit Recommendation Implementation Not Contained in the Financial Statement Audits

In order to ensure the timely completion of corrective actions for all recommendations contained in audits prepared by the OIG and GAO, a report should be provided to PFM on a monthly basis. This monthly report will include the status of ALL open audit recommendations for ALL audits currently in tracking and/or resolution. If delays have occurred in implementing audit recommendations, a concise statement of the reasons for the delay along with a revised target date must be provided.

If a bureau/office reports consistently on time and is achieving a green status, PFM may approve quarterly reporting

NOTE: The progress reports for FMFIA material weaknesses, audited financial statement material weaknesses, noncompliance issues, as well as other recommendations contained in the audited financial statement audits are to be submitted to PFM monthly.

Based on the progress information provided by the bureaus, PFM will prepare a summary scorecard for the Assistant Secretary - PMB, with an information copy to each bureau ICC and Audit Liaison Officer. The information in these reports will be used to determine bureau status in accomplishing the GPRA goal for audit recommendation implementation.

Validation of the Completion of Material Weakness Corrective Action Plans

As in previous years, bureaus must verify the completion of material weakness corrective action plans. Documentation for the correction of noncompliance issues and FMFIA weaknesses should also be verified, maintained, and made available upon request. Bureaus will be expected to maintain appropriate supporting documentation for each corrective action plan in a central location for subsequent review and validation by the Department and/or OIG staff. Retention of records is dependent on individual records retention schedules.

Mid-year and Year End Progress Meeting

Bureaus/offices are required to participate in a mid-year and year-end progress meeting with PFM, PMB, and 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 follow-up 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.

CHAPTER 5
ADDENDUM A
Corrective Action Plan for Material Weaknesses and Noncompliance Issues Audited Identified in Financial Statements
As of (date) ______________________________

Bureau:

Title of Material Weakness or Noncompliance Issue:

Check One: Material Weakness ___ Noncompliance Issue ___ FMFIA ___

Carryover Issue or New this Fiscal Year:

Brief Description of Material Weakness or Noncompliance Issue:

Planned Correction Date Reported in PAR:

Current Planned Correction Date (NTE June 30): (explain reasons for any date change)

Program/Organizational Component Where Weakness or Issue Resides:

Accountable Officials: (Name, Title, Telephone Number & E-mail Address)

- **Headquarters: ___________________________________**
- **Field-level: ___________________________________**

Funding Amount Committed for Corrective Actions: $________________

Appropriation Account: _______________________

Summary of Corrective Action Plan:

Quarterly Corrective Action Milestones: (list specific actions/milestones and targeted correction dates (*) by fiscal quarter in ascending order, and total resources associated with and committed to each action/milestone. As each specific milestone is completed, list the correction date, and where appropriate, the location of the supporting documentation for review upon request by PFM, OIG or the independent auditors).

Metrics: List the metric(s) that will be used to demonstrate progress (not to include achievement of corrective action milestones) and those that will be used to demonstrate that the corrective actions taken remedied the deficiency.

CHAPTER 5
ADDENDUM B
Key Audit Follow-up Terms

***Disallowed Cost* -** An incurred cost questioned by the audit organization that management has agreed should be repaid by the grantee.

***External Audit* -** A single or grant audit, or a contractor claim audit.

***Final Action* -** The completion or implementation of all actions to be taken regarding audit recommendations.

***Final GAO Report* -** GAO's final report to the Congress on its findings and recommendations.

***Financial Statement Audit* -** An audit conducted by the OIG or an independent auditor of the financial statements of a bureau/office.

***GAO Audit* -** An audit or review of Departmental programs that is conducted by the GAO at the request of the Congress, mandated by legislation, or for other purposes determined by the GAO to be in the best interest of the federal government.

***GAO Draft Report* -** A GAO report providing the analysis, findings, and conclusions of an audit.

***GAO Entrance/Exit Conference* -** Meetings held at the initiation and completion of GAO's audit work.

***Management Decision* -** The evaluation by management of the findings and recommendations made by the auditor and the issuance of an appropriate corrective action plan.

