

**U.S. Department of Veterans Affairs**

**Office of Business Oversight (OBO)  
Internal Controls Service (ICS)**

**Internal Control Stakeholder Procedures Manual**

**April 2009**



## Introductory Letter

The U.S. Department of Veterans Affairs (VA) is fully committed to the principles of the revised Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Internal Control and to the timely and effective implementation of this guidance. Strengthening Agency-wide internal control is a critical component of our financial management improvement strategy. Everyone within VA is responsible for internal control.

VA has adopted the guidance of the Chief Financial Officers Council (CFOC) in developing its A-123, Appendix A, program. The CFOC is comprised of Federal Agency CFOs and Deputy CFOs, as well as representatives from OMB and Treasury. In July 2005, the CFOC published its Implementation Guide for OMB Circular A-123, Appendix A, to provide guidance to agencies in understanding the requirements of the Circular and in implementing a process for assessing the effectiveness of their internal control over financial reporting. While the activities in the guide are not necessarily required, they are widely accepted as a valid approach and provide a useful roadmap for executing the requirements of A-123, Appendix A.

As recommended by the CFOC, VA has established a Senior Assessment Team (SAT). The SAT, chaired by the Assistant Secretary for Management (CFO), provides oversight and accountability for VA's internal control over financial reporting. The Office of Business Oversight (OBO), Internal Controls Service (ICS), is responsible for designing and maintaining an internal controls monitoring program. Other key stakeholders include the Strategic Management Council (SMC), Process Owners and Process Owner Liaisons.

This procedures manual describes the roles and responsibilities of the various VA stakeholders for implementing the requirements of the revised Circular. The activities covered in this manual relate to VA Directive 0071 which sets forth the policies, responsibilities, and authority of VA officials and organizations for the management and oversight of internal control over financial reporting. This manual expands upon the roles outlined in the Directive and provides specific templates and instructions for each stakeholder group to carry out its assigned responsibilities. We are proud of our progress to date in implementing the requirements of A-123, Appendix A. We hope that the tools and instructions contained within this manual will continue to promote fiscal accountability.

Sincerely,

Robert J. Henke  
U.S. Department of Veterans Affairs  
Assistant Secretary for Management

## Contact Information

Joseph W. Bauernfeind  
Director of Office of Business Oversight  
810 Vermont Avenue  
Washington, D.C. 20420  
(202) 461-6420

Roger Drye  
Director of Internal Controls Service  
1701 Directors' Blvd.  
Suite 900  
Austin, Texas 87844  
(512) 438-6208

Marios Parpounas  
Associate Director for Financial Controls Division  
1701 Directors' Blvd.  
Suite 900  
Austin, Texas 87844  
(512) 438-6218

## Purpose and Objectives

The purpose of this A-123, Appendix A, procedures manual is to define the roles, responsibilities coordination, communication, and processes for A-123, Appendix A, stakeholders. This manual was developed by the U.S. Department of Veterans Affairs (VA), Office of Business Oversight (OBO), Internal Controls Service (ICS) for internal VA distribution to stakeholders including the Senior Assessment Team (SAT), Management and Quality Assurance Service, Chief Information Officers, Process Owner Liaisons, Process Owners, program managers, Administration CFOs, and other relevant parties. There are three primary objectives of this manual:

- To document standard processes and procedures that - in conjunction with the annual Appendix A Annual Review Plan - will guide the conduct of the entire lifecycle of A-123, Appendix A, activities
- To provide a standard set of tools and templates for use during the A-123, Appendix A, assessment
- To document the agreed-upon governance for A-123, Appendix A, activities, including roles and responsibilities, coordination, and communication

In developing this manual, ICS has drawn upon A-123 guidance from the Office of Management and Budget (OMB) and the Chief Financial Officers Council (CFOC).

This manual contains introductory sections and is then organized by assessment phase - Planning; Evaluating; Testing; Concluding, Internal Reporting, and Correcting; and External Reporting. Appendix G contains a Stakeholder Responsibility Matrix and is organized by stakeholder, rather than phase.

# Table of Contents

<u>Section</u>	<u>Page</u>
<b>Background .....</b>	<b>6</b>
<b>Objectives of Internal Control over Financial Reporting .....</b>	<b>7</b>
<b>Guidance for Performing A-123 Activities by Phase.....</b>	<b>8</b>
<b>I: Planning .....</b>	<b>14</b>
I.1 Establish organizational structure.....	14
I.2 Identify significant financial reports.....	15
I.3 Update Master Process List .....	16
I.4 Conduct quantitative analysis .....	17
I.5 Confirm/update KFPs that generate material and immaterial line items.....	20
I.6 Recommend in-scope KFPs (material).....	20
I.7 Conduct qualitative analysis (risk assessment) .....	21
I.8 Recommend Administrations/Programs/Locations .....	25
I.9 Identify financial reporting assertions .....	28
I.10 Consider cross-servicing entities: customers and providers.....	31
I.11 Integrate and coordinate with other control-related activities .....	37
I.12 Determine assurances needed from components.....	38
I.13 Plan for an updated assurance statement in the Performance and Accountability Report (PAR).....	39
Planning: Inputs and Outputs.....	42
<b>II: Evaluating .....</b>	<b>46</b>
II.1 Evaluate internal control at the entity level.....	47
II.2 Evaluate internal control at the KFP level .....	49
II.3 Understand IT structure and associated risks .....	67
<b>III: Testing.....</b>	<b>72</b>
III.1 Develop Test Plan .....	72
III.2 Test key controls .....	76
<b>IV: Concluding, Internal Reporting, and Correcting.....</b>	<b>83</b>
IV.1 Conclude on control effectiveness.....	83
IV.2 Correct Findings .....	88
IV.3 Monitor CAPs and verify completion.....	88
<b>V.1 Report externally.....</b>	<b>90</b>
<b>Appendices.....</b>	<b>93</b>
<b>Appendix A – CFOC Guide Crosswalk to Procedures Manual .....</b>	<b>93</b>
<b>Appendix B – Glossary of Acronyms .....</b>	<b>95</b>
<b>Appendix C – Glossary of Terms .....</b>	<b>96</b>
<b>Appendix D – The Five Standards of Internal Control.....</b>	<b>104</b>
<b>Appendix E – Information Processing Objectives/CAVR .....</b>	<b>113</b>
<b>Appendix F – Flowchart Instruction.....</b>	<b>114</b>
<b>Appendix G – Stakeholder Responsibility Matrix.....</b>	<b>116</b>
<b>Appendix H – Alternative Procedures for Evaluating Controls of Cross-Servicing         Providers .....</b>	<b>117</b>

Appendix I – Risk-Based Testing .....	119
Appendix J – Testing Types .....	120
Appendix K – Organizational Structure .....	122
Appendix L – Detail Framework for Evaluating Control Exceptions and Deficiencies	124
Appendix M – Templates and Checklists .....	139
Appendix N – Sample Narrative and Flowchart.....	141
Appendix O – Risks and Control Objectives.....	146
<b>Template Appendices.....</b>	<b>152</b>
Appendix 1 - Financial Statement Assertions Template .....	153
Appendix 2 - RCM Template .....	154
Appendix 3 - Location Selection Recommendations Template .....	155
Appendix 4 - SAS 70 Assessment Checklist.....	156
Appendix 5 - GCC Template .....	157
Appendix 6 - Documentation Quality Control Checklist .....	158
Appendix 7 - KFP-Level Test Plan Template.....	159
Appendix 8 - Evidence Request List Template .....	160
Appendix 9 - Test Sheet .....	161
Appendix 10 - Exception Log Template.....	162
Appendix 11 - Testing Quality Review Checklist.....	163
Appendix 12 - Finding Outline Worksheet.....	164
Appendix 13 - Corrective Action Plan Template .....	165

## Background

Federal managers have been subject to internal control reporting requirements for many years. Major Federal internal control-related laws and regulations include the Federal Managers' Financial Integrity Act of 1982 (FMFIA) (Pub. L. No. 97-255) and OMB Circular A-123, which require agencies to establish and maintain internal control. The agency head should annually evaluate and report on the control and financial systems that protect the integrity of Federal programs. The requirements of FMFIA serve as an umbrella under which other reviews, evaluations, and audits should be coordinated and considered to support management's assurances on the effectiveness of internal control. OMB A-123, Appendix A, mandates a specific methodology for assessing internal controls over financial reporting and details management's responsibility for the following:

- **Establishing a Senior Assessment Team.** The Circular encourages VA to establish a senior assessment team that includes senior executives and derives its authority and support from the head of the agency or the Chief Financial Officer. The senior assessment team is responsible for oversight over the assessment process. (Planning Phase)
- **Evaluating Internal Control at the Entity Level.** The Circular requires VA to evaluate the five Components of internal control that have an overarching or pervasive effect on VA. (Evaluating Phase and Appendix D)
- **Evaluating Internal Control at the Key Financial Process Level.** The Circular requires VA to evaluate the design and operating effectiveness of controls at the account, disclosure, and related process level (including transactions and systems). (Evaluating Phase)
- **Documenting Controls and Assessing their Effectiveness.** The Circular requires VA to document VA's internal controls over financial reporting, test their effectiveness, and identify deficiencies. (Evaluating Phase, Testing Phase and Concluding, Internal Reporting and Correcting Phase)
- **Reporting Management's Assurance in the Annual Performance and Accountability Report (PAR).** The Circular requires VA's management to include an assurance statement on the effectiveness of internal control over financial reporting in its annual PAR. (External Reporting Phase)
- **Correcting Material Weaknesses.** The Circular requires VA to ensure the prompt and proper resolution and implementation of corrective action on identified material weaknesses. (Concluding, Internal Reporting, and Correcting Phase)

## Objectives of Internal Control over Financial Reporting

Internal control over financial reporting is intended to provide reasonable assurance regarding the reliability of financial reporting. Internal controls are important because they prevent a loss or misuse of government assets. Financial reporting starts at the initiation of a transaction and ends with the reporting. Therefore, internal controls over the transaction process involve controls around specific processes at every step including the controls over transaction initiation, maintenance of records, recording of transactions, and final reporting. In addition, they also include the prevention/detection of unauthorized acquisition, use, or disposition of VA's assets in relation to the transaction. Personnel at all levels of VA are therefore responsible for implementing and carrying out internal controls as part of their daily operations.

Reliability of financial reporting means that management can reasonably make the following assertions:

- The financial report is presented in the proper form and any required disclosures are present (presentation and disclosure (PD))
- All reported transactions actually occurred during the reporting period and all assets and liabilities exist as of the reporting date (existence and occurrence (EO))
- All assets are legally owned by VA and all liabilities are legal obligations of VA (rights and obligations (RO))
- All assets, liabilities, and transactions that should be reported have been included and no unauthorized transactions or balances are included (completeness (CO))
- All assets and liabilities have been properly valued, and where applicable, all costs have been properly allocated (valuation (VA))

In addition to the above assertions, OMB Circular A-123 establishes the following assertions as they relate to reliability of financial reporting:

- The transactions are in compliance with applicable laws and regulations (LR)
- All assets have been safeguarded against fraud and abuse
- Documentation of internal control, all transactions, and other significant events is readily available for examination

Defining VA's internal controls in terms of these objectives will be the basis to support the Secretary's assurance statement on the effectiveness of internal control over financial reporting included as a subset to section 2 of FMFIA reporting.

## Guidance for Performing A-123 Activities by Phase

VA has adopted the guidance of the Chief Financial Officers Council (CFOC) in developing its A-123, Appendix A, program. The CFOC is comprised of Federal Agency CFOs and Deputy CFOs, as well as representatives from OMB and Treasury. In July 2005, the CFOC published its Implementation Guide for OMB Circular A-123, Appendix A, to provide guidance to assist agencies in understanding the requirements of the Circular and in implementing a process for assessing the effectiveness of their internal control over financial reporting. While the activities in the guide are not necessarily required, they are widely accepted as a valid approach and provide a useful roadmap for executing the requirements of A-123, Appendix A. The CFOC defines five basic steps which can be grouped into the following four phases:

- **Planning.** During this phase, management defines the scope of the assessment and documents key decisions.
- **Evaluating.** This phase involves understanding and documenting key financial processes (KFPs), identifying key controls, evaluating the design of controls, and conducting an entity-level control assessment.
- **Testing.** This phase involves assessing the operating effectiveness of key controls.
- **Concluding, Reporting, and Correcting.** During this phase, the assessment team disseminates the assessment results for internal and external reporting, and works with stakeholders to correct and monitor deficiencies identified during the Evaluating or Testing Phases.

This manual addresses each of the four phases covered in the Guide and the key activities performed within each phase. The activities have been reordered to better reflect the order in which they are typically performed. Appendix A of this guide provides a crosswalk between the CFOC Guide and this manual. Additionally, VA has included a fifth phase on External Reporting. While this is described in Phase IV of the CFOC Guide, it is included as a separate section in this manual for clarity and flow.



The table below provides an overview of the phases and key activities:

Phase	Overview	Key Activities
Planning	The Planning Phase involves a top-down approach to determine the documentation necessary and the nature, timing, and extent of testing of controls to be performed for each significant line item and related account, disclosure, and key financial process. During this phase, the assessment team will develop an Appendix A Annual Review Plan which clearly addresses scoping decisions.	<ul style="list-style-type: none"> <li>▪ Establish organizational structure</li> <li>▪ Determine scope of significant reports</li> <li>▪ Determine materiality</li> <li>▪ Conduct risk assessment</li> <li>▪ Plan for an updated assurance statement in the PAR</li> </ul>
Evaluating	The purpose of the Evaluating Phase is to gain an understanding of entity level controls and key financial processes (KFP). At the KFP level, the assessment team will document KFPs, identify key controls, and evaluate the design of controls.	<ul style="list-style-type: none"> <li>▪ Evaluate internal control at the entity level</li> <li>▪ Evaluate internal control at the KFP level <ul style="list-style-type: none"> <li>- Document KFPs and controls</li> <li>- Evaluate control design</li> <li>- Evaluate the controls of cross-servicing providers</li> </ul> </li> <li>▪ Understand IT infrastructure and associated risks</li> </ul>
Testing	The purpose of the Testing Phase is to assess the operating effectiveness of the controls to ensure that they are properly designed.	<ul style="list-style-type: none"> <li>▪ Develop Overall Test Plan</li> <li>▪ Test key controls <ul style="list-style-type: none"> <li>- Develop process-level test plans</li> <li>- Identify control gaps</li> </ul> </li> </ul>
Concluding, Internal Reporting, and Correcting	This phase of the assessment describes the process for evaluating test results, classifying deficiencies, reporting to internal and external stakeholders, correcting weaknesses, and monitoring corrective action activities.	<ul style="list-style-type: none"> <li>▪ Conclude on control effectiveness</li> <li>▪ Report control weaknesses</li> <li>▪ Correct deficiencies and weaknesses</li> <li>▪ Monitor corrective action plans</li> </ul>
External Reporting	This phase involves communicating the assessment results in the Statement of Assurance in the Performance and Accountability Report (PAR).	<ul style="list-style-type: none"> <li>▪ Complete Statement of Assurance</li> </ul>

The following ***Responsibility Assignment Matrix (RAM)*** identifies the party responsible for leading the performance of each step as well as other parties that should participate in completing each step. Appendix G includes similar information but is organized by Stakeholder.

WBS #	Phase or Task Name		Secretary	SMC	CFO	SAT	OBO/ICS	VA personnel	PO Liaisons	Process Owners
<b>Key:</b> ⊗ - Responsible X - Involved										
<b>I</b>		<b>Planning</b>								
1		<b>Establish organizational structure</b>	X	X	X	X	⊗			
2		<b>Identify significant financial reports</b>				X	⊗			
3		<b>Update Master Process List</b>				X	⊗			
4		<b>Conduct quantitative analysis</b>								
	1	Calculate materiality				X	⊗			
	2	Apply materiality to financial statement line items				X	⊗			
	3	Identify material line items				X	⊗			
	4	Identify immaterial line items				X	⊗			
5		<b>Confirm/update KFPs that generate material and immaterial line items</b>				X	⊗			
6		<b>Recommend in-scope KFPs (material)</b>				X	⊗			
7		<b>Conduct qualitative analysis (risk assessment)</b>								
	1	Identify qualitative risk factors				X	⊗			
	2	Assess risks associated with immaterial KFPs				X	⊗			
	3	Recommend additional in-scope KFPs				X	⊗			
8		<b>Recommend administrations/programs/locations</b>				X	⊗			
9		<b>Identify financial reporting assertions</b>				X	⊗			
10		<b>Consider cross-servicing entities: customers and providers</b>								
	1	Determine whether a service organization is being used				X	⊗			
	2	Determine whether the outsourced activities, processes, and functions generate the significant line items				X	⊗			
	3	Determine whether an annual assurance statement or a SAS 70 exists and is sufficient in scope				X	⊗			
	4	Plan for alternative procedures if an Annual Assurance Statement or SAS 70 does not exist				X	⊗			
11		<b>Integrate and coordinate with other control-related activities</b>				X	⊗			
12		<b>Determine assurances needed from components</b>				X	⊗			
13		<b>Plan for an updated assurance statement in the Performance and Accountability Report (PAR)</b>		X		X	⊗			
<b>II</b>		<b>Evaluating</b>								
1		<b>Evaluate internal control at the entity level</b>								

WBS #	Phase or Task Name	Secretary	SMC	CFO	SAT	OBO/ICS	VA personnel	PO Liaisons	Process Owners
<b>Key:</b> ⊗ - Responsible X - Involved									
	1	Develop assessment tool				⊗			
	2	Identify sample				⊗			
	3	Administer assessment				⊗			
	4	Analyze and report results			X	⊗			
<b>2</b>		<b>Evaluate internal control at the process level</b>							
	1	Document business processes and key controls							
	1	Gather information				⊗	X	X	X
	2	Develop narratives				⊗	X	X	X
	3	Develop flowcharts				⊗	X	X	X
	4	Develop risk/control matrices				⊗			X
	5	Perform quality control activities				⊗		⊗	⊗
	6	Retain documentation				⊗			⊗
	2	Identify key controls				⊗		X	X
	3	Evaluate control design				⊗			X
	4	Evaluate the controls of cross-servicing providers and service organizations							
	1	Assess results of SAS 70 reports				⊗	X		X
	2	Perform alternate procedures				⊗	X		X
<b>3</b>		<b>Understand IT structure and associated risk</b>							
	1	Assess general computer controls				⊗	X		X
	2	Assess application controls				⊗	X		X
<b>III</b>		<b>Testing</b>							
	1	<b>Develop test plan</b>							
	1	Determine which controls will be tested			X	⊗			
	2	Identify who will perform the testing			X	⊗			
	3	Determine when testing will be performed			X	⊗			
	4	Determine where testing will be performed			X	⊗			
	5	Determine how controls will be tested (inquiry, inspection, observation, re-performance)			X	⊗			
	6	Define sample sizes			X	⊗			
	7	Determine what testing documentation (workpapers) will be developed and retained			X	⊗			
<b>2</b>		<b>Test key controls</b>							

WBS #	Phase or Task Name	Secretary	SMC	CFO	SAT	OBO/ICS	VA personnel	PO Liaisons	Process Owners
<b>Key:</b> ⊗ - Responsible X - Involved									
	1	Develop process-level test plans				⊗			
	2	Request evidence				⊗			
	3	Conduct tests				⊗			
<b>IV</b>		<b>Concluding, Internal Reporting, and Correcting</b>							
	1	Conclude on control effectiveness			⊗	X			X
	<b>2</b>	<b>Correct findings</b>							
	1	Prepare CAPs				X	X	X	⊗
	2	Review CAPs			X	⊗			
	3	Implement corrective actions				X	X	X	⊗
	<b>3</b>	<b>Monitor CAPs and verify completion</b>							
	1	Monitor correction action efforts			X	⊗		X	X
	2	Report CAP status to SAT			X	⊗		X	
	3	Conduct verification				⊗		X	
	4	Conduct validation				⊗			
<b>V</b>		<b>External Reporting</b>	X	X	X	⊗	X		

**I: Planning**

# I: Planning

Planning is a key component of developing and implementing an internal control assessment. During this phase, management will make key recommendations that drive the assessment process. Management will determine the scope of the assessment, materiality thresholds, roles and responsibilities, testing locations, and schedules. The decisions made during the Planning Phase impact future activities in the remaining phases. Senior management and the SAT have primary responsibility for conducting Planning Phase activities with significant input from ICS.

Developing a comprehensive Appendix A Annual Review Plan is critical to the success of an assessment. This plan will help management document its assessment approach and communicate to stakeholders both within and outside of VA. A detailed plan uses a top-down approach, includes an analysis of qualitative and quantitative factors, and addresses materiality, cross-service entities, site rotation schedules, and financial statement assertions. According to the CFOC guide, the plan should also include the following elements:

- Description of the SAT, its authority and members
- Plans to use contractors to perform or assist in the assessment
- Strategy for communicating with VA management and employees regarding the assessment
- Key planning decisions of the SAT<sup>1</sup>

Activities I.1 through I.11 provide details on items that will be included in VA's final Appendix A Annual Review Plan. The following table illustrates the required inputs and key outputs of the Planning Phase.

Activities / Steps	Inputs	Key Outputs
I. Planning (i.e., Develop Appendix A Annual Review Plan) - all steps	<ul style="list-style-type: none"> <li>▪ Risk assessments / Analyses</li> <li>▪ Management Recommendations and SAT Decisions</li> </ul>	Appendix A Annual Review Plan (with detailed appendices)

IT control reviews are performed by several groups within VA for compliance with various regulatory and/or internal VA audit requirements (i.e., OMB A-127, OMB A-123, FISMA etc.). Each group performs separate planning activities and administers separate corrective action monitoring and effectiveness review programs. Recognizing that there is some opportunity for coordination between these groups, VA will conduct an annual planning session with the various groups that provide oversight for and/or perform IT controls review activities. In addition to ICS, these groups will include VA's System Quality Assurance Service (SQAS), and the Office of Information and Technology (OI&T).

\* \* \* \* \*

## I.1 Establish organizational structure

The establishment of a clear organizational structure demonstrates senior management support for the internal controls assessment process. The organizational structure clearly identifies VA

---

<sup>1</sup> CFOC Implementation Guide for A-123, Appendix A, page 21

stakeholder groups, their primary role in the assessment, and the reporting relationships of each group to the others. Because an organizational structure already exists (Appendix K), management will confirm that no changes will be made for the current assessment period. ICS will document the organizational structure in the Appendix A Annual Review Plan.

\* \* \* \* \*

## I.2 Identify significant financial reports

A top-down approach will be used in planning the assessment of internal controls over financial reporting. This type of approach starts with the significant VA-wide financial reports and works back to the key financial processes, controls, and supporting documentation. A top-down approach helps focus the assessment on the items that are most material and pose the greatest risk to the Department. The SAT has primary responsibility for determining the scope of financial reporting and the material line items to be tested, but will likely seek input and assistance from ICS. The SAT has the flexibility to determine which financial reports are significant.

At a minimum, the following reports will be considered significant:

- Annual Financial Statements
  - Consolidated Balance Sheet
  - Consolidated Statement of Net Cost
  - Consolidated Statement of Changes in Net Position
  - Combined Statement of Budgetary Resources
  - Notes to the Consolidated Financial Statements
- Quarterly Financial Statements (Quarter 4 only)
  - Consolidated Balance Sheet
  - Consolidated Statement of Net Cost
  - Combined Statement of Budgetary Resources

VA may also consider including budget execution reports if such reports are particularly significant to VA operations or if management feels the reports may relate to control issues. The following budget execution reports may be included:

- SF – 132 – Apportionment and Reapportionment Schedule
- SF – 133 – Report on Budget Execution and Budgetary Resources
- P&F Schedule – Budget Program and Financing
- FMS 2108 – Year End Closing Statement

In order to identify the significant reports, management will complete the following steps:

- **Develop scoping recommendations and present to SAT**

ICS will prepare recommendations on which reports are significant to VA. The Director of ICS will share these recommendations with the SAT.

- **Review and approve significant reports**

The SAT will review the recommendations provided by ICS and determine if additional reports should be included or recommended reports should be excluded.

- **Document decisions in Appendix A Annual Review Plan**

Final determination of significant financial reports will be clearly documented in the Appendix A Annual Review Plan.

\* \* \* \* \*

### I.3 Update Master Process List

ICS will update VA's Master Process List of key financial processes that have an impact on financial reporting. A key financial process (KFP) is any sequence of transactions that enables an entity to complete tasks and achieve its objectives.

- **Review Master Process List**

ICS will obtain the Master Process List from the previous fiscal year and review the list of KFPs included on the list. ICS will confirm the activities that generate the balance of each line financial statement line item. A portion of the Master Process List is shown below. Note that this framework should be applied to all in-scope financial statements (as determined in Activity I.2).

Financial Statement Account Category				
Statement Line Item Number		VA Component		
		Key Financial Process		
1				<b>INTRA-GOVERNMENTAL ASSETS</b>
1	1			Fund Balance with Treasury
1	1	1	1	Medical Care
1	1	2	1	Compensation and Benefits
1	2			Investments
1	2	2	1	Insurance
1	3	1	1	Other Assets
2				<b>PUBLIC ASSETS</b>
				.....
				.....

*Master Process List*

- **Update list (if needed)**

ICS will also review the Department's structure to verify that any group's activities which impact the financial statements are included within a KFP. ICS will update the Master Process List. The Director of ICS should be consulted regarding any changes to the list.

- **Create/confirm numbering scheme**

ICS has assigned a reference number to each KFP, as indicated on the ICS Master Process List. The reference numbers will be used during the documentation, testing, and reporting phases to link related information.

\* \* \* \* \*

## I.4 Conduct quantitative analysis

VA will consider both qualitative and quantitative factors when identifying significant line items and determining KFPs. Quantitative analysis involves measuring the financial significance of an amount, transaction, or discrepancy. OMB Circular A-123 defines materiality for financial reporting in the following terms:

"The risk of error or misstatement that could occur in a financial report that would impact management's or users' decisions or conclusions based on such report"<sup>2</sup>

### I.4.1 Calculate Materiality

From a quantitative perspective, materiality has four components: a materiality base; planning materiality; design materiality; and A-123 materiality.<sup>3</sup> Design materiality is used to determine the A-123 materiality.

- **Calculate materiality**

ICS will calculate and document each component of materiality.

- **Materiality Base.** The materiality base is the element of the financial statements or report that is most significant to the primary users of the statements. The materiality base should generally be the greater of total assets or expenses (net of adjustment for intra-governmental balances and offsetting balances). Other materiality bases that might be considered include total liabilities, revenues, and appropriations. The Department will confirm its materiality base selection with the OIG and external auditors.

For the purposes of calculating materiality, VA will use its prior fiscal year consolidated financial statements. If current year balances are expected to be significantly different from prior year balances, the Department will estimate the year-end balance of the line item used as the materiality base. For example, VA may choose Intra-governmental Assets as its materiality base.

Materiality Base	Reported FY 2006
Intra-governmental assets	\$29,162

- **Planning Materiality.** Planning materiality is a preliminary estimate of materiality in relation to the consolidated financial statements. Planning materiality is used to assess whether aggregated misstatements at the level of individual significant line items (and, similarly, the aggregated deficiencies in an audit of internal control) are material to the consolidated financial statements.

Planning materiality is generally 3% of the materiality base<sup>4</sup>; however, management will use judgment in evaluating whether the computed level is appropriate. The assessment team will consider adjusting the materiality base for the impact of such items as unfunded liabilities, contingencies, and other items that may not be reflected in the materiality base but that may be important to the financial statement user.

---

<sup>2</sup> OMB Circular A-123, page 23.

<sup>3</sup> Definitions adapted from the GAO/PCIE Financial Audit Manual, section 230.

<sup>4</sup> GAO/PCIE Financial Audit Manual, section 230.

Planning materiality is calculated from the materiality base:

Base	Factor	Planning Materiality
Intra-governmental Assets \$29,162	3%	\$875

- **Design Materiality.** Design materiality is the portion of planning materiality that has been allocated to line items and related accounts and disclosures. To provide an allowance for the aggregation of misstatements across individual accounts and for detection risk (the risk that controls will fail to detect a material misstatement), the GAO/PCIE Financial Audit Manual recommends that design materiality be one-third (33.3%) of planning materiality.

Continuing with the example above, design materiality is calculated as follows:

Base	Factor	Design Materiality
Planning Materiality \$875	33.3%	\$292

ICS will document planning materiality and design materiality levels along with the rationale behind the levels.

