Implementation Guide for

OMB Circular A-123,

Management's Responsibility for Internal Control

Appendix A, Internal Control over Financial Reporting

Chief Financial Officer's Council

July 2005

UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer
Assistant Secretary for Administration
Washington, D.C. 20230

MEMORANDUM FOR CFO Council Members

FROM: James L. Taylor
Deputy Chief Financial Officer and
Chair, Financial Management Policies and Practices
Committee - CFO Council

SUBJECT: Final A-123 Implementation Guide

Attached is an Implementation Guide to assist departments and agencies covered by the revised OMB Circular A-123. It specifically addresses the additional requirements included under Appendix A, Internal Control Over Financial Reporting, which directs management to become more proactive in overseeing internal controls related to financial reporting.

This Guide is the result of extensive collaboration among CFO Act agencies, the President's Council on Integrity and Efficiency (PCIE) and OMB; as well as comments and suggestions from the audit and vendor communities. It has been developed as a CFO Council document, which will be posted to our website, http://www.cfoc.gov (at the Financial Management Policies and Practices page), and revisited once the initial reporting for A-123 is complete in FY 06.

To help affected agencies implement A-123, the Policy and Practices Committee will be hosting informal discussion sessions to address issues that arise and share best practices. Council members will be notified of the dates and locations for these sessions. In addition, we will continue to accept any comments or suggestions for the Guide at A-123comments@doc.gov.

cc: Clay Johnson
Linda Combs

Implementation Guide for
OMB Circular A-123, Management's Responsibility for Internal Control
Appendix A, Internal Control over Financial Reporting

Implementation Guide for
OMB Circular A-123, Management's Responsibility for Internal Control
Appendix A, Internal Control over Financial Reporting

INTRODUCTION

- ***Purpose of this Implementation Guide***
- ***Background***
- ***Internal Control Standards***
- ***Strengthened Requirements***
- ***The Assessment Process***

Purpose of this Implementation Guide

This Implementation Guide provides federal agencies with further guidance to implement and comply with OMB Circular A-123, Management's Responsibility for Internal Control, Appendix A, Internal Control over Financial Reporting (A-123, Appendix A). This document is intended to assist federal managers with implementing a process for assessing the effectiveness of the entity's internal control over financial reporting.

It should be understood that this guide is not an authoritative part of A-123. This guide was written to assist federal entities with documenting, testing, and assessing internal control effectiveness. Therefore, the guide can and should be modified to fit the circumstances, conditions, and structure of each entity.

A-123, as well as this Implementation Guide, is *intended for management,* it is not audit guidance. A-123 prescribes management's responsibilities for internal control and this Implementation Guide provides additional guidance for management to conduct the assessment of internal control over financial reporting. Agencies that are required or elect to receive an audit opinion on the internal control over financial reporting should consult with their auditors during the planning phase to ensure the agency's approach and implementation are appropriately aligned with the audit.

Background

The objective of the Federal Managers' Financial Integrity Act of 1982 (FMFIA) is to provide reasonable assurance 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." The revisions to A-123 serve to emphasize management's focus on ensuring effective internal control over financial reporting is established and maintained throughout the federal government.

The passage of the Sarbanes-Oxley Act of 2002 (SOX) 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. SOX requires that management of publicly traded companies strengthen their processes for assessing and reporting on the internal control over financial reporting. While SOX created a new requirement for managers of publicly traded companies to report on the internal control over financial reporting, federal managers have been subject to similar internal control reporting requirements for many years.

A joint committee of representatives from the Chief Financial Officer's Council and the President's Council on Integrity and Efficiency was formed and tasked with reviewing the requirements for publicly traded companies as stipulated in SOX and determining how these requirements might apply to federal agencies, and recommending any necessary changes to the existing guidance on internal controls.

The joint committee recommended that an appendix be added to A-123 to strengthen the process management uses to assess internal control over financial reporting. OMB accepted the committee's recommendation and revised A-123 in December 2004. The revised circular can be found on OMB's web page at www.whitehouse.gov/omb. The revised A-123 becomes effective beginning with fiscal year 2006. A-123, Appendix A addresses internal control over financial reporting and is required for the 24 Chief Financial Officer (CFO) Act agencies.

Internal Control Standards

Internal control, in the broadest sense, includes the plan of organization, and the 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.

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

Management is responsible for developing and maintaining internal control activities that encompass the following categories to meet the above objectives:

- Control Environment,
- Risk Assessment,
- Control Activities,
- Information and Communications, and
- Monitoring[1]

See Section II of A-123 for a detailed discussion of the above internal control standards.

Strengthened Requirements

A-123, Appendix A emphasizes management's responsibility for establishing and maintaining effective internal control over financial reporting. In general, A-123, Appendix A strengthens requirements in three main areas:

- Documentation
- Monitoring
- Reporting

A-123, Appendix A also requires that documentation be maintained not only of the controls in place but also of the assessment process and methodology management used to support its assertion as to the effectiveness of the internal control over financial reporting. In addition, A-123 requires that management perform monitoring activities that include direct testing of the controls as part of the assessment process.

A-123 also requires a separate assurance statement from management on the effectiveness of internal control over financial reporting. This assurance statement should be incorporated into management's overall assurance statement provided under the requirements of the FMFIA. (Refer to Exhibit 6, on pages 63-65, for illustrative templates of the assurance statements.)

A summary chart that details the significant changes to A-123 precedes the Circular.

[1] OMB Circular A-123, Management's Responsibility for Internal Control

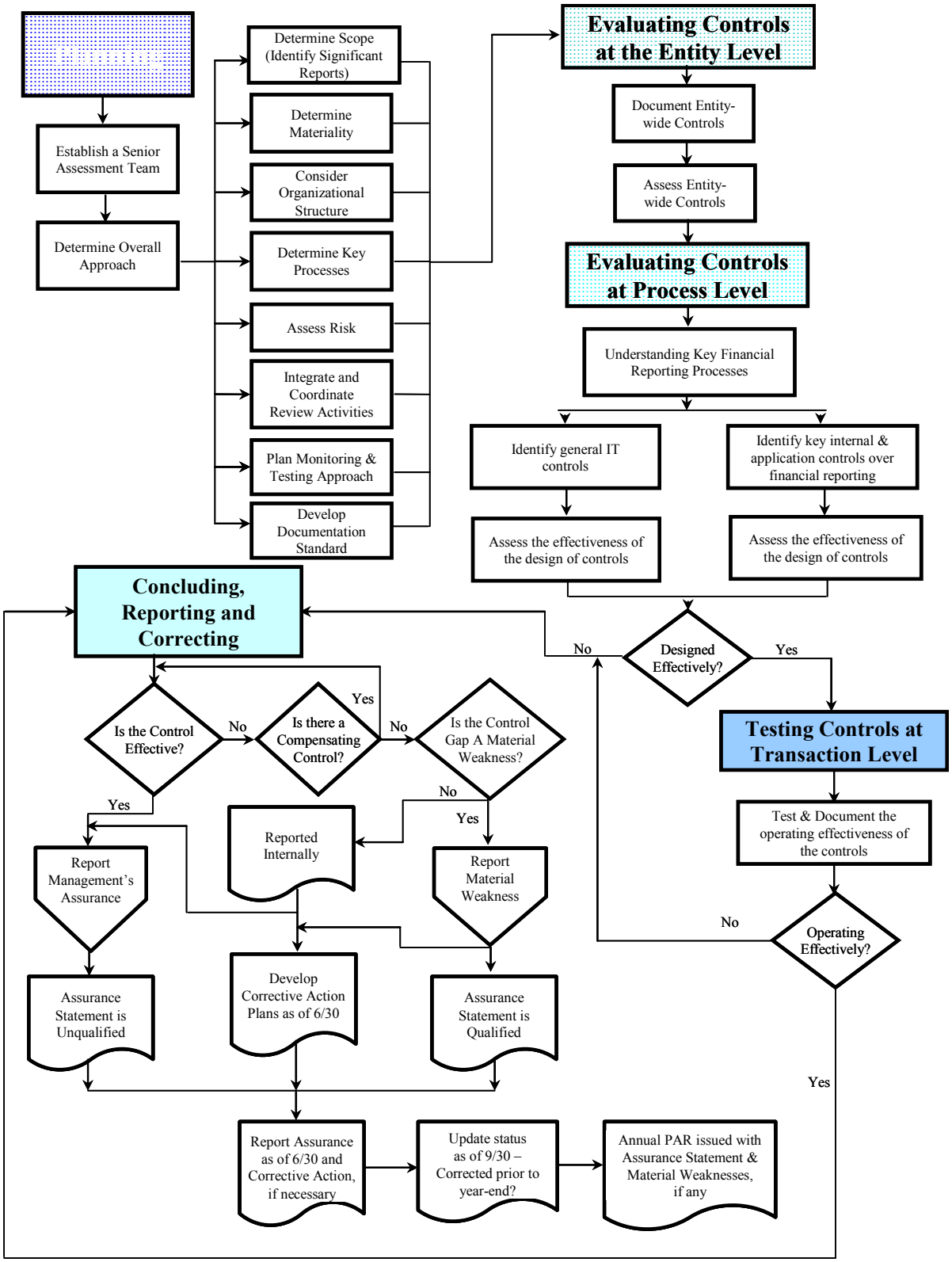
The Assessment Process

There are five basic steps in performing the assessment of the effectiveness of internal control over financial reporting. The steps are:

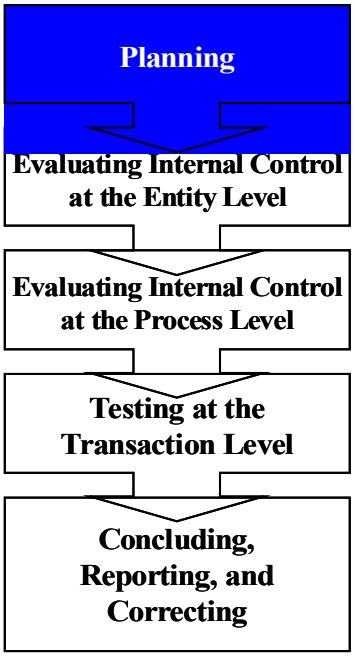
- Step 1: Planning;
- Step 2: Evaluating Internal Control at the Entity Level;
- Step 3: Evaluating Internal Control at the Process Level;
- Step 4: Testing Control Design and Operating Effectiveness at the Transaction Level; and
- Step 5: Concluding, Reporting, and Correcting.

Documentation occurs within each of the basic steps outlined above, whether documenting the assessment methodology during the planning step or documenting key processes and test results during the evaluation and testing steps. This guide is structured to provide additional guidance to management on each of these steps.