***Notification Letter* -** A GAO letter that provides a brief description of planned audit work.

***Oral Briefing* -** A briefing by GAO auditors to the Congressional requester which concludes the audit.

***Program Audit* -** An audit of programs operated by or funded by the Department.

***Referral* -** The process by which the OIG sends audit reports to the audit follow-up official for resolution and/or tracking of final implementation action.

***Resolution* -** The point at which agreement is reached regarding actions to be taken to implement audit recommendations.

***Single Audit* -** An audit of a grantee which is comprised of an audit of the entity's major federal and state award programs, conducted by state or local auditors.

***Questioned Cost* -** A cost that is questioned by auditors because the cost is not supported by adequate documentation.

SECTION 6
CHAPTER 1
AUDIT REPORTS ISSUED BY
THE GOVERNMENT ACCOUNTABILITY OFFICE
(GAO)

This chapter discusses the Department's responsibilities associated with audit follow-up in connection with audits issued GAO. The chapter provides information on the types of audits issued by GAO, the Department's role, the function of the Departmental Audit Follow-Up Official, the responsibility of the Office of Financial Management (PFM), responsibility of the program assistant secretary, the function of the audit liaison officer (ALO) at the program assistant secretary level, the responsibility of the audit liaison officer at the bureau level, and the responsibility of program staff.

Types of GAO Audits

GAO conducts two types of audits:

- Financial Audits - Financial audits include an examination of financial statements and financial related information and an audit opinion on whether the financial statements are fairly stated.

- Performance Audits - Performance audits are objective and systematic reviews which provide an independent assessment of the performance of a government function.

Although the objectives and scope of GAO's financial and performance audits differ, the term "audit" is used synonymously throughout this chapter for financial and performance audits.

In addition to performing audits, GAO also uses its auditors to develop questions for use at Congressional hearings, to perform other investigative work, and to develop methods or approaches which are applied in evaluating new and proposed programs. Additionally, GAO conducts a wide range of governmentwide surveys.

SECTION 6
CHAPTER 2
ROLES AND RESPONSIBILITIES

Department of the Interior's Responsibility - The Department is responsible for fully cooperating with GAO as it conducts its audits and ensuring that information, advice, and guidance from the audits are used for the maximum benefit of the Department.

Assistant Secretary - Policy, Management and Budget and Designated Agency Audit Follow-up Official - The Assistant Secretary serves as the Audit Follow-Up Official for the Department. The Assistant Secretary is responsible for the overall audit follow-up function, which includes audits issued by the GAO. The Assistant Secretary is responsible for ensuring all GAO draft and final audit reports are acknowledged within the Department and that any recommendations agreed to by the Department are tracked through full implementation of the corrective action(s).

Office of Financial Management (PFM) - The Department's Office of Financial Management has been delegated the responsibility for program management of the audit follow-up function. PFM is specifically responsible for:

- Receiving all correspondence from GAO initiating work within the Department;

- Transmitting GAO's correspondence initiating new work electronically within one day, when possible, to the affected program assistant secretary, the assistant secretary level ALO, the bureau ALO, the Department Budget Office, and to Departmental offices with program oversight;

- Ensuring that an entrance conference is scheduled with GAO when the work will involve more than one bureau (If GAO's work involves one program area, PFM is responsible for ensuring that the ALO for the affected bureau has scheduled an entrance conference and communicated the date and time to Departmental offices 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 with appropriate program officials;

- Receiving the draft GAO report for the Department; designating an organization to respond, transmitting the report, and establishing reasonable deadlines for the Department's response;

- Receiving the final GAO report for the agency; 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 the Department is responsive to all recommendations contained in the report (PFM is also responsible for ensuring that all Departmental offices with program oversight have reviewed and surnamed the proposed Departmental response);

- Tracking agreed to corrective actions through full implementation and providing GAO with the information necessary to complete its closure of the recommendation; and

- Notifying the program and bureau ALO's of Departmental closure and GAO concurrence.