- **A-123 Materiality.** The GAO/PCIE recommends that A-123 materiality (Testing Materiality) be equal to or less than Design Materiality. Many Federal Agencies calculate A-123 Materiality as 75% of Design Materiality. A-123 materiality can then be calculated as follows:

Base	Factor	A-123 Materiality
Design Materiality \$292	75%	\$219

When identifying significant line items, ICS will disaggregate the components of line items and related footnote disclosures to determine whether any of the components are individually significant. For example, the “Other Assets” line item on the consolidated balance sheet may include multiple accounts or classes of transactions which are connected to different risks or controls. In this case, these accounts/components should be assessed separately. Other examples include the following:

- Revenue streams having different characteristics (e.g., product revenues versus fee revenues)
- Contract-driven service fees versus expenses for materials and supplies.

If any of these components exceed the design materiality threshold, it should be considered significant, even though it is not separately presented in the financial statements.

- **Review materiality (Director of ICS and SAT)**

The Director of ICS will review the materiality calculation and supporting documentation and will present it to the SAT. The SAT may consider confirming the calculation with the independent auditor and/or the OIG. ICS will update the calculation based on any feedback, and then request concurrence from the SAT. (Note that the materiality documentation is

formally approved by the SAT as part of their review of the Appendix A Annual Review Plan.)

- **Document materiality in Appendix A Annual Review Plan**

ICS will document the approved materiality calculation in the Appendix A Annual Review Plan.

### **I.4.2 Apply materiality to financial statement line items**

ICS will apply materiality to financial statement line items in order to identify the significant line items. Each line item on each in-scope financial statement will be compared with the materiality level determined in the previous section.

The following table shows an example of *a portion of* the consolidated balance sheet. The example compares each line item to the \$219 materiality threshold calculated in the previous section and indicates whether the line item is significant.

<b>Consolidated Balance Sheet</b>		
<b>As of September 30, 2006</b>		
(In Millions of Dollars)		
<b>Assets</b>	<b>2006</b>	<b>Material?</b>
Intra-governmental Assets		
Fund Balance with Treasury	16,129	<b>Yes</b>
Investments	12,873	<b>Yes</b>
Accounts Receivable, Net	107	<b>No</b>

- **Apply the materiality threshold to all in-scope financial statements**

ICS will compare the materiality threshold to each line item in order to identify significant line items. Each line item on each in-scope financial statement will be compared with the materiality level determined

### **I.4.3 Identify material line items**

Using the results of Activity I.4.2, ICS will compile a list of material financial statement line items.

### **I.4.4 Identify immaterial line items**

Using the results of Activity I.4.2, ICS will compile a list of immaterial financial statement line items. The purpose of this list is to ensure that the immaterial line items are considered as part of the qualitative risk assessment (see Activity I.7).

\*\*\*\*\*

## I.5 Confirm/update KFPs that generate material and immaterial line items

In Activity I.3, ICS updated the Master Process list to indicate which process(es) correspond to each line item. ICS will now review the Master Process List and focus on the material line items.

In order to confirm the KFPs that will be documented and assessed as part of the A-123, Appendix A, assessment, VA must confirm which KFPs generate the balances in the significant line items. The Master Process List (list of KFPs) is a key source of data for completing this mapping.

- Obtain updated Master Process List

Financial Statement Account Category			
Statement Line Item Number			
VA Component			
Key Financial Process			
1			INTRA-GOVERNMENTAL ASSETS
1	1		Fund Balance with Treasury
1	1	1	Medical Care
1	1	2	Compensation and Benefits
1	2		Investments
1	2	2	Insurance
1	3	1	Other Assets
2			PUBLIC ASSETS
			.....
			.....

- List KFPs that generate material line items

ICS will compare the list of material line items (from Activity I.4.3) with the Master Process List to determine which processes are in-scope (based on materiality).

\* \* \* \* \*

## I.6 Recommend in-scope KFPs (material)

Once ICS staff have determined the material line items and the processes that correspond to those line items, they should share the list with the Director of ICS and document the list of materially significant KFPs in the Appendix A Annual Review Plan. This list represents the *material* KFPs that will be in scope for the current fiscal year. The Director of ICS must provide explicit approval for any recommendations that remove a material line item from the scope of the assessment.

The results of the risk assessment (qualitative analysis) described in Activity I.7 will indicate whether additional *immaterial* line items should be considered within the scope of the assessment.

\* \* \* \* \*

## I.7 Conduct qualitative analysis (risk assessment)

The next activity in the Planning Phase is to identify the qualitative risks within each KFP that may result in a material misstatement in the financial statements.<sup>5</sup> A qualitative analysis, sometimes called a risk assessment, is a critical tool used to prioritize the assessment of controls and can be used to identify, analyze, and manage risks relevant to achieving the objectives of reliable financial reporting, safeguarding of assets, and compliance with relevant laws and regulations.

As with the previous activities in the Planning Phase, the SAT is accountable for completion of the qualitative analysis, but will delegate responsibility to ICS. ICS will keep OBO informed of its progress and will document its methodology. The table below presents an example of how the qualitative analysis can be documented.

Key Financial Process	Risk Rating						Comments/ Rationale
	Factor 1		Factor 2		Factor 3		
Process Name	Likelihood Rating	Impact Rating	Likelihood Rating	Impact Rating	Likelihood Rating	Impact Rating	OVERALL
	Factor Rating		Factor Rating		Factor Rating		
Example: Funds Management	3	3	3	5	1	1	2.67
	3		4		1		

Activities 1.7.1 and 1.7.2 described below provide details on the scoring methodology and qualitative assessment process shown above.

### I.7.1 Identify qualitative risk factors

Each KFP will be evaluated on relevant qualitative risk factors. The table below presents some standard risk factors which may be applicable.

Qualitative Risk Factors
<b>Compliance Risk</b> <ul style="list-style-type: none"> <li>- Significance of applicable laws and regulations</li> <li>- New or amended laws, regulations, or accounting standards</li> </ul>
<b>Human Capital Risk</b> <ul style="list-style-type: none"> <li>- Changes to people/process owners</li> <li>- Workload stress</li> <li>- Knowledge/expertise of personnel/process owners</li> <li>- Sufficient resources</li> <li>- Restructuring or budget cutbacks which may include downsizing and changes in supervision and segregation of duties</li> <li>- New personnel or significant personnel changes</li> </ul>

<sup>5</sup> Risk assessments can be completed by process or by financial statement line item. The CFO Implementation Guide gives instructions for conducting a line item assessment. However, it is more often organized by process as described in this manual.

<p><b>Operational Risk</b></p> <ul style="list-style-type: none"> <li>- Degree of decentralization</li> <li>- Changes in the operating environment</li> <li>- Significantly new or changed programs or operations</li> <li>- Significantly new or changes to process or policy</li> </ul>
<p><b>Complexity</b></p> <ul style="list-style-type: none"> <li>- KFP is complicated and/or involves numerous people or groups</li> <li>- Nature of transactions is non-routine</li> <li>- Extent of manual processes or applications</li> <li>- Need for accounting estimates</li> </ul>
<p><b>IT Risk</b></p> <ul style="list-style-type: none"> <li>- Number of systems and interfaces</li> <li>- New or revamped information systems</li> <li>- New technology</li> </ul>
<p><b>Volume of transactions</b></p> <ul style="list-style-type: none"> <li>- Number of transactions in a given period</li> </ul>
<p><b>Fraud/Misappropriation Risk</b></p> <ul style="list-style-type: none"> <li>- Inherent risk of errors or irregularities due to fraud, considering opportunities and incentives for fraud</li> </ul>
<p><b>Entity-level Control Risks</b></p> <ul style="list-style-type: none"> <li>- Risks associated with the overall control environment, including tone at the top, the assignment of authority and responsibility, consistent policies and procedures, and entity-wide initiatives</li> <li>- Known deficiencies related to entity-level controls based on previous assessments</li> </ul>
<p><b>Historical Risk</b></p> <ul style="list-style-type: none"> <li>- Known deficiencies or findings</li> <li>- Open material weaknesses or significant deficiencies</li> <li>- Politically sensitive</li> <li>- Draws media or regular attention</li> </ul>

*Examples of Risk Factors*

- **Define/recommend risk factors**

Using the list provided above as a guide, ICS will develop a list of recommended qualitative risk factors that are applicable to VA.

- **Review risk factors**

The Director of ICS will review the list of relevant factors and will present the risk factors to OBO and the SAT for concurrence.

## 1.7.2 Assess risks associated with each immaterial KFP

ICS will work with representatives from the KFP to assign a recommended risk rating for each factor, for each *immaterial* KFP. The three ratings (high, moderate, and low) are defined as follows:

High	The possibility of misstatement due to the risk factor is substantial; the KFP has a significant impact on the financial statements; or historical risk is high
Moderate	The possibility of misstatement due to the risk factor is moderate or the KFP is subject to an average degree of error
Low	A misstatement due to the risk factor is unlikely or would have a minimal impact on the financial statements

*Risk Rating Definitions*

To assess the risk, ICS will complete the following steps.

- **Identify representatives within each KFP**

ICS will identify leads for each KFP. The qualitative analysis should be performed by individuals who have sufficient knowledge of the processes and associated risks.

- **Conduct workshops with KFP leads**

ICS will hold workshops with KFP leads, the Director of ICS, Associate Director, and other interested representatives. During these workshops, the group will discuss qualitative risk factors and come to agreement on the risk ratings for each factor within each KFP, and each KFP as a whole. ICS should ask KFP leads what they believe are the greatest risks that "keep them up at night."

- **Assign recommended ratings for each qualitative factor**

ICS and KFP leads will determine the recommended risk ratings for each qualitative factor within a given KFP. They will consider risk likelihood and risk impact in its determination of risk ratings:

Risk Type	Definition
Risk Likelihood	Measure of the relative potential that the inherent risk represented by the risk statement might occur given the general environment
Risk Impact	Measure of the magnitude/severity of the effect the risk might cause given the general environment, considering both the nature and the effects of the risk

ICS should assign both a likelihood and impact rating score of low, moderate, or high for each factor. A score of low is assigned 1 point; moderate, 3 points; and high, 5 points.

Rating	Score
Low	1
Moderate	3
High	5

ICS will then calculate the average of the likelihood and impact scores in order to assign an overall factor rating. The average scores correspond to the following risk levels:

Average	Risk Level
1	Low
2-4	Moderate
5	High

The table below illustrates the possible score combinations and outcomes:

Likelihood	+ Impact	= Factor Risk Rating
Low (1)	Low (1)	Low (1)
Low (1)	Moderate (3)	Moderate (2)
Low (1)	High (5)	Moderate (3)
Moderate (3)	Low (1)	Moderate (2)
Moderate (3)	Moderate (3)	Moderate (3)
Moderate (3)	High (5)	Moderate (4)
High (5)	Low (1)	Moderate (3)
High (5)	Moderate (3)	Moderate (4)
High (5)	High (5)	High (5)

- **Determine recommended overall qualitative risk level**

Once ICS has recommended ratings for each risk factor, it will recommend an overall qualitative risk level. In order to assign this risk level, ICS will use the same averaging technique described above. Factor risk ratings (determined by the magnitude and likelihood scores) will be averaged for all factors in a given KFP. The result will yield the overall qualitative risk level for a KFP based on the table below:

Average	Risk Level
1	Low
2-4	Moderate
5	High

- **Document qualitative analysis methodology**

ICS must clearly document its methodology. The table below presents an example of how the qualitative analysis can be documented, and may be included as an appendix to the Annual Review Plan.

Key Financial Process	Risk Rating						Overall	Comments/ Rationale
	Factor 1		Factor 2		Factor 3			
Process Name	Likelihood Rating	Impact Rating	Likelihood Rating	Impact Rating	Likelihood Rating	Impact Rating	OVERALL	
	Factor Rating		Factor Rating		Factor Rating			
Example: Funds Management	3	3	3	5	1	1	2.67	
	3		4		1			

- **Review qualitative analysis (Director of ICS)**

The Director of ICS will review the analysis. If the Director has any changes, ICS staff will update the documentation and resubmit for Director approval.

- **Review qualitative analysis (SAT)**

The Director of ICS will brief the SAT on the analysis and request feedback. ICS will work with the Director and the SAT to finalize the analysis.

### **I.7.3 Recommend additional in-scope KFPs**

Using the results of the qualitative analysis, ICS will determine which immaterial KFPs should be added to the list of in-scope processes. (Recall that all material KFPs are in scope, regardless of the results of the risk assessment.) For example, if a KFP does map to a material line item but has been the focus of increased OMB scrutiny due to historical findings, ICS may recommend that it be considered within the scope of the assessment.

- **Develop scoping recommendations**

ICS will review the results of the qualitative analysis to determine which immaterial KFPs should be added to the list of in-scope processes. ICS should clearly document their rationale for inclusion of each additional KFP.

- **Review scoping recommendations**

The Director of ICS will review the scoping recommendations. If the Director has any changes, ICS staff will update the documentation and resubmit for Director approval.

- **Document in-scope KFPs in Appendix A Annual Review Plan**

Once the Director of ICS has approved the analysis and scoping recommendations, ICS will include the list of in-scope KFPs and all supporting documentation in the Appendix A Annual Review plan. (Recall that the completed plan will be reviewed by the SAT at the conclusion of the Planning Phase.)

\* \* \* \* \*

## I.8 Recommend Administrations/Programs/Locations

Because VA has three administrations (Veterans Health Administration, Veterans Benefits Administration, and National Cemetery Administration) and multiple locations, VA must develop an assessment approach that covers the Department as a whole. VA faces a unique challenge in obtaining coverage since the Department has over 1,300 facilities throughout the country. ICS, OBO and the SAT will determine the best approach to conduct a Department-wide assessment. The SAT will consult OMB for guidance and to receive approval on its approach. The Appendix A Annual Review Plan will detail which locations will be selected and how the location selection will rotate from year to year.

- **Obtain Location Selection Recommendations template** 

ICS will obtain the Location Selection Recommendations template from SharePoint. The table below shows a screenshot of the template. Refer to Appendix 3 for a larger screenshot:

Department of Veterans Affairs							
Location Selection Recommendations							
In-Scope Key Financial Process	Organization				Program(s)	Recommended Locations	Comments/ Rationale
	VHA	VBA	NCA	Dept			
List In-Scope KFP	Mark each applicable administration/organization with an X				Indicate all program(s) each KFP impacts (i.e., Medical Research, Insurance, etc.)	List Recommended Location 1 List Recommended Location 2 List Recommended Location 3...	Rationale for Location 1 Rationale for Location 2 Rationale for Location 3
Funds Management	X	X	X	X	Med care Med care Med care	VACO Dallas VISN Chicago VA Regional Office	Provides 28% coverage Known Issues at this location Program has undergone significant personnel changes

*Location Selection Recommendations*

- **Complete template**

ICS will work as a team to develop a recommended location selection approach. ICS will complete the following fields in the template.

Field	Description
In-Scope KFP	List each in-scope KFP (as determined in Activity I.7.3)
Organization	Mark each applicable administration/organization with an X
Programs	Indicate all program(s) each KFP impacts (i.e., Medical Research, Insurance, etc.)
Recommended Locations	List all locations that are recommended to be in the scope of the assessment
Rationale	Document the rationale for each recommended location (see guidance below)

- **Document rationale for recommendations**

ICS will document its rationale for recommending each location. The following table lists *suggested* factors that might impact whether a location is included in the assessment.

Factor	Considerations
Financial Data	- Do we have access to financial data that would direct us to this location?
Program Presence	- Does VA perform the program associated with the KFP at this location?
Significance of process	- How significant is the process (based on data or institutional knowledge)?
Known Issues	- Are there any known weaknesses at particular locations? - Have there been recent findings at this location during OIG, MQAS or other assessments?
Nature of program	- Has the program/location undergone any significant changes? - Is the location inherently susceptible to risk?
Coverage	- What is the total value of transactions processed? Does it meet the materiality threshold? - What percentage of the total transactions are processed at this location?
Other Knowledge about the Site	- Are there other factors that would contribute to including the location in the assessment?
Entity-level Evaluation	- Are there any known deficiencies related to entity-level controls at this location? - Did the previous year's entity-level assessment indicate potential issues at a particular location?
Logistical Considerations	- Are certain locations located in close proximity, for efficient use of testing resources? - How does the timeline for A-123 site visits correspond with a location's participation in other Department-wide activities (i.e., visits from the external auditor)?

ICS should use the template to thoroughly document why each location was recommended for the assessment. The *Rationale* column cannot be left blank.

- **Review recommendations**

The Director of ICS will review the location selection form, and, if needed, will work with ICS staff to revise the recommendations.

- **Document recommendations in Annual Review Plan**

The Director-approved location selection recommendations will be included in the Annual Review Plan, for review and approval by the SAT.

\* \* \* \* \*

## I.9 Identify financial reporting assertions

ICS will determine which relevant financial reporting assertions apply to the significant line items. (Recall that the significant line items were identified in I.3.2.) This step is an important aspect of planning for the following reasons:

- Identifying assertions at the line item level will help ICS ensure that their assessment covers all *relevant* assertions for each significant line item. In a later step, ICS will verify that key controls exist to support the relevant assertions determined in this step.
- Identifying the assertions at the line item level will help ICS develop tests that cover all *relevant* assertions for each significant line item.
- Determining relevant assertions prior to testing to minimize the likelihood of testing controls that address assertions that are not relevant to a particular significant account

The acronym PERCV represents the five assertions:

- Presentation and Disclosure. The financial report is presented in the proper form and any required disclosures are present (*Is it recorded in the right place?*)
- Existence or Occurrence. All reported transactions actually occurred during the reporting period and all assets and liabilities exist as of the reporting date (*Did it happen and when?*)
- Rights and Obligations. All assets are legally owned by VA and all liabilities are legal obligations of the Department (*Do we own or owe what we think we do?*)
- Completeness and Accuracy. All assets, liabilities, and transactions that should be reported have been included and no unauthorized transactions or balances are included (*Is anything missing?*)
- Valuation or Allocation. All assets and liabilities have been properly valued, and where applicable, all costs have been properly allocated (*Are the numbers right?*)

Additionally, A-123 defines three additional assertions:

- The transactions are in compliance with applicable laws and regulations
- All assets have been safeguarded against fraud and abuse
- Documentation of internal control, all transactions, and other significant events is readily available for examination

Relevant assertions are assertions that have a meaningful bearing on whether the account or disclosure is fairly stated. The degree to which an assertion is relevant to each significant account will vary. For example, assertions about valuation may not be relevant to the accounts receivable account unless there is doubt regarding collectability; however, assertions about existence and completeness are always relevant. Additionally, the assessment team may focus on assertions about presentation and disclosure separately in connection with the period-end financial reporting process. In determining whether a particular assertion is relevant, ICS will consider the following factors:

- The nature of the assertion
- The volume of transactions or data related to the assertion

- The nature and complexity of systems, including information technology systems that the Agency uses to process and control information that supports the assertion<sup>6</sup>

Although the financial statement assertions appear to be similar to the information processing objectives (Completeness, Accuracy, Validity, Restricted Access - CAVR), there is not a one-for-one relationship, and they are used for different purposes. Information processing objectives/CAVR (covered in Appendix E) are used to evaluate the design effectiveness of controls, particularly application controls, within a KFP. Financial statement assertions are representations by management as to the fair presentation of the financial statements.

- **Obtain Financial Statement Assertions template** 

ICS has developed a template for identifying the financial statement assertions. The template is available on SharePoint. Refer to Appendix 1 for a larger screenshot:

- **Complete Financial Statement Assertions template**

ICS will complete the following columns in the template:

- Financial Statement
- Financial Statement Line Item
- Financial Statement Assertions - the assertions that are relevant to that particular line item
- Amount - the dollar amount in millions for the line item
- Key Financial Process - the main process that feeds the line item
- Sub-Process - processes within the primary process which feed the line item
- Critical Systems - applications which impact the relevant line item

**Department of Veterans Affairs  
Financial Statement Assertions**

(In Millions)

Legend															
Financial Statement		Financial Statement Assertions													
BS	Balance Sheet	P	Presentation & Disclosure												
SBR	Statement of Budgetary Resources	E	Existence/Occurrence												
SNC	Statement of Net Cost	R	Rights/Obligations												
SCNP	Statement of Change in Net Position	C	Completeness/Accuracy												
		V	Valuation/Allocation												
		Additional Assertions													
		L&R	Compliance with Laws & Regulations												
		F	Safeguarded against fraud and abuse												
		D	Documentation												

Financial Statement	Financial Statement Line Item	P	E	R	C	V	L&R	F	D	FY 20XY Amount	Key Financial Process	Sub Process	Critical Systems
Use abbreviations above	List each line item as it appears on the financial statement	Mark an X in the column for each relevant assertion								Enter the dollar amount from the financial statement in thousands	Enter the primary process that feeds the line item.	Enter the sub-process or sub-processes that relate to the line item	List any critical applications that impact the primary process and line item.

*Financial Statement Assertions Template*

<sup>6</sup> PCAOB, Auditing Standard No. 2

- **Obtain RCM template** 

ICS will obtain the approved RCM from SharePoint. The template includes a sample RCM based on the PP&E Personal Property Disposal sub-process documented in *Appendix N*. Refer to Appendix 2 for a larger screenshot:

Department of Veterans Affairs  
Risk/Control Matrix

Key Financial Process

Risk		Control Objective	Risk Level (H, M, L)	Expected Key Control	Control Reference Number	Actual Control Activity	Process Owner (Name, title, division)	Information Processing Objectives	Financial Statement Assertions	Control Description	Gap Description
								Completeness (C) Accuracy (A) Validity (V) Restricted Access (R) Existence and Ownership (E/O) Valuation and Allocation (VA) Rights and Obligations (R/O) Compliance (Com) Presentation (Pres) (Disclosure) (D) Manual (M) or Automated (A)	Existence/Occurrence Rights and Obligations Completeness Valuation or Allocation Fraud, Waste and Abuse Compliance Documentation	Application (if Automated) Frequency of Control Key Controls or Controls (N)	

*RCM Template*

- **Document financial statement assertions in Appendix A Annual Review Plan and RCM**

ICS will document, in the Appendix A Annual Review Plan, the financial statement assertions for each line item. Additionally, ICS will document the financial statement assertions in the RCM for each KFP. At a minimum, ICS will specify the assertions that apply to the KFP at the top of the RCM table. Identifying the assertions related to each control (columns within the body of the table) is optional.

- **Populate RCM with risks, control objectives, and risk level**

For each KFP, ICS will complete the first three columns of the RCM by populating the risks, control objectives, and corresponding risk level for each KFP. Risks and control objectives are based on how a KFP *should be* designed rather than how it is working in practice. For example, within Financial Reporting, some of the risks may include the following:

- Inaccurate changes to the chart of accounts result in financial reporting errors
- Incorrect postings result in inaccuracies in subsidiary ledgers and the general ledger
- Budgetary and Proprietary accounts do not balance causing an inaccuracy in the Statement of Budgetary Resources
- Adjustments are inaccurate, incomplete, and not made in the correct accounting period

ICS should complete the following information in the RCM template:

Title	Definition
Risk	Risk is the threat that an event, action, or non-action will have an adverse affect on the ability to achieve one's objectives. The potential negative outcome that could result if a control activity does not exist to meet the goal of the control objective.
Control Objective	A reasonable assurance that is meant to be provided by the active and effective operational use of a control. Describes the purpose of a control activity as a policy, procedure, or activity put into place by management to offset identified risks. An example of a control objective: "To ensure only individuals with appropriate responsibility have the ability to record appropriations in the GL."
Risk Level	Each risk and control objective should be assigned a risk level of high, medium, or low.

⇒ **Appendix O** includes suggested risks and control objectives for some of the common processes.

- **Identify and document expected key controls**

For each KFP, ICS will identify the controls necessary to effectively address the relevant financial statement assertions. These controls will be deemed the key control that should be in place. A key control is a control, or set of controls, that addresses the relevant assertions for a financial statement line item. These expected key controls will be documented in the RCM and, in phase II.2, compared to the actual control activities being performed. These key controls will include both manual and automated, or application, controls. In subsequent years, when the KFP documentation is updated, additional KFP steps and control activities may be added to these documents in order to provide further detail and enable a more comprehensive assessment.

During the Evaluating Phase (Activities II.2.1.4 and II.2.3), ICS will identify the control activities within each KFP and map those to the expected key controls and financial statement assertions. If controls within a KFP do not address all of the expected key controls and/or relevant assertions specified for that KFP, the controls may not be properly designed.

\* \* \* \* \*

## **I.10 Consider cross-servicing entities: customers and providers**

VA may use outside service organizations to process financial data. Service organizations include Federal agencies, state organizations, and commercial companies. Management is ultimately responsible for the internal control over its financial information and, therefore, the assessment team may need to assess the design and operating effectiveness of the service organization's internal control, including all five components of internal control.

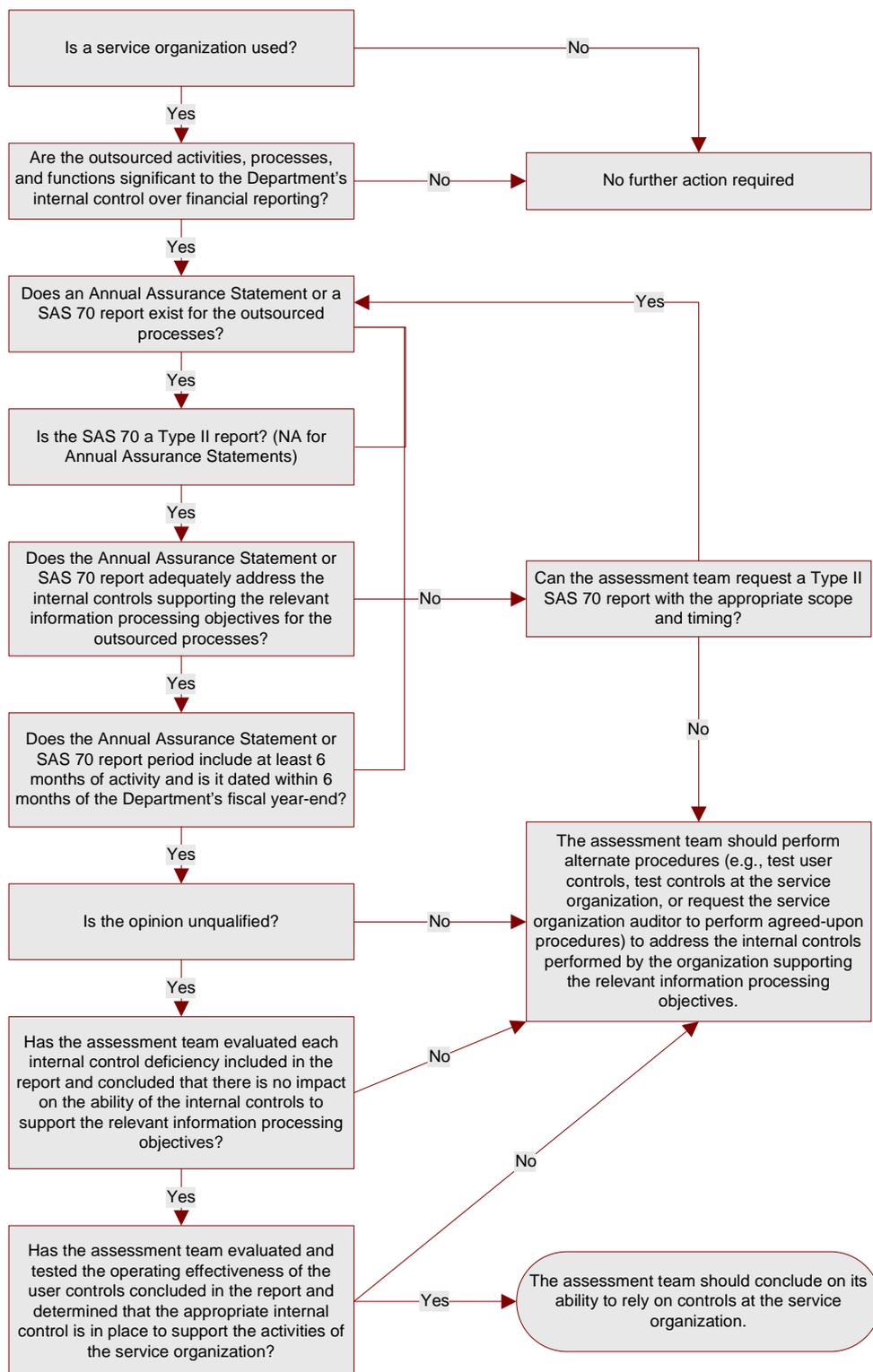
The ICS assessment team will identify and document a summary of its service organizations. The summary will detail key information about VA's outsourcing arrangement with each (i.e., summarizing the services provided, indicating whether the Department is allowed to audit the service organization, determining whether a Statement on Auditing Standards No. 70 (SAS 70) report exists, and noting the expiration date of the contract) and track the results of and rationale

for decisions, based on the following decision tree. To develop an accurate summary, ICS will identify the systems used to generate the line items associated with each in-scope KFP. ICS will then determine where those systems reside and whether a service organization is being used.