Flowchart of the Five-Step Process



STEP 1: PLANNING



- ***Organizational Structure***
- ***Determine Overall Approach: A Top-Down Focus***
- ***Integrate and Coordinate with Other Control-Related Activities***
- ***Determine Scope of Significant Financial Reports***
- ***Determine Materiality***
- ***Determine Key Processes Supporting Material Line Items***
- ***Financial Reporting Assertions***
- ***Risk Assessment***
- ***Documentation***
- ***Monitor Control Effectiveness***
- ***Plan for an Updated Assurance Statement in the PAR***

Planning is the most critical step in this process. All key decisions that drive the assessment are made during the planning phase. During this phase management must decide the scope of the assessment (which financial reports to review), materiality thresholds and testing schedules as well as other key decisions. Defining the scope too broadly or setting an excessively low materiality threshold will result in unnecessary and unwarranted test work on processes and controls that are not fundamental to the agency as a whole. In contrast, defining the scope too narrowly or setting a high materiality threshold will result in too little testing and the inability to properly assess the controls.

Organizational Structure

Senior management support for the assessment process is critical to its success. The establishment of a Senior Assessment Team, or a similar structure, is strongly encouraged. Throughout this document, Senior Assessment Team is used for reference, and does not indicate that a Senior Assessment Team is required. The Chief Financial Officer (CFO) should lead the Senior Assessment Team and should include senior executives from the offices most directly affected by the assessment identified and selected by management. The success of an agency's assessment will primarily depend on the ability of the Senior Assessment Team to effectively carry out or direct the assessment. The Senior Assessment Team may be a subset of the Senior Management Council, another recommended, but not required, body.

As noted earlier, the Senior Assessment Team and Senior Management Council are not mandatory organizational structures. However, management should ensure that the assignment of authorities, participation, responsibilities, and accountability noted in this and the following sections are integrated into the selected or existing organizational structure. The integration of these principles are critical to management's success at ensuring that it has appropriate support for the subsequent assurance.

The Senior Management Council is responsible for assessing and monitoring deficiencies in internal control resulting from the overall FMFIA assessment process, which includes the three objectives of an internal control framework: effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations. The Senior Management Council should advise the agency head of the status of corrections to existing material weaknesses and apprise the agency head of any new material weaknesses that may need to be reported to the President and the Congress through the annual Performance and Accountability Report (PAR). The CFO should be a member of the Senior Management Council. The Senior Assessment Team will report to the CFO, who will coordinate with the Senior Management Council. The responsibilities and membership of the Senior Assessment Team are discussed in the following paragraphs.

Responsibilities

The Senior Assessment Team provides oversight and accountability for the agency's internal control over financial reporting. The Senior Assessment Team assists management to implement an internal control framework and foster an organizational environment that supports continuous awareness of internal controls. It should be clearly communicated that this assessment is not intended to be an annual exercise, but continuous efforts throughout the year to meet the responsibilities of documenting, assessing, and monitoring internal controls and correcting weaknesses. To put it simply, monitoring and improving internal control is a continuous process. However, the agency is required to report on its efforts annually in its PAR.

The Senior Assessment Team should, at a minimum, be responsible for:

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

- Ensuring that the staff and contractor personnel are adequately trained to conduct the assessment;
- Determining the assessment design and methodology;
- Ensuring that adequate policies and methods are in place to document the assessment design, methodology and results;
- Analyzing the results of testing and assessment;
- Reporting on the results of the assessment; and
- Monitoring the progress of implementing corrective actions.

Membership

While the assessment of the effectiveness of internal control over financial reporting is a CFO-led effort, key processes that need to be reviewed may overlap with other areas within the organization. Management should utilize its professional judgment and discretion when selecting members for the Senior Assessment Team and may consider representatives from the various business areas within the department or agency, such as:

- Accounting / Finance
- Information Technology
- General Counsel
- Operations
- Procurement
- Human Resources
- Facilities and Administration
- Budget
- Internal Review
- OIG (serving in an advisory capacity only)

Management should seek perspectives from the OIG, in an advisory capacity only, to facilitate efficiencies with the financial statement audit and other OIG activities. The Senior Assessment Team should seek perspectives from the OIG and other independent auditors when planning the assessment and maintain periodic communications throughout the process. This type of coordination will avoid surprise, allow for effective communications and potentially result in efficiencies with the financial statement audit.

Additionally, it will be important that the Chief Information Officer (CIO) actively participate as a member of the Senior Assessment Team to monitor and review the testing

and documentation of the information technology (IT) controls related to financial reporting, since this may be a significant part of the assessment.

Refer to Exhibit 1, on page 47 for examples of organizational structures.

Determine Overall Approach: A Top-Down Focus

With the addition of Appendix A to A-123, management is required to test the effectiveness of controls in place over financial reporting in order to support its assurance statement. Prior to the implementation date of Appendix A (effective beginning fiscal year 2006), agencies may have supported management's assurance statement with self-evaluations and surveys throughout the organization. The self-evaluations and surveys were typically elevated through the chain of command. As agencies prepare to implement the strengthened monitoring requirements in Appendix A, a top-down approach should be used in planning the separate assessment of internal control over financial reporting.

The assessment of internal control over financial reporting is conducted to provide management's assurance at the agency-wide level. A top-down approach to planning, testing, and documenting internal control over financial reporting would start with the significant agency-wide financial reports and work back to the key processes, controls, and supporting documentation. The Senior Assessment Team will determine the scope of financial reporting, the assessment design and methodology, and the material items to be tested. Management has the flexibility to determine significant financial reports.

The Senior Assessment Team will communicate its planned procedure and determinations throughout the agency and monitor the agency's progress in implementing the strategy communicated. Such determinations will include: documentation standards, testing requirements, considerations with regard to component units, multiple locations, key systems, and cross-servicing arrangements. The top-down approach is suggested to help focus the agency's resources on the items most material and most at risk to the agency's financial reporting.

Agencies should consider qualitative, as well as quantitative factors when determining which line items and key processes to review. The Senior Assessment Team may identify key processes that may not be material to the financial statement balances, but may warrant management's attention due to the risk associated with the activity or programs that are of particular interest to the President, the Congress, or the public.

Assurances Needed from Components

The Senior Assessment Team will need to ensure sufficient testing is performed to obtain assurance regarding the effectiveness of internal control over financial reporting for the agency as a whole. This will involve obtaining appropriate assurances from component units of the agency. To gain an understanding of internal control and subsequently test its effectiveness, the Senior Assessment Team will have to communicate the assessment objectives and level of coordination needed from component units. This communication can be accomplished through memoranda, briefings, or conferences from the Senior Assessment Team to component level management.

Assurances needed from component units will vary based upon its involvement with key business processes, uniformity of business processes and controls that impact material line items on financial reports, and management's risk assessment. The Senior Assessment Team will tell the component unit which functions and processes must be part of the agency-wide assessment.

Multiple Locations

Management needs to consider the agency's structure when planning the assessment. If an agency has multiple locations, the Senior Assessment Team will need to develop, document and communicate an appropriate testing approach. A testing approach should include, but is not limited to how the sample will be selected and how the rotation schedule will impact the location. Agencies with multiple operating units, geographical locations or reporting units will need to determine which locations should be included in the assessment.

Management may consider significant locations based on the potential for a material misstatement. Management may consider whether locations have specific significant risks individually or when combined with other locations. Management should also consider the consistency of systems across operating units, geographical locations or reporting units. If systems are the same, samples should reflect an appropriate cross-section of all locations. If systems and processes are unique, management should then consider the significance and impact of the system on financial reporting.

In the case of controls performed in multiple locations (regions), management should consider: the consistency with which control procedures are conducted at the various locations; the portion of activity flowing through the location; the risk of misstatement; past testing results; and ultimately the locations that will be included in test work. Management will need to develop and communicate a testing approach when multiple locations exist (test sample from each location or rotate locations).

Refer to Exhibit 2, beginning on page 49, for examples of internal agency communications using the top-down approach.

Cross-Servicing Entities: Customers and Providers

When an Agency is a Customer

Services provided by a cross-servicing entity or service organization are considered part of an entity's information system if they affect any of the following:

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

If the services provided are part of the entity's information system as defined above, the user's Senior Assessment Team should consider the activities of the cross-servicing entity or service organization in making its assessment of internal control over financial reporting. Management should then coordinate with the material outside service providers to obtain an annual assurance statement that highlights key controls and the results of annual testing. The objectives and timing of the external service provider's assurance statement should be aligned with the agency's annual assessment.

If an external review (e.g., Type II SAS 70[2]) is currently conducted for cross-servicing functions as required by OMB Memorandum, *M-04-11 Service Organization Audits, the Senior Assessment Team should obtain the results or coordinate with the reviewer to*

[2] In accordance with the AICPA Statement on Auditing Standards (SAS) No. 70, Service Organizations, service organizations may disclose their control activities and process to their customers and their customers' auditors in a uniform reporting format. A SAS II 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report ("Service Auditor's Report") including the auditor's opinion is issued to the service organization at the conclusion of a SAS II 70 examination. A SAS II 70 service audit report includes an opinion on the service organization's description of controls placed in operation and whether controls had been placed in operation as of a specific date, and a description of controls for which tests of operating effectiveness were performed. A SAS II 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes.

determine the extent to which the review affects the agency's assurance testing. As with the independent audit of the financial statements, efficiencies can be achieved by coordinating with the independent auditor performing the review of the cross-servicing function. Refer to the *Evaluating Controls of Cross-Servicing Providers and Service Organizations* section, page 29, for a further discussion of how a Type II SAS 70 review may be relied upon by management in conducting its own assessment.

When an Agency is a Provider

When your agency is the provider of financial processing services, the Senior Assessment Team must identify the population of services and agencies for which the agency provides cross-servicing functions. Once the population is defined, management will have to coordinate with customer agencies to determine if the services provided are material to the customer agency's financial operations. If the services provided are material, then the provider agency management must identify the major controls affecting the customer agency and coordinate the timing of the assessment and resulting assurance statement for appropriate reliance by the customer agencies.

Integrate and Coordinate with Other Control-Related Activities

Federal agencies are subject to numerous legislative and regulatory requirements that promote and support an effective internal control framework. Similarly, numerous reviews are performed by management, or on management's behalf, throughout the year in order to comply with various laws and regulations.

Agencies should strive to integrate control related activities within the control framework outlined in A-123. In particular, management should identify opportunities to integrate and coordinate in order to leverage the internal reviews already being performed. For example, internal reviews are required by the Federal Information Security Management Act of 2002 (FISMA) and the Improper Payments Information Act of 2002 (IPIA). Management should consider the results of these reviews to identify gaps between baseline control activities and the documentation and the assessment process for financial reporting.

The results of the work performed under these laws may also be used to support management's assertion as to the effectiveness of the internal controls. The desired approach would be to design the testing and assessment to accomplish all requirements in the most efficient manner.

Coordination with Other Internal Reviews

The Senior Assessment Team needs to integrate its assessment under Appendix A with other related assessments. This coordination should include:

- Determining the universe of assessments performed by the agency that may impact control objectives related to financial reporting. This can be accomplished by coordinating with the appropriate agency offices.
- Identifying the agency offices and officials responsible for the assessments.
- Meeting with officials to identify the objectives of assessments and determine whether there is any overlap with the Appendix A assessment objectives.
- Ensuring that all control objectives are met in an efficient manner.

It will be important for the Senior Assessment Team to coordinate the assessment under Appendix A with the agency personnel in charge of leading other assessments related to financial reporting.