Program Assistant Secretary - The program assistant secretary is responsible for insuring 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 audit liaison officer at the assistant secretary level. It is preferable that the program assistant secretary level ALO is 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 follow-up 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 the Department.

Bureau Director - The bureau director is responsible for insuring that the program assistant secretary is provided with a document for signature in a timely manner to ensure that GAO and Congress are provided with a response within the timeframe allotted. The bureau director is also responsible for designating an official to function as the audit liaison officer at the bureau level.

Bureau Audit Liaison Officer - The ALO is responsible for program management of the audit follow-up function at the bureau/office level. The bureau ALO is responsible for:

- Coordinating audit activity at the bureau and program office level;
- Scheduling entrance/exit conferences with GAO;
- Receiving both draft and final reports for the bureau;
- Coordinating internal bureau surnames;
- Providing proposed response to the assistant secretary ALO; an
- Maintaining a current status of corrective actions on open recommendations; providing a status update to PFM semiannually; and, providing closure memoranda to PFM.

- Tracking agreed to corrective actions through full implementation and providing GAO with the information necessary to complete its closure of the recommendation; and

- Notifying the program and bureau ALO's of Departmental closure and GAO concurrence.

Program Assistant Secretary - The program assistant secretary is responsible for insuring 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 audit liaison officer at the assistant secretary level. It is preferable that the program assistant secretary level ALO is 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 follow-up 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 the Department.

Bureau Director - The bureau director is responsible for insuring that the program assistant secretary is provided with a document for signature in a timely manner to ensure that GAO and Congress are provided with a response within the timeframe allotted. The bureau director is also responsible for designating an official to function as the audit liaison officer at the bureau level.

Bureau Audit Liaison Officer - The ALO is responsible for program management of the audit follow-up function at the bureau/office level. The bureau ALO is responsible for:

- Coordinating audit activity at the bureau and program office level;
- Scheduling entrance/exit conferences with GAO;
- Receiving both draft and final reports for the bureau;
- Coordinating internal bureau surnames;
- Providing proposed response to the assistant secretary ALO; an
- Maintaining a current status of corrective actions on open recommendations; providing a status update to PFM semiannually; and, providing closure memoranda to PFM.

SECTION 6
CHAPTER 3
GAO AUDIT PROCESS

Notification Letters

The Department is notified by letter addressed to the Director of PFM of the initiation of GAO audits. The PFM GAO desk officer notifies the program assistant secretary, the assistant secretary ALO, the bureau/office ALO, the Department Budget Office, 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 requesters name, additional information if the audit is mandated by legislation, and the name of the team within GAO assigned to perform the audit. GAO's notification letter usually also 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 Conferences

Entrance conferences are held to formally acquaint Departmental staff with the GAO team assigned to conduct the audit. At the entrance conference, the GAO team summarizes what the Congressional requestor has asked GAO to provide, furnishes an outline of the proposed work, timeframes involved, scheduled site visitations, any questions or requests for documentation GAO requires, and responds to any questions by Departmental staff regarding the conduct of the audit. Entrance conferences ensure that Departmental staff fully understand the scope of the proposed audit.

Entrance conferences are scheduled by the bureau/office ALO, unless they involve more than one program area. If reviews involve more than one program area, the PFM GAO desk officer will schedule the entrance conference and notify the affected bureau ALO's and Departmental offices.

Actual GAO Audit

The actual GAO audit period is usually twelve to sixteen months. GAO initiates its work with the notification letter, followed by an entrance conference, the survey phase (which is the work development stage), and the actual audit. GAO concludes their assignment with an exit conference with program staff prior to issuance of the draft report.