The assessment team will consider the following steps when evaluating the procedures to perform over its service organizations:

- **Determine whether a service organization is being used**
- **Determine whether the outsourced activities, processes, and functions generate the significant line items**
- **Determine whether an annual assurance or a SAS 70 exists and is sufficient in scope**
- **Plan for alternative procedures if an annual assurance statement or SAS 70 does not exist**

This process, which is primarily the responsibility of ICS, is summarized in the following decision tree and explained further in the remainder of this section and in Activity II.2.4.



Annual Assurance Statement or SAS 70 Decision Tree

### **I.10.1 Determine whether a service organization is being used**

Many agencies outsource activities to service organizations (other agencies or commercial companies). However, not all service organizations will be within the scope of this assessment. Generally, a service organization would need to be considered for management's assessment only when the outsourced activities constitute a significant process or function performed by a third party that generates information significant to the financial reporting process. Services are considered part of an entity's information system if they affect the following:

- A class 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

When identifying service organizations, the assessment team will distinguish between service organizations and specialists. For example, management may use a specialist to perform the following activities:

- Valuations
- Determinations of physical characteristics relating to quantity on hand or condition
- Determinations of amounts derived by using specialized techniques or methods
- Interpretations of technical requirements, regulations, or agreements

These specialists are not part of an outsourced process and would not need to be evaluated as if they were part of VA's internal control over financial reporting. However, the output of a specialist's work is often significant to the financial statements. Thus, management should have controls in place (such as a means to evaluate the specialist's professional qualifications) to assess whether the specialist has the required skills and knowledge in the particular field to make an appropriate determination. Management and the assessment team should also understand the following:

- The objectives and scope of the specialist's work
- The methods or assumptions used
- How the methods or assumptions used compare to those used in the preceding period

### **I.10.2 Determine whether the outsourced activities, processes, and functions generate the significant line items**

The ICS assessment team will consider only outsourced operations that are part of processes the assessment team deems significant to the KFPs specified in the Appendix A Annual Review Plan. This can be accomplished by mapping the outsourced activities to the KFPs.

If the activities being performed at the service organization are considered significant to the Department's internal control over financial reporting for the in-scope KFPs, the assessment team will proceed with the following steps.

### **I.10.3 Determine whether an annual assurance statement or a SAS 70 exists and is sufficient in scope.**

#### ***Annual Assurance Statements***

If an agency uses the services of another organization (cross-servicing entity), the serviced agency will obtain the organization's annual assurance statement. The annual assurance statement must include an assessment of the effectiveness of the organization's internal control over financial reporting as it relates to the services being provided.

#### ***SAS 70s***

A SAS 70 will be obtained if the service is being provided by an organization outside of VA (i.e., other Federal agencies, state agencies, and commercial organizations). SAS 70 allows a service organization (such as one performing internal accounting services) to obtain a single audit report for use by its clients' auditors to plan and conduct audits of financial statements. One of the objectives of SAS 70 was to preclude the need for each user auditor to conduct its own audit of the service organization's controls.

If the assessment team determines that the controls at the service organization must be assessed, the assessment team will determine if a Type II SAS 70 report exists. A Type II report assesses whether the controls are operating effectively (i.e., the controls are tested by the service organization's auditor). Because OMB Circular A-123 requires management to assess the design and operating effectiveness of its internal control over financial reporting, a Type I report cannot be used for the assessment team's assessment to support operating effectiveness.

#### ***Considerations regarding Annual Assurance Statements and SAS 70s***

- **Scope of the Review.** The report should cover the KFPs and controls relevant to the assessment team's assessment process. To ensure that this objective is met, the assessment team will collaborate with its service organization to determine the scope of the Annual Assurance Statement or SAS 70 report. These reports should cover (1) the relevant information processing objectives/CAVR that are addressed at the service organization and (2) the general computer controls for any applications relevant to the assessment team's assessment process.

Some service organizations have multiple processing sites. The assessment team will ensure that the processing location responsible for providing its services is covered by the report. If not, additional procedures will be required.

- **User Controls.** In most situations, to conclude that effective internal control over financial reporting exists, the assessment team will demonstrate effective controls at both VA and the service organization. The Department's controls over the service organization are referred to as "user controls" and are typically documented in the Annual Assurance Statement or SAS 70 report. The assessment team will evaluate and test these controls. For example, the integrity of outsourced payroll processing will depend on the integrity of the inputs from VA, including information relating to new employees, terminations, and salary increases.

If VA is responsible for providing this information to the service organization, the user controls vis-à-vis this information will be important to ensure the overall integrity of the payroll-processing output from the service organization.

- Period of Time Covered. The assessment team will consider the period of time covered by the Annual Assurance Statement or Type II SAS 70 report. A report dated earlier than six months prior to VA's fiscal year-end date would result in limited benefits because of the extent of additional procedures that would be necessary. However, if a report's date is too close to year-end, the assessment team may be unable to obtain the report in sufficient time to allow for evaluation and remediation.

As the intervening period between the date of the Annual Assurance Statement or SAS 70 report and the year-end of the Department increases, the assessment team will consider update procedures. The assessment team will consider whether, during the intervening period, there have been any of the following issues:

- Changes in personnel with whom management interacts at the service organization
  - Changes in reports or other data received from the service organization
  - Changes in contracts or service level agreements with the service organization
  - Errors in the service organization's processing
- Additional Procedures. In some cases, an Annual Assurance Statement or a Type II SAS 70 report will not be sufficient for the assessment team's assessment of internal control over financial reporting. For example, if an organization outsources substantially all general-ledger and transaction-processing functions to a service organization, the organization may conclude that an Annual Assurance Statement or a Type II SAS 70 report would not provide sufficient evidence of operating effectiveness due to the significance of the outsourced processes. In this situation, the assessment team will assess whether additional procedures need to be performed to evaluate the design and operating effectiveness of the service organization's controls. Conversely, if a service organization performs routine payroll processing for many customers, it is likely that the service organization's clients would conclude that an Annual Assurance Statement or a Type II SAS 70 report sufficiently assesses the design and operating effectiveness of the service organization's controls.
  - Documentation. Key decisions made regarding service organizations and the use of assurance statements and SAS 70s will be documented as part of the Planning Phase. Assurance statements and SAS 70s that are received from service organizations will be retained as part of the assessment team's documentation. The assessment team does not need to document processes that occur at the service organization, but does need to document how user controls are performed within VA. User controls would need to be tested as part of the Testing Phase of management's assessment.
  - Timing. Obtaining an Annual Assurance Statement from a cross-servicing organization or a Type II SAS 70 report from a Federal, state, or commercial entity for the first time can be a lengthy process. The service organization may need to remediate certain processes, and thus it often takes six months to a year to obtain a final report after a request is made. Accordingly, agencies using commercial service organizations should make this determination as soon as possible.

Activity II.2.4 in the Evaluating Phase provides additional information on evaluating the controls of cross-servicing providers and assessing SAS 70 results.

### **I.10.4 Plan for alternative procedures if an Annual Assurance Statement or SAS 70 does not exist**

If an Annual Assurance Statement or Type II SAS 70 report cannot be obtained, or the report obtained does not adequately address the information processing objectives/CAVR required by

the assessment team, alternative procedures will be performed over the service organization's internal control. Appendix H provides more information on alternative procedures.

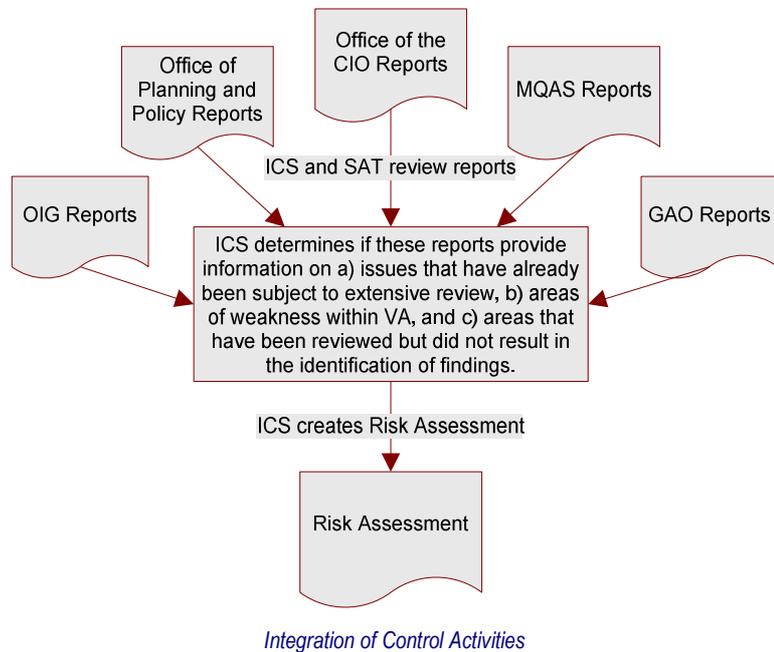
ICS will document its approach for addressing cross-servicing entities in its Appendix A Annual Review Plan.

\* \* \* \* \*

## I.11 Integrate and coordinate with other control-related activities

VA is subject to several laws and regulations regarding internal controls including the Federal Financial Management Improvement Act (FFMIA), the Government Performance and Results Act (GPRA), the CFO Act, the Improper Payments Information Act of 2002 (IPIA) and the Federal Information Security Act (FISMA). Internal and external coordination is critical to ensure that internal control activities are properly integrated with many related activities already underway.

Management will strive to integrate control-related activities in order to promote efficiency and avoid duplication of work. Some of these activities may include policy compliance reviews, management studies, productivity indices, and best practices. The results of work performed for other regulations may also be used to support management's assertion of the effectiveness of internal controls under A-123. The SAT and ICS will review reports prepared by the Office of Inspector General (OIG), the Office of the CIO, the Office of



Policy and Planning, Management Quality and Assurance Service (MQAS), and the Government Accountability Office. These reports may provide information on a) issues that have already been subject to extensive review, b) areas of weakness within VA; and c) areas that have been reviewed but did not result in the identification of findings. ICS can use the information as an input to the risk assessment and to determine which KFPs warrant further assessment.

ICS will also use alternative sources of evidence during the Testing Phase. Possible sources of other testing may include the following:<sup>7</sup>

- Management reviews conducted a) expressly for the purpose of assessing internal control, or b) for other purposes with an assessment of internal control as a by-product of the review
- Program evaluations

<sup>7</sup> OMB Circular, A-123, Appendix A, page 13.

- Reviews of financial systems which consider whether the requirements of FFMIA and OMB Circular No. A-127, Financial Management Systems are being met
- Annual evaluations and reports pursuant to FISMA and OMB Circular No. A-130, Management of Federal Information Resources
- Annual reviews and reports pursuant to IPIA to the extent they pertain to controls over financial reporting
- Type II SAS 70 report or annual assurance statement in the case where servicing is performed by the organization

VA's external auditor is also responsible for assessing the Department's internal controls. The SAT will work with the auditor to create efficiencies in the financial statement audit and the A-123, Appendix A, process. According to the CFOC Implementation Guide, management should take the following actions:

- 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., significant deficiencies and material weaknesses), and investigate the reasons for any reporting differences.

\* \* \* \* \*

## **I.12 Determine assurances needed from components**

The SAT is responsible for ensuring that sufficient testing is performed regarding internal control over financial reporting for VA as a whole. In previous fiscal years, VA has prepared a Department-wide assurance statement rather than request assurances from individual Administrations or locations. In the Appendix A Annual Review Plan, ICS will document the rationale for this approach.

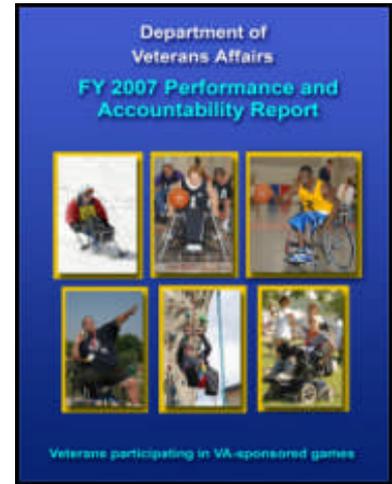
\* \* \* \* \*

## I.13 Plan for an updated assurance statement in the Performance and Accountability Report (PAR)

VA is required to provide an assurance statement over the effectiveness of control over financial reporting as of June 30. This statement is a sub-statement of the overall Statement of Assurance required under Section 2 of the FMFIA.

The SAT will work closely with ICS to develop a project plan that will allow the Secretary to sign the statement of assurance on internal control for inclusion in the Annual Performance and Accountability Report (PAR) issued in November.

The following schedule will assist the SAT in meeting the required deadline for submission of the annual statement:



2007 Performance and Accountability Report

July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	March	April	May	June	July	Aug	Sept	Oct
Planning															
					Evaluating										
									Testing						
											Concluding and Internal Reporting				
Correcting															
														External Reporting	

- **Review/approve Appendix A Annual Review Plan**

The Director of ICS will brief the SAT on the Appendix A Annual Review Plan described in Activities I.1 - I.12. ICS will work with the SAT to revise the plan if needed. The SAT must approve the final plan.

- **Develop project plan**

Following SAT approval of the Appendix A Annual Review Plan, ICS will develop a project plan which outlines key activities and deliverables. When developing a project plan, ICS will consider the following:

- Resources (contractor and civilian)
- Dependencies and predecessors
- Scheduling issues (audit site visits, training dates, Federal holidays)

The following table lists the key activities for each phase, suggested dates, and key outputs. At a minimum, this information will be included in the project plan.

Phase	Key Activities	Dates	Key Outputs
Planning	<ul style="list-style-type: none"> <li>• Scope assessment (I.1- 1.13)</li> </ul>	July - January	<ul style="list-style-type: none"> <li>• Annual Appendix A Annual Review Plan</li> <li>• Appendix A Annual Review Plan Appendices</li> </ul>
	<ul style="list-style-type: none"> <li>• Conduct quantitative analysis (I.4)</li> </ul>	July	
	<ul style="list-style-type: none"> <li>• Conduct qualitative analysis (risk assessment) (I.7)</li> </ul>	August - December	
	<ul style="list-style-type: none"> <li>• Integrate and coordinate with other control-related activities (I.11)</li> </ul>	Ongoing	
	<ul style="list-style-type: none"> <li>• Plan for an updated assurance statement in the PAR (I.13)</li> </ul>	October - January	
Evaluating	<ul style="list-style-type: none"> <li>• Evaluate internal control at the entity level (II.1)</li> </ul>	December - February	<ul style="list-style-type: none"> <li>• Entity assessment questionnaire and results</li> </ul>
	<ul style="list-style-type: none"> <li>• Document key financial processes (II.2.1) and identify key controls (II.2.3)</li> </ul>	January - February	<ul style="list-style-type: none"> <li>• Documentation packages -narratives and flowcharts</li> <li>• Risk/Control Matrices (RCM)</li> <li>• Quality control checklists</li> </ul>
	<ul style="list-style-type: none"> <li>• Evaluate control design (II.2.2)</li> </ul>	February	<ul style="list-style-type: none"> <li>• Completed RCMs</li> </ul>
	<ul style="list-style-type: none"> <li>• Evaluate controls of cross-servicing providers (II.2.4)</li> </ul>	March - April	<ul style="list-style-type: none"> <li>• Cross-servicing providers assessment and results</li> </ul>
	<ul style="list-style-type: none"> <li>• Understand IT structure (II.3)</li> </ul>	March - April	<ul style="list-style-type: none"> <li>• IT General Computer Control assessment results</li> </ul>
Testing	<ul style="list-style-type: none"> <li>• Develop Test Plan (III.1)</li> </ul>	April	<ul style="list-style-type: none"> <li>• Overall Test Plan</li> </ul>
	<ul style="list-style-type: none"> <li>• Develop process-level test plans (II.2.1)</li> </ul>	April - May	<ul style="list-style-type: none"> <li>• Process-level test plans</li> </ul>
	<ul style="list-style-type: none"> <li>• Request evidence (III.2.2) and conduct tests (III.2.3)</li> </ul>	May - June	<ul style="list-style-type: none"> <li>• Workpapers (test sheets)</li> </ul>

Phase	Key Activities	Dates	Key Outputs
Concluding, Internal Reporting, and Correcting	<ul style="list-style-type: none"> <li>Conclude on control effectiveness (IV.1)</li> </ul>	June - August	<ul style="list-style-type: none"> <li>Exception Log (Final)</li> <li>Finding Outline Worksheets</li> </ul>
	<ul style="list-style-type: none"> <li>Correct Findings (IV.2)</li> </ul>	Ongoing, as Findings are identified	<ul style="list-style-type: none"> <li>Corrective Action Plans (CAPs)</li> </ul>
	<ul style="list-style-type: none"> <li>Monitor CAPs and verify completion (IV.3)</li> </ul>	Ongoing, as CAPs are developed	<ul style="list-style-type: none"> <li>CAPs</li> <li>Entries into Corrective Action Tracking System (CATS)</li> <li>CATS Status Reports</li> </ul>
External Reporting	<ul style="list-style-type: none"> <li>Report externally (V.1)</li> </ul>	September - November	<ul style="list-style-type: none"> <li>Statement of Assurance</li> </ul>

The following table displays key SAT meeting dates and the purposes of those meetings:

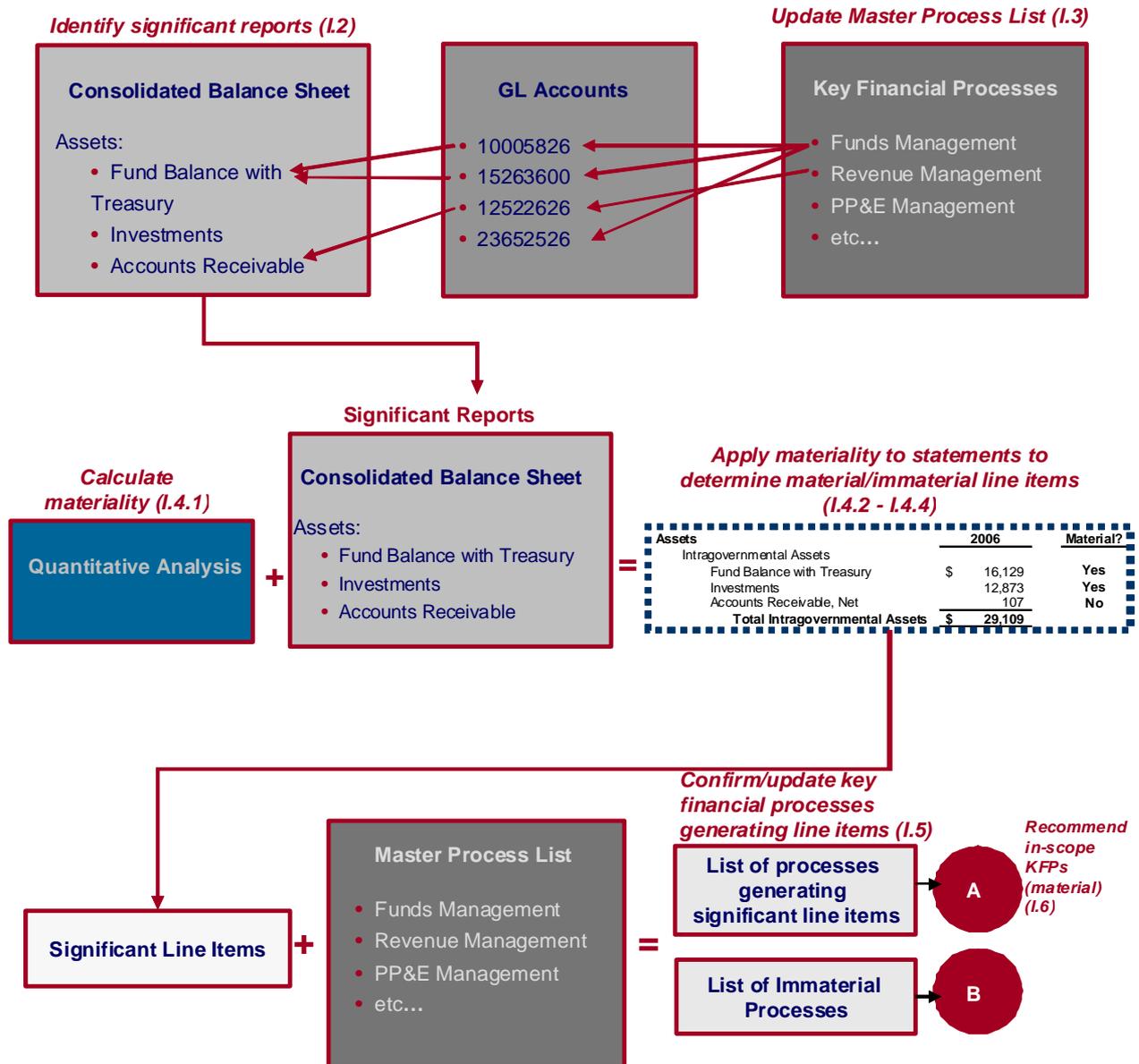
Date	Purpose
November / December	<ul style="list-style-type: none"> <li>Present results of the qualitative and quantitative analyses</li> <li>Review and approve Appendix A Annual Review Plan</li> </ul>
May	<ul style="list-style-type: none"> <li>Present preliminary test results</li> </ul>
August	<ul style="list-style-type: none"> <li>Present findings</li> </ul>
September	<ul style="list-style-type: none"> <li>Approve Draft Corrective Action Plans and Draft Statement of Assurance</li> </ul>
October	<ul style="list-style-type: none"> <li>Approve Final Statement of Assurance</li> </ul>

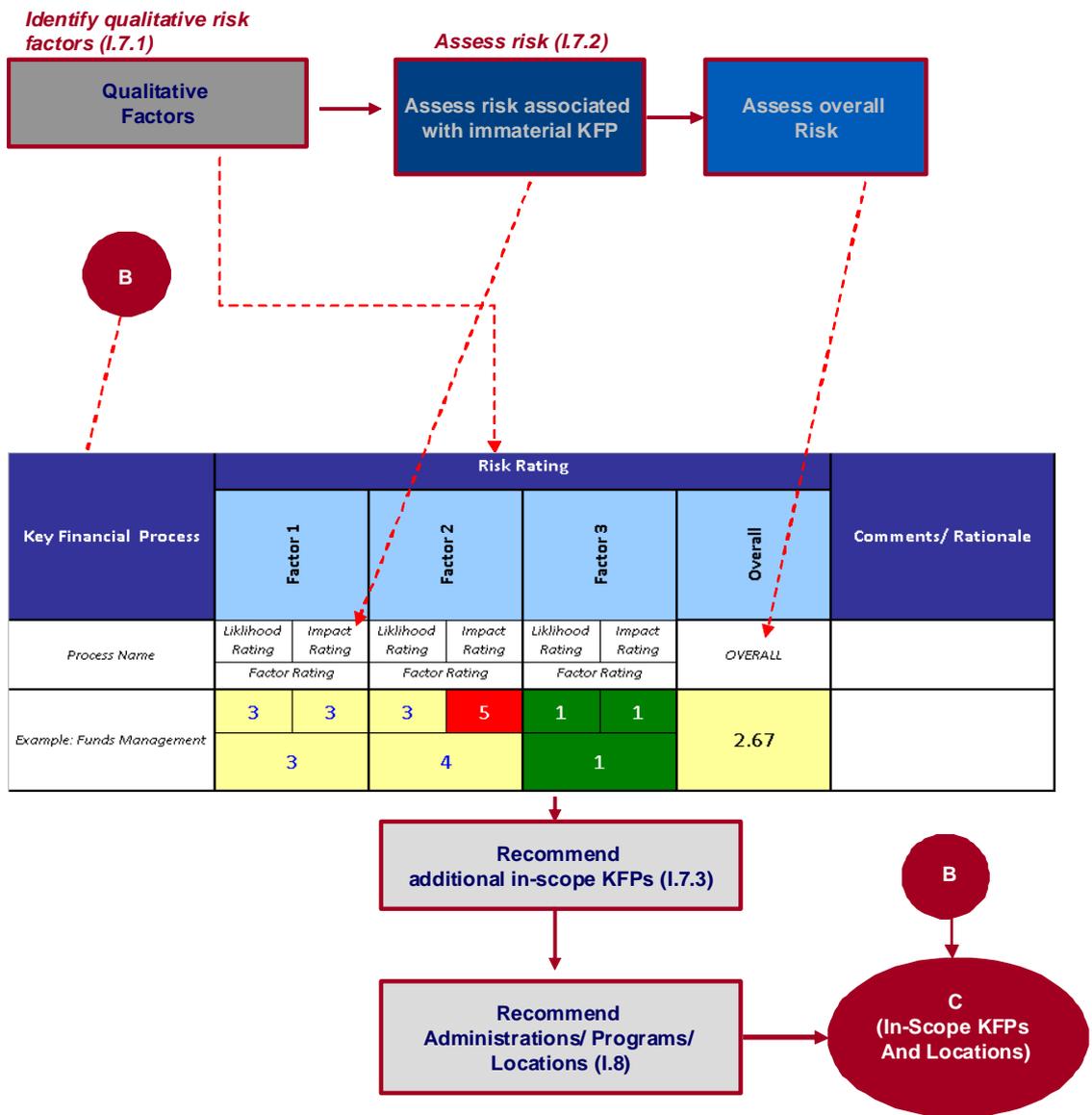
- Monitor progress**

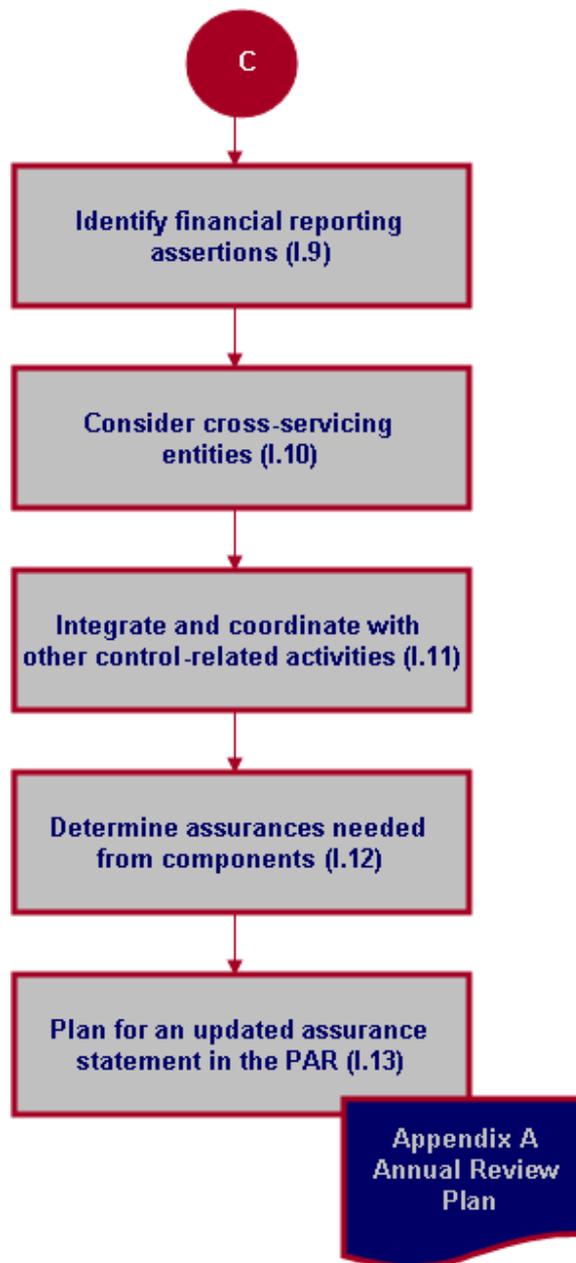
ICS will monitor progress against the project plan and provide regular updates to the Director of ICS.

## Planning: Inputs and Outputs

The following information flow charts depict the inputs used and outputs derived during the Planning Phase.