Coordination within Your Agency

To ensure the objectives of the assessment of internal control over financial reporting are reached in an effective and efficient manner, proper communication within your agency is vital. Management's assessment of internal control over financial reporting under Appendix A shares many of the same control objectives mandated by existing financial reporting related legislation, including:

- Chief Financial Officers Act of 1990, as amended (CFO Act)
- Federal Financial Management Improvement Act of 1996 (FFMIA)
- Federal Information Security Management Act of 2002 (FISMA)
- Improper Payments Information Act of 2002 (IPIA)

Coordination with the Annual Financial Statement Audit

The CFO Act requires agencies to both establish and assess internal control related to financial reporting through the preparation of financial statements by management and the audit of these statements by an independent auditor (OIG or an independent public accounting firm).

The methodology and documentation utilized by management in conducting its assessment of internal control over financial reporting is similar to that used in conducting the financial audit. For example, OMB Bulletin 01-02, *Audit Requirement for Federal Financial Statements,* requires auditors to:

> *…Obtain an understanding of the components of internal control… and assess the level of control risk relevant to the assertions embodied in the classes of transactions, account balances, and disclosure components of the financial statements. For those internal controls that have been properly designed and placed in operation, the auditor shall perform sufficient tests to support a low assessed level of control risk.*

Agency management should work with the independent auditor to create efficiencies in the financial statement audit and Appendix A assessment processes. Agency management should:

- Seek the perspective of the OIG or an independent auditor to see whether management's determination of significant accounts, major classes of transactions, and relevant assertions are consistent with those identified by the financial statement auditor. Differences may exist between management's and the auditor's assessment due to factors such as materiality. Generally, management's materiality threshold will be lower than the threshold for the financial statement audit.
- Facilitate the exchange of information (i.e., sharing of documentation), where possible, between management and the auditors relating to their collective understanding of internal control over financial reporting. This exchange should enable both parties to gain a more comprehensive understanding of the financial reporting processes and to identify key controls.
- Coordinate the timing of control testing and determine the level of reliance the financial statement auditor plans to place on the results of management's testing of key controls. (**Note:** Management cannot substitute the auditor's documentation or testing of key controls for its own assessment under Appendix A.)
- Compare the results of management's Appendix A assessment of control over financial reporting with the financial statement audit report on internal control (i.e., reportable conditions and material weaknesses), and investigate the reasons for any reporting differences.

Coordination with Parties External to Your Agency

Typically, federal agencies are engaged in cross-servicing agreements, as both providers (service organization) and customers (user organization), with other federal agencies to process financial data. Examples of services include:

- General Accounting (e.g., processing transactions, financial reporting)
- Payroll (e.g., personnel functions, time tracking, disbursements)
- Grants (e.g., authorization and payments)
- Claims processing centers and other data processing functions

In addition to federal cross-servicing agreements, agencies can have relationships with outside service organizations to process financial data. Examples include:

- Loan Origination and Servicing
- Benefit Payments Processing

While outside organizations may process financial data, management is ultimately responsible for the internal control over financial reporting. Refer to the *Cross-Servicing Entities: Customers and Providers* section on page 11 for a further discussion.

Determine Scope of Significant Financial Reports

The Senior Assessment Team should recommend to management clear and concisely defined parameters for the scope of financial reports to be assessed. Management is responsible for the final determination of the scope and needs to clearly communicate the parameters. Scope determines both the *breadth* and *depth* of financial reporting.

The *breadth* of financial reporting details the financial reports that are included in the scope. A-123 provides management the flexibility to determine which financial reports are significant. At a minimum, agencies should include the basic quarterly and year-end consolidated financial statements in their assessment of internal control over financial reporting. The basic financial statements include the Balance Sheet, Statement of Net Cost, Statement of Changes in Net Position, Statement of Budgetary Resources, Statement of Financing, Statement of Custodial Activity, Statement of Social Insurance, and the accompanying Notes to the financial statements.

It is up to agency management to determine what other significant financial reports to include in their assessment of internal control over financial reporting. Other key financial reports that could be relied upon by management or oversight entities may be considered. For example, agencies may choose to include budget execution reports (e.g., SF-132 – *Apportionment and Reapportionment Schedule*, SF-133 – *Report on Budget Execution and Budgetary Resources*, P&F Schedule *(Budget Program and Financing)*, and FMS-2108 – *Year End Closing Statement*). Agencies may also want to include specific information on major or other programs in the assessment process. Programs that have large appropriations, a high degree of public visibility (e.g., the Decennial Census for the Department of Commerce) or represent areas of concern for agency managers and stakeholders (e.g., Management Scorecard, Performance Metrics, or purchase and travel card controls and reports) may be included.

The *depth* of the financial reporting process is determined by management and includes processes and controls that would materially affect financial statement or note disclosure balances. Depth decisions also relate to the extent of testing undertaken for various component units and geographic locations.

Determine 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 a report. Management must consider how an error would affect management or operations that rely on the key financial reports within the assessment scope. An error that would materially affect the day-to-day decisions based on these key reports would be considered a material error. Since the financial reporting objectives for the day-to-day management and operations are different than the objectives of the third party user of the financial statements, it stands that materiality will be different for each type of report.

Materiality is a function of management's professional judgment and discretion. Therefore, management should consider key business areas and programs that impact financial statement results and include these considerations when determining materiality. Management must determine if there is more than a remote likelihood that errors or misstatements in a financial report individually or in the aggregate could have a material effect on the financial report. The different types of materiality amounts, defined below, are useful in ensuring that adequate work is performed to make this determination.

Reporting materiality is the overall materiality that serves as the threshold of reporting weaknesses in internal controls that could result in a material misstatement of the financial report. In order to determine the requisite level of effort requisite to detect such weaknesses, management should establish planning and testing materiality at levels lower than reporting or overall materiality. Using a lower level of materiality for testing controls will increase the likelihood that management would detect control weaknesses that could lead to a financial report being materially misstated.

Planning materiality is used to determine significant accounts, elements, or disclosures in a financial report. Planning materiality is generally a percentage of reporting or overall materiality. For example, if reporting materiality is $10 million, planning materiality might be set at $7 million.

Testing materiality is used to determine the extent of controls testing relative to each significant account, element, or disclosure. Testing materiality is generally a percentage of planning materiality.

Materiality determinations for planning, testing, and reporting on management's assessment of internal control over financial reporting should be based on quantitative and qualitative considerations:

- Quantitative considerations—one or more materiality bases should be determined for each financial report that is included in the scope of the assessment. For a balance sheet, the materiality base might be total assets reported. For a statement of net costs, the materiality base might be total income or total expenses. The

materiality base would be used to determine the reporting or overall materiality, which in turn would be used to calculate planning and test materiality.

- Qualitative considerations—management should consider not only quantitative measures of materiality, but qualitative as well. For example, certain accounts or elements of a financial report may be significant due to the interest of OMB, the public or oversight committees.

Management should document its initial determination of materiality, the rationale and basis for the materiality determination, and that materiality was reconsidered at least immediately prior to concluding on the assessment and determining what control weaknesses must be reported.

Additional considerations include:

- Individually significant components—a consolidated financial report could include component financial information that is individually significant to the consolidated report. In such instances, establishing materiality levels based on the consolidated totals could result in other components effectively being considered as immaterial, although they may be significant components. In this case, management should establish separate materiality bases for the financial report so that one component does not unduly overshadow other significant components.
- Common systems—if management is testing controls over common systems that feed more than one financial report included in the assessment, it should consider using the lowest materiality levels among the reports to efficiently design the testing of the common systems.
- Changing conditions during assessment—management should be aware that conditions could change during the course of the assessment process that affect materiality decisions. Therefore, the assessment process should factor in the possibility of reassessing materiality decisions prior to the decision-making process related to what control weaknesses to report.

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

When determining material line items on the key financial reports, management may want to consider the types of materiality that auditors consider when determining if the planned nature, timing, and extent of procedures are appropriate. However, keep in mind that management must consider how day-to-day management and operations that rely on the key financial reports would be affected. An error that would materially affect the day-to-day decisions based on these key reports would be considered a material error. The concepts contained in this document are only suggestions. Management has the full

authority to implement a different approach to determining material line items on its key financial reports.

Determine Key Processes Supporting Material Line Items

Business processes are the foundation of the internal control assessment and support significant material balances on the financial reports. When defining key business processes, management should review financial statements and related disclosures, as well as cycle memoranda, flowcharts, and any other analyses that are available to management. In addition to key business processes, management should consider key systems and locations or component units that are critical to the business processes.

A business process is a sequence of events, consisting of the methods and records used to establish, identify, assemble, analyze, classify, and record (in the general ledger) a particular type of transaction. Examples include:

- Cash receipts and disbursements,
- Collection of accounts receivable,
- Purchase and sale of inventory,
- Customer billing, and
- Payroll.

A line item or account-related accounting application consists of the methods and records established to report an entity's recorded transactions and to maintain accountability for related assets and liabilities. Line item or account-related processes consist of methods to report transactions and demonstrate accountability, examples include:

- Fund balances with treasury,
- Accounts receivable,
- Inventory control,
- Property and equipment, and
- Accounts payable.[3]

The Senior Assessment Team should crosswalk line items or accounts to business cycles as shown in Exhibit 3, see page 55.

[3] GAO Financial Audit Manual Section 240.03

Financial Reporting Assertions

Management needs to identify which relevant financial reporting assertions apply to the material line items. The acronym **PERCV** (as in PERCEIVE) is often used to remember the five assertions, which are:

- **P**resentation and Disclosure;
- **E**xistence or Occurrence;
- **R**ights and Obligations;
- **C**ompleteness and Accuracy;
- **V**aluation or Allocation.

An example of Risk Analysis that shows how each of the Financial Reporting Assertions should be correlated with line items or accounts is displayed in Exhibit 4; see pages 56-58.

Risk Assessment

Risk assessment is an internal management process for identifying, analyzing and managing risks relevant to achieving the objectives of reliable financial reporting, safeguarding of assets and compliance with relevant laws and regulations. Management should prepare a summary of specific risks of misstatement for each significant line item, which will be used in determining 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. Management should assess the control or combined risk for each assertion, document the assessment, and prepare the testing plan. Refer to Exhibits 4 (page 56) and 5 (page 59) for sample templates of the summary of risks.

The types of risks identified may be adapted for use by agency managers in determining their testing plan for the internal control over financial reporting.

- **Inherent risk** – the susceptibility of an assertion to misstatement, assuming there are no related specific control activities. Inherent risk factors include: the nature of the agency's programs, transactions and accounts and whether the agency had significant audit findings.
- **Control risk** – the risk that misstatements will not be prevented or detected by the agency's internal control (assessed separately for each significant financial statement assertion in each significant cycle or accounting application). Refer to the *Financial Reporting Assertions* section above for the financial statement assertions.
- **Combined risk** – the likelihood that a material misstatement would occur (inherent risk) and not be prevented or detected on a timely basis by the agency's internal control (control risk).

- **Fraud risk** – the risk that there may be fraudulent financial reporting or misappropriation of assets that causes a material misstatement of the financial statements.