Exit Conferences

An exit conference is held between GAO and program staff at the conclusion of its work. <u>It is important for senior management to ensure that appropriate officials attend the exit conference</u> or are provided with a summary of the exit conference. The exit conference is where the GAO Team provides the Department with a Statement of Facts which summarizes its findings and possible report recommendations, if any. Departmental officials have the opportunity at the exit conference to offer clarifying information or provide GAO with updated information.

Departmental staff also have the opportunity after the exit conference to begin preparing for the issuance of the draft report. ALOs ensure 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. This is important because it eliminates last minute coordination between the assistant secretary's office and program staff and ensures that the Department will be able to respond to GAO within prescribed timeframes.

Issuance of Draft Report

When the GAO draft report is issued to the agency, it is formally transmitted to the Department for review and comment. PFM receives all draft reports for the Department and transmits draft reports to the assistant secretary-level ALO, the bureau/office ALO, the Department's Budget Office, and Departmental offices with program oversight, along with guidance for preparing the Department's response. Draft reports usually have a response turnaround period of 7 to 30 calendar days. The Department's policy is to provide **written comments on all GAO products with recommendations** unless otherwise requested by GAO. When GAO has requested that comments be provided orally, the comments must be developed in writing and shared with Departmental offices with program oversight in the same manner as the coordination of written responses. It is the responsibility of the PFM GAO desk officer to ensure that GAO captures the oral comments as presented.

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 draft report's recommendations have been addressed in the proposed response. If a draft report involves more than one bureau/office within the Department, the PFM GAO desk officer will either assign responsibility for coordinating each bureau's comments into one consolidated Departmental response to a specific bureau/office ALO, or the PFM GAO desk officer will request comments from each involved bureau/office. At this point, the PFM GAO desk officer will consolidate the comments into one Departmental response, which will be signed by the Department's Designated Agency Audit Follow-Up Official.

Issuance of Final Report

GAO's final report is issued to the Secretary of the Interior and received in PFM on behalf of the Secretary. PFM provides copies of the final report to the program assistant secretary ALO, the involved bureau/office ALO, the Departmental Budget Office, and all other Departmental offices with program oversight. If GAO's final report contains recommendations to the Secretary of the Interior, the Department 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 on GAO's recommendations. The PFM GAO desk officer assigns responsibility for the response to the appropriate program assistant secretary. If the GAO Final Report involves more than one program assistant secretary area of responsibility, the Department's response should be prepared for the Designated Agency Followup official's signature.

Processing of Government Accountability Office (GAO) Audit Reports

Mandated by Legislation

GAO Initiative

Congressional Request

- **Notification by GAO to DOI of Audit Beginning**
- **Entrance Conference**
- **Actual Review**
- **Exit Conference**
- **Issuance of Draft Report (Comment Period of 7 to 30 days)**
- **Issuance of Final Report (Comment/Response Period of 60 days)**
- **Track "Agreed To" Recommendations through Implementation**
- **Closure with GAO Concurrence**

Processing GAO Draft Audit Reports

PFM receives report for Secretary and transmits to Audit Liaison Office (ALO) for response

Bureau ALO transmits to program staff

Proposed response transmitted to A/S-ALO* for review and senior management concurrence

A/S-ALO transmits proposed response to PFM

PFM reviews for content, that all recommendations have been addressed, and coordinates Departmental surnames

Response returned to A/S-AOL for signature of program Assistant Secretary

PFM waits for final report

*** A/S-ALO: Assistant Secretary level audit liaison officer**

Processing GAO Final Audit Reports

PFM receives report for Secretary and transmits to ALO for response

Bureau ALO transmits to program staff

Proposed response transmitted to A/S-ALO for review & senior management concurrence (A/S surname required)

A/S-ALO transmits proposed response to PFM

PFM reviews for content, that all recommendations have been addressed, and coordinates Departmental surnames

Response returned to A/S-ALO for signature of program Assistant Secretary

PFM tracks corrective action through full implementation

PFM seeks GAO concurrence that full implementation has been achieved

PFM notifies A/S-ALO and bureau ALO of closure and removes from tracking