**II: Evaluating**

## II: Evaluating

The Evaluating phase involves understanding the key financial processes that support material line items and the controls over those KFPs. It includes assessing controls at the entity level as well as documenting KFPs, identifying key controls, and evaluating manual and IT controls. The table below reflects the required inputs and the key outputs of this phase.

The **Responsibility Assignment Matrix (RAM)** developed during the Planning Phase identifies the party responsible for leading the performance of each step as well as other parties that should participate in completing each step.

Activities / Steps	Inputs	Key Outputs
II.1 - Evaluate internal control at the entity level	None or Appendix A Annual Review Plan (if entity-level plan is included)	<ul style="list-style-type: none"> <li>▪ Assessment tool / Survey questions</li> <li>▪ Survey responses / Meeting minutes</li> <li>▪ Entity-level assessment results</li> </ul>
II.2 - Evaluate internal control at the KFP level	Appendix A Annual Review Plan: <ul style="list-style-type: none"> <li>▪ Key financial processes</li> <li>▪ Locations</li> <li>▪ Numbering scheme</li> </ul>	<ul style="list-style-type: none"> <li>▪ Process Narratives</li> <li>▪ Process Flowcharts</li> <li>▪ Risk/control Matrices</li> </ul>
II.3 - Understand the IT infrastructure and associated risks	Appendix A Annual Review Plan: <ul style="list-style-type: none"> <li>▪ Key financial processes</li> </ul>	<ul style="list-style-type: none"> <li>▪ IT General Computer Control assessment results</li> <li>▪ Cross-servicing provider assessment results</li> </ul>

\* \* \* \* \*

## II.1 Evaluate internal control at the entity level

Entity-level controls address the five elements of internal control as defined by the Government Accountability Office (GAO) and the Committee of Sponsoring Organizations (COSO). These five elements are Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. In addition to these five elements, entity-level controls may also include other controls that are pervasive in nature and that VA has determined to be necessary in order to carry out its operations.

As part of the assessment, ICS will document, test, and evaluate the design and effectiveness of the five standards of internal control. While the SAT is ultimately responsible for the entity controls evaluation, the Director of ICS will coordinate the effort and assign a sub-team within ICS to collect information and analyze results. Because entity level controls form the foundation for other controls, the testing and evaluation of these controls will occur early in the assessment phase. Weaknesses or deficiencies noted within these foundation controls will need to be corrected as soon as possible in order to prevent the weakening of other internal controls.

### II.1.1 Develop assessment tool

With the exception of the Control Activities element, evaluating entity level controls is generally accomplished through observation, inquiry, and inspection rather than the detailed transaction-level testing. (The Control Activities component will be tested with detailed testing as described in Phase III. Testing of this manual.) Interviews, questionnaires, and checklists are usually helpful at the entity level. GAO has prepared a tool to assist in the evaluation of entity controls. The Internal Control Management and Evaluation Tool are available on the GAO website. Other tools are also available including online survey tools and interview protocols.

- **Determine goal of entity assessment**

ICS will determine its goal for the entity assessment. Are there certain elements of internal control that are of particular interest to the SAT? Will the assessment focus on all five elements each year?

- **Develop survey questions**

ICS will develop survey questions or extract appropriate parts of the GAO tool to meet its goal. The questions will address both culture/control environment and the underlying documentation or support for control activities (e.g., policies and procedures).

**Key Outputs**

**Assessment Tool / Survey Questions**

### II.1.2 Identify sample

ICS will determine which individuals to survey or interview as part of the entity-level assessment. The sample will include representatives from various parts of VA and at various levels. However, ICS may consider weighing the sample towards OCFO personnel since A-123, Appendix A, is focused on management's control over financial reporting. Both VA management and staff will be included in the sample in order to determine whether there is a difference between management and employees' views of entity-level controls.

### II.1.3 Administer assessment

- **Determine administration method**

ICS will work with the SAT to determine the most appropriate administration method based on the selected assessment tool. For example, a checklist is suitable for web-based administration, whereas a face-to-face interview is more appropriate for open-ended questions.

- **Administer survey and/or conduct interviews**

Once ICS has determined the administration method, they will administer the survey and/or conduct interviews. For a web-based survey, ICS will plan for a response time of about two weeks. Interviews will be scheduled for approximately one-hour in length.

- **Prepare meeting minutes**

Any information gathered during interviews will be documented in meeting minutes and saved in TeamMate (the ICS document repository). Any supporting documentation will be retained as part of the workpapers.

<b>Key Output</b>	Survey Responses / Meeting Minutes
-------------------	------------------------------------

### **II.1.4 Analyze and report results**

Upon completion of the entity-level assessment, ICS will review the results and supporting documentation. This includes conducting an analysis of verbal feedback and a review of documentation. ICS will extract themes relating to the five elements of internal control (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring). For example, within Control Environment, themes may center on ethical tone, code of conduct, and ethics training.

Any findings will be reported to the SAT and addressed during the Concluding, Internal Reporting, and Correcting Phase.

For each of the above steps, ICS will develop and maintain detailed documentation including method of sample selection, interview protocols, test results, and analysis.

⇒ *Appendix D* describes in more detail the five Components of internal control and factors that the assessment team will consider when documenting, testing, and evaluating these Components and the level where it will be documented.

<b>Key Output</b>	Entity-Level Assessment Results
-------------------	---------------------------------

\* \* \* \* \*

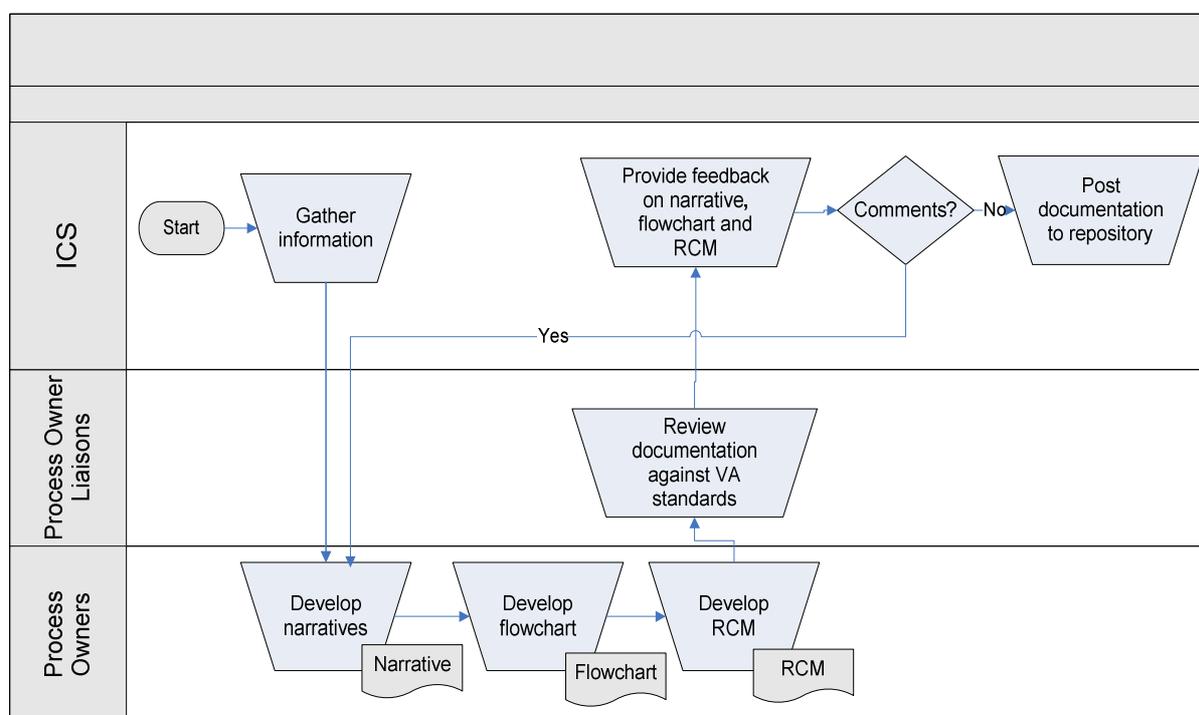
## II.2 Evaluate internal control at the KFP level

Internal control is an integral component of an agency's management that provides reasonable assurance in the achievement of the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with laws and regulations. Documentation forms the basis for establishing written descriptions of KFPs which are used to evaluate control design and effectiveness. Further, OMB Circular A-123, Appendix A, requires the SAT to document its understanding of VA's internal control over financial reporting.<sup>8</sup>

### II.2.1 Document key financial processes and key controls

The documentation will identify the key controls performed as part of the in-scope KFPs specified in the Appendix A Annual Review Plan.

ICS and the Process Owners will share responsibility for developing the documentation, reviewing it to verify that it is clear to someone with no knowledge of the process, and confirming its accuracy. The flowchart below illustrates the ideal documentation process.



#### II.2.1.2 Gather information

Creating documentation for a given KFP begins with developing a basic understanding of the KFP and identifying the appropriate Process Owners.

- **Identify Process Owner Liaisons and Process Owners**

SAT members will identify Process Owner Liaisons for each in-scope KFP. Process Owner Liaisons will identify Process Owners who perform the processes. The Process Owner Liaisons will also coordinate activities and facilitate communications between ICS and the Process Owners.

- **Review existing documentation**

<sup>8</sup> CFOC Implementation Guide for A-123, Appendix A, page 28.

Prior to contacting Process Owners, ICS will review existing documentation related to the KFP including cycle memos, relevant VA policies, and other internal documentation. Existing documentation will be saved in TeamMate.

### **II.2.1.3 Develop narratives**

Narratives are used to break down processes into individual, granular control activities. The individual KFP steps will be extracted from the meeting minutes, cycle memos, or other supporting documentation provided by the Process Owner (i.e., Standard Operating Procedures, Procedural memos).

- **Determine appropriate numbering for assigned KFP**

ICS and the Process Owners will use the numbering scheme assigned to their KFPs. The numbering scheme, which organizes documentation according to major KFPs, is included in the Master Process List.

- **Conduct interviews**

ICS and the Process Owners will call station points of contact (POCs) to arrange interviews and/or workshops with ICS and the Process Owners to gain an understanding of KFPs. The information gathered is the foundation for the A-123 process documentation. Often a single KFP will have more than one Process Owner. Ideally, all of the individuals involved in a given KFP would participate in the workshop. In cases where this is not possible, one-on-one or small group interviews work as well.

ICS and the Process Owners will facilitate interviews, being sure to ask the following questions:

- What is the risk being addressed?
- What is the control activity?
- Why is the activity performed?
- Who (or what system) performs the control activity?
- When (or how often) is the activity performed?
- What mechanism is used to perform the activity (reports and systems)?

Tip: Elements of good documentation include references to the following:

- Financial statement line items and general ledger accounts included in the cycle
- Processing documents
- Inputs, activities, and outputs
- Policies and procedures governing transactions
- Provisions of laws and regulations (e.g., the process used by management to ensure compliance with laws and regulations such as the Anti-deficiency Act)
- 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, etc.)
- Monitoring activities
- Relationship to other KFPs

When documenting a KFP, there is typically an associated IT element. As the interview discussion develops, it is important to ask the Process Owner how IT assists in the KFP and specifically what systems they use to perform their duties. For example, if a Process Owner

states "Once an invoice is received, it is posted," the interviewer should follow up by asking the following questions:

- Where is the invoice posted?
- What steps are performed to post the invoice?
- Who has approval and or access authority to perform the same function?

Additional IT questions could include the following:

- What systems/applications support the KFP?
- When do you use the systems/applications indicated in the course of the KFP?
- What types of reports are generated from these systems in the course of the KFP?
- How often are these reports generated?
- If an inspection is not in place, are there associated IT mitigating controls?

The following table provides tips on interviewing and gathering information for documentation:

Tip	Details
Determine the start and end point of a particular KFP	<ul style="list-style-type: none"> <li>▪ Consider what would initiate the particular KFP, keeping in mind that sometimes the KFP is actually initiated in a separate sub-KFP</li> <li>▪ Recognize that the end point will be often be how data is reported into the financial system and hits the general ledger</li> </ul>
Make contact with Process Owners before the interview	<ul style="list-style-type: none"> <li>▪ Briefly explain the purpose of the interview</li> <li>▪ Confirm the meeting time and place</li> <li>▪ Specify exactly which areas will be covered so the Process Owner can invite all of the necessary people to the meeting (this will help avoid inconsistencies in the description of the KFP since differences can be resolved during the interview)</li> <li>▪ Request that Process Owners bring copies of relevant documentation (reconciliations, journal vouchers, etc.)</li> </ul>
Ask open-ended questions	<ul style="list-style-type: none"> <li>▪ Ask Process Owners to demonstrate how certain tasks are completed</li> <li>▪ Questions should seek to obtain the <i>who, what, when, why, and how</i> of the activity.</li> </ul>
Take notes and obtain documentation	<ul style="list-style-type: none"> <li>▪ Gather as many sample documents as possible (reconciliations, reports, journal vouchers, screen prints, etc.)</li> <li>▪ Consider taking notes directly on sample documents. These notes can then be scanned and electronically included with the meeting minutes and work papers</li> </ul>

- **Prepare meeting minutes**

ICS will write meeting minutes based on discussions with Process Owners. The meeting minutes will document the following:

- Meeting date, time, and location
- Names and titles of participants
- Meeting purpose
- Definition of the KFP
- Process start and end points

- Detailed description of the activities, inputs, outputs, general ledger accounts, and policies related to the KFP

If clarification is needed, ICS may send the meeting minutes to the Process Owners for review and comment. ICS will retain meeting minutes in TeamMate (the ICS document repository).

- **Obtain Documentation template** 

ICS and the Process Owners will obtain and use the approved Documentation template, which includes a section for the KFP narrative. The template is available on SharePoint; additionally, a sample narrative is included as *Appendix N* of this manual.

There are three columns in the KFP narrative: Key Process Activity, Process Owner, and Control Matrix Reference.

Process Activity	Process Owner	Control Matrix Reference
<b>Background:</b> [An overview of the KFP including scope (KFP starting and ending points)]		
X.Y.Z.A [Step Title] [Description of step]	[Title]	
X.Y.Z.B [Step Title] [Description of step]	[Title]	C - X.Y.2

*Narrative within Documentation Template*

- **Complete narrative portion of Documentation template**

ICS and the Process Owners will use the meeting minutes to complete the following fields for each step of the KFP:

- Process Activity. Individual process activities refer to single, distinct actions that occur in the overall KFP. Activities should focus on relevant policies and procedures, impacted financial statement accounts and assertions, and manual and automated controls in place. When a KFP is broken out into activities, the activities should be presented in a manner that tells a story, in order from start to finish. Descriptions of activities should be comprehensive enough to facilitate a clear understanding of the KFP, identify general and key controls that are in place, and highlight any control gaps that may exist. The description of the KFP should start with the material financial statement line item and move backward through the summarizing KFP. The end point is the initiation of the transaction.
- Process Owner. The Process Owner signifies the organizational unit or group that takes ownership of the specific activity within the KFP (e.g., Accounts Payable or Industrial Property Division). The Process Owner does not have to be the same for the entire KFP, as control of activities within the KFP can transfer between different individuals/groups multiple times. Titles of specific individuals who perform activities within the KFP should be included in the activity text. While the meeting minutes may include individual names, the narratives will identify people by title only.
- Control Matrix Reference. After the process activities are built, the assessment team will determine which activities are controls. A control is a policy, procedure, or activity put in place by management to offset identified risks and ensure that its mission and directives

are essentially carried out. Not every activity is a control. Activities that are controls are signified with C#, where '#' corresponds to the step number. Additionally, append the node number of the activity step to the C# designation. It should read, C – 1.1.3.1, for example, signifying that the control is associated with step 1.1.3.1. This numbering will be used to populate the Risk/Control Matrix (RCM), ensuring that it can be tied to the process narrative.

- **Complete additional information within the Documentation template**

In addition to the narrative, ICS and the Process Owners will complete the following sections of the Documentation template:

- Significant Accounts. Enter the account number, account name, and financial statement line item for the main accounts affected by the KFP.
- Policies and Procedures. Document the policies and procedures that relate to the KFP.
- Interfaces with Other KFPs. Document touch points with other KFPs. For example, the Accounts Payable sub-process may reference a separate sub-process for the rejection of invalid invoices.
- Significant Documents or Reports. List any reports or outputs generated during the KFP. For example, if the Process Owner prepares an SF-424 reconciliation as part of the Funds Management KFP, the SF-424 form should be listed.
- Sources of Information. List the names, title and interview date for each person interviewed.

<b>Key Output</b>	<b>KFP Narrative</b>
-------------------	----------------------

⇒ See **Appendix N** for a sample narrative based on existing VA documentation of the Personal Property Disposals sub-process within the Property, Plant, and Equipment Management KFP.

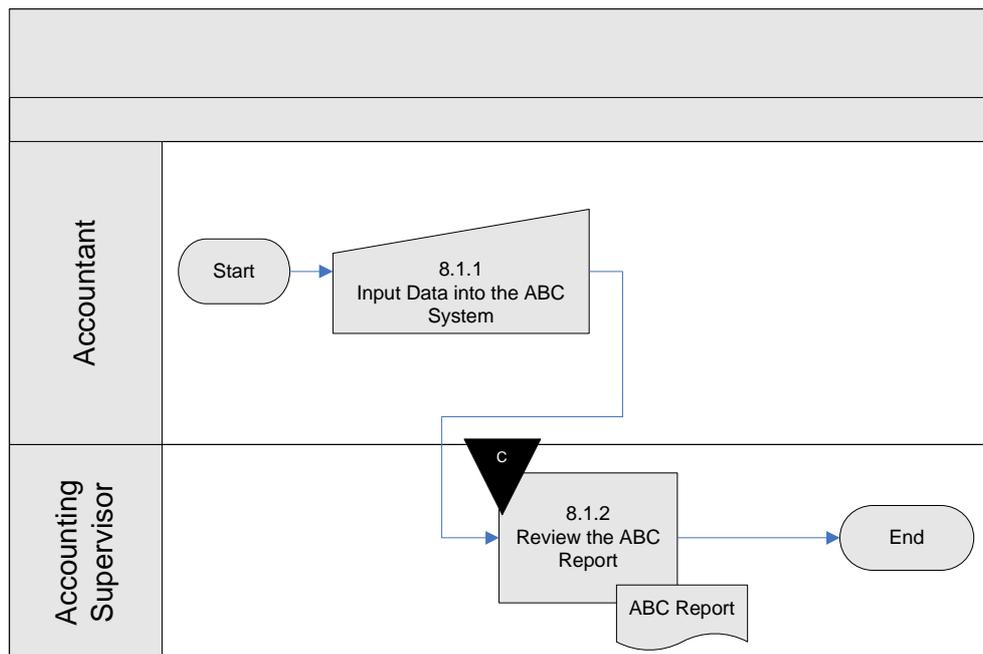
### II.2.1.4 Develop flowcharts

ICS and the Process Owners will develop flowcharts to complement their narratives. Flowcharts graphically depict the sequential flow of a process through events as objects, using a number of shapes. The flowcharts tie back to the narratives through "node numbers" that are placed on each object, directly corresponding to each control activity number in the narrative. Flowcharts are less detailed than the narratives, capturing only the principal steps in the KFP.

A simple example of a narrative and its corresponding flowchart is displayed below.

KFP Activity	Process Owner	Control Matrix Reference
<b>8.1.1 Input Data into XYZ System</b> The Accountant reviews the payment data from Treasury and enters the data into the XYZ system. The accountant prints the ABC report from the XYZ system.	Accountant	
<b>8.1.2 Review ABC Report</b> The Accounting Supervisor reviews the ABC report and signs/dates the report as evidence of review.	Accounting Supervisor	C - 8.1.2

Narrative



Flowchart

⇒ **Appendix N** includes a complete sample narrative and corresponding flowchart based on a Property, Plant and Equipment sub-process.

- **Obtain Visio template** 

ICS and the Process Owners will obtain the approved Visio template for flowcharts. The flowcharts will then be embedded in the documentation template with the corresponding narrative.

- **Create flowchart in Visio**

Using the narrative, ICS and the Process Owners will develop a corresponding flowchart in Microsoft Visio. There are three key components of the cross-functional flowchart: header, swimlanes, and key controls.

- Header (Title Bar). Header entries will follow the X.Y.Z numbering scheme discussed above and defined in the Appendix A Annual Review Plan.
- Swimlanes. Bands, or "swim lanes", are used in cross-functional flowcharting to highlight the relationship and timing between participants (actors) in the KFP. Each band belongs to an "actor". Actors are defined as the job role that performs the activity, such as AP Clerk or Property Accountant. If a flow continues across multiple pages, and an actor is not part of the KFP on one of those pages, the empty swimlane should remain on the page whenever space allows in the event the actor comes back into play on a future page.
- Controls. In the narrative, the assessment team-identified controls. If a narrative's KFP activity is determined to be a control, an inverted triangle (black fill with white text) is placed over the top left corner of the corresponding shape in the flow. The control number (C#) without the activity reference (1.1.1.3) is placed inside the triangle.

Additional flowchart guidance, including the usage of shapes, can be found in [Appendix F](#).

**Key Output**

Flowchart (within Documentation template)

- **Insert flowchart into documentation package**

ICS and the Process Owners will save their flowcharts in Visio and then use copy-and-paste-special to copy the flowchart from Visio and paste it into the Word documentation package as a picture.



### II.2.1.5 Develop Risk/Control Matrices

Once ICS and the Process Owners have prepared documentation for the in-scope KFPs, they will identify key controls within the KFPs in a Risk/Control Matrix (RCM). An RCM lists all controls (both key and non-key) and captures additional detail around each. The goals of the RCM are as follows:

- Identify key controls and assess the design of controls
- Determine if the controls in place adequately mitigate the risks and meet the stated control objectives

- **Obtain RCM**

ICS and the Process Owners will obtain the RCM from SharePoint. During the Planning phase, the RCM was populated with risks, control objectives, risk level, financial statement assertions and expected key controls.

- **Update risks and control objectives**

ICS and the Process Owners will confirm the risks, control objectives, and expected key controls for each KFP. Since control objectives and risk are based on how a KFP *should be* designed rather than how it is working in practice, this step can actually be completed before the documentation step. For example, within Financial Reporting, some of the risks may include the following:

- Inaccurate changes to the chart of accounts result in financial reporting errors
- Incorrect postings result in inaccuracies in subsidiary ledgers and the general ledger
- Budgetary and Proprietary accounts do not balance causing an inaccuracy in the Statement of Budgetary Resources
- Adjustments are inaccurate, incomplete, and not made in the correct accounting period

- **Populate RCM with actual control activity information**

ICS and the Process Owners will use the narratives to complete the remaining columns of the RCM template in Excel. At a minimum, the RCM should include the key controls that correspond to risks and the expected key controls. Note that if there is a control objective and risk that does not have a corresponding control, the remaining columns within that row should be left blank. (This will be covered further in Activity III.2.3)

Title	Definition
Control Reference Number	Used as a unique identifier for tracking, consolidation, and aggregation purposes. This number corresponds to the documentation and is determined by numbering scheme specified in the Appendix A Annual Review Plan.
Actual Control Activity	Indicates the KFP to which the control objective and control activity apply. The control activity can be obtained directly from the KFP narrative. (This may or may not be the same as the Expected Key Control documented during the Planning Phase.)
Process Owner	Used to identify the owner and key contact personnel. The Process Owner's title (rather than name) should be used.

Title	Definition
Information Processing Objective (optional)	<p>Describes management's goal in relation to controls to help support management's implicit financial statement assertions. The Information Processing Objectives are:</p> <ul style="list-style-type: none"> <li>▪ Completeness of records (C)</li> <li>▪ Accuracy of records (A)</li> <li>▪ Validity of records (V)</li> <li>▪ Restricted access to assets and records (R)</li> </ul> <p>See <i>Appendix E</i> for details on the information processing objectives.</p>
Financial Statement Assertions (optional)	<p>Lists the financial statement assertions that the control addresses. These are as follows:</p> <ul style="list-style-type: none"> <li>▪ Presentation and Disclosure (PD)</li> <li>▪ Existence or Occurrence (EO)</li> <li>▪ Rights and Obligations (RO)</li> <li>▪ Completeness (CO)</li> <li>▪ Valuation or Allocation (VA)</li> <li>▪ Laws and Regulations (LR)</li> </ul> <p>Recall that the assertions were mapped to the financial statement line items and KFPs during the Planning Phase (See Activity I.9). The top portion of the RCM (completed during the Planning Phase) indicates the financial statement assertions for the process as a whole.</p> <p>In the Evaluating Phase, the assertions are being associated with individual risks and controls. If a process does not have any gaps, the group of controls within the process will address all relevant assertions identified in Activity I.9.</p> <p><i>Appendix E</i> also includes details on the financial reporting assertions.</p>
Preventive or Detective	<p>Preventive controls (P) are typically "front-end" actions/activities that deter errors in financial reporting, whereas detective controls (D) are actions/activities that serve the purpose of discovering errors in financial reporting that have already been processed. For example, journal voucher approval is a preventative control while a reconciliation is a detective control.</p>
Manual or Automated?	<p>Indicates whether a control is being performed manually, or if it is automated. For automated controls, a column has been included so that the application used to perform the control can be noted as well.</p>
Application (if Automated)	<p>For manual controls, this column should be marked "N/A". For automated controls, the application used to perform the control should be noted.</p>
Frequency of Control	<p>The frequency of the control activity is important in determining the minimum sample size. Typically, the frequency of a control is one of the following:</p> <ul style="list-style-type: none"> <li>▪ Annually</li> <li>▪ Semi-annually</li> <li>▪ Quarterly</li> <li>▪ Monthly</li> <li>▪ Weekly</li> <li>▪ Daily</li> <li>▪ Multiple times per day</li> </ul> <p>In cases where a control happens as a result of a trigger event, it will be assumed that the control is "continuous" (for sample, size selection purposes).</p>



### II.2.1.6 Perform quality control activities

Process Owners, Process Owner Liaisons and ICS are all responsible for quality control. Quality control procedures involve checking for accuracy and consistency across outputs (narratives, flowcharts and RCMs) and ensuring that outputs are prepared on schedule. The Documentation Quality Review Checklist is a tool that can be used to review documentation. Refer to Appendix 6 for a larger screenshot:

Department of Veterans Affairs A-123, Appendix A, Assessment					
Documentation Quality Review Checklist					
Document Name					
Originator(s)					
Deliverable Due Date					
Date Provided					
Reviewers: Place check marks in each of the boxes to indicate review of the attribute. Initial and date the bottom of the column as evidence of your review.					
	Process Owner	Process Owner Liaison	ICS	Other	Other
<b>Narrative</b>					
Describes the complete process as defined by VA					
Is formatted in accordance with template					
Contains clear descriptions of activities and controls					
Specifies Process Owners for each step					
Contains clear activity/step headings (Verb+object)					
Addresses all various scenarios (i.e. - What if the supervisor does not approve the JV?)					
Contains correct spelling, grammar, formatting					
<b>Flowchart</b>					
Displays consistent step names and numbers with narrative and RCM					
Uses correct shapes for each step					
Displays start and end points					
Includes yes/no options for all decision boxes					
Contains correct spelling, grammar, formatting					
<b>Risk Control Matrix</b>					
Is consistent with narrative and flowchart					
Contains all required fields					
Includes correct identification of objectives and risks					
Identifies key controls					
Identifies application name for all automated controls					
Contains correct spelling, grammar, formatting					
Initials					
Date					

*Documentation Quality Review Checklist*

- **Complete Documentation Quality Review checklist (ICS/Process Owners)** 

ICS and Process Owners will complete the Documentation Quality Review checklist and send the completed checklist with the documentation package to respective Liaisons.

- **Complete Documentation Quality Review checklist (Liaisons)** 

Process Owner Liaisons will complete the Documentation Quality Review checklist and submit the completed checklist with the documentation package to ICS.

- **Complete Documentation Quality Review checklist (ICS)** 

ICS will determine if any other stakeholders, such as the Associate Director for Financial Controls Division or the Director of ICS, should review the documentation and finalize the quality checklist. The necessary stakeholders will complete and retain the checklist with the final documentation.

- **Provide status updates (Process Owner Liaisons)**

Process Owner Liaisons are responsible for reporting progress as requested by ICS. At a minimum, Process Owners may be asked to report status of documentation (not started, interviewing, drafting, reviewing, or complete) and an estimated completion date for each assigned sub-process.

### ***II.2.1.7 Retain documentation***

ICS will retain documentation and quality control checklists in TeamMate.