Documentation

Documenting or updating existing documentation of the key processes and the internal controls over those processes should be prepared by staff knowledgeable in the respective areas. Documenting these processes and related controls also includes the IT systems through which the transactions flow. In addition to documenting the key processes and related controls, the agency needs to document its assessment methodology and how key decisions were made during the Planning step of the assessment process.

The level of detail of the documentation should ensure management understands the entire financial reporting process and can identify how processes relate to financial reporting assertions, potential errors or misstatements, and control objectives. Other financial reporting process documentation considerations could include:

- A walkthrough of key processes including examples of the processing documents;
- Process relationship to financial statement line items, significant accounts, group of accounts, and major classes of transactions;
- Inputs, activities, and outputs in place to accomplish the processes control objectives;
- Policies and procedures governing transactions;
- Identification of key financial reporting controls;
- Significant provisions of laws and regulations;
- Computer information systems used to support the process;
- Performance measures used by management to ensure operational controls are in place (e.g., fund balances with treasury, suspense accounts, delinquent accounts receivable, EFT payments, prompt pay statistics, etc.);
- Monitoring activities in place to ensure controls are functioning properly; and
- Relationships to other financial reporting processes.

Documenting the Plan and Methodology

The Senior Assessment Team must document the assessment methodology, 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; and
- Key components of the assessment methodology and guide such as:
  - The understanding obtained and the evaluation of the design of each of the five components 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 components at which testing was performed
  - The process and decisions supporting a testing plan (e.g., rotational testing schedule – see *Risk-Based Approach* section on page 35)
  - The extent to which the Senior Assessment Team relied on the work of others, such as for cross-servicing entities or service organizations, and how the Senior Assessment Team determined the adequacy of such work
  - Other information that could affect management's certification of its internal control over financial reporting
- The actions taken to correct identified deficiencies.

Documenting the Assessment and Test Results

The Senior Assessment Team must have documentation readily available to support each annual assessment performed. The Senior Assessment Team must clearly communicate to the staff and contractors performing the tests, that the staff and contractors need to document the procedures performed, evidence obtained, and conclusions reached with respect to relevant internal controls over financial reporting for each assertion embodied in the financial reports. Documentation should include the following:

- Information about how significant transactions are initiated, authorized, recorded, processed, and reported.
- Sufficient information about the flow of transactions to identify the points at which material misstatements due to error or fraud could occur.
- Controls designed to prevent or detect fraud, including who performs the controls and the related segregation of duties.

- Controls over the period-end financial reporting process.
- Controls over safeguarding of assets.
- The results of management's testing and evaluation.

Documentation might take many forms, such as paper, electronic files, or other media, and can include a variety of information, including policy manuals, process models, desk procedures, flowcharts, job descriptions, documents, and forms. The form and extent of documentation will vary depending on the size, nature, and complexity of the entity or financial report.

Documentation should be prepared in sufficient detail to provide a clear understanding of its purpose, source, and the conclusions reached. Also, the documentation should be organized to provide a clear link to the significant findings or weaknesses reported. Documentation must contain sufficient information to enable a knowledgeable person having no previous connection with the assessment to understand the nature, timing, extent, and results of the procedures performed, evidence obtained, and conclusions reached; and to determine who performed the work and the date the work was completed.

Management should also consider implementing policies regarding documentation retention, if such policies do not already exist.

Monitor Control Effectiveness

The Senior Assessment Team will monitor activities related to internal control over financial reporting. Monitoring is a process that assesses the quality of an organization's internal control, evaluates the design and operation of controls on a timely basis and takes corrective actions as necessary. There are three important aspects to a sound monitoring process:

- Monitoring activities need to be developed and performed regularly to ensure the related control is operating as intended.
- The results of the monitoring activities need to be evaluated, classifying any noted deficiencies into three categories: inconsequential or simple deficiency, reportable condition, or material weakness.
- Corrective action plans should be developed to resolve all deficiencies that are cost beneficial to correct. A process for tracking the status of the corrective action plans should also be implemented.

Monitoring Activities

Testing controls may be accomplished through continuous monitoring activities, separate evaluations or a combination of the two. The design of monitoring activities should provide periodic evaluation of significant control activities, including IT controls.

Monitoring occurs in the normal course of operations. It includes regular management and supervisory activities and other actions personnel take in performing their duties. Monitoring may also take the form of management reviews and sign-offs, analytical procedures, comparisons of control totals, account reconciliations, and system alert reports. In addition to management, internal auditors or external parties may also perform continuous monitoring activities.

The scope and frequency of separate evaluations will depend primarily on the assessment of risks and the effectiveness of continuous monitoring procedures. Management may take a risk-based approach to testing. However, where risk is low, controls are stable and there are no deficiencies, testing can be rotated to a maximum of every three years.

Since many agencies rely heavily on information and financial systems to process and report data, agencies should implement and conduct a combination of continuous monitoring and separate evaluations of information technology controls. Federal Information System Controls Audit Manual (FISCAM) and Certification and Accreditation review processes may play a significant role in monitoring the operating effectiveness of general and application controls over financial systems.

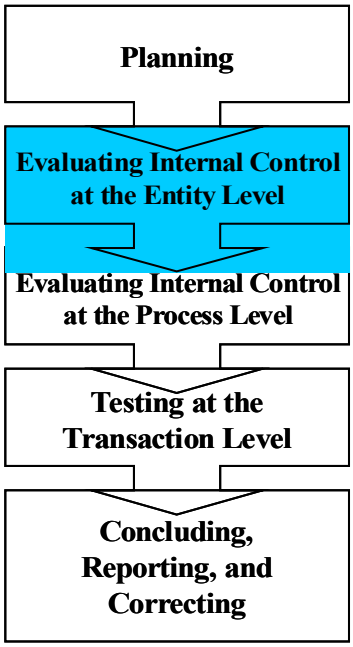
Refer to the *Internal Control Management and Evaluation Tool*[4] issued by GAO in August 2001 for a list of factors to consider when developing monitoring activities.

Plan for an Updated Assurance Statement in the PAR

Management must plan the procedures necessary to update its assurance provided as of June 30th for reporting in the annual PAR issued in November. These procedures may entail validating that corrective actions to remediate a reported material weakness were effective. The procedures also entail assessing the status of management and independent auditor testing of controls from the date of the assessment through the PAR issuance date to determine if any unreported material weaknesses exist.

[4] The *Internal Control Management and Evaluation Tool*, is available on GAO's website, www.gao.gov.

STEP 2: EVALUATING INTERNAL CONTROL AT THE ENTITY LEVEL



Entity-wide level controls can have a pervasive effect on the organization. As such, this is a logical starting point in an overall assessment of effectiveness of internal control over financial reporting in any department or agency. Evaluation at the entity-wide level can also provide information that will aide in determining the nature and extent of internal control testing that may by required at the transaction or process level. Consideration should be given to the five standards of internal control[5] that can have a pervasive effect on the risk of error or fraud:

- **Control Environment** – Management and employees have a positive and supportive attitude toward internal control and conscientious management. Management conveys the message that integrity and ethical values must not be compromised. The agency demonstrates a commitment to the competence of its personnel and employs good human capital policies and practices. Management has a philosophy and operating style that is appropriate to the development and maintenance of effective internal control. The agency's organizational structure and the way in which it assigns authority and responsibility contribute to effective internal control. The agency has a good working relationship with Congress and oversight groups.
- **Risk Assessment** – The agency has established clear and consistent entity-wide objectives and supporting activity-level objectives. Management has made a thorough identification of risks, from both internal and external sources, which may affect the ability of the agency to meet those objectives. An analysis of those risks has been performed, and the agency has developed an appropriate approach for risk management. In addition, mechanisms are in place to identify changes that may affect the agency's ability to achieve its financial reporting objectives.
- **Information and Communication** – Information systems are in place to identify and record pertinent operational and financial information relating to internal and external events. That information is communicated to management and others within the agency who need it and in a form that enables them to carry out their duties and responsibilities efficiently and effectively. Management ensures that effective external communications occur with groups that can affect the achievement of the agency's missions, goals, and objectives. The agency

[5] Internal control standards are based upon GAO's, Standards for Internal Control in the Federal Government, November 1999, "Green Book."

employs various forms of communications appropriate to its needs and manages, develops, and revises its information systems in a continual effort to improve communications.

- **Control Activities** – Appropriate policies, procedures, techniques, and control mechanisms have been developed and are in place to ensure adherence to established directives. Proper control activities have been developed for each of the agency's activities. The control activities identified as necessary are actually applied properly.
- **Monitoring** – Agency internal control monitoring assesses the quality of performance over time. It does this by implementing procedures to monitor internal control on a continuous basis as a part of the process of carrying out its regular activities. It includes ensuring that managers know their responsibilities for internal control and control monitoring. In addition, separate evaluations of internal control are periodically performed and the deficiencies found are investigated. Procedures are in place to ensure that the findings of all audits and other reviews are promptly evaluated, decisions are made about the appropriate response, and actions are taken to correct or otherwise resolve the issues promptly.

Evaluating internal control at the entity-wide level is generally accomplished through observation, inquiry, and inspection, rather than the detailed testing that lends itself to the transaction or process level internal controls. Control Activities is the one factor where detailed testing would be required. In general, questionnaires and checklists are most useful at the entity-wide level. GAO has developed a useful tool to assist agencies in assessing internal control at the entity-wide level[6]. Similar tools are available from other sources. Using one of these tools or the agency's own instrument, the following factors should be understood and evaluated:

- Control Environment
  - Integrity and Ethical Values
  - Commitment to Competence
  - Management's Philosophy and Operating Style
  - Organizational Structure
  - Assignment of Authority and Responsibility
  - Human Resource Policies and Practices
  - Oversight Groups
- Risk Assessment
  - Establishment of Entity-wide Objectives
  - Establishment of Activity-level Objectives

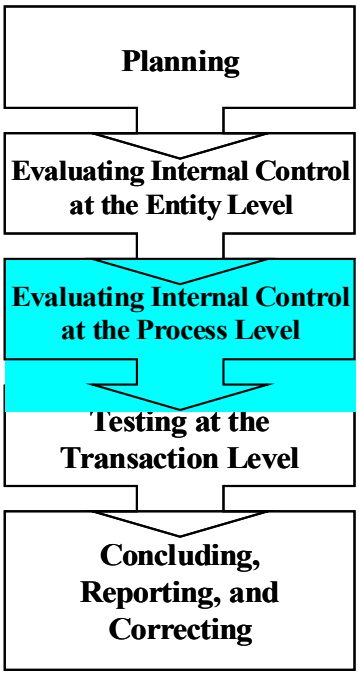
[6] The *Internal Control Management and Evaluation Tool*, is available on GAO's website, www.gao.gov.