## II.2.2 Evaluate control design

In assessing the design of controls, ICS and the Process Owners will determine whether the controls will, if operating as intended, provide reasonable assurance that management's information processing objectives/CAVR are being met in relation to the relevant financial statement assertions for all significant accounts and disclosures. While ICS and the Process Owners share responsibility for this task, it may be difficult for Process Owners to evaluate their own KFPs. ICS will serve as an independent perspective and assist in the design evaluation.

- **Complete the evaluation columns of the RCM template**

The RCM discussed in Activity II.2.1.5 is a useful tool for documenting control design. ICS should complete the following columns of the RCM template in order to document the control design:

Title	Definition
Design Gap (Y/N)	Indicates whether a control is designed effectively. In cases where a design gap exists, it is also necessary to fill out the columns prioritizing and describing the gap.
Gap Description	Describes in detail why the control design is considered to be inadequate, and the impact of the design gap.

When evaluating the design of controls, key questions to consider include the following:

- Are there any objectives/risks that were not matched to corresponding controls? (These would be indicated by blank rows in the RCM.)
- Do the control activities in place cover all information processing objectives (CAVR)?
- Do the control activities in place cover all associated financial statement assertions? In other words, is there at least one key control that addresses each of the relevant assertions specified in the Planning Phase. (See Activity I.5)
- Are there mismatches between a control activity in place and the associated CAVR?
- Are there excessive control activities addressing a single CAVR or assertion?
- Is there an appropriate balance of preventive and detective controls?

If the answer to any of the above questions is "no", a control gap may be present. Other considerations regarding the evaluation of control design is included in the following table<sup>9</sup>:

Consideration	Detail
The alignment between the controls and the risks identified (i.e., whether the KFPs and related controls appear to be effective in achieving management's stated objectives and managing its risks)	<p>The appropriateness of a control alignment relates to the control's directness and selectivity.</p> <ul style="list-style-type: none"> <li>▪ The more direct the alignment/relationship, the more effective the control may be in achieving the objective.</li> <li>▪ Selectivity refers to the magnitude of the amount, or the significance of other criteria or distinguishing characteristics, that a specific control will identify as an exception condition.</li> </ul>

<sup>9</sup> CFOC Implementation Guide for A-123, Appendix A, Page 28. Based upon the GAO/PCIE Financial Audit Manual, Section 340.

Consideration	Detail
Frequency of the control - whether the control will detect or prevent the risk identified on a timely basis (i.e., in some cases, a detective control may be adequate, but in other cases, an entity should ensure adequate preventative controls are in place)	The regularity with which controls are applied can determine the effectiveness of the control. Generally, the more frequently a control is applied, the greater the likelihood that it will be effective.
Knowledge and experience of the people involved in performing the controls	The person applying a control should have the necessary knowledge and expertise to properly apply it. The lesser the person's experience and skills, the less likely that the control will be effective (i.e., effectively applied). Also, the effective application of a control is generally adversely affected if the activity (1) is performed by an employee who has an excessive volume of work or (2) is not performed carefully.
Segregation of duties relevant to the process being controlled	Lack of segregation of duties over control activities and monitoring controls hinders the effectiveness of the control. For example, an effectively designed control activity such as a reconciliation of Fund Balance with Treasury to Treasury records should be considered ineffective if the related monitoring activity of supervisory review of the reconciliations is performed by the same person.
Timeliness in addressing issues and exceptions that result from the control activity (follow-up procedures)	A control's effectiveness is dependent on the effectiveness of follow-up procedures. To be effective, these procedures should be applied on a timely basis and should (1) determine whether control exceptions represent misstatements and (2) correct all misstatements noted. For example, as a control, an accounting system may identify and put exception transactions into a suspense file or account. Lack of timely follow-up procedures to (1) reconcile and review the suspense file or account and (2) correct items in the suspense file or account would render the control ineffective.
Reliability of the information used in the performance of the control	If the control is contingent upon specified data, the reliability of the information will determine the effectiveness of the control. For example, if one of the controls over compliance with the Prompt Pay Act requires management to review a system-derived management information report that ages receipt of invoices, the control will be rendered ineffective if the controls over the system (General or Application controls) used to produce the management information report are determined to be ineffective (i.e., unreliable).
Period covered by the control	To be effective, the controls should be in place during the period under assessment.

ICS will also evaluate controls based on the level of assurance provided by the control. In evaluating the level of assurance provided by a given control, ICS will consider the nature of the control, how the control is applied, the consistency with which it is applied, and who applies it.

The degree of assurance over internal control will vary based on several factors, including those listed below:

Less Assurance	Greater Assurance
Manual control	Automated control
Complex control (requires many steps, multiple calculations, etc.)	Simple control (single step, single calculations, etc.)
Control is performed by a junior, inexperienced person	Control is performed by an experienced manager
Detective control (detects a potential problem after a transaction is executed)	Preventive control (prevents a problem)
Single control	Multiple, overlapping controls
High-level control (analytics)	Detailed, transaction-level control
Control uses sampling	Control involves checking all items
Control takes place well after the transaction	Control occurs in real time (i.e., as the transaction takes place)

*Factors Affecting the Degree of Assurance over Internal Control*

Management's evaluation of design effectiveness is important because only properly designed controls can mitigate risk. Thus, ICS will document its evaluation in a clear and comprehensive manner within the "Gap Description" column of the RCM.

- **Review design assessment (Associate Director)**

The Associate Director for the Financial Controls Division will review the assessment columns of the RCM. Once the Associate Director has reviewed and approved all RCMs within a given KFP, he will inform the Director that the RCMs are ready for Director review.

- **Review design assessment (Director of ICS)**

The Director of ICS will review the completed RCM. If needed, the Director will seek guidance from OBO, SAT, or the OIG in order to finalize design gaps and design deficiencies.

- **Update Exception Log**

ICS will enter exceptions related to control design (missing and poorly designed controls) into an Exception Log. The Exception Log template and instructions for completing in are described in Activity IV.1.

## **II.2.3 Identify key controls**

Within the RCM, ICS and the Process Owners will identify the key controls. A key control is a control, or set of controls, that addresses the relevant assertions for a financial statement line item. RCMs assist in the identification of key controls and the presentation of controls-related analysis. Controls over effectiveness and efficiency of operations and compliance with laws and regulations that have a direct and material impact over financial reporting will be included in the RCMs. Documentation related to the design will include a description of controls over the prevention and detection of fraud, including who performs the control and the related segregation of duties.

Key controls will be determined using the following steps:

- **Identify controls that cover the most PERCV and CAVR elements for each control objective.**

For example, if a control covers seven out of the ten PERCV and CAVR elements, it may be a key control whereas, if a control covers only two out of the ten elements, it may be a mitigating control.

- **Determine the control that addresses the most control objectives and select it as a key control.**

For example, “Supervisor reviews and approves the reconciliation of time reports to time sheets performed by the Analyst” addresses more control objectives than “Analyst reconciles time reports to time sheets and notes any discrepancies in a log.”

Sample key controls from the Property, Plant and Equipment key financial process

- The Facility Director reviews the Investment Matrix to ensure that it is complete and accurate and authorizes and approves the matrix with a signature and date.
- The Property Management Specialist sends a copy of the Inspection Report as well as an email to the Contracting Officer at the National Acquisition Center to notify the Contracting Officer of the completion of the inspection.

- **Select a control as key if it is the only control for a PERCV or CAVR element**
- **Be sure to select at least one key control for each control objective**
- **Mark a "Y" in the Key Control Column of the RCM template for each key control**

## II.2.4 Evaluate the controls of cross-servicing providers and service organizations

Cross-servicing providers and service organizations are entities outside of VA that process financial data. The use of such organizations was covered in detail in Activity I.10. During the Evaluating Phase, ICS will perform its assessment of service organization controls.

### II.2.4.1 Assess results of SAS 70 reports

In assessing the results of the SAS 70 reports, ICS will determine whether the failure of any controls would diminish the ability of VA to place reliance on the application reviewed. For example, the failure of the controls related to two control objectives and the fact that several control objectives have not been met does not necessarily diminish the ability of VA to place reliance on the reviewed application because the nature of the control failures is such that any risk related to VA financial statements is minimal. Also, it is important to note that if a failure is identified, but mitigating controls have been applied, the application could be considered reliable.

- **Obtain SAS 70 Assessment Checklist template** 

ICS has developed a SAS 70 checklist template in Microsoft Excel. ICS will obtain the template from SharePoint. Refer to Appendix 4 for a larger screenshot:

SAS 70 Assessment Checklist		
Cross-servicing organization		
Report Title		
Report Date		
Question	Y/N	Notes
Are controls in place to provide reasonable assurance that physical and logical access to VA mainframe and client-server resources, using computer terminals at client locations, is restricted to authorized individuals?		
Are controls in place to provide reasonable assurance that designated individuals, at client locations, comply with VA security policies, standards, and procedures?		
Are controls in place to provide reasonable assurance that audit reports of system use made available by VA are reviewed?		
Are controls in place to provide reasonable assurance that VA receives prompt written notification of changes for individuals who are authorized to add, change, and delete user access to VA application production regions?		

*SAS 70 Assessment Checklist*

- **Complete SAS 70 Assessment Checklist**

ICS will review the SAS 70 reports and complete a SAS 70 Assessment Checklist for each service provider. The checklist addresses the following questions:

- Are controls in place to provide reasonable assurance that physical and logical access to VA mainframe and client-server resources, using computer terminals at client locations, is restricted to authorized individuals?
- Are controls in place to provide reasonable assurance that designated individuals at client locations comply with VA security policies, standards, and procedures?
- Are controls in place to provide reasonable assurance that audit reports of system use made available by VA are reviewed?
- Are controls in place to provide reasonable assurance that VA receives prompt written notification of changes of individuals who are authorized to add, change, and delete user access to VA application production regions?

- Are controls in place to provide reasonable assurance that client custom programming changes are appropriately documented, reviewed, tested, and implemented?
- Are controls in place to provide reasonable assurance that comprehensive user acceptance testing for any fixes and enhancements are performed and communicated to the responsible individual(s)?
- Are controls in place to provide reasonable assurance that the record-retention (e.g., off-line storage) requirements for financial statements are documented and communicated to the responsible individual(s)?
- Are controls in place to provide reasonable assurance that on-line retention and archiving of VA data has been established and communicated to the responsible individual(s)?
- Are controls in place to provide reasonable assurance that Computer Incident Response procedures have been developed in coordination with the responsible individual(s)?
- Are controls in place to provide reasonable assurance that the production cycles are properly maintained and changes to them are timely communicated to the responsible individual(s)?
- Are controls in place to provide reasonable assurance that obligations are not incurred in excess of the available budgetary amounts?
- Are controls in place to provide reasonable assurance that appropriate users review output reports for completeness and accuracy?
- Are controls in place to provide reasonable assurance that the transactions processed are complete, accurate, and appropriately authorized and approved?
- Are controls in place to provide reasonable assurance that erroneous data is corrected and resubmitted?
- Are controls in place to provide reasonable assurance that incompatible job functions surrounding the processing of VA transactions are identified and pertinent policies and procedures are enforced to segregate these job functions?

- **Review SAS 70 Assessment Checklist**

The Associate Director for the Financial Controls Division within ICS will review the SAS 70 Assessment Checklist and sign/date the bottom of the checklist as evidence of his review.

- **Retain documentation**

ICS will retain the checklists in TeamMate.

### ***II.2.4.2 Perform alternate procedures***

If an annual assurance statement or SAS 70 does not exist, ICS will conduct the alternate procedures outlined in its Appendix A Annual Review Plan. Refer to *Appendix H* for an explanation of alternative procedure options.

<b>Key Output</b>	<b>Cross-servicing provider assessment results</b>
-------------------	--

\* \* \* \* \*

## II.3 Understand IT structure and associated risks

IT controls fall into two categories: general computer controls and IT application controls. General controls include controls over the IT environment, computer operations, access to programs and data, program development, and program changes. These controls represent the foundation of the IT control structure. They help ensure the reliability of data generated by IT systems and support the affirmation that systems operate as intended and that output is reliable.

Application controls refer to the transactions and data controls that ensure the completeness and accuracy of records and the validity of the entries resulting from both manual and programmed processing. Examples of application controls include data input validation, agreement of batch totals, and the accuracy of reports. These controls vary based on the business purpose of the specific application. Application controls also include interface controls, which help ensure the privacy and security of data transmitted between applications.

The A-123 assessment of general computer and application controls should be coordinated with other IT-related assessments, where possible, as documented in the Appendix A Annual Review Plan (see Activity I.13 of this manual). The plan also documents which systems (for application controls) and host environments (for general controls) should be included in the current year's assessment.

### II.3.1 Assess general computer controls

As part of its assessment, ICS must evaluate general computer controls (GCCs). GCCs are pertinent for all applications. The objectives of general controls are to ensure a controlled operating environment is maintained for the development and functioning of applications. As such, all relevant control environments should be assessed.

VA's Office of Information and Technology (OI&T) conducts FISMA internal assessments based on the control requirements listed in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, as required by VA Directive 6500. As part of its assessment, ICS should consider Certification and Accreditation (C&A) documentation, FISMA assessments, and other Department-wide efforts in order to determine what additional testing - if any- needs to be completed in order to meet the guidelines established in the Federal Information System Controls Audit Manual (FISCAM), and to satisfy the level of testing required by A-123.

The steps below provide VA with an IT internal control framework to help VA effectively identify and document its general computer controls. Several of these frameworks exist; however, FISCAM was created by the GAO as the primary methodology to evaluate general computer controls and application controls for financial systems in Federal Government agencies.

- **Determine relevant FISCAM elements**

Although FISCAM should be used to help VA identify and document its general computer controls, VA should carefully consider which of FISCAM's "critical elements" (control objectives) and related "control activities" are relevant to its specific risks and unique IT environment. VA may not need to include all control activities specified by FISCAM, or may need to include others not specified by FISCAM. Additional controls are often included from NIST SP 800-53 "Recommended Security Controls for Federal Information Systems."

Accordingly, VA should use judgment to tailor FISCAM, so it is appropriate to the size and complexity of the IT environment. The security categorization of information and information systems completed by VA as a result of Federal Information Processing

Standards (FIPS) Publication 199 can help the Department appropriately tailor FISCAM for each system. According to FIPS Publication 199, “the security categories [low, moderate, and high] are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfil its legal responsibilities, maintain its day-to-day functions, and protect individuals.” This security categorization is based on the following three security objectives: confidentiality, integrity, and availability.

The following table is an overview of what will be documented for each of the major categories of FISCAM and how the financial statement assertions link to each of these categories.

FISCAM Category	What Should be Documented?	Financial Statement Assertions Affected
Security Management (SM), FISCAM Section 3.1	The design of the entity-wide security controls pertaining to in-scope applications and IT environments. (Note: As indicated in Section 3, the in-scope applications are those that play a role within the processes/cycles that are considered significant to the financial statements.)	All
Access Control (AC), FISCAM Section 3.2	The design of the access controls pertaining to in-scope applications and IT environments.	All – but most relevant to completeness and existence
Configuration Management (CM), FISCAM Section 3.3	The design of the system configuration controls necessary to provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended,	All
Segregation of Duties (SD), FISCAM Section 3.4	The design of the segregation of duties controls pertaining to in-scope applications and IT environments.	All
Contingency Planning (CP), FISCAM Section 3.5	The design of the system contingency controls pertaining to in-scope applications and IT environments as necessary for the operating environment.	All – but most relevant to completeness and existence

*Overview – Documentation by FISCAM Category*

- **Obtain GCC template** 

General Computer Controls should be evaluated once for each environment (e.g., operating environment [Mainframe, Active Directory] or host site) in which they operate, and they apply to all applications hosted within that environment.

The Appendix A Annual Review Plan indicates which environments/host sites are in scope for the current fiscal year. GCCs can be documented in their own evaluation template, which

is categorized by FISCAM area. There will be one GCC form for each in-scope environment. The ICS-approved template is located on SharePoint. Refer to Appendix 5 for a larger screenshot:

Department of Veterans Affairs						
General Computer Controls Assessment						
Environment (Host Site):						
VACO						
FISCAM Reference	Element (Control Objective)	Description and Frequency of Control Activity	Control Techniques	P or D (1)	A or M (2)	Control Effective (Y/N)?
Five domains within FISCAM include: Security Management (SM), FISCAM Section 3.1; Access Control (AC), FISCAM Section 3.2; Configuration Management (CM), FISCAM Section 3.3; Segregation of Duties (SD), FISCAM Section 3.4; Contingency Planning (CP), FISCAM Section 3.5.	Describe the purpose of the control activity	Explain the actual activity being performed and how often the activity is performed, e.g., daily, weekly, monthly, annually	Describe the requirements associated with an effective control for this control activity	Indicate the control approach as either preventive or detective	Identify the control activity as automated (performed using a system or application) or manual (requires human intervention or judgment)	Indicate the control design as effective (Y) or not effective (N)
AC-2.1	Resource owners have identified authorized users and their access is authorized.	Access authorizations are (a) documented on standard forms and maintained on file, and (b) evidence of management approval is retained. Daily activity.	1. Appropriate business owners periodically review current access levels and determine whether users and their associated access rights remain appropriate. Documentation of management review and corrective actions taken are retained. 2. Inactive users' accounts are monitored and removed after a predetermined period of inactivity (i.e., 120 days)	P	M	Y

GCC Template

- **Complete GCC template**

The assessment team should complete the fields in the GCC template.

- **Environment/Host Site.** Specify the environment for the particular GCC assessment. (Note that there will be a completed GCC template for each in-scope environment.)
- **FISCAM Reference.** Specify one of the five domains within FISCAM which are: Security Management (SM), Access Controls (AC), Configuration Management (CM), Contingency Planning (CP), and Segregation of Duties (SD)
- **Critical Element (Control Objective).** Describe the purpose of the control activity
- **Description and Frequency of Control Activity.** Explain the actual activity being performed and how often the activity is performed, e.g., daily, weekly, monthly, annually
- **Control Techniques.** Describe the requirements associated with an effective control for this control activity
- **Preventive or Detective?** Indicate whether the control is preventative (P) or detective (D)
- **Manual or Automated?** Identify the control activity as 'A' for automated (performed using a system or application) or 'M' for manual (requires human intervention or judgment)
- **Control Effective?** Indicate the control design as effective (Y) or not effective (N)

**Key Output**

Cross-servicing provider assessment results

### II.3.2 Assess application controls

Application software handles business transactions. Many key processes involve applications and, therefore, contain an associated IT element. The Director of ICS is responsible for coordinating the documentation and assessment of both manual and IT controls. The CFOC implementation guide notes, "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."<sup>10</sup> The documentation and assessment of application controls is part of the documentation and assessment of business process-level controls, and consideration should be given to FISCAM Chapter 4, Evaluating and Testing Business Process Application Controls. See steps in Activity II.2. All of these steps apply to application controls as well as manual controls.

\* \* \* \* \*

---

<sup>10</sup> CFOC Implementation Guide for A-123, Appendix A, page 31.

**III: Testing**

### III: Testing

Once the assessment team has documented controls and evaluated the design of those controls, they will test properly-designed, key controls to validate their effectiveness. The ultimate goal of testing a control is to verify that it is functioning properly (i.e., as designed). ICS staff and Process Owners will conduct testing, with oversight from the Director of ICS, OBO, and SAT. ICS will retain evidence of testing to support the assessment.

One of the most critical activities for ICS is to develop an overall Test Plan. Like the Appendix A Annual Review Plan developed in the Planning Phase, the Test Plan documents VA's approach to testing. This plan is described in detail in a later section of this guide.

Testing will be conducted by objective personnel. The person performing the test will not be the person responsible for performing the control, or report directly to the person performing the control.

The responsibilities for the stakeholders involved in the Testing Phase are displayed in the table below:

Activities / Steps	Inputs	Key Outputs
III.1- Develop Test Plan	Appendix A Annual Review Plan: <ul style="list-style-type: none"> <li>▪ Key Financial Processes</li> <li>▪ Locations</li> <li>▪ Resources</li> <li>▪ Project Schedule</li> </ul>	<ul style="list-style-type: none"> <li>▪ Overall Test Plan</li> <li>▪ KFP-level test plans</li> </ul>
III.2 - Test key controls	<ul style="list-style-type: none"> <li>▪ KFP-level test plans</li> </ul>	<ul style="list-style-type: none"> <li>○ Evidence request list</li> <li>○ Testing documentation and results (completed KFP-level test plan templates and Test Sheets)</li> <li>○ Exception Log</li> </ul>

\* \* \* \* \*

#### III.1 Develop Test Plan

During the initial years of A-123, Appendix A, VA will test key controls in order to verify that controls are operating effectively. ICS will document its testing approach, as well as other planned testing procedures. This documentation may be included in an overall Test Plan or in the Appendix A Annual Review Plan covered in Phase I.

VA will consider using a risk-based approach. More information regarding risk-based testing approaches is included in *Appendix I*. Regardless of whether VA uses a risk-based approach, its Test Plan will address the following items:

- Which controls will be tested (entity-level, manual controls, application controls, GCCs)
- Who will perform the testing (ICS, Process Owners, contractors)
- When testing will be performed
- Where testing will be performed

- How controls will be tested (inquiry, inspection, observation, re-performance)
- What sample sizes will be used
- What testing documentation (workpapers) will be developed and retained

Each of these testing dimensions is discussed in more detail in the following section.

### **II.1.1 Determine which controls will be tested**

ICS will demonstrate that controls covering the five Components of internal control (*Appendix D*) are operating effectively relative to significant line items and related accounts, disclosures, KFPs, and locations. In general, ICS will test key controls that are in place and properly designed. They will exclude the following controls:

- Controls deemed to be non-existent or insufficient in operation or design by VA management, GAO, OIG, or Independent Public Auditors. In these instances, ICS will determine if remediation is underway, and if not, recommend that corrective actions be implemented.
- Controls tested during other reviews such as SAS 70, FISMA, or FFMIA compliance reviews. The team will review assessment results, applicable reports, or supporting documentation and incorporate results into the overall assessment of controls.
- Remediated controls that have not been in operation for a sufficient period of time to assess operating effectiveness (See *Appendix I* on Risk-based Testing).

ICS will document which controls will be tested in the Overall Test Plan.

### **III.1.2 Identify who will perform the testing**

It is important that Process Owners and personnel completing the control activities are trained and knowledgeable about the assessment of controls within their KFPs. If Process Owners are involved in testing, ICS will ensure that the testers are objective. The person performing the test should not be the person responsible for performing the control, or report directly to the person performing the control. ICS will document who will perform the testing in the Test Plan.

### **III.1.3 Determine when testing will be performed**

ICS will schedule testing in the late spring or summer. This will facilitate VA's ability to prepare its Statement of Assurance as of June 30 for inclusion in the annual PAR issued in November. The test population will be transactions occurring from July 1 through June 30. OMB's A-123 Frequently Asked Question Memorandum states:

“The year-end financial reporting controls in place for the prior fiscal year may be included in the current year’s assessment, if the control environment has remained fairly stable.”<sup>11</sup>

ICS will also plan to conduct additional testing in the late summer and early fall to address any changes in the control environment that occurred between June 30 and the end of the fiscal year. ICS will document the testing schedule in the Test Plan.

### **III.1.4 Determine where testing will be performed**

The locations selected and the testing performed at each location will follow from the decisions made during the Planning Phase. See Activity I.8 for additional guidance. ICS will document where testing will be performed in the Test Plan.

---

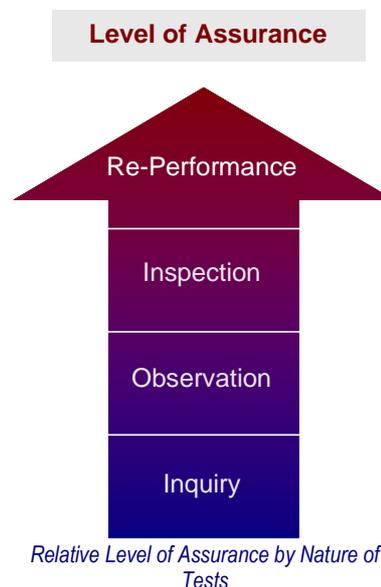
<sup>11</sup> OMB A-123 Frequently Asked Question Memorandum, April 2006

### III.1.5 Determine how controls will be tested (inquiry, inspection, observation, re-performance)

ICS will determine how controls will be tested based on the nature and frequency of the control. The type of the tests to be performed is classified into four categories: inquiry, observation, inspection, and re-performance. ICS will likely use a combination of testing types. The testing types are described in *Appendix J*.

Combining two or more of these tests will provide greater assurance than using only one technique. The more significant the account, disclosure, or KFP and the more significant the risk, the more important it is to determine if audit evidence extends beyond one testing technique. The nature of the control also influences the nature of the tests of controls that will be performed. Most manual controls will be tested through a combination of inquiry, observation, examination, or re-performance.

ICS will document the overall approach to testing in the Test Plan. When developing KFP-level test plans (Activity III.2.1), the team will determine how best to test each individual control.



### III.1.6 Define sample sizes

The sample size selected for testing will be based on the significance of the control in question and the level of assurance desired. The fewer items tested, the greater the risk of an erroneous conclusion. Thus, when a single manual control provides the sole support for a financial statement assertion relative to a significant line item, ICS will consider increasing its sample size. This decision will be made after considering other evidence available (e.g., self-assessment results or evidence from other monitoring controls). The combination of evidence will provide a high level of assurance that the control is operating effectively. When no exceptions are found, these sample sizes will also provide a high level of assurance that the control is operating effectively. Sample sizes will be based on the frequency of a control.

The chart below is a recommendation from CFOC guide.

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

*Sample Size Guidance*

In cases where a control happens as a result of a trigger event, the assessment team will assume that the control is "ongoing" for sample size selection purposes.

Any deviations from the sample sizes specified in the Test Plan will be clearly documented in the workpapers for the specific test. For example, if a control occurs every time a reimbursable

agreement is initiated and a particular site initiated 23 agreements over the course of the year, the testing team would review all 23 agreements and document the reason for not testing a sample of 45 (in this case, the population is less than the minimum sample).

The Test Plan will specify the number of exceptions allowed in order for a test to pass. A standard practice is to allow one exception for a sample of 45 or more, and no exceptions for samples less than 45.

ICS will document the sample size guidance and pass/fail criteria in the Test Plan.

### **III.1.7 Determine what testing documentation (workpapers) will be developed and retained**

A-123, Appendix A, requires management to have "well-defined documentation processes that contain an audit trail, verifiable results, and specify document retention periods so that someone not connected with the procedures can understand the assessment process."<sup>12</sup>

ICS has prepared templates for KFP-level test plans, test sheets, and exception log. Process Owners and ICS staff are required to use the templates to create consistency. At the conclusion of the testing period, ICS will coordinate the process of storing electronic test files. Approved templates will be included as attachments to the Test Plan.

ICS will document what testing documentation will be retained in the Test Plan.

- **Draft Overall Test Plan**

ICS will draft the test plan according to the specifications discussed above.

- **Review Test Plan**

The Director of ICS will review the Test Plan prior to the start of any field work. The Director will obtain feedback from OBO and the SAT as needed.

- **Retain documentation**

ICS will store the approved Test Plan on SharePoint.

\* \* \* \* \*

---

<sup>12</sup> OMB Circular, A-123, Appendix A, page 6.

## III.2 Test key controls

As part of testing key controls, the assessment team will develop KFP-level test plans, request test samples, document results and identify control gaps. Each of these sub-steps is shown below:



Test Key Controls

Testing teams will be comprised of a Site Lead/Supervisor and testers. The Associate Director will assign a Supervisor to each test location. Supervisors are responsible for managing testers and reviewing their work.

### III.2.1 Develop KFP-level test plans

In addition to the overall Test Plan (covered in Activity III.1), testers will prepare a detailed test plan for each KFP. The detailed test plans, which document the elements of the test and the results, will facilitate management review and approval.