- Risk Identification
- Risk Analysis
- Managing Risk During Change

- Information and Communication
  - Information
  - Communication
  - Forms and Means of Communication
  - Frequency of Communications
- Control Activities
  - General Application
  - Common Categories of Control Activities
  - Control Activities Specific for Information Systems
    - Entity-wide Security Management Program
    - Access Control
    - Application Software Development and Change Control
    - System Software Control
    - Segregation of Duties
    - Service Continuity
    - Authorization Control
    - Completeness Control
    - Accuracy Control
    - Control Over Integrity of Processing and Data Files
- Monitoring
  - Continuous Monitoring
  - Separate Evaluations
  - Audit Resolution

STEP 3: EVALUATING INTERNAL CONTROL AT THE PROCESS LEVEL

- ***Understanding Key Financial Reporting Processes***
- ***Identifying Key Controls***
- ***Understanding Control Design***
- ***Evaluating Controls of Cross-Servicing Providers and Service Organizations***
- ***Documenting Key Business Processes and Related Key Controls***
- ***Understanding the IT Infrastructure and Associated Risks***



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

Understanding Key Financial Reporting Processes

Agency management should develop a crosswalk analysis that ties key business processes to material financial report line items or accounts. An example is provided in Exhibit 3. For each significant line item or account, managers should have an understanding of how potential deficiencies in key business processes could adversely impact financial reporting. Using this analysis, agency management can then identify control objectives (e.g., personnel should be prevented from having uncontrolled access to both assets and records) and relevant control techniques (e.g., segregation of asset custody from record keeping function) to achieve those objectives.

Identifying Key Controls

A key control is a control, or set of controls, that address the relevant assertions for a material activity (e.g., financial statement line item) or significant risk. At the point that management is ready to test controls, and in order to focus test work, management must identify the key controls in place.

Management should maintain an inventory of the key controls that require evaluation. When the inventory of controls has been identified, management must then evaluate and prioritize the overall impact of the activities on the reliability of financial reporting. Management should also ensure that all reporting assertions have been addressed for each financial statement line item. Once the prioritization and assertions have been identified, the Senior Assessment Team can begin its determination of the type and level of testing necessary to provide assurance that financial reporting is reliable.

Understanding Control Design

Once the Senior Assessment Team has documented its understanding of key financial reporting processes, it should also document its understanding of the design of controls that are relevant to financial reporting. The Senior Assessment Team's understanding of control design should relate the impact on the line item or account where the potential misstatement could occur, the control objective, and the control technique. Key questions to consider include[7]:

- 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?

To determine the control technique's design effectiveness, the Senior Assessment Team should focus on the[8]:

- Directness of the control technique in relation to the financial reporting assertion;
- Frequency of the control's application;
- Experience and skills of personnel performing the control;
- Separation of duties; and
- Procedures followed when a control identifies an exception condition.

[7] The illustrative considerations are based upon the GAO/PCIE *Financial Audit Manual*, Section 340.

[8] Ibid.

Evaluating Controls of Cross-Servicing Providers and Service Organizations

When evaluating the controls in place at cross-servicing providers or service organizations, the Senior Assessment Team should determine the extent of procedures needed, which may include:

- Performing tests of the entity's controls over the activities of the cross-servicing organization or service organization (e.g., re-performance of selected items processed by the cross-servicing organization or service organization, or reconciling output reports with source documents); or
- Performing tests of controls at the cross-servicing organization or service organization; or
- Obtaining a service auditor's report on controls placed in operation and tests of operating effectiveness (e.g., Type II SAS 70 report) or a report on the application of agreed-upon procedures that describes the relevant tests of controls.

The Senior Assessment Team should also obtain the annual assurance statement from the cross-servicing provider's management that highlights the key controls and results of annual testing. Initially, the Senior Assessment Team should determine whether the activities, processes and functions provided by the service organization are significant to the assessment of internal control over financial reporting. If the activities are significant, the Senior Assessment Team should:

- Determine whether the current Type II SAS 70 report is sufficient in scope. This includes the time period covered by the test of controls and its relation to the date of management's assessment and the applications covered.
- Obtain an understanding of the controls at the cross-servicing provider or service organization that are relevant to the entity's (customer) internal control over financial reporting and the controls at the entity (customer) over the activities of the cross-servicing organization or service organization.
- Obtain evidence that the controls at the cross-servicing provider or service organization, which are relevant to management's (customer) assertion, are operating effectively.

A financial service provider's Type II SAS 70 report should be deemed reliable with no further testing required for their client agencies in those areas covered by the Type II SAS 70 report. For the financial service provider, the Type II SAS 70 reporting process may be incorporated into management's assessment of internal control over financial reporting. An unqualified opinion on the Type II SAS 70 provides evidence that the controls are operating effectively and no additional testing is required.

However, the Senior Assessment Team should consider whether testing exceptions exist. If testing exceptions exist (or the opinion was qualified), additional procedures will have to be performed and may include the following:

- Performing tests of the entity's controls over the activities of the cross-servicing organization or service organization (e.g., re-performance of selected items processed by the cross-servicing organization or service organization, or reconciling output reports with source documents); or
- Performing tests of controls at the cross-servicing organization or service organization.

Documenting Key Business Processes and Related Key Controls

Knowledgeable staff or contractors should document the key financial reporting processes and the related key controls. Typical forms of documentation could include:

- Organization charts,
- Flowcharts,
- Questionnaires,
- Decision tables,
- Policy or accounting manuals,
- Cycle or process memoranda, and
- Checklists.

During the initial years of the assessment, management should take advantage of any pertinent documentation available, such as process and transaction cycle memoranda from the OIG or other independent auditors (IPA). This should be considered as a potential source, or starting point. However, management might decide that the documentation of its own processes would provide a greater understanding. An opportunity to share this already existing information can be helpful in establishing a baseline prior to management undertaking its own documentation and test-work of key controls. It is important to emphasize that use of information from the OIG or IPAs does not remove the agency's ownership of the process and its responsibility for internal control design, adequacy, and related testing.

Once existing documentation has been obtained, the Senior Assessment Team should ensure documentation is current and contains enough detail to support the assessment. Outdated documentation poses the risk to the Senior Assessment Team that the most current control environment is not sufficiently understood. To ensure documentation is up to date, management is encouraged to develop retention policies and procedures to account for changes in processes as they relate to changes in control environments.

Understanding the IT Infrastructure and Associated Risks

Understanding the IT Infrastructure

As information technology evolves, it plays an increasingly important role in the development of internal control over financial reporting. It is critical that technology-based controls are also assessed. Although assessing computer-related controls generally requires specific expertise and procedures not employed in the evaluation of manual controls, the evaluation of computer-related controls should be planned in conjunction with the evaluation of manual internal control over financial reporting.

The agency should first develop a thorough understanding of the financial reporting operations and how these operations are supported by automated systems. This should include obtaining an overview of each computer application significant to financial reporting.

After gaining an understanding of the entity's operations, the Senior Assessment Team should assess the inherent and control risks as they relate to information systems. The Senior Assessment Team should then (1) identify conditions that significantly increase inherent and control risks and (2) conclude whether these conditions preclude the effectiveness of specific control techniques in significant applications. The assessment team identifies specific inherent risks and control structure weaknesses based primarily on an understanding of the entity's operations. These factors are general in nature and require the Senior Assessment Team's judgment in determining (1) the extent of procedures to identify the risk and weaknesses and (2) the impact of such risks and weaknesses on the entity's operations and financial reports.

For each inherent risk or control structure weakness identified, the Senior Assessment Team should document the nature and extent of the risk or weakness, the conditions that gave rise to that risk or weakness, and the specific information or operations affected. The Senior Assessment Team should also document other considerations that may mitigate the effects of identified risks and weaknesses.

The primary inherent risk factors that the Senior Assessment Team should consider are the nature of the entity's programs and accounts, and any prior history of significant problems. For example, accounts involving subjective management judgments, such as loss allowances, are usually higher risk than those involving objective determinations.

Computerized operations can introduce additional inherent risk factors not present in manual systems. The assessment team should (1) consider each of the following factors and (2) assess the overall impact of computer processing on inherent risk.

- Uniform processing of transactions.
- Automatic processing.
- 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.

Assessing IT Risk

The general methodology that should be used to assess computer-related controls involves evaluating:

- General controls at the entity-wide or installation level.
- General controls as they are applied to the application(s) being examined, such as a payroll system or a loan accounting system.
- Application controls, which are the controls over input, processing, and output of data associated with individual applications.

As part of assessing control risk, the assessment team should make a preliminary assessment of whether computer-related controls are likely to be effective. This assessment is based primarily on discussions with personnel throughout the entity, including program managers, system administrators, information resource managers, and system security managers; on observations of computer-related operations; and on reviews of written policies and procedures. Controls that are not properly designed or would not be effective may indicate weaknesses that are required to be reported.

Based on the assessment of inherent and control risks, including the preliminary evaluation of computer-based controls, the assessment team should identify the general control techniques that are properly designed to be effective and that, therefore, should be tested to determine if they are in fact operating effectively.

General Controls

There are six major categories of general controls that should be considered:

- Entity-wide security program, planning, and management.
- Access controls.
- Application software development and change controls.
- System software.
- Segregation of duties.
- Service continuity.

Application Controls

Application controls generally involve ensuring that:

- Data prepared for entry are complete, valid, and reliable.
- Data are converted to an automated form and entered into the application accurately, completely, and on time.
- Data are processed by the application completely and on time, and in accordance with established requirements.
- Output is protected from unauthorized modification or damage and distributed in accordance with prescribed policies.

Documenting IT Controls

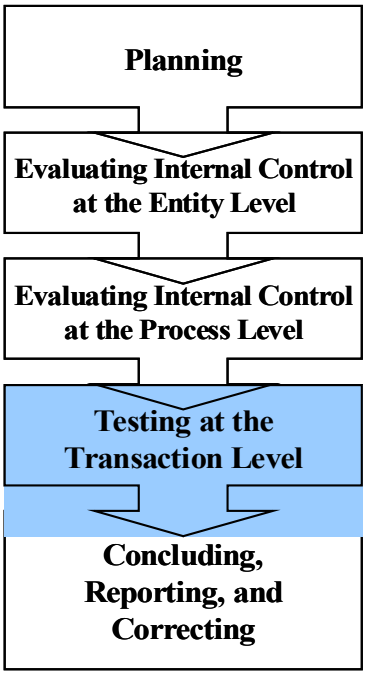
Documentation should include copies of written policies and procedures, written memoranda, flowcharts of system configurations and significant processes, etc. The documentation should identify the control objectives and related control points designed to achieve those objectives.

The list below is intended to provide guidance to management. However, management should exercise professional judgment in the determination of the level of documentation that is required. Documentation of the understanding of the entity and significant computer applications related to financial reporting should include:

- The significance and nature of the programs and functions supported by the automated systems.
- The types of computer processing performed (stand alone, distributed, or networked).

- The specific hardware and software comprising the computer configuration, including (1) the type, number, and location of primary central processing units and peripherals, (2) the role of microcomputers, and (3) how such units are interconnected.
- The nature of software utilities used at computer processing locations that provide the ability to add, alter, or delete information stored in data files, database, and program libraries.
- The nature of software used to restrict access to programs and data at computer processing locations.
- Significant computerized communications networks, interfaces to other computer systems, and the ability to upload or download information.
- Significant changes since the prior evaluation.
- The general types and extent of significant purchased software used.
- The general types and extent of significant software developed in-house.
- How (interactive or non-interactive) and where data are entered and reported.
- The approximate number of transactions processed by each significant system.
- The organization and staffing at the entity's data processing and software development sites, including key staff and organization changes since the prior evaluation.
- The entity's reliance on service bureaus or other agencies for computer processing support.
- Results of past internal and external reviews, including those conducted by inspector general staff and consultants specializing in security matters.

STEP 4: TESTING AT THE TRANSACTION LEVEL



- ***Risk-Based Approach***
- ***Testing Key Controls***

Risk-Based Approach

Management may take a risk-based approach in determining when to test key controls. Once a baseline is established on the operating effectiveness of key controls, not all key controls must be tested every year. The risk-based approach generally requires that controls are stable, there are no known deficiencies, and that controls will be tested at least every three years. Specifically, risk-based testing is permitted in the following circumstances:

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

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

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

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

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

- The control is fully automated as opposed to a manual control or partially automated control that is dependent on some manual intervention to be effective,
- Management has verified that adequate change controls exist over the automated control,

- No changes in the design or operation of the control have occurred since the control was last tested,
- There are no known significant weaknesses of such control, and
- The control has been tested in the past three years.

Management should document its risk-based testing plan and how it complies with the above requirements.

Testing Key Controls

There are four basic types of tests that can be performed on key controls. The ultimate goal of testing a control is to validate that it is functioning effectively (i.e., addressing a relevant assertion or program risk). When preparing a testing plan, the purpose is to document planned procedures to gain evidence to support the operating effectiveness of each control. The basic control tests are listed below in order of assurance they provide (i.e., re-performing a control procedure provides greater assurance that the procedure is in place and functioning than simply inquiring whether a control is in place and functioning); however, inquiry by itself does not provide sufficient evidence whether a control is functioning.

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

In determining how extensively a key control procedure should be tested (i.e., sample size or type of test performed), management should consider the complexity of the key control as well as the frequency with which the control is performed. A highly complex control that is performed daily should be tested more often than a less complex control performed annually. After considering the complexity of a control, the following are examples of sample sizes based on the frequency of the performance of the control: annually – 1; quarterly – 2; monthly – 3; weekly – 10; daily – 30; and recurring – 45. In addition, whether the control is manual or automated should also be considered. Ultimately, management should use its best judgment to determine how extensively a key control will be tested. Management should use judgment in the design of its procedures for testing key controls.

Identifying control gaps

Internal controls should be designed to detect and prevent a material misstatement from entering the financial statements and financial reports used by the organization. Anytime a material misstatement is noted, a control gap exists and when noted, management should ask: are there controls in place, are the controls currently in place adequately designed, or are they simply not functioning effectively?

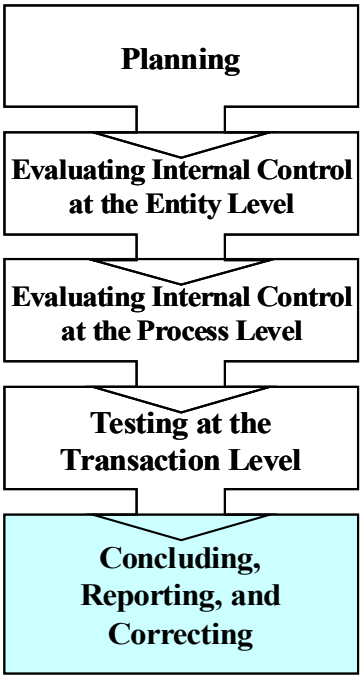
However, a more proactive approach should be considered. Management should list all of the material financial activities as well as the assertions relevant to a given financial activity or risks to a given program and then identify the controls that address each of the assertions and risks. Next, each control should be assessed to determine if it is adequately designed and finally, each control should be reviewed (tested) to determine if it is functioning effectively. Refer to Exhibit 5 for an illustrative template that can be used to track and monitor the efforts noted above.

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. Control gaps may relate to the operation of a control or the design of a control. A *deficiency in operation* exists when a properly designed control does not operate as intended, or when the person performing the control does not possess the necessary authority or qualification to perform the control effectively. A *deficiency in design* exists when a control necessary to meet the control objective is missing or an existing control is not properly designed so that even if the control operates as designed, the control objective is not always met. When management encounters a control gap, they should consider the extent of the gap and the effect that the gap will have in their assurance statement and determine whether compensating controls exist that mitigate the program risk or risk of misstatement.

Identifying compensating controls

A *compensating control* is a technique or other effort(s) designed to mitigate a control design deficiency, or ineffective operation or implementation of a control, or the simple lack of control over a financial process or program. Management, when determining whether the relevant assertions for the reported financial statement line items noted above are addressed, should consider the existence of compensating controls.

STEP 5: CONCLUDING, REPORTING, AND CORRECTING DEFICIENCIES AND WEAKNESSES



- ***Concluding on Effectiveness***
- ***Reporting***
- ***Correcting Deficiencies and Weaknesses***

Concluding on Effectiveness

Test results will support management's judgment whether a control is functioning adequately or not. Exceptions noted in test-work over properly designed internal controls would indicate ineffectiveness. Management must consider the extent of a deficiency in such cases. Deficiencies can range from a *simple deficiency* (e.g., missing initials indicating a supervisor's review on 1 of 26 reconciliations sampled) to a *significant deficiency* (e.g., only 8 monthly reconciliations were performed for the year) to a *material weakness* (e.g., reconciliation of several key accounts were not performed throughout the year, only at year-end). A simple deficiency is an internal control deficiency that creates minimal exposure for management and is generally an anomaly. A significant deficiency usually indicates a history of internal control deficiencies that when consolidated equate to a reportable condition. A-123[9] defines the deficiencies as noted below:

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 ─ An internal control deficiency, or combination of internal 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

[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 Statement of Federal Financial Accounting Standard (SFFAS) No. 5, Accounting for Liabilities of the Federal Government, as the chance of the future event, or events, occurring is slight.

financial statements, or other significant financial reports, that is more than inconsequential[11] 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.

When reviewing test results, the Senior Assessment Team must consider the likelihood and degree of potential for misstatement in order to assign the level of deficiency to be reported. When all results have been reported, management can then make the determination if the consolidation of deficiencies are incidental, consolidate to create a reportable condition or rise to the level of material weakness for reporting in the assurance statement.

Reporting

Internal reporting

The Senior Assessment Team will decide based on their analysis of the findings and recommend which reportable conditions, when aggregated, may be deemed material weaknesses to the agency as a whole. Management will consider these deficiencies when recommending the level of assurance the agency head should provide on the internal control over financial reporting. By centralizing the reporting process, agencies will be able to better support their level of assurance on the effectiveness of internal control over financial reporting, as well as the FMFIA assurance statement.

Internal control deficiencies and reportable conditions that are not deemed material weaknesses to the agency, as a whole should be tracked internally. Corrective action plans should be developed and implemented. Management should review the progress against the corrective action plans periodically.

[11] 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 than inconsequential.

External reporting

Reporting required as of June 30 (including material weaknesses)

The agency is required to provide a statement of assurance over the effectiveness of internal controls over financial reporting as of June 30 of the fiscal year in the Performance and Accountability Report (PAR). The PAR is published after September 30 because it includes the agency's audited financial statements that are prepared using balances as of September 30. The assurance statement included in the PAR 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 controls over financial reporting are effective. The statement can be categorized as follows:
  - Unqualified – No material weaknesses noted
  - Qualified - Material weaknesses were noted, but not pervasive
  - Statement of No Assurance – No assessment process is in place or noted material weaknesses were pervasive.

Illustrative templates of the Annual Assurance Statement are provided in Exhibit 6 (pages 63-65) of this implementation guide.

The assurance statement related to the assessment performed under Appendix A acts as a subset of the Overall Statement of Assurance reported pursuant to Section 2 of the FMFIA legislation. Internal control over financial reporting is one of the three control objectives (i.e., effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations) assessed under FMFIA, Section 2. To create efficiencies in assessing internal control objectives management should integrate its assessment of operational and compliance controls with financial reporting controls assessed under Appendix A.

Reporting required as of September 30 (including material weaknesses)

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

Changes in status after June 30 but before September 30
(e.g., remediation activities, additional weaknesses)

Due to the differences in the timing of the assessment of internal control over financial reporting and reporting the results in the agency's PAR report, there is potential for a change in the status of the assessed effectiveness of internal control. 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 correction action taken, and that it has been resolved. Resolution can be reported if the control is in place for a sufficient period to be properly tested.
- 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.

To ensure accurate assessment and reporting of control effectiveness, agency management needs to develop a process to identify changes in the internal control environment that could potentially impact management's assessed effectiveness of internal control over financial reporting. To identify changes after June 30 agency management can:

- Survey management of material component units to identify any potential changes in the internal control environment that require assessment.
- Communicate with agency officials leading other departmental assessments, reviews, and audits to determine if any potential material weaknesses were identified that were not detected during the Appendix A assessment.
- Perform testing to validate the effectiveness of corrective actions if material weaknesses were reported as resolved.

Correcting Deficiencies and Weaknesses

Corrective Action Plans

The Senior Assessment Team will work with the responsible officials and personnel to determine which deficiencies are cost beneficial to correct. A corrective action plan, including targeted milestones and completion dates, will be drafted and progress will be monitored. Agency management may, at its discretion, track findings considered to be less than a reportable condition. Remediation plans for FFMIA and FMFIA may be included in the corrective action plans improving internal control over financial reporting.

The Senior Management Council will review and monitor the corrective action plans that have been approved by the Senior Assessment Team. The corrective action plans for material weaknesses should be drafted by the process owners and responsible officials. The Senior

Assessment Team will communicate the status of the corrective action plans developed for material weaknesses to the Senior Management Council on a regular basis. The Senior Management Council will be responsible for determining if the progress is sufficient or if additional action must be taken to expedite the remediation process. The Senior Management Council may delegate the authority to approve the proposed corrective action plans and remediation progress for deficiencies less than material weaknesses to the Senior Assessment Team. Corrective action plans will be updated on a periodic basis and made available to OMB at its request.

Deficiencies[12] exist when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, prevent or detect misstatements on a timely basis. Deficiencies are identified as a result of reviews performed pursuant to legislative and regulatory requirements that promote and support effective internal control including management's assessment of internal control over financial reporting.[13]

Once identified, agency managers are responsible for taking timely and effective action to correct the deficiency. Corrective action plans are the mechanism whereby management presents the procedures the agency will follow to resolve deficiencies. The extent to which corrective actions are tracked by the agency should be commensurate with the severity of the deficiency. The benefits of having well defined corrective actions plans include the following[14]:

- Consistency in addressing internal control deficiencies,
- Concurrence on remediation activities,
- Transparency in defining accountability and responsibility to ensure results are achieved, and
- Improved decision-making on the status of remediation activities.