- **Obtain KFP-level test plan template** 

ICS will obtain the approved KFP-level test plan template from SharePoint. The template includes a sample KFP-level template based on the sample PP&E documentation in *Appendix N*. Refer to Appendix 7 for a larger screenshot:

Department of Veterans Affairs											
Test Plan											
Key Financial Process:											
Reference Number	Location	Risk	Control Objective	Actual Control Activity	Process Owner	Frequency	Sample Size	Test Steps	Workpaper Reference Number	Test Result	Summary of Results
C - 6.1.1.2	VACO	Unauthorized disposal transactions	Disposals of fixed assets and removals from service are properly authorized	The designated Custodial Officer reviews the Turn-in Request for completeness and accuracy of the request. If the Custodial Officer approves the Turn-in Request, the Custodial Officer sends the approved Turn-in Request to Property Management Specialist. I	Custodial Officer	Continuous	45	A. Obtain a list of all equipment disposals between 10/1/07 to 5/31/08. B. For the sample selected obtain Turn-In Request (Form 2237) and print out the equipment preventative maintenance repair record from AEMS/MERS C. Verify that the Turn-In Request is approved (signed and dated) by the Custodial Officer D. Compare info on Turn-In Request to AEMS/MERS to verify accuracy.	X.Y.Z	Failed	Three of 45 Turn-In Requests were not signed by the Custodial Officer.

KFP-level Test Plan Template

- **Complete KFP-level test plans**

Test plans will cover all controls that are selected for testing. ICS will specify the following key elements in the KFP-level test plan:

- **Reference Number.** The reference number of key controls comes from the RCM. All controls from the RCM will be included in the KFP-level test plan. If the control is not

being tested, ICS will include an explanation (e.g., the control is not properly designed) in the Test Steps column.

- Location. Because a control may be tested at more than one location and test steps may differ by location, this field identifies the location/site of the testing. If a control is being tested at multiple sites, it should be listed in the test plan separately (i.e., in separate rows).
- Risk and Control Data (Risk, Control Objective, Actual Control Activity, and Process Owner). These attributes describe the control and should come directly from the RCM developed in Phase II: Evaluating
- Process Owner. The test plan will include the Process Owner's name, title, and division
- Frequency. The frequency of the control activity is important in determining the minimum sample size. The control may occur daily, weekly, monthly, quarterly, semi-annually, annually, or on an ongoing basis. In cases where a control happens as a result of a trigger event, ICS will assume that the control is "ongoing" for sample size selection purposes.
- Sample Size. The sample size is based on frequency in accordance with the overall Test Plan
- Test Steps. The test steps (or test attributes) describe the procedures that will be performed for each test
- Workpaper Reference Number. The template includes a workpaper reference number to direct readers to the testing details. This will be completed after testing is conducted
- Test Result. The plan will indicate whether the test passed or failed. This will be completed after testing is conducted
- Summary Test Results. The plans provide a brief description of any exceptions noted during the test. This will be completed after testing is conducted.

Sample Test Steps: Funds Management SF224 Reporting and Reconciliation
1) Obtain the selected SF224 reconciliation. 2) Verify the Statement of Transactions Report is signed by the Accountant. 3) Verify the SF224 Monitoring and Control Reconciliation is signed and dated by the Certifying Officer. 4) Reperform the reconciliation on a sample basis by tying the data to the supporting documentation.

The KFP-level test plan has one row for each key control. A single test can address more than one control; however, this must be clearly documented in the KFP-level test plan.

### III.2.2 Request evidence

The completed KFP-level test plan will be used to determine the evidence required for testing.

- **Obtain Evidence Request List template** 

ICS will create obtain the Evidence Request List template from SharePoint. There will be one Evidence Request List for each site. Refer to Appendix 8 for a larger screenshot:

Department of Veterans Affairs									
Evidence Request List									
Date									
Key Financial Process									
Sub-Process									
As part of the A-123, Appendix A assessment, the Internal Control Service is beginning the testing phase of the assessment. We have identified below evidence that will be needed to allow us to test the operating effectiveness of controls identified during documentation. Upon compilation of the evidence, please group all appropriate Item Numbers together (in folders, binder clips, etc). Thank you for your continued help with our assessment.									
Notes: Please be prepared with copies of all requested evidence. The assessment team will not be able to return original copies back to process owners.									
Note: If you are not the responsible party for the specific item, please forward this list onto the appropriate personnel/department.									
Sample Item Number	Location	Key Financial Process	Sub-process	Control Reference Number	Process Owner	Document Description	Evidence Requested	Date Due	Note
A unique ID number beginning with 1	Name of the site	Relevant key financial process	Relevant sub-process	Control reference number from the RCM	Name and Title of the Process Owner	Requested test sample/documentation including a description of all supporting documentation	Identifying information (dates, invoice numbers, etc) for selected sample	Date due to testing team	
1	VACO	Funds Management	Accounts Payable	C - 1.3.5.6	Joe Smith, Accountant	Approved invoices and all supporting documentation	Invoice numbers: 2533563 6786366 5678260	05/15/08	

Evidence Request List Template

- **Create Evidence Request Lists**

ICS will create evidence request lists and inform Process Owners of the selected sample so they can gather the required documentation. Requests will be specific and include the following:

- Summary Information. Sample Item Number, Location, KFP, Sub-process, Control reference number, Process Owner
- Document Description. The list will clearly describe what is required for testing (i.e., Suspense Account Journal Vouchers and all supporting documentation)
- Evidence Dates Requested. The list will specify the samples required (i.e., Reconciliations for the months ending January 31, 2007, February 28, 2007 and July 31, 2007.)
- Due Date to ICS

When developing the testing schedule, ICS will provide Process Owners with enough time to pull and make copies of the evidence requested.

- **Send Evidence Request Lists to site/station points of contact**

Two weeks prior to the site visit, ICS will email the completed Evidence Request List to the site/station point of contact.

- **Collect and copy test evidence**

Site points of contact will coordinate with Process Owners to collect and organize test samples. Process Owners will make copies of requested evidence since ICS will not return test samples. Additionally, samples should be grouped together (in folders or with paper clips)

and be clearly labeled with the sample item number that corresponds to the evidence request list.

### III.2.3 Conduct tests

The assessment team will conduct the tests specified in the KFP-level test plans using the evidence provided by Process Owners. The testing procedures and results will be sufficiently documented to allow an independent person to understand and re-perform the test.

Documentation will include the identification of items tested (for example, the title and date of the report, invoice numbers, and check numbers), who performed the test, the test results, and the overall conclusion.

- **Complete test steps**

ICS will complete test steps for each test as specified in the KFP-level test plan. Testing procedures will differ depending on the type of test. When appropriate, ICS will mark hardcopy workpapers (actual test evidence) with a red pencil. For example, when testing a reconciliation, ICS may tie numbers from the reconciliation to supporting documentation. Hardcopies of all potential exceptions will be retained.

ICS will document any irregular issues relating to a particular test or sample. For example, the testing team will document whether a control was put in place in the middle of the year and, therefore, has a sample size that is less than the required guidance.

- **Document test results on test sheets** 

Test procedures and results will be documented on test sheets. Test sheets are located as tabs within the KFP-level test plan file. ICS will create one test sheet for each test performed. ICS will document the following information on the test sheet for the respective test.

- KFP and Sub-Process.
- Basic Test Information. Reference Number, Location, Control Activity, Control Frequency, Sampling Unit, Sample Size, Test Results (Pass/Fail), Number of Deviations, Exceptions, Sampling Procedure Performed
- Control Attribute Information. Control Attribute Description, Sample Number, Sample Date, Sample Title, Control Attribute, Work Paper Reference
- Additional Information. Notes, Testing Performed By, Testing Completed On, Testing Reviewed By, Testing Reviewed On

Test Results
<p>Test results should reference the <i>issue</i> and <i>number of deviations</i>.</p> <p><b>Sample Exception:</b></p> <p>The Finance Division could not provide documentation of the reconciliation of the monthly In-force system report on overdue accounts receivable and past due payment notices for the three months sampled.</p>



- **Review test workpapers and complete Testing Quality Review Checklist** 

The Supervisor will review the test sheet and all exceptions for each control. The Supervisor will review a sampling of the remaining test evidence. The Supervisor should consider the following questions during his/her review:

- Do the test steps meet the desired objective?
- Were the test steps carried out correctly?
- Were the test steps sufficiently documented?
- Are all exceptions documented?
- Does the exception logically follow the test procedures and is it clearly communicated?

The Supervisor will complete the "Reviewed By" fields at the bottom of the test sheet as evidence of his/her review. In addition, the supervisor will complete the Testing Quality Review Checklist.

- **Brief Director of ICS**

The Supervisor will hold a one-hour conference call with the Director of ICS to brief him on each site visit and discuss exceptions. The Associate Director and all testers involved in the KFP will also participate in the conference call. The conference call will take place within two weeks of the site visit.

- **Review workpapers**

The Associate Director of the Financial Controls Division and the Director of ICS will review all testing documentation including KFP-level test plans, test sheets, and hardcopy workpapers (binders). The Associate Director and the Director will use the Testing Quality Review checklist as a guide for his/her review. Refer to Appendix 11 for a screenshot of the template.

**IV: Concluding, Internal Reporting, and Correcting**

---

## IV: Concluding, Internal Reporting, and Correcting

The SAT is responsible for concluding on the results of the assessment, reporting these conclusions to appropriate stakeholders, and correcting the identified deficiencies and weaknesses. A-123, Appendix A, requires VA to issue an annual assurance statement on the effectiveness of internal control over financial reporting, including the identification of any material weaknesses. The assurance statement on the effectiveness of internal control over financial reporting is a subset of the overall Statement of Assurance and is based on the results of the internal control assessment. The Statement of Assurance must be included in VA's annual PAR.

In order to complete the activities within this phase, ICS will perform the activities on behalf of the SAT under the guidance of the Director of ICS. The **Responsibility Assignment Matrix (RAM)** developed during the Planning Phase identified the party responsible for leading the performance of each step as well as other parties that should participate in completing each step. The table below illustrates the key inputs and outputs within the Concluding, Internal Reporting, and Correcting Phase.

Activities / Steps	Inputs	Key Outputs
IV.1 - Conclude on control effectiveness	<ul style="list-style-type: none"> <li>KFP-level test plans and test results</li> <li>Entity assessment results</li> <li>GCC evaluation results</li> <li>Cross-servicing entities evaluation results</li> </ul>	<ul style="list-style-type: none"> <li>Documentation of control gaps (Exception Log)</li> <li>Finding Outline Worksheets</li> <li>Conclusion/categorization of findings (on Finding Outline Worksheets)</li> </ul>
IV.2 - Correct Findings	<ul style="list-style-type: none"> <li>Finding Outline Worksheets</li> </ul>	<ul style="list-style-type: none"> <li>Corrective Action Plans</li> </ul>
IV.3 - Monitor CAPs and verify completion	<ul style="list-style-type: none"> <li>Corrective Action Plans</li> </ul>	<ul style="list-style-type: none"> <li>Status Reports</li> </ul>

\* \* \* \* \*

### IV.1 Conclude on control effectiveness

In order to enable the SAT to conclude on control effectiveness, ICS will review the results of both the Evaluating and Testing Phases. ICS staff will compile an Exception Log and evaluate the significance of any exceptions. In this step, ICS will analyze exceptions and identify/categorize findings.

Findings may relate to either the design or operation of a control. Design issues, covered in Activity II.2.2, occur when a control does not exist (*design gap*) or cannot meet the control objective, even if it is functioning as intended (*design deficiency*). During the Evaluating Phase of the assessment, design gaps and design deficiencies were documented in the RCMs and Exception Log. (Recall that poorly designed controls are not tested because they should first be remediated.)

- Enter operating deficiencies into Exception Log** 

Using the individual test sheets, ICS will update the listing of exceptions (design gaps and design deficiencies from the RCM, operating deficiencies from the testing workpapers and

any exceptions resulting from the review of cross-service entities) into an Exception Log. There will be one master Exception Log that covers all KFPs. The Exception log is a working document that ICS should update throughout the assessment phases.

The Exception Log will assist ICS and the SAT in assessing and classifying internal control deficiencies during the Concluding, Internal Reporting, and Correcting Phase of the A-123, Appendix A, effort.

The table below shows a screenshot of the Exception Log template. Refer to Appendix 10 for a larger screenshot:

Department of Veterans Affairs Exception Log													
Date													
ID Number	Key Financial Process	Sub-Process	Location	Key Control Number	Potential Risk	Control Activity	Frequency	Exception/Finding	Cause (if known)	Suggested Corrective Action	Management Response	Exception/Finding Type (Design Deficiency, Design Gap, Operating Deficiency)	Notes
Unique identifier	Relevant process	Relevant Sub-process	Location	Key control number from the RCM	Risk for the key control, as stated in the RCM	Control Activity, as stated in the RCM	As stated in the RCM	If a design gap, copy from the RCM under "design gap." If an operating deficiency, copy from the Test Plan under "summary test results."		What should be done to solve the problem?		Select appropriate finding type	
1	Property Management	Personal Property	VACO	C-3.4.1.1.22	PRR/E acquisitions were not authorized resulting in misappropriation of Capital funds.	The Branch Head reviewed the JV and reconciled the JV with the supporting documentation. If any discrepancies existed, he/she would return the JV to the Property Accountant to resolve the error. If no discrepancies exist, he/she would sign and date the JV and return to the Property Accountant. He/she printed and attached screenshots of the PC information (acquisition document control number) and costs.	Continuous	Four exceptions noted. One exception was due to posting prior to JV approval. One exception due to lack of JV approval date. One exception due to lack of supporting documentation. One exception due to inability to reconcile with supporting documentation.	Cause unknown	Sign and date JV's prior to posting.	Agreed with corrective action	Operating Deficiency	

Exception Log Template

- **Analyze data in Exception Log and identify findings**

Exceptions from the log may or may not constitute findings. Exceptions can be grouped together to form Findings. ICS should hold a "working meeting" to analyze the exception log and identify *preliminary* findings. (Note that findings are not official until they have been reviewed and approved by the Director of ICS and the SAT.) If possible, the ICS staff members analyzing the data in the log should not be the same people that originally identified the exceptions. This enables ICS to consider the exceptions in aggregate, and identify exceptions that may not have been clearly documented.

During the meeting, ICS will review the data Exception Log and can use the sort/filter functions in Microsoft Excel to analyze exceptions by KFP, location, and control ID. This review will enable ICS to look for trends and group exceptions into findings.

As part of the analysis, ICS should consider compensating controls. A compensating control is an activity designed to mitigate another control design deficiency, ineffective operation of a control, or a control gap. These controls were documented in the narrative during the Evaluation Phase. Compensating controls should be taken into account when assessing the likelihood of a misstatement occurring and not being prevented or detected. In addition, a compensating control may limit the potential magnitude of a deficiency (e.g., the compensating control only operates above a given dollar amount). However, the existence of a compensating control does not affect whether a control deficiency exists. If ICS believes there are compensating controls in place that could address the financial statement assertion or risk resulting from the issue, it will consider and validate the following questions:

- Is the compensating control effective?
- Would the compensating control identify an error and address the assertion?

ICS may document its consideration of compensating controls on the Exception Log in the Notes column.

- **Obtain Finding Outline Worksheet template** 

ICS will obtain the Finding Outline Worksheet template located on SharePoint. For VA-wide issues noted, these exceptions/issues by site will be consolidated and rolled up into individual findings. Refer to Appendix 11 for a screenshot of the Findings Outline Worksheet template.

- **Complete Finding Outline Worksheet (draft)**

ICS will use the Finding Outline Worksheet to document the condition, criteria, cause, effect, recommendation, and proposed severity rating for presentation to SAT as described below:

Condition- description of the finding (what is happening)

Criteria- policies or requirements supporting the control (what should be happening)

Cause- reason for the deficiency

Effect- effect of the deficiency on financial reporting

Recommendation- recommended steps for correcting the deficiency

Severity rating- potential of the deficiency to have an impact on financial reporting  
(Determination of this rating is described later in this section)

- **Categorize findings**

ICS will use the draft Finding Outline Worksheet to assist with the categorization of findings. Findings can range from an *internal control deficiency* to a *significant deficiency* to a *material weakness*. A simple deficiency is a finding that creates minimal exposure for management and is generally an anomaly. A significant deficiency usually indicates a history of findings that when consolidated, equate to a *material weakness*.

While A-123, Appendix A, still classifies deficiencies as internal control deficiencies, reportable conditions and material weaknesses, VA consulted with OMB and will use the new terms and definitions from the Statement on Auditing Standards No. 112 (SAS 112) for audits. These definitions were effective for audits ending on or after December 15, 2006. SAS 112 classifies deficiencies as internal control deficiencies, significant deficiencies, and material weaknesses.

- Internal Control Deficiency. Exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. Control deficiencies are internal to the organization and are not reported externally. (Example: missing initials indicating a supervisor's review on one of 26 reconciliations sampled)
- Significant Deficiency. 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<sup>13</sup> likelihood that a misstatement of the entity's financial statements will not be prevented or detected. (Example: only eight monthly reconciliations were performed for the year)

---

<sup>13</sup> The term "remote" is defined in SFFAS No. 5, Accounting for Liabilities of the Federal Government, as the chance of the future event, or events, occurring is slight.

- Material Weakness. A significant deficiency, or combination of significant deficiencies, that results in more than a remote<sup>14</sup> likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected. (Example: reconciliation of several key accounts was not performed throughout the year, only at year-end).

The categorization of control deficiencies is not necessarily linked to materiality or a dollar amount and is subjective in nature. Considering both the *likelihood* of misstatement and the potential *magnitude* for misstatement is a useful framework for categorizing deficiencies.

- Likelihood. An event is considered *remote* if the chance of occurrence is slight. The following factors impact likelihood:
  - The nature of the financial statement accounts, disclosures, and assertions involved
  - The susceptibility of the related assets or liability to loss or fraud (that is, greater susceptibility increases risk)
  - The subjectivity, complexity, or extent of judgment required to determine the amount involved (that is greater subjectivity, complexity, or judgment, like that related to an accounting estimate, increases risk)
  - The cause and frequency of known or detected exceptions for the operating effectiveness of a control
  - The interaction or relationship of the control with the other controls (that is, the interdependence or redundancy of the control)
  - The interaction of the deficiencies
  - The possible future consequences of the deficiency
- Magnitude. In evaluating magnitude, a misstatement is considered *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. The following factors may impact magnitude:
  - The financial statement amounts or total of transactions exposed to the deficiency (a potential misstatement that is less than 20% of overall financial statement materiality may be inconsequential)
  - The volume of activity in the account balance or class of transactions exposed to the deficiency that has occurred in the current period or that is expected in future periods

Statement on Auditing Standards No. 112 (SAS 112) provides the following guidance for evaluating magnitude:

"In determining whether a potential misstatement would be more than inconsequential, the auditor should consider qualitative and quantitative factors. Inconsequential in this context is not the same concept as the threshold amount the auditor establishes in an audit of financial statements below which known and likely misstatements need not be accumulated. For example, for the purposes of evaluating control deficiencies, a potential misstatement that is less than 20 percent of overall financial statement materiality may be considered

---

<sup>14</sup> Ibid.

inconsequential, before considering qualitative factors. However, a potential misstatement that is less than 20 percent of overall financial statement materiality may be considered more than inconsequential as a result of qualitative factors risk of error or misstatement that could occur in a financial report that would impact management’s or users’ decisions or conclusions based on such report”<sup>15</sup>

The following criteria can be used to assess the classification of an internal control deficiency:

Likelihood of Misstatement		Potential Magnitude of Misstatement		Classification of Deficiency
More than remote	AND	Material	=	Material Weakness
More than remote	AND	More than inconsequential	=	Significant Deficiency
Remote	OR	Inconsequential	=	Control Deficiency

Appendix L provides a detailed framework for assessing deficiencies.

ICS will include the proposed categorization on the Finding Outline Worksheet.

- **Review Finding Outline Worksheets and categorizations (ICS Supervisor or Associate Director)**

An ICS Supervisor (or the Associate Director) will review the Findings Outline Worksheets for completeness, clarity, and supporting evidence. ICS staff will work with Process Owners to update the worksheets to reflect his/her comments. The supervisor will sign and date each Finding Outline Worksheet as evidence of review/concurrence.

- **Review Finding Outline Worksheets and categorizations (Director of ICS)**

The Director of ICS will review the Findings Outline Worksheets and provide ICS staff with comments. ICS staff will work with Process Owners to update the worksheets to reflect the Director's comments. The Director will sign and date each worksheet as evidence of review/concurrence.

- **Present recommendations to SAT**

The Director of ICS will share the Finding Outline Worksheets (for significant deficiencies and material weaknesses only) with the SAT and work with the SAT to agree on the final set of findings, recommendations, severity ratings. If needed, ICS will contact Process Owners for additional information as they revise the worksheets.

- **Update Finding Outline Worksheets with SAT recommendations**

ICS will update the Finding Outline Worksheets based on final SAT decisions. The worksheet has a section for an SAT member's signature; however, the SAT may opt to provide approval verbally or via email. In those cases, ICS will document SAT approval on the worksheet.

\* \* \* \* \*

---

<sup>15</sup> SAS No. 112.

## **IV.2 Correct Findings**

[Insert Task K Deliverable here]

## **IV.3 Monitor CAPs and verify completion**

[Insert Task K Deliverable here]

**V: External Reporting**

## V.1 Report externally

VA is required to provide a statement of assurance on the effectiveness of internal control over financial reporting, as of June 30, in its annual PAR. The assurance statement on the effectiveness of internal control over financial reporting is a subset of the overall Statement of Assurance reported pursuant to Section 2 of the FMFIA legislation.

The assurance statement on the effectiveness of internal control over financial reporting is required to include the following:

- A statement of management’s responsibility for establishing and maintaining adequate internal control over financial reporting for VA
- A statement identifying OMB Circular A-123, Management’s Responsibility for Internal Control, as the framework used by management to conduct the assessment of the effectiveness of VA's internal control over financial reporting
- An assessment of the effectiveness of VA'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<sup>16</sup>

The **Responsibility Assignment Matrix (RAM)** developed during the Planning Phase identified the party responsible for leading the performance of this step. The table below illustrates the key inputs and outputs within the External Reporting Phase.

Activities / Steps	Inputs	Key Outputs
V.1 - Report externally	<ul style="list-style-type: none"> <li>▪ Documentation of control gaps (Exception Log)</li> <li>▪ Finding Outline Worksheets</li> <li>▪ Conclusion/categorization of findings (on Finding Outline Worksheets)</li> <li>▪ Status Reports from CATS</li> </ul>	<ul style="list-style-type: none"> <li>▪ Statement of Assurance</li> </ul>

- **Draft assurance statement**

Once the SAT and ICS agree on the classification of deficiencies, ICS will draft an assurance statement and present it to the Director of ICS for review. Exhibit 6 of the CFOG Guide provides sample Statement of Assurance templates.

- **Review assurance statement (Director of ICS)**

The Director of ICS will review the statement, work with ICS staff to make any necessary changes, and submit the statement to the SAT for review.

- **Review assurance statement (SAT)**

---

<sup>16</sup> CFOG Implementation Guide for A-123, Appendix A, page 42.

The SAT will review the statement, work with the Director of ICS to make any necessary changes, and submit the statement to the Secretary for signature and inclusion in the PAR.

- **Sign assurance statement**

The Secretary will review and sign the assurance statement for inclusion in the annual PAR.



## Appendices



## Appendices

### Appendix A – CFOC Guide Crosswalk to Procedures Manual

CFOC Implementation Guide		VA Implementation Guide	
Activity	Page Number	Phase	Activity
<b>Step 1: Planning</b>	<b>6-23</b>		
• Organizational Structure	6	I. Planning	I.1: Establish organizational structure
• Determine Overall Approach: Top-Down Focus	9	I. Planning	Introduction to Phase I: Planning
• Integrate and Coordinate with Other Control-Related Activities	12	I. Planning	I.11: Integrate and coordinate with other control-related activities
• Determine Scope of Significant Financial Reports	15	I. Planning	I.2: Identify significant financial reports
• Determine Materiality	16	I. Planning	I.4: Conduct quantitative analysis
• Determine Key Processes Supporting Material Line Items	18	I. Planning	I.5: Confirm/update KFPs that generate material and immaterial line items
• Financial Reporting Assertions	19	I. Planning	I.9: Identify financial reporting assertions
• Risk Assessment	19	I. Planning	I.7: Conduct qualitative analysis (risk assessment)
• Documentation	20	I. Planning	Referenced throughout Phase I: Planning
• Monitor Control Effectiveness	22	I. Planning	Referenced throughout all phases
• Plan for an Updated Assurance Statement in the PAR	23	I. Planning	I.13: Plan for an updated assurance statement in the Performance and Accountability Report (PAR)
<b>Step 2: Evaluating Internal Control at the Entity Level</b>	<b>24-26</b>	<b>II. Evaluating</b>	<b>II.1: Evaluate internal controls at the entity level</b>
<b>Step 3: Evaluating Internal Control at the Process Level</b>	<b>27-34</b>		
• Understanding Key Financial Reporting Processes	27	II. Evaluating	II.2: Evaluate internal control at the process level

CFOC Implementation Guide		VA Implementation Guide	
Activity	Page Number	Phase	Activity
• Identifying Key Controls	27	II. Evaluating	II.2: Evaluate internal control at the process level
• Understanding Control Design	28	II. Evaluating	II.2: Evaluate internal control at the process level
• Evaluating Controls of Cross-Servicing Providers and Service Organizations	29	II. Evaluating	II.2: Evaluate internal control at the process level
• Documenting Key Business Processes and Related Key Controls	30	II. Evaluating	II.2: Evaluate internal control at the process level
• Understanding the IT Infrastructure and Associated Risks	31	II. Evaluating	II.3: Understand IT structure and associated risks
Step 4: Testing at the Transaction Level	35-37		
• Risk-Based Approach	35	III. Testing	III.1: Develop Test Plan
• Testing Key Controls	36	III. Testing	III.2: Test key controls
Step 5: Concluding, Internal Reporting, and Correcting Deficiencies and Weaknesses	38-45		
• Concluding on Effectiveness	38	IV. Concluding, Internal Reporting, and Correcting	IV.1: Conclude on control effectiveness
• Reporting	39	IV. Concluding, Reporting, and Correcting	V: External Reporting
• Correcting Deficiencies or Weaknesses	41	IV. Concluding, Reporting, and Correcting	IV.2: Correct findings

## Appendix B – Glossary of Acronyms

Acronym	Term
CAP	Corrective Action Plan
CFO Act	Chief Financial Officers Act of 1990
CFOC	Chief Financial Officer's Council
CobiT	Control Objectives for Information and Related Technology
COSO	Committee on Sponsoring Organizations
FFMIA	Federal Financial Management Improvement Act of 1996
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Act
FMFIA	Federal Managers' Financial Integrity Act of 1982
GAO	General Accountability Office
GCC	General Computer Controls
GPRA	Government Performance and Results Act
GMRA	Government Management Reform Act of 1994
ICS	Internal Controls Service
IG Act	Inspector General Act of 1978
IPIA	Improper Payments Information Act of 2002
MQAS	Management Quality and Assurance Service
KFP	Key Financial Process
OBO	Office of Business Oversight
OIG	Office of Inspector General
OMB	Office of Management and Budget
PAR	Performance Annual Review
PCAOB	Public Company Accounting Oversight Board
RCM	Risk Control Matrices
SAS 70	Statement on Auditing Standards No. 70
SAT	Senior Assessment Team
SMC	Strategic Management Council
SoV	Summary of Validation
SOX	Sarbanes-Oxley Act of 2002
Yellow Book	GAO Government Auditing Standards

## Appendix C – Glossary of Terms

This implementation guide uses many key terms when discussing how management will evaluate its internal control over financial reporting. The following is a list of these key terms and their definitions:

### Adjusted Exposure

Gross exposure (see definition below) multiplied by the upper limit deviation rate.

### Application Controls

Automated control procedures (e.g., calculations, posting to accounts, generation of reports, edits, control routines, etc.) or manual controls that are dependent on IT (e.g., the review by an inventory manager of an exception report when the exception report is generated by IT). When IT is used to initiate, authorize, record, process, or report transactions or other financial data for inclusion in financial statements, the systems and programs may include controls related to the corresponding assertions for significant accounts or disclosures or may be critical to the effective functioning of manual controls that depend on IT.

### Automated Controls

Automated controls encompass those control procedures performed by a computer.

### Compensating Controls

Controls that operate at a level of precision that would result in the prevention or detection of a misstatement that was more than inconsequential or material, as applicable, to annual or interim financial statements. The level of precision should be established considering the possibility of further undetected misstatements.

### Complementary Controls

Controls that function together to achieve the same control objective.

### Component

Formerly referred to as bureaus, or operational elements, or distinct departmental offices within an Agency.

### Control Deficiency

A deficiency in the design or operation of a control that does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

- A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if it operates as designed, the control objective is not always met
- A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively

### Control Objective

The objective(s) related to internal control over financial reporting to achieve the assertions that underlie an organization's financial statements.