To optimize effectiveness, corrective action plans should go beyond capturing and tracking actions to resolve deficiencies. Plans should include measurable indicators of compliance and resolution to assess and validate progress throughout the resolution cycle. In cases where clear measures are not available, comprehensive, or of sufficient quality, it may be acceptable to use qualitative measures (e.g., milestones or "proxies") to judge success in achieving desired outcomes. These qualitative indicators can be further strengthened when supported by peer reviews (e.g., expert panels or Inspectors General) or other means. For example, if an agency

---

[12] As defined in OMB Circular A-123 - Management's Responsibility for Internal Control, Section V, Exhibit 1

[13] As defined in OMB Circular A-123 - Management's Responsibility for Internal Control, Section III

[14] Deloitte, Taking Control A Guide to Compliance with Section 404 of the Sarbanes-Oxley Act of 2002

has a material weakness over financial management and reporting processes, the agency may identify a milestone when it completes standard operating procedures for reporting.

The procedures in and of themselves don't resolve the deficiency. Agency management should also perform follow-up control tests to verify whether the procedures and controls are working (e.g., measures to assure accurate postings and accounting). The follow-up control tests would become the indicators of compliance and could be further assessed by the expert panel (e.g., Senior Management Council) to validate effectiveness. By identifying measurable indicators, agency management and OMB have a common reference point to better assess progress and more rapidly make course corrections to ensure timely and effective resolution.

To facilitate corrective action plan preparation, accountability, monitoring, and communication, agencies are encouraged to construct a corrective action planning framework to facilitate stakeholder oversight and ensure accountability for results. This framework should address the needs of the agency personnel responsible for carrying out the resolutions tasks, agency leadership responsible for oversight, and external stakeholders (e.g., OMB). Therefore, agencies must prepare detailed plans that can be summarized for both internal and external reporting. Figure 1 illustrates a framework that agencies can use to facilitate stakeholder oversight and ensure accountability for results. The Corrective Action Framework can be applied to resolution efforts required by other federal statutes (e.g., Federal Financial Management Improvement Act of 1996, Improper Payments Information Act of 2002, Federal Information Security Management Act of 2002).

Figure 1, Corrective Action Framework

Corrective Action Document	Stakeholder Group	Corrective Action Timeframe	Measure
Executive Summary	• OMB • Agency Management	• Long-term • Annual	• Final Compliance Indicator(s) / Target(s)
Corrective Action Plan Management Summary	• OMB • Agency Senior Management Council	• Long-term • Annual • Short-term	• Mid-Term Compliance Indicator(s) / Target(s)
Detailed Corrective Action Plan	• OMB • Agency Senior Management Council • Agency Personnel	• Long-term • Annual • Short-term	• Short-Term Compliance Indicator(s) / Target(s)

A summarized executive summary plan (similar to an executive overview) should be reported in an agency's annual Performance and Accountability Report (PAR) in the Management's Discussion & Analysis under a new section entitled "Management Assurances." The agency

should also prepare and make available a management summary for use by internal management as well as for OMB review.

Lastly, the agency should prepare a comprehensive corrective action plan that lists the detailed actions that agency personnel must perform to resolve the weakness. These documents should tie together by sharing elements such as the following:

- A summary description of the deficiency,
- The year first identified,
- The targeted corrective action date (the date of management follow-up),
- The agency official responsible for monitoring progress,
- The indicators, statistics, or metrics used to gauge resolution progress (in advance of audit follow-up) to validate the resolution of the deficiency, and
- The quantifiable target or otherwise qualitative characteristic (e.g., milestone) that reports how resolution activities are progressing.

Each more detailed version of the corrective action plan should provide further detail of the elements identified above so that interim actions and progress can be monitored and progress assessed. For example, the management summary should include interim milestones together with subordinate indicator(s) or target(s) of compliance and resolution. Each agency should determine the final level of plan details, but in general, agencies may want to prepare the documentation such that the following is true:

- The PAR corrective action executive summary captures and reports activities from an annual timeframe,
- The management summary captures and reports activities from a quarterly timeframe, and
- The detailed corrective action plan such that it captures and reports activities from (at a minimum) a monthly timeframe.

Using this approach allows agencies to prepare a framework that distinguishes between short-term (e.g., monthly, quarterly), annual, and long-term objectives. Further, it supports other performance improvement initiatives such as the President's Management Agenda (PMA) where agencies' quarterly progress is measured relative to its achieving annual or longer-term goals and standards.

To implement this framework, the Senior Management Council, or similar forum(s), have ownership and accountability for resolving deficiencies. These forums should use the corrective action plans as a guide or roadmap for discussion as well as in determining when sufficient action has been taken to declare that a deficiency has been corrected. Examples of Senior Management Council oversight activities include the following:

- Ensuring timely corrective action plans are developed for all deficiencies identified by the Senior Assessment Team and auditors,
- Demonstrating commitment to resolving deficiencies as evidenced by resource deployment and frequent and regular monitoring of corrective action progress,
- Timely review of documented progress in completing corrective actions,
- Substantial validation of corrective action effectiveness,
- Assuming full responsibility for the remediation of deficiencies, and
- Determining whether corrective actions have been substantially completed, and the remaining actions are minor in scope and are scheduled to be completed within the next fiscal year.

Exhibits

EXHIBITS

Exhibit 1: Samples of Organizational Structure

A: Office of Personnel Management

In June 2004 the Office of Personnel Management (OPM) initiated an agency-wide internal control and risk management approach for ensuring that effective internal controls are in place. The OPM approach included the establishment of the Center for Internal Control and Risk Management (CICRM) within the Office of the Chief Financial Officer (OCFO). Further, the OPM approach includes the identification and assessment of risks on an integrated agency-wide basis that provides a proactive course to risk management aimed at focusing and directing attention on areas of high risk.

An Associate Chief Financial Officer, who reports directly to the Chief Financial Officer (CFO), heads the CICRM. The CICRM is focused at ensuring the establishment of and adherence to effective administrative and accounting controls within OPM, helping fulfill management's due diligence responsibilities and complementing the work of the Office of Inspector (OIG). Other significant responsibilities of the CICRM include: advising the Director, Associate Directors, Office Heads, and CFO on matters of internal control and risk management; serving as the agency's oversight manager for developing, evaluating, monitoring, and recommending internal controls and risk management policies and procedures; enhancing the agency's awareness of internal controls; conducting internal control reviews, evaluations and analyses of the agency's operations; and assisting OPM program offices in identifying, evaluating, monitoring, and managing their risks. The CICRM is taking a lead role in agency planning for and implementing the newly revised OMB Circular A-123, *Management's Responsibility for Internal Control*.

The CICRM consists of two groups comprised of 14 staff members: the Risk Management Group and the Audit Coordination Group. The Center staff is a diverse team, consisting of individuals with backgrounds in financial and performance auditing, information technology, management analysis, and procurement, with operational and oversight experience. The Risk Management Group is responsible for conducting reviews of program operations; assisting program offices in identifying risks and conducting internal control reviews; issuing reports of findings and making recommendations to improve internal controls and risk management; and conducting outreach activities to explore best practices found in the public and private sectors. The Audit Coordination Group serves as a liaison to the OIG on audits of agency operations; tracks and monitors audit follow-up and resolution activities; and maintains an early warning system for identifying problem areas, emerging trends, and systemic issues pertaining to internal controls and risk management.

Exhibit 1: Samples of Organizational Structure

B: Social Security Administration

SSA has an established organization responsible for oversight and coordinating many of the internal control monitoring activities, coordinating and updating the internal controls documentation, evaluating the sufficiency of the design of internal controls and supporting SSA's Senior Management Council referred to as the Executive Internal Control (EIC) Committee. To meet the spirit of the Senior Assessment Team concept introduced in the revised A-123, this organization within SSA has developed and plans to implement the Quarterly Monitoring Program (QMP).

The purpose of the QMP is to centralize the reporting and analysis of the monitoring activity results since no single organization performs all monitoring activities within SSA. By centralizing the reporting process, SSA will be able to better support its assessment of the design and operating effectiveness of the agency's internal controls.

Quarterly, personnel responsible for performing monitoring activities will summarize the results of their tests and report the findings to DFPS for evaluation. The design of certain monitoring activities conducted at SSA lend themselves to identifying deficiencies in control design as well as deficiencies in control operations. For example, the Financial Management System (FMS) Review Program ensures the integrity of the data processed by SSA's programmatic, debt management and financial systems using GAO's Federal Information Security Control Audit Manual (FISCAM). The review is conducted to provide an evaluation of the system to assess the processes used in designing and developing the system, the systems engineering and general management aspects of the system, the system's security measures, and the general and administrative controls relevant to the system, and the system's application controls and functions. The findings resulting from the FMS review program identify poorly designed controls, lack of controls and controls that are not operating correctly. Therefore, findings may include incidents of non-compliance with policies and procedures, problems or malfunctions reported, unexpected sample results, etc.

The oversight organization will assess all reported deficiencies to determine which of the three objectives of internal control have not been adhered to. The deficiencies will then be analyzed against the material weakness and reportable condition definitions for each objective of internal control contained in A-123.

On a quarterly basis, this organization will communicate the status of major monitoring activities and any information related to new internal control deficiencies to SSA's CFO, who is also a member of the EIC committee. The CFO will discuss the deficiencies and the recommended classifications with the EIC committee as needed. SSA's CFO is responsible for considering all deficiencies and all other relevant information when recommending the level of assurance the agency head should provide on the internal control over financial reporting as well as the overall FMFIA statement of assurance.

Exhibit 2: Sample Communication

A: CFO Announcement

From: CFO
Sent: [DATE]

To: MANAGEMENT OFFICIALS, OIG

Subject: CFO announcement of internal control review work

As noted in the [DATE] Senior Staff meeting, the agency is undertaking an important effort to identify key internal controls and to document and test them to determine whether they are operating effectively. The agency has placed a significant emphasis on internal controls in the past, and there are a number of initiatives underway to improve existing processes and systems. However, recent changes in OMB Circular A-123, Management's Responsibility for Internal Control, have caused the Office of Inspector General and the financial statement auditors to ask that we gather additional evidence to further support departmental and the agency Federal Managers Financial Integrity Act (FMFIA) statements. As a result, I have asked the [INTERNAL REVIEW DEPARTMENT] to make changes to our existing FMFIA process to include a risk assessment process (see below) and for them to engage a CPA firm (a competitive selection process is currently underway) to document and test controls relating to the 10 cycles that encompass the agency financial statements. While additional cycles may be added in subsequent years, as necessary, this year we will be focusing on the following 10 cycles:

Cycle	Department/Organization	Contact
Present Value of Future Benefits Liability	Insurance Operations Department Financial Operations Department	
Benefit Payments	Financial Operations Department Insurance Operations Department	
Benefit Determination	Financial Operations Department Insurance Operations Department	

Cycle	Department/Organization	Contact
Single-Employer Contingencies	Corporate Finance and Negotiations Department Corporate Policy and Review Department Financial Operations Department Insurance Operations Department Office of the General Counsel	
Losses from Completed and Probable Terminations	Financial Operations Department	
Non-Recoverable Future Financial Assistance	Insurance Operations Department Financial Operations Department Corporate Policy and Review Department Office of the General Counsel	
Premiums	Financial Operations Department Contracts and Controls Review Department	
Treasury/Investment	Financial Operations Department	
Financial Reporting	Financial Operations Department	
Budget	Budget Department Financial Operations Department All Other Departments	

Work will likely begin in late [MONTH] and will continue until all cycle evaluations are completed. Work on the Benefit Determination, Benefit Payments, and the Present Value of Future Benefits Liability cycles will have first priority, but it is expected that work will be done on all cycles concurrently. Some cycles only impact certain departments; however, all departments are impacted by the Budget cycle. Consideration of IT controls will also be a factor during the cycle evaluations.

The [INTERNAL REVIEW DEPARTMENT] will be responsible for oversight, coordination, and facilitation of this effort; however, it is important to note that the responsibility for internal

controls remains with individual department directors and managers. The [INTERNAL REVIEW DEPARTMENT] has dedicated staff for this effort; however, the support of departments will be needed with respect to interviews with personnel and gathering data in response to CPA firm requests. In advance of the contract award, you will be contacted by the [INTERNAL REVIEW DEPARTMENT] staff to obtain necessary background information. Please begin to assemble policies and procedures, past audit reports, process flowcharts, and other materials that would help the auditors gain an understanding of the cycles related to your applicable areas. Getting requested information on a timely basis will help the agency meet important reporting timeframes. You will be contacted by staff members of the [INTERNAL REVIEW DEPARTMENT] next week to answer any questions you may have. Our overall objective is for each department to submit their existing inventory of policies and procedures to the [INTERNAL REVIEW DEPARTMENT] not later than [DATE].

While this effort will provide input regarding whether the agency internal controls within these cycles are properly designed and operating effectively, it is also important for the agency to develop a risk assessment process so that we may be able to self-identify what changes are needed to our internal controls based on changes to the agency's internal environment (e.g., moving away from manual process to automated processes or implementing new systems) and changes to the agency's external environments (e.g., poor business outlook for a particular industry). Manager risk assessment is a fundamental component of an effective internal control structure. I have asked the [INTERNAL REVIEW DEPARTMENT] to make changes to the existing [MANAGEMENT CONTROL DIRECTIVE] and the FMFIA statement processes to include a risk assessment component. The [INTERNAL REVIEW DEPARTMENT] will be sending out an initial risk assessment questionnaire that is designed as a first attempt at gathering such data without requiring a significant amount of time. Further information on this effort will be forthcoming from the [INTERNAL REVIEW DEPARTMENT].

I ask that you support this important initiative to help ensure that our internal controls adequately safeguard the agency assets, provide for compliance with laws and regulations, and support the production of accurate and timely financial reports.

Exhibit 2: Sample Communication

B: Agency's Control Environment

From:	Deputy Director of [INTERNAL REVIEW DEPARTMENT]
Sent:	[DATE]
To:	Management
Cc:	Internal Control Project, Consultants
Subject:	Discussion Requested Regarding the Agency's Control Environment

Hello everyone…the [CONSULTANTS] have requested, as part of their effort in evaluating our internal controls, to meet with agency executives to discuss the agency's control environment - one of the five key components of an effective internal structure. The [CONSULTANT'S] partner and director will be conducting the interviews and would like to complete these interviews over the next two weeks. The interviews should most likely take either 1/2 hour or an hour at most. They will definitely want to interview those at the very high levels of management and will be interviewing selected department directors as well. They will contact your administrative assistants to determine your availability. If you have questions or any concerns, please let me know. Thanks.

As background information, an evaluation of the control environment generally focuses on things such as management's attitude or approach towards internal controls and compliance with laws and regulations, management philosophy and operating style, structure of the organization, etc. One example of a control environment factor is the existence of a Code of Ethics for management and employees. Such a document lets senior management communicate to its managers and employees that ethical business practices are valued. Additional information is included in the attachment:

ATTACHMENT

Control Environment Overview:

In order to foster a positive 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.

A positive control environment is the foundation for a sound system of internal controls. It provides discipline and structure as well as the climate which influences the quality of internal control. Several key factors affect the control environment. One factor is the **integrity and ethical values** maintained and demonstrated by management and staff. Agency management plays a key role in providing leadership in this area, especially in setting and maintaining the organization's ethical tone, providing guidance for proper behavior, removing temptations for unethical behavior, and providing discipline when appropriate. Another factor is management's **commitment to competence**. All personnel need to possess and maintain a level of competence that allows them to accomplish their assigned duties, as well as understand the importance of developing and implementing good internal control. Management needs to identify appropriate knowledge and skills needed for various jobs and provide needed training, as well as candid and constructive counseling, and performance appraisals.

Management's **philosophy and operating style** also affect the environment. This factor determines the degree of risk the agency is willing to take and management's philosophy towards performance-based management. Further, the attitude and philosophy of management toward information systems, accounting, personnel functions, monitoring, and audits and evaluations can have a profound effect on internal control. Another factor affecting the environment is the agency's **organizational structure**. It provides management's framework for planning, directing, and controlling operations to achieve agency objectives. A good internal control environment requires that the agency's organizational structure clearly define key areas of authority and responsibility and establish appropriate lines of reporting.

The environment is also affected by the manner in which the agency delegates **authority and responsibility** throughout the organization. This delegation covers authority and responsibility for operating activities, reporting relationships, and authorization protocols. Good **human capital policies and practices** are another critical environmental factor. This includes establishing appropriate practices for hiring, orienting, training, evaluating, counseling, promoting, compensating, and disciplining personnel. It also includes providing a proper amount of supervision.

A final factor affecting the environment is the agency's **relationship with the Congress and central oversight agencies such as OMB**. Congress mandates the programs that agencies undertake and monitors their progress and central agencies provide policy and guidance on many different matters. In addition, **Inspectors General and internal senior management councils** can contribute to a good overall control environment.

Exhibit 3: Key Business Processes Cross-walk to Material Financial Reporting Line Items (adapted from the GAO/PCIE Financial Audit Manual)

	Transaction-related Accounting Applications					Line Item/Account-related Accounting Applications					
Line Items or Accounts	**Billing**	**Cash Receipts**	**Purchasing**	**Cash Disbursements**	**Payroll**	**Cash**	**Accounts Receivable**	**Inventory**	**Property**	**Accounts Payable**	**Obligation**
Cash or FBw/T		X		X	X	X					
Accounts Receivable	X	X					X				
Inventory	X		X					X			
Property			X						X		
Liabilities			X	X						X	
Revenue	X										
Expenses			X		X						
Obligations			X	X							X

Exhibit 4: Account Risk Analysis (adapted from the GAO/PCIE Financial Audit Manual)

ENTITY: *XYZ Agency (XYZ)*

DATE OF FINANCIAL STATEMENTS: *9/30/XX*

LINE ITEM: Accounts Receivable - Net

ACCOUNT RISK ANALYSIS FORM

FILE: _____

PREPARER:_____
REGION: _____
DATE: _____

Page ____ of ____

PLANNING PHASE					EVALUATION PHASE			TESTING PHASE		
Account		Financial Statement Assertions/Risks	Inherent, Fraud, and Control Risk Factors	Cycle/ Accounting Application	Effectiveness of Control Design Activities	Control Risk	Combined Risk	Frequency Dates	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*
		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*

ENTITY: *XYZ Agency (XYZ)*

ACCOUNT RISK ANALYSIS FORM

PREPARER:_____
REGION: _____
DATE: _____

DATE OF FINANCIAL STATEMENTS: *9/30/XX*

FILE: _____

LINE ITEM: Accounts Receivable - Net

Page ____ of ____

PLANNING PHASE					EVALUATION PHASE			TESTING PHASE		
Account		Financial Statement Assertions/Risks	Inherent, Fraud, and Control Risk Factors	Cycle/ Accounting Application	Effectiveness of Control Design Activities	Control Risk	Combined Risk	Frequency Dates	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*

ENTITY: *XYZ Agency (XYZ)*

ACCOUNT RISK ANALYSIS FORM

PREPARER:_____
REGION: _____
DATE: _____

DATE OF FINANCIAL STATEMENTS: *9/30/XX*

FILE: _____

LINE ITEM: Accounts Receivable - Net

Page ____ of ____

PLANNING PHASE					EVALUATION PHASE			TESTING PHASE		
Account		Financial Statement Assertions/Risks	Inherent, Fraud, and Control Risk Factors	Cycle/ Accounting Application	Effectiveness of Control Design Activities	Control Risk	Combined Risk	Frequency Dates	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*
Line Item Total	*$876,000,000*	***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*

Exhibit 5: 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)

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.]

ENTITY: *XYZ Agency (XYZ)*

SPECIFIC CONTROL EVALUATION

PREPARER:_____
DATE OF FINANCIAL STATEMENTS: *9/30/XX*

FILE: _____

REGION: _____
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*		

ENTITY: *XYZ Agency (XYZ)*

SPECIFIC CONTROL EVALUATION

PREPARER:_____
DATE OF FINANCIAL STATEMENTS: *9/30/XX*

FILE: _____

REGION: _____
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*	

ENTITY: *XYZ Agency (XYZ)*

SPECIFIC CONTROL EVALUATION

PREPARER:_____
DATE OF FINANCIAL STATEMENTS: *9/30/XX*

FILE: _____

REGION: _____
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.

Exhibit 6A: Illustrative Template for a Statement of Assurance

Statement of Assurance

The [Agency's] 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 [Agency] 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 OMB Circular A-123, *Management's Responsibility for Internal Control*. Based on the results of this evaluation, the [Agency] 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, 2xxx was operating effectively and no material weaknesses were found in the design or operation of the internal controls.

In addition, the [Agency] 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 [Agency] can provide reasonable assurance that its 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 control over financial reporting.

Agency Head Signature

Date

Exhibit 6B: Illustrative Template for a Qualified Statement of Assurance

Statement of Qualified Assurance

The [Agency's] 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 [Agency] 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 [Agency] 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 OMB Circular A-123, *Management's Responsibility for Internal Control*. Based on the results of this evaluation, the [Agency] identified [number] material weakness(es) in its internal control over the effectiveness and efficiency of operations and compliance with applicable laws and regulations as of September 30, 2xxx. 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 [Agency] 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 [Agency] identified [number] material weakness(es) in its internal control over financial reporting as of June 30, 2xxx. 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 control over financial reporting.

Agency Head Signature

Date

Exhibit 6C: Illustrative Template When an Entity Cannot Provide a Statement of Assurance

Statement of No Assurance

The [Agency's] 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 [Agency] is unable to provide 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 [Agency] conducted its assessment of the effectiveness of internal control in accordance with OMB Circular A-123, *Management's Responsibility for Internal Control*. Based on the results of this evaluation, the [Agency] identified [number] material weakness(es) in its internal control over the effectiveness and efficiency of operations and compliance with applicable laws and regulations as of September 30, 2xxx. 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 [Agency] 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 [Agency] did not fully implement the requirements included in OMB Circular A-123 and therefore cannot provide assurance that its internal control over financial reporting as of June 30, 2xxx was operating effectively. A summary of actions the [Agency] will take to comply with the Circular A-123 requirements is included in Exhibit [xx].

Agency Head Signature

Date