## De minimis

The full expression is *de minimis non curat lex*. This is a Latin phrase which means "the law does not care about very small matters". It can be used to describe a Component part of a wider transaction, where it is in itself insignificant or immaterial to the transaction as a whole, and will have no legal relevance or bearing on the end result.

## Design Effectiveness

Internal control over financial reporting is designed effectively when the controls in place would meet the control objectives and be expected to prevent or detect errors or fraud that could result in material misstatements in the financial statements.

## Detective Control

Detective controls have the objective of detecting errors or fraud that has already occurred that could result in a misstatement of the financial statements.

## Entity-Level Controls

Entity-level controls are controls management has in place to provide assurance that appropriate controls exist throughout the organization, including at the individual locations or operational units. Entity-level controls include the following<sup>17</sup>:

- Controls within the control environment, including tone at the top, the assignment of authority and responsibility, consistent policies and procedures, and entity-wide initiatives, such as codes of conduct and fraud prevention
- Management's risk assessment process
- Centralized processing and controls
- Controls to monitor other controls, including the activities of the OIG, senior management, and self-assessment programs
- The period-end financial reporting process
- Approved policies that address the entity's significant control and risk management practices

## Financial Reporting <sup>18</sup>

Includes annual financial statements of an agency as well as significant internal and external financial reports that could have a material effect on a significant spending, budgetary or other financial decision of the agency or that is used to determine compliance with laws and regulations on the part of the agency.

## Financial Statement Assertions

Management and the IPA should document and test internal control over relevant financial statement assertions. Financial statement assertions are defined as representations by management that are embodied in the financial statement Components and can be classified in the following broad categories<sup>19</sup>:

- **Existence or Occurrence:** This assertion addresses whether assets or liabilities of the entity exist at a given date and whether recorded transactions have occurred during a given period

---

<sup>17</sup> PCAOB AS 2.

<sup>18</sup> OMB Circular A-123, page 22.

<sup>19</sup> *Ibid.*

- **Completeness:** This assertion addresses whether all transactions and accounts that should be presented in the financial statements are so included
- **Valuation or Allocation:** This assertion addresses whether asset, liability, equity, revenue, and expense Components have been included in the financial statements at appropriate amounts
- **Rights and Obligations:** This assertion addresses whether assets are the rights of the entity and liabilities are the obligations of the entity at a given date
- **Presentation and Disclosure:** This assertion addresses whether particular Components of the financial statements are properly classified, described, and disclosed

Additionally, A-123 defines three additional assertions:

- The transactions are in compliance with applicable laws and regulations (compliance)
- All assets have been safeguarded against fraud and abuse
- Documentation of internal control, all transactions, and other significant events is readily available for examination

Although the financial statement assertions appear to be similar to the information processing objectives/CAVR, there is not a one-for-one relationship, and they are used for different purposes. Information processing objectives/CAVR are used to evaluate the design effectiveness of controls, particularly application controls, within a KFP. Assertions are representations by management as to the fair presentation of the financial statements.

## General Computer Controls

General computer controls are one of the types of information processing controls included in the internal control Component of control activities. These are the processes and procedures that are used to manage and control an entity's information technology activities and computer environment. The Federal Information System Controls Audit Manual (FISCAM) was created by the Government Accountability Office (GAO) as the primary tool used by agencies within the Federal government to evaluate their IT controls.

## Gross Exposure

A worst-case estimate of the magnitude of amounts or transactions exposed to the deficiency with regard to annual or interim financial statements, without regard to the upper limit deviation rate or likelihood of misstatement, and before considering complementary, redundant, or compensating controls. The following factors affect gross exposure:

- The annual or interim financial statement amounts or total transactions exposed to the deficiency
- The volume of activity in the account balance or class of transactions exposed to the deficiency that has occurred in the current annual or interim period or that is expected in future periods

## Inconsequential

- Potential misstatements equal to or greater than 20% of overall annual or interim financial statement materiality are presumed to be more than inconsequential
- Potential misstatements less than 20% of overall annual or interim financial statement materiality may be concluded to be more than inconsequential as a result of the consideration of qualitative factors, as required by AS 2

## Information Processing Objectives/CAVR

The four information processing objectives (completeness, accuracy, validity, and restricted access – sometimes referred to as “CAVR”) are a standard means to assess the integrity of the data that flows through a process. The four Components of CAVR are listed below.

Information Processing Objective	Definition
<b>Completeness</b>	<ul style="list-style-type: none"> <li>• All recorded transactions are accepted by the system (only once)</li> <li>• Duplicate postings are rejected by the system</li> <li>• Any transactions that are rejected are addressed and fixed</li> </ul>
<b>Accuracy</b>	<ul style="list-style-type: none"> <li>• Key data elements for transactions (including standing data) that are recorded and input to the computer are correct</li> <li>• Changes in standing data are accurately input</li> </ul>
<b>Validity</b>	<ul style="list-style-type: none"> <li>• Transactions, including the alteration of standing data, are authorized</li> <li>• Transactions, including standing data files, are not fictitious and they relate to the organization</li> </ul>
<b>Restricted Access</b>	<ul style="list-style-type: none"> <li>• Unauthorized amendments of data are barred from the system</li> <li>• The confidentiality of data is ensured</li> <li>• Entity assets are physically protected from theft and misuse</li> <li>• The segregation of duties is ensured</li> </ul>

Although control activities that achieve the information processing objectives do not always provide us with direct comfort on financial statement assertions, the following table may be useful in linking our controls work to the financial statement assertions, assuming that the KFP to which the controls relate is designed effectively.

Information Processing Objective	Financial Statement Assertion
Completeness	Completeness, Existence/Occurrence
Accuracy	Valuation/Allocation
Validity	Existence/Occurrence, Rights & Obligations
Restricted Access	Most, except for Rights & Obligations

## Internal Control <sup>20</sup>

An integral Component of an organization’s management that provides reasonable assurance that the following objectives are being achieved:

- Effectiveness and efficiency of operations
- Reliability of financial reporting

<sup>20</sup> GAO Standards for Internal Control in the Federal Government (Green Book), page 6.

- Compliance with applicable laws and regulations
- Safeguarding of assets

### Internal Controls Service

The Internal Controls Service (ICS) is part of the Office of Business Oversight. Its role with regard to A-123, Appendix A, is to complete the following activities:

- Evaluate and perform tests of controls
- Document procedures performed, evidence obtained, and conclusions reached

### Internal Control over Financial Reporting

A process designed by, or under the supervision of, the agency head and chief financial officers, and effected by senior management, management, and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements and other reports for internal and external purposes. This process involves the maintenance of records, the recording of transactions, and the prevention/detection of unauthorized acquisition, use, or disposition of the entity's assets.<sup>21</sup>

Internal control over financial reporting should assure the safeguarding of assets from waste, loss, unauthorized use, or misappropriation as well as assure compliance with laws and regulations pertaining to financial reporting.<sup>22</sup>

### Internal Control Standards <sup>23</sup>

The Federal Managers' Financial Integrity Act of 1982 (FMFIA) requires the Government Accountability Office (GAO) to issue standards for internal control in government. These standards provide the overall framework for establishing and maintaining internal control and for identifying and addressing major performance and management challenges and areas at greatest risk of fraud, waste, abuse, and mismanagement. These standards define the minimum level of quality acceptable for internal control in government and provide the basis against which internal control is to be evaluated. These standards apply to all aspects of an agency's operations: programmatic, financial, and compliance. The GAO has identified and defined the five standards of internal control as follows:

1. **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.
2. **Risk Assessment** – internal control should provide for an assessment of the risks the agency faces from both external and internal sources.
3. **Control Activities** – internal control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the agency's control objectives.
4. **Information and Communications** – information should be recorded and communicated to management and others within the entity who need it and in a form and

---

<sup>21</sup> Adapted from PCAOB AS 2.

<sup>22</sup> OMB Circular, A-123, Appendix A, page 22.

<sup>23</sup> GAO Standards for Internal Control in the Federal Government (Green Book), page 3 - 9.

within a timeframe that enables them to carry out their internal control and other responsibilities.

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

### **Management Assertions** <sup>24</sup>

Management is required to include an assurance statement on the effectiveness of internal control over financial reporting in its annual Performance and Accountability Report. This statement is based on management's assessment of the effectiveness of an agency's internal control over financial reporting.

### **Management Controls**

Management controls are the organization, policies, and procedures used by agencies to reasonably ensure that (i) programs achieve their intended results; (ii) resources are used consistent with agency mission; (iii) programs and resources are protected from waste, fraud, and mismanagement; (iv) laws and regulations are followed; and (v) reliable and timely information is obtained, maintained, reported and used for decision making.

### **Manual Controls**

Manual controls encompass those controls performed manually, not by computer systems.

### **Material Weakness**

A significant deficiency, or combination of significant deficiencies, 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.

### **Materiality** <sup>25</sup>

The risk of error or misstatement that could occur in a financial report that would impact management's or users' decisions or conclusions based on such report.

### **Operational Effectiveness**

Internal control over financial reporting is operating effectively when a properly designed control is operating as designed and the individual performing the control possesses the necessary authority and qualifications to perform the control effectively.

### **Opinion on Internal Control** <sup>26</sup>

The auditor's opinion on internal control is based upon the auditor's evaluation of the entity's internal control and the results of other audit procedures. The opinion may be unqualified, unqualified with reference to deficiencies, qualified, or adverse. Additionally, there may be restrictions on the scope of the procedures that result in a qualified opinion or a disclaimer of opinion.

CFO Act agencies generally receive a report on internal control which is not the same as an opinion.

### **Potential Misstatement**

An estimate of the misstatement that could result from a deficiency with a more-than-remote likelihood of occurrence.

---

<sup>24</sup> OMB Circular, A-123, Appendix A, page 29.

<sup>25</sup> OMB Circular, A-123, Appendix A, page 23.

<sup>26</sup> GAO/PCIE Financial Audit Manual, Sec. 500.38.

## Preventive Control

Preventive controls have the objective of preventing errors or fraud from initially occurring that could result in a misstatement of the financial statements.

## Key Financial Process (KFP)

A key financial process is any sequence of transactions that enables an entity to complete tasks and achieve its objectives. These transactions may range, in order of complexity, from performing simple activities (such as processing invoices), to managing key elements of operations (such as an inventory management system), to executing functional tasks (such as maintaining an organization's financial records), to cross-functional elements (such as the entity's Human Resources Department).

## KFP Risk Assessment

As part of the scoping exercises, management should identify the primary KFPs. In order to evaluate the extent of documentation and testing over each KFP, management should perform a risk assessment of each KFP. This risk assessment involves the identification of relevant risks to achieving the financial reporting objectives related to each account affected by each KFP. Higher risk KFPs will be subject to a greater extent of documentation and testing.

## Reasonable Assurance

The concept of reasonable assurance encompasses the understanding that there is a remote likelihood that material misstatements will not be prevented or detected on a timely basis. Although not absolute assurance, reasonable assurance is, nevertheless, a high level of assurance.

## Remote or Remote Likelihood

As defined in Statement of Federal Financial Accounting Standards (SFFAS) No. 5, the term "remote" is used when the chance of the future event, or events, occurring is slight.

## Report on Internal Control <sup>27</sup>

A report on internal control (in which no opinion is issued) is a by-product report, a report that provides a limited degree of assurance about internal control. When no opinion is issued, the report on internal control is not the primary objective of the engagement. If the purpose of the audit is not to render an opinion on internal control, the auditor should report material weaknesses and other deficiencies in internal control, or state that no material weaknesses were found.

## Senior Assessment Team <sup>28</sup>

The team should be comprised of senior executives and derive its authority and support from the Secretary and/or the Chief Financial Officer. The team could take many forms such as a financial management improvement committee or as a subset of the Senior Management Council. The senior assessment team is responsible for the following:

- Oversight of the assessment process
- Ensuring that assessment objectives are clearly communicated throughout the agency
- Ensuring that the assessment is carried out in a thorough, effective, and timely manner
- Identifying and ensuring adequate funding and resources are made available

---

<sup>27</sup> GAO/PCIE Financial Audit Manual, Sec. 500.49.

<sup>28</sup> OMB Circular, A-123, Appendix A, page 24.

- Identifying staff and/or securing contractors to perform the assessment
- Determining the scope of the assessment, i.e., those financial reports covered by the assessment
- Determining the assessment design and methodology

### **Significant Account and Disclosure**

An account or disclosure is significant if there is a more-than-remote likelihood that the account or disclosure could contain misstatements that individually, or when aggregated with others, could have a material effect on the financial statements, considering the risks of both overstatement and understatement.

### **Strategic Management Council**

Serve as a collaborative and deliberative body through providing oversight and guidance to the SAT on final decisions and recommendations concerning the A-123, Appendix A, program. The CFO should be a member of the Strategic Management Council. The Senior Assessment Team will report to the CFO, who will coordinate A-123, Appendix A, activities with the Strategic Management Council.

### **Sub-process (Sub-KFP)**

A sub-process is a group of transactions for which specific accounting procedures and controls are established by an entity's management. For example, a revenue and receivables KFP may include sub-processes, such as invoicing, pricing, or processing of receipts.

### **Test Objective**

The design of the test of a control activity is to determine whether the control is operating as designed. The test should consider the following:

- The nature of the control and the definition of an exception
- The frequency with which the control operates
- The desired level of assurance in combination with the reliability of the control, for example, whether the control is designed to achieve the control objective alone or in combination with other controls
- The number of exceptions expected

### **Upper Limit Deviation Rate**

The statistically derived estimate of the deviation rate based on the sample results, for which there is a remote likelihood that the true deviation rate in the population exceeds this rate (refer to American Institute of Certified Public Accountants (AICPA) Audit and Accounting Guide, Audit Sampling).

### **Walkthrough**

A walkthrough is the process in which a transaction is traced from origination through the entity's information systems until the transaction is reflected in the entity's financial reports. A walkthrough should encompass the entire process of initiating, authorizing, recording, processing, and reporting individual transactions and controls for each KFP, including controls to address the risk of fraud.

## Appendix D – The Five Standards of Internal Control

The Government Accountability Office (GAO) issues the *Standards for Internal Control in the Federal Government* commonly referred to as the “Green Book”<sup>29</sup>. These standards provide the overall framework for establishing and maintaining internal control and for identifying and addressing major performance challenges and areas at greatest risk for fraud, waste, abuse, and mismanagement.

As part of the assessment, the assessment team should document, test, and evaluate the design and effectiveness of the five standards of internal control. Because these standards form the foundation for all other controls implemented within an organization, it is important to document these controls during the Planning Phase of the assessment. Testing and evaluating these controls may be completed as part of the Planning Phase or during the very early stages of the Testing Phase. However, it is recommended that the testing and evaluation of these foundation controls occur as early in the assessment phase as possible. Weaknesses or deficiencies noted within these foundation controls will need to be corrected as soon as possible to prevent the weakening of other internal controls.

### Control Environment

The control environment establishes the overall tone for the organization and is the foundation for all other Components of internal control. It provides discipline and structure as well as the climate which influences the quality of internal control<sup>30</sup>. The GAO identified seven sub-Components of the control environment:

- Integrity and ethical values
- Commitment to competence
- Management’s philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human capital policies and practices
- Relationship with Congress and central oversight groups (i.e., OMB, Inspector General, Senior Management Councils)

The assessment team should also address anti-fraud and abuse, programs and entity governance when evaluating the control environment<sup>31</sup>.

### Anti-Fraud and Abuse Considerations

Controls should be evaluated that are intended to address the risks of fraud and abuse and have at least a reasonably possible likelihood of having a material effect on the financial statements.<sup>32</sup>

Abuse is distinct from fraud. When abuse occurs, no law or regulation is violated. Rather, the conduct of a program or entity falls far short of behavior that is expected to be reasonable and necessary business practices by a prudent person.<sup>33</sup>

---

<sup>29</sup> [Standards for Internal Control in the Federal Government, GAO Report # GAO/AIMD-00-21.3.1 \(11/99\)](#).

<sup>30</sup> Ibid.

<sup>31</sup> PCAOB AS 2.

<sup>32</sup> Ibid.

<sup>33</sup> [Adopted from the GAO Government Auditing Standards](#) commonly referred to as the “Yellow-Book”, paragraph 4.19.

Effective anti-fraud and abuse programs include the following key elements:

- Code of conduct/ethics
- Hotline/whistleblower program
- Hiring and promotion (i.e., background checks)
- Investigation and remediation of identified fraud
- Oversight
- Risk assessment

The assessment team should consider each of these elements in its documentation and evaluation of its anti-fraud and abuse program. Additionally, the assessment team's documentation should adequately support its assessment of anti-fraud programs and controls by conducting the following activities:

- Providing sufficient information regarding the flow of transactions, which enables management to determine where material misstatements could occur as a result of fraud
- Determining which controls prevent and detect fraud
- Determining (1) who will perform the controls and (2) the related segregation of duties

### **Qualitative Analysis (Risk Assessment)**

Another Component of internal control is risk assessment. For an organization to exercise effective control, it should establish clear, consistent objectives and understand the risks it faces in achieving those objectives. Risk assessment is the identification and analysis of relevant risks associated with achieving the objectives, such as those defined in strategic and annual performance plans developed under the Government Performance and Results Act, and forming a basis for determining how risks should be managed.<sup>34</sup>

The assessment team needs to comprehensively identify risks and should consider all significant interactions between the entity and other parties as well as internal factors at both the entity-wide and activity level. Risk identification methods may include qualitative and quantitative ranking activities, management conferences, forecasting and strategic planning, and consideration of findings from audits and other assessments.<sup>35</sup>

According to the Green Book, once risks have been identified, they should be analyzed for their possible effect. Risk analysis generally includes estimating the risk's significance, assessing the likelihood of its occurrence, and deciding how to manage the risk and what actions should be taken. The specific risk analysis methodology used can vary by organization because of differences in organizations' missions and the difficulty in qualitatively and quantitatively assigning risk levels. Because governmental, economic, industry, regulatory, and operating conditions continually change, mechanisms should be provided to identify and deal with any special risks prompted by such changes.

### **Control Activities**

Control activities are the policies and procedures that help to ensure that management's directives are implemented. They help ensure that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and

---

<sup>34</sup> Adopted from the *Standards for Internal Control in the Federal Government*, GAO Report # GAO/AIMD-00-21.3.1 (11/99),

<sup>35</sup> Ibid

accountability for stewardship of government resources and achieving effective results.<sup>36</sup> Control activities occur throughout the organization, at all levels, and in all functions. The activities involve approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, maintenance of records, and segregation of duties.

There are many different types of control activities including preventive controls, detective controls, manual controls, computer controls, and internal controls. Control activities address specified information processing objectives/CAVR (completeness, accuracy, validity, and restricted access), such as ensuring completeness and accuracy of data processing. The following chart includes certain control activities that are commonly performed by personnel at various levels in organizations, as indicated by the Green Book.

Activity	Detail
Top Level Reviews of Actual Performance	Management should track major agency achievements and compare these to the plans, goals, and objectives established under the Government Performance and Results Act.
Reviews by Management at the Functional or Activity Level	Managers also need to compare actual performance to planned or expected results throughout the organization and analyze significant differences.
Management of Human Capital	<p>Effective management of an organization’s workforce, its human capital, is essential to achieving results and an important part of internal control. Management should view human capital as an asset rather than a cost. Only when the right personnel for the job are on board and are provided the right training, tools, structure, incentives, and responsibilities is operational success possible. Management should ensure that skill needs are continually assessed and that the organization is able to obtain a workforce that has the required skills that match those necessary to achieve organizational goals. Training should be aimed at developing and retaining employee skill levels to meet changing organizational needs. Qualified and continuous supervision should be provided to ensure that internal control objectives are achieved.</p> <p>Performance evaluation and feedback, supplemented by an effective reward system, should be designed to help employees understand the connection between their performance and the organization’s success. As a part of its human capital planning, management should also consider how best to retain valuable employees, plan for their eventual succession, and ensure continuity of needed skills and abilities.</p>

---

<sup>36</sup> Ibid

Activity	Detail
Controls Over Information Processing	A variety of controls are performed to check accuracy, completeness, and authorization of transactions. Data entered into computer applications is subject to edit checks or matching to approved control files. An obligation, for example, is accepted only upon an approved requisition and availability of funds. Numerical sequences of transactions are accounted for. File totals are compared and reconciled with prior balances and with control accounts. Exceptions are investigated and reported to supervisors as necessary. Development of new systems and changes to existing systems are controlled, and access is checked to ensure the user performing the update is authorized to do so.
Physical Control Over Vulnerable Assets	An agency should establish physical control to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, securities, inventories, and equipment which might be vulnerable to risk of loss or unauthorized use. Such assets should be periodically counted and compared to control records.
Establishment and Review of Performance Measures and Indicators	Activities need to be established to monitor performance measures and indicators. These controls could call for comparisons and assessments relating different sets of data to one another, so analyses of the relationships can be made and appropriate actions taken. Controls should also be aimed at validating the propriety and integrity of both organizational and individual performance measures and indicators.
Segregation of Duties	Key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud. This should include separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets. No one individual should control all key aspects of a transaction or event. For example, a manager authorizing obligations would not be responsible for entering obligations into financial management systems or handling the payment of invoices.
Proper Execution of Transactions and Events	Transactions and other significant events should be authorized and executed only by persons acting within the scope of their authority. This is the principal means of assuring that only valid transactions to exchange, transfer, use, or commit resources and other events are initiated or entered into. Authorizations should be clearly communicated to managers and employees.
Accurate and Timely Recording of Transactions and Events	Transactions should be promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event from the initiation and authorization through its final classification in summary records. In addition, control activities help to ensure that all transactions are completely and accurately recorded.

Activity	Detail
Access Restrictions to and Accountability for Resources and Records	Access to resources and records should be limited to authorized individuals, and accountability for their custody and use should be assigned and maintained. Periodic comparison of resources with the recorded accountability should be made to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.
Appropriate Documentation of Transactions and Internal Control	Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form. All documentation and records should be properly managed and maintained. These examples are meant only to illustrate the range and variety of control activities that may be useful to an agency's managers. They are not all inclusive and may not include particular control activities that an agency may need. Furthermore, an agency's internal control should be flexible to allow agencies to tailor control activities to fit their special needs. The specific control activities used by a given agency may be different from those used by others due to a number of factors. These could include specific threats they face and risks they incur; differences in objectives; managerial judgment; size and complexity of the organization; operational environment; sensitivity and value of data; and requirements for system reliability, availability, and performance.

These examples are just a very few among a myriad of control procedures performed every day throughout an organization that serve to enforce adherence to established protocols, and to keep entities on track toward achieving their objectives.

**Information and Communication**

For an organization to run and control its operations, it should have relevant, reliable, and timely communications relating to internal as well as external events. Information is needed throughout the organization to achieve all of its objectives. The information and communication Component includes the systems that support the identification, capture, and exchange of information in a form and timeframe that enable personnel to carry out their responsibilities and financial reports to be generated accurately. Information and communication also spans all of the other Components of internal control.

Program managers need both operational and financial data to determine whether they are meeting their agencies' strategic and annual performance plans and meeting their goals for accountability for effective and efficient use of resources. For example, operating information is required for development of financial reports. This covers a broad range of data from purchases, subsidies, and other transactions to data on fixed assets, inventories, and receivables. Operating information is also needed to determine whether the organization is achieving its compliance requirements under various laws and regulations. Financial information is needed for both external and internal uses. It is required to develop financial statements for periodic external

reporting, and, on a day-to-day basis, to make operating decisions, monitor performance, and allocate resources.<sup>37</sup>

Pertinent information should be identified, captured, and distributed in a form and timeframe that permits people to perform their duties efficiently. Effective communications should occur in a broad sense with information flowing down, across, and up the organization. In addition to internal communications, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders who may have a significant impact on the organization achieving its goals. Moreover, effective information technology management is critical to achieving useful, reliable, and continuous recording and communication of information.<sup>38</sup>

Management should focus on understanding the systems and processes that are important in the accumulation of financial data, including the system of controls that safeguard information, the processes for authorizing transactions, and the system for maintaining records. When evaluating the information and communication Component of internal control over financial reporting, management should consider the methods used to accumulate and disseminate information:

- Accounting systems
- Policy manuals (including financial reporting manuals)
- Management's reports
- Newsletters
- Accounting policy updates
- Technical updates
- Staff meetings
- Training

When evaluating information and communication, the assessment team should consider quality, for example, ascertaining whether the following conditions are true:

- Content is appropriate – Is the needed information available?
- Information is timely – Is it available when required?
- Information is current – Is it the latest available?
- Information is accurate – Is the data correct?
- Information is accessible – Can the data be obtained easily by appropriate parties?

All of these questions should be addressed by the system design. If not, it is probable that the system will not provide the information that management and other personnel require to ensure accurate financial reporting.

---

<sup>37</sup> Adopted from the *Standards for Internal Control in the Federal Government*, GAO Report # GAO/AIMD-00-21.3.1 (11/99),

<sup>38</sup> Ibid

## Monitoring

Monitoring is the continuous process management uses to assess the quality of internal control performance over time. There are three sub-Components to monitoring:

Monitoring Sub-Components	
Ongoing Monitoring	Ongoing monitoring occurs in the ordinary course of operations. Ongoing monitoring includes regular management and supervisory activities and other actions personnel take in performing duties that assess the quality of the internal control system's performance.
Separate Evaluations/ Periodic Monitoring	Periodic monitoring involves less frequent (i.e., monthly or quarterly) activities by senior management. The scope and frequency of separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures. Separate evaluations may take the form of self-assessments as well as review of control design and direct testing of internal control. Separate evaluations also may be performed by the agency Inspector General.
Reporting Deficiencies	The monitoring Component should also include a process for reporting deficiencies to the appropriate level of management and undertaking corrective action efforts in a timely manner.

### *Monitoring Sub-Components*

According to the Green Book, monitoring of internal control should also include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. Managers are to take the following actions:

- Promptly evaluate findings from audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate agencies' operations
- Determine proper actions in response to findings and recommendations from audits and reviews
- Complete, within established timeframes, all actions that correct or otherwise resolve the matters brought to management's attention

The resolution process begins when audit or other review results are reported to management, and is completed only after action has been taken that (1) corrects identified deficiencies, (2) produces improvements, or (3) demonstrates that findings and recommendations do not warrant management action.

Examples of monitoring controls are listed below:

- Inspector General reviews
- Management reviews
- Self-assessments
- Reconciliations
- Fluctuation analytics
- Exception reports

The following table demonstrates the factors that should be documented for each Component of internal control and examples of items that may be included as part of the documentation:

Internal Control Component	Factor	Example of Items to be included in Documentation
Control Environment	<ul style="list-style-type: none"> <li>• Integrity and ethical values</li> <li>• Commitment to competence</li> <li>• Management’s philosophy and operating style</li> <li>• Organizational structure</li> <li>• Assignment of authority and responsibility</li> <li>• Human Resource Policies and Practices</li> <li>• Oversight groups</li> </ul>	<ul style="list-style-type: none"> <li>• Human Resource Policies and Procedures Manuals</li> <li>• Organization charts</li> <li>• Entity Standards for Ethical Conduct</li> <li>• Training Policies</li> <li>• Security Handbooks</li> <li>• Whistleblower Policies</li> <li>• Operational Handbooks</li> <li>• Job Descriptions including responsibilities</li> <li>• Relationships with oversight groups</li> <li>• Related communications at appropriate levels</li> </ul>
Risk Assessment	<ul style="list-style-type: none"> <li>• Establishment of entity-wide objectives</li> <li>• Establishment of activity-level objectives</li> <li>• Risk identification</li> <li>• Risk analysis</li> <li>• Managing risk change</li> </ul>	<ul style="list-style-type: none"> <li>• Policies and procedures used to identify internal and external risks</li> <li>• Entity objectives and associated risks to achievement</li> <li>• Risk analyses and assessments</li> <li>• Related communications at appropriate levels</li> </ul>
Control Activities	<ul style="list-style-type: none"> <li>• Policies, procedures, techniques, and mechanisms in place to ensure activities are properly controlled.</li> </ul>	<ul style="list-style-type: none"> <li>• Management objectives</li> <li>• Planning and reporting systems</li> <li>• Analytical review and analyses</li> <li>• Policies and procedures related to segregation of duties</li> <li>• Policies and procedures related to safeguarding of records</li> <li>• Physical and access controls</li> <li>• Related communications at appropriate levels</li> <li>• Entity-wide security management program</li> <li>• Application controls</li> <li>• Service continuity</li> <li>• Related communications at appropriate levels</li> </ul>

Internal Control Component	Factor	Example of Items to be included in Documentation
Information and Communication	<ul style="list-style-type: none"> <li>• Process for obtaining and disseminating internal and incoming external information</li> <li>• Process for identifying, capturing, and distributing information</li> <li>• Process of ensuring effective internal and external communication occurs</li> <li>• Forms and means of communication</li> <li>• Disaster recovery</li> </ul>	<ul style="list-style-type: none"> <li>• Financial Reporting Procedures Manual</li> <li>• Accounting Policies and Procedures</li> <li>• Organizational structures indicating lines of communication relevant to financial reporting</li> <li>• Entity Policies related to distribution of information</li> <li>• Disaster recovery procedures</li> <li>• Type and sufficiency of reports produced</li> <li>• Communication of control-related duties and responsibilities</li> <li>• Manner in which information system development is managed</li> <li>• Related communications at appropriate levels</li> </ul>
Monitoring	<ul style="list-style-type: none"> <li>• Ongoing monitoring</li> <li>• Separate evaluations</li> <li>• Reporting deficiencies</li> </ul>	<ul style="list-style-type: none"> <li>• Self assessments</li> <li>• Process for identifying the need of self-assessments</li> <li>• Process for reviewing and evaluating self-assessments</li> <li>• Process for reviewing and evaluating OIG and GAO external audit reports</li> <li>• Process for identifying and completing and reporting corrective actions</li> <li>• Related communications at appropriate levels</li> </ul>

*Components of Internal Control*

## Appendix E – Information Processing Objectives/CAVR

The four information processing objectives (completeness, accuracy, validity, and restricted access — sometimes referred to as CAVR) are a standard means to assess the integrity of the data that flows through a process. The four components of CAVR are listed below.

Information Processing Objective	Definition
Completeness	<ul style="list-style-type: none"> <li>• All recorded transactions are accepted by the system (only once)</li> <li>• Duplicate postings are rejected by the system</li> <li>• Any transactions that are rejected are addressed and fixed</li> </ul>
Accuracy	<ul style="list-style-type: none"> <li>• Key data elements for transactions (including standing data) that are recorded and input to the computer are correct</li> <li>• Changes in standing data are accurately input</li> </ul>
Validity	<ul style="list-style-type: none"> <li>• Transactions, including the alteration of standing data, are authorized</li> <li>• Transactions, including standing data files, are not fictitious and they relate to the organization</li> </ul>
Restricted Access	<ul style="list-style-type: none"> <li>• Unauthorized amendments of data are barred from the system</li> <li>• The confidentiality of data is ensured</li> <li>• Entity assets are physically protected from theft and misuse</li> <li>• The segregation of duties is ensured</li> </ul>

### *Information Processing Objectives/CAVR*

Although control activities that achieve the information processing objectives do not always provide direct comfort on financial statement assertions, the table below may be useful in linking controls work to the financial statement assertions, assuming that the KFPs to which the controls relate is designed effectively.

Information Processing Objective	Financial Statement Assertion
Completeness	Completeness, Existence/Occurrence
Accuracy	Valuation/Allocation
Validity	Existence/Occurrence, Rights & Obligations
Restricted Access	Most, except for Rights & Obligations

Note that in the table above, Restricted Access links to most assertions. Restricted access to assets and records means that data is protected against unauthorized amendments, its confidentiality is ensured, and physical assets are protected. This is similar to the control environment or tone at the top in that it links to many assertions. If we know that the physical assets are protected, we have contributed to our "existence/occurrence" assertion. If we know that access to the system is restricted, we may have contributed to our "existence/occurrence", "completeness", and "valuation" assertions.

## Appendix F – Flowchart Instruction

Flowcharts provide details of activities, tasks, responsibilities, and key decision points in a given KFP. The purpose of the flowcharts is to identify control points in the KFP and the control activities performed by the users.

Flowcharts are divided by "swim lanes" that contain descriptive shapes. Each shape represents a particular occurrence within the KFP. Specific KFP activity, decision point or reference is described within the shape. The movement of a KFP model travels from left to right in a timeline fashion.

Specific definitions of the various elements contained within the flowchart presentation:

**Swim Lanes.** Indicate the specific entity or organizational unit responsible for handling a KFP or making a decision. Swim lanes are presented horizontally with titled position marked vertically on the left side of the flowchart.

**Phases.** Specific phases are identified as a set of activities grouped together. Separate phases can be shown on the same flowchart, divided by a vertical line.

**Shapes.** The specific shapes are symbols meant to identify actions or documents.

### Flowchart Legend

	<b>Terminator:</b> Marks the beginning or end of a KFP. Usually contains the word "start" or "end".
	<b>On-page connector:</b> Indicates that the flow continues on the same page where a matching symbol containing the same number has been placed
	<b>Off-page connector:</b> Indicates that the KFP continues on another (different) page where a matching symbol containing the same number has been placed
	<b>General process:</b> Denotes a general task that should be done. It can represent a single step or an entire sub-process within a larger process.
	<b>Manual process:</b> Denotes a task that is performed using manual means
	<b>Document:</b> Denotes a printed document or report
	<b>Prepare:</b> Typically denotes a task that requires a user to complete a form or document or assemble a package
	<b>Decision:</b> Denotes a decision or branching point. This symbol will always have a "yes" and a "no" branch depending on the answer to the decision. The "yes" and "no" branches may lead to more decision blocks or to another process block.
	<b>Input/Output:</b> Represents material or information entering or leaving the system, such as a customer order (input) or a product (output)
	<b>Manual Input:</b> Denotes a step requiring manual entry of data (such as keying in values on a spreadsheet)

	<b>Stored Data:</b> Indicates a general step where data gets stored
	<b>Direct Data:</b> Another term for "random access" or hard disk storage (as opposed to "sequential data" which is stored in a structure)
	<b>Sequential Data:</b> Denotes data stored on tape
	<b>Display:</b> Indicates a step that displays data to the end user
	<b>Flow-Line:</b> Lines that indicate the sequence of steps and the direction of the flow
	<b>Transfer of Control:</b> Denotes that the control of the process has been transferred from one Process Owner or organization to another
	<b>Control:</b> Denotes that the step in the KFP contains a non-key internal control
	<b>Key Control:</b> Denotes that the step in the KFP contains a key internal control
	<b>Annotation:</b> Used at will for whatever reason – questions, additional details, etc. Annotations should not be present in the finished product – if they contain details or explanations, the content should be moved to the narrative.

## Appendix G – Stakeholder Responsibility Matrix

Group	Role	Phase of Implementation Guide	Activity
Secretary	Involved	I. Planning	1
		V. External Reporting	1
SMC	Involved	I. Planning	1, 13
		V. External Reporting	1
CFO	Involved	I. Planning	1
SAT	Responsible	IV. Concluding, Internal Reporting, and Correcting	1
		V. External Reporting	1
	Involved	I. Planning	1-13
		II. Evaluating	1.4
		III. Testing	1
		IV. Concluding, Internal Reporting, and Correcting	2.2, 3.1, 3.2
IV. External Reporting	1		
OBO/ICS	Responsible	I. Planning	1-13
		II. Evaluating	1-3
		III. Testing	1-2
		IV. Concluding, Internal Reporting, and Correcting	2.2,3
	Involved	IV. Concluding, Internal Reporting, and Correcting	1, 2.1, 2.3
		V. External Reporting	1
VA personnel	Involved	II. Evaluating	2.1.1-2.1.3, 2.4, 3
		IV. Concluding, Internal Reporting, and Correcting	2.1, 2.3
PO Liaisons	Responsible	II. Evaluating	2.1.5
	Involved	II. Evaluating	2.1.1- 2.1.4, 2.2, 2.3
		IV. Concluding, Internal Reporting, and Correcting	2.1, 2.3, 3.1-3.3
Process Owners	Responsible	II. Evaluating	2.1.5-2.1.6
		IV. Concluding, Internal Reporting, and Correcting	2.1, 2.3
	Involved	II. Evaluating	2.1, 3
		IV. Concluding, Internal Reporting, and Correcting	1,3.1

## Appendix H – Alternative Procedures for Evaluating Controls of Cross-Servicing Providers

If an Annual Assurance Statement or Type II SAS 70 report cannot be obtained, or the report obtained does not adequately address the information processing objectives/CAVR required by the assessment team, alternative procedures should be performed over the service organization's internal control. These procedures may include one or more of the following:

- Perform tests of controls at the service organization
- Obtain a report on the application of agreed-upon procedures that describes the tests of relevant controls
- Perform tests of the user controls over the activities of the service organization

### Perform tests of controls at the service organization

If VA's contract with the service organization has a "right to audit" clause or the Department is otherwise permitted by the service organization to perform an audit, the assessment team may have its own personnel review and test the controls at the service organization. This review would be similar to the assessment that the assessment team would perform on its internal processes. The review would need to cover the control activities at the service organization, as well as any relevant controls covering the other four Components of internal control (including general computer controls).

### Obtain a report on the application of agreed-upon procedures that describes the tests of relevant controls

An agreed-upon procedures report may be used if it provides a level of evidence similar to a SAS 70 report. If an agreed-upon procedures report is to be relied upon, the assessment team should consider the following factors:

- The service organization's controls that (1) are relevant to VA's internal control over financial reporting and (2) cover all five Components of internal control (including general computer controls)
- The time period covered and the nature and results of the tests that the service auditor applied to the service organization's controls to validate that they are operating effectively

### Perform tests of the user controls over the activities of the service organization

The assessment team should assess whether its user controls would provide adequate assurance by considering whether (1) a breakdown of control at the service organization could lead to a misstatement that is more than inconsequential and (2) management's user controls would detect or prevent the misstatement in a timely manner.

For example, assume that an entity uses a service organization to process payroll. On one occasion, the service organization erroneously inputs the wrong payment amount for a new employee, causing the overall payroll amount to be incorrect. If management performs an independent review of the total amount that was paid at every pay period, the error would be detected, researched, and resolved before the error was recorded in the organization's financial records. In this case, the assessment team may be able to rely on its own user controls.

User controls may take the following forms:

- **Input/Output Controls.** In most outsourcing situations, the entity will have some access to the information processed by a service organization. In some cases, this information may enable

the organization to fully reconcile the service organization's results with the results of an independent source. For example, an entity using a payroll service organization could compare the data submitted to the service organization with reports or information received from the service organization after the data has been processed. The entity also could re-compute a sample of the payroll amounts for clerical accuracy and review the total amount of the payroll for reasonableness.

- **Performance Monitoring.** Management may have a process for monitoring the service organization's performance in relation to various metrics, as typically defined in a service level agreement. Most of these metrics will be tailored to specific operations. In some situations, however, such monitoring may provide some indirect assurance that the service organization's controls are operating properly. For example, management may regularly review the security, availability, and processing integrity of service-level agreements and related contracts with third-party service organizations.

A designated individual would be responsible for regularly monitoring the third party's performance and reporting whether or not that performance meets certain criteria.

- **Process Controls.** In some outsourcing situations, the entity's user controls may be closely tied to the service organization's processes and provide direct assurance over their operation. For example, an entity that has outsourced its IT development to a service organization may choose to document, track, approve, and test all application changes internally, thus retaining significant control over the IT development process.

Typically, the assessment team's testing of its user controls that pertain to a service organization is not as effective as the assessment team's testing of controls that are in place at the service organization itself. Accordingly, the assessment team should determine whether an assessment of the organization's user controls alone is sufficient to establish the reliability of the relevant information processing objectives/CAVR. The assessment team may rely solely on testing its own user controls in situations where (1) such controls cover all relevant assertions over the accounts and disclosures affected by the outsourced processes and (2) the significance and risk of processing at the service organization to VA's financial statements is low.

## Appendix I – Risk-Based Testing

During the initial years of A-123, Appendix A, VA should test all key controls in order to ensure that all controls are operating effectively. Once a baseline is established, ICS can consider implementing a risk-based approach which requires that stable controls with no known deficiencies can be tested every three years. The CFOC provides the following guidelines regarding risk-based testing:<sup>39</sup>

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

- There are no known weaknesses in the function of the control
- The control has been tested within the past three years
- 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, the following is true:

- There are no known significant weaknesses of such control
- The control has been tested within the past three years
- There have been no changes in the design or operation of the control since it was last tested
- 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 following is true:

- The control is fully automated as opposed to a manual control or is a 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
- The control has been tested in the past three years

Should VA opt for a risk-based approach, ICS should document its approach, as well as other testing procedures, in an overall Test Plan.

---

<sup>39</sup> CFOC Implementation Guide for A-123, Appendix A, page 35.

## Appendix J – Testing Types

The nature of the tests to be performed is classified into four categories: inquiry, observation, inspection, and re-performance. These categories are described below.

### Inquiry

Inquiry tests are conducted by making either oral or written inquiries of VA personnel involved in the application of specific control activities to determine what they do or how they perform a specific control activity. Such inquiries are typically open-ended. Generally, evidence obtained through inquiry is the least reliable audit evidence and will be corroborated through other types of control tests (observation or inspection). Inquiring about a control's effectiveness does not, by itself, provide sufficient audit evidence of whether a control is operating effectively. The reliability of evidence obtained from inquiry depends on the following factors:

- The competence, experience, knowledge, independence, and integrity of the person of whom the inquiry was made. The reliability of evidence is enhanced when the person possesses these attributes.
- Whether the evidence was general or specific. Evidence that is specific is usually more reliable than evidence that is general.
- The extent of corroborative evidence obtained. Evidence obtained from several entity personnel is usually more reliable than evidence obtained from only one.
- Whether the evidence was provided orally or in writing. Generally, evidence provided in writing is more reliable than evidence provided orally.<sup>40</sup>

### Observation

Observation tests are conducted by observing entity personnel actually performing control activities in the normal course of their duties. Observation generally provides highly reliable evidence that a control activity is properly applied; however, it provides no evidence that the control was in operation at any other time. Consequently, observation tests should be supplemented by corroborative evidence obtained from other tests (such as inquiry and inspection) about the operation of controls at other times. However, observation of the control provides a higher degree of assurance than inquiries, and may be an acceptable technique for assessing automated controls.<sup>41</sup>

### Inspection

Inspection of evidence often is used to determine whether manual controls are being performed. Inspection tests are conducted by examining documents and records for evidence (such as the existence of initials or signatures) that a control activity was applied to those documents and records.

System documentation, such as operations manuals, flow charts, and job descriptions, may provide evidence of control design but does not provide evidence that controls are actually operating and being applied consistently. To use system documentation as part of the evidence of effective control activities, additional evidence on how the controls were applied is required.

Since documentary evidence generally does not provide evidence concerning how effectively the control was applied, supplemental inspection tests with observation and/or inquiry of persons

---

<sup>40</sup> Definition adapted from the GAO/PCIE [Financial Audit Manual](#), section 350.

<sup>41</sup> Ibid.

applying the control are required. For example, the testing effort should supplement inspection of initials on documents with observation and/or inquiry of the individual(s) who initialled the documents to understand the procedures they followed before initialling the documents.

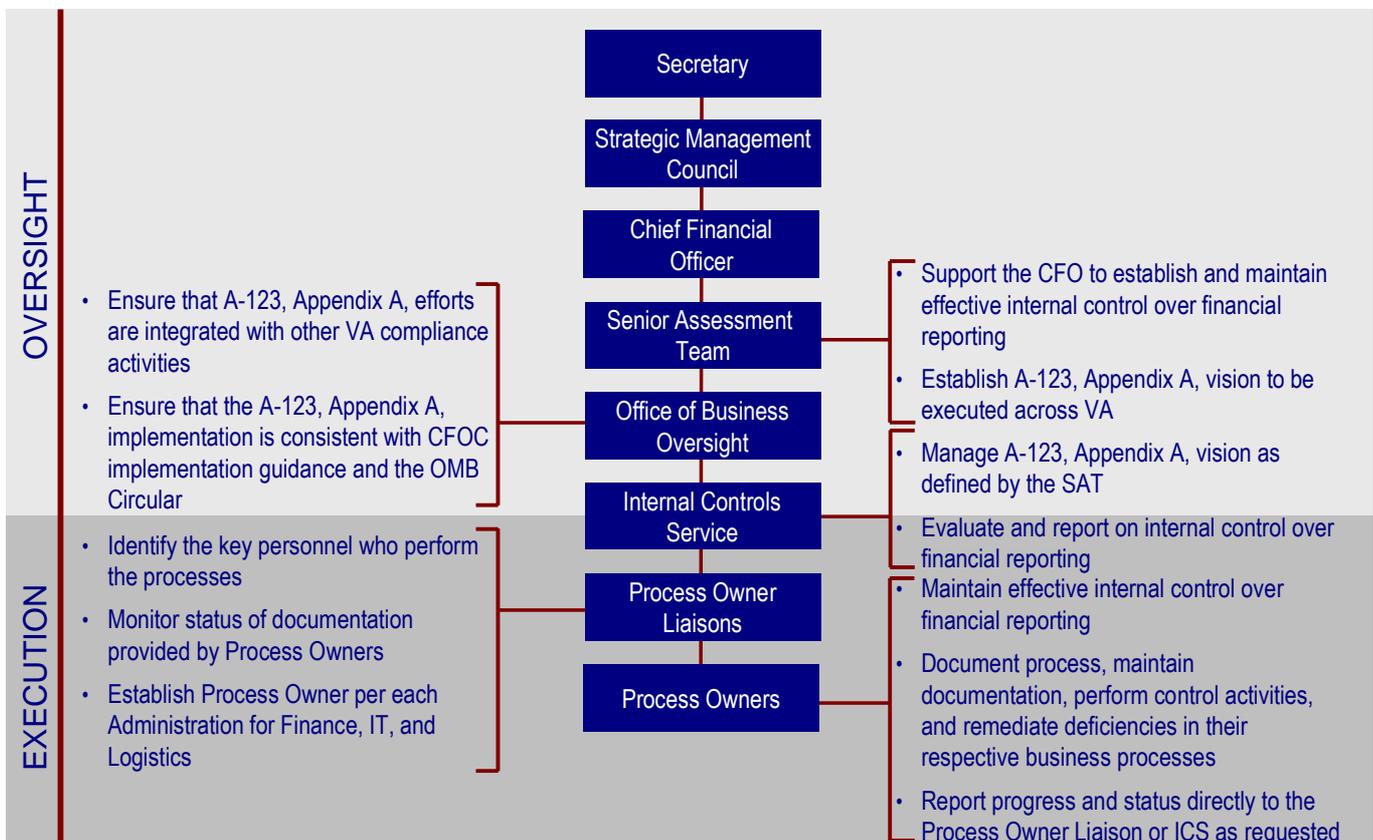
### **Re-performance**

It will normally be necessary to re-perform controls to obtain sufficient evidence of their operating effectiveness. For example, a signature on a voucher package by an approved signer does not necessarily mean that the person carefully reviewed the package before signing. The package may have been signed based on a cursory review (or without any review). As a result, the quality of the evidence regarding the effective operation of the control might not be sufficiently persuasive. If that is the case, the testing effort will include re-performing the control (e.g., checking prices, extensions, and additions) as part of the test of the control. In addition, it might involve inquiring of the person responsible for approving voucher packages what he or she looks for when approving packages and how many errors have been found within voucher packages. The testing effort might also inquire of supervisors as to whether they have any knowledge of errors that the person responsible for approving the voucher packages failed to detect. Because the control is being re-performed, it is not necessary to select high value items for testing or to select different types of transactions.

## Appendix K – Organizational Structure

The reporting structure will consist of a combination of groups that work cohesively to conduct an efficient assessment. The CFO is accountable for establishing and maintaining effective internal control over financial reporting through the A-123, Appendix A, assessment, but vests this authority to the SAT. The Director of ICS, with guidance from OBO, will assume program management responsibilities for overseeing the execution of the assessment process. OBO will ensure that the assessment process is both integrated with other VA compliance activities and consistent with the approach provided in the CFOC Guide.

The Director of ICS will manage and oversee the activities performed and outputs developed by the Process Owner Liaisons, Process Owners, and ICS staff. Under the ICS Director's oversight, Process Owners will document KFPs, maintain documentation, remediate deficiencies, as appropriate, and report progress to their Process Owner Liaisons. ICS will conduct control testing. Process Owner Liaisons will report progress directly to the Director of ICS. OBO will report A-123, Appendix A, assessment status to the SAT.



The overarching goal is to create an environment that instills the importance of creating and maintaining effective internal control over financial reporting. The roles and responsibilities of each group are reflected in the following table:

Group	Role
Secretary	<ul style="list-style-type: none"> <li>• Sign the statement of assurance on internal control over financial reporting</li> </ul>
Strategic Management Council (SMC)	<ul style="list-style-type: none"> <li>• Provide oversight and guidance to the SAT on final decisions and recommendations concerning the A-123, Appendix A, program</li> <li>• Serve as a collaborative and deliberative body</li> </ul>

Group	Role
Chief Financial Officer (CFO)	<ul style="list-style-type: none"> <li>• Provide a quarterly update to the SMC regarding A-123, Appendix A, program progress</li> <li>• Accountable for the establishment of an effective internal control program over financial reporting</li> <li>• Serve as the Chairman for the SAT</li> </ul>
Senior Assessment Team (SAT)	<ul style="list-style-type: none"> <li>• Assist CFO in his responsibility for establishing and maintaining effective internal control over financial reporting</li> <li>• Provide recommendations to the Secretary on the Department's statement of assurance</li> </ul>
Office of Business Oversight (OBO)	<ul style="list-style-type: none"> <li>• Manage the communication process with the SAT</li> <li>• Ensure that the A-123, Appendix A, efforts are integrated with other VA compliance activities</li> <li>• Ensure that the A-123, Appendix A, implementation is consistent with CFOC implementation guidance and the OMB Circular</li> </ul>
Internal Controls Service (ICS)	<p><i>ICS Director:</i></p> <ul style="list-style-type: none"> <li>• Manage the implementation and execution of VA's OMB A-123, Appendix A, internal controls activities as defined by the SAT</li> <li>• Provide program/project management for the A-123, Appendix A, implementation - direct, plan, oversee, and report on the status of the implementation of A-123, Appendix A, in accordance with defined standards and guidance</li> </ul> <p><i>ICS Staff:</i></p> <ul style="list-style-type: none"> <li>• Serve as the assessment team</li> <li>• Evaluate and perform tests of controls and/or work with contractors to perform test of controls</li> <li>• Document procedures performed, evidence obtained, and conclusions reached</li> </ul>
Process Owner Liaisons	<ul style="list-style-type: none"> <li>• Identify the key personnel, i.e., Process Owners, who perform the KFPs to be documented and assessed</li> <li>• Manage the outputs of the Process Owners, review each output against VA standards, submit those outputs to ICS in a timely manner, and report progress as requested by ICS.</li> </ul>
Process Owners	<ul style="list-style-type: none"> <li>• Perform key financial processes as part of their normal daily operations</li> <li>• Document their responsible KFPs, maintain current and relevant documentation, develop corrective action plans, complete activities associated with the plans, and report progress directly to the Process Owner Liaison or ICS Director as requested</li> </ul>

## Appendix L – Detail Framework for Evaluating Control Exceptions and Deficiencies

The following detail framework should be used to specifically measure the magnitude and likelihood of various types of internal control deficiencies in order to determine their classification.

*NOTE: The following guidance was adapted from A Framework for Evaluating Control Exceptions and Deficiencies, Version 3, 12/20/2004. The framework was created by the Big 4 and other Accounting Firms and accounting educators. The whitepaper was created based on guidance available in AS2. The framework is based on the authors' views and is not intended to be applied universally and mechanically, but rather, with professional judgment.*

*This framework uses the deficiencies categorizations from A-123 (control deficiency, reportable condition, material weakness) rather than the categorizations from SAS 112 (deficiency, significant deficiency, material weakness). However, the framework can be applied to the SAS 112 categorizations.*

The evaluation of individual exceptions and deficiencies is an iterative process. Although this discussion depicts the evaluation process as a linear progression, it may be appropriate at any point in the process to return to and reconsider any previous step based on new information.

In applying the framework, the following should be considered in determining which chart(s) to use for evaluating individual exceptions and deficiencies:

- **Chart 1** is used to evaluate and **determine whether an exception** noted in performing tests of operating effectiveness **represents a control deficiency**
- **Chart 2** is used to evaluate and classify control deficiencies in manual or automated **controls that are directly related to achieving relevant financial statement assertions**
- **Chart 3** is used to evaluate and classify deficiencies in **general computer controls (GCC)** that are intended to support the continued effective operation of controls related to one or more relevant financial statement assertions. If an application control deficiency is related to or caused by a GCC deficiency, the application control deficiency is evaluated using Chart 2 and the GCC deficiency is evaluated using Chart 3.
- **Chart 4** is used to evaluate and classify control **deficiencies in pervasive controls other than GCC**. Such control deficiencies generally do not directly result in a misstatement. However, they may contribute to the likelihood of a misstatement at the process level.

After evaluating and classifying individual deficiencies, consideration should be given to the aggregation of the deficiencies using the guiding principles outlined in “Consider and Evaluate Deficiencies in the Aggregate” below.

### Chart 1 – Evaluating Exceptions Found in the Testing of Operating Effectiveness

This decision tree is to be used for evaluating exceptions found in the testing of operating effectiveness.

## General

The testing of controls generally relates to significant processes and major classes of transactions for relevant financial statement assertions related to significant accounts and disclosures.

Therefore, the underlying assumption is that all exceptions/deficiencies resulting from the testing should be evaluated because they relate to line items and related accounts and disclosures that are material to the financial statements taken as whole and other significant financial reports.

The purpose of tests of controls is to achieve a high level of assurance that the controls are operating effectively. Therefore, the sample sizes used to test controls should provide that level of comfort. The sampling tables provided in this guide are based on statistical principles and generally result in a high level of assurance where no exceptions are noted. In cases in which samples are selected using a statistically-based approach, sample sizes for frequently operating manual controls that result in less than a 90% level of confidence that the upper limit deviation rate does not exceed 10% typically would not provide a high level of assurance.<sup>42</sup>

The magnitude of a control deficiency (i.e., deficiency, reportable condition, or material weakness) is evaluated based on the impact of known and/or potential misstatements on annual and interim financial statements.

While some of the concepts discussed here relate to statistical sampling, the framework does not require the use of statistical sampling. A statistical sample is (1) selected on a random or other basis that is representative of the population and (2) evaluated statistically. In tests of internal controls, it may be impractical to select samples randomly, but they should be selected in an unbiased manner.

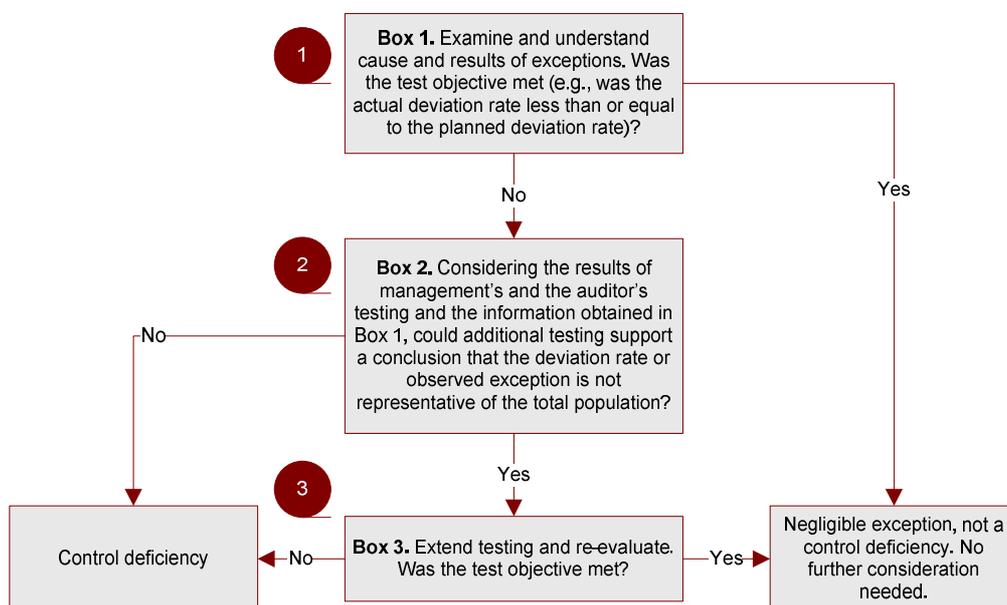


Chart 1

<sup>42</sup> Refer to the AICPA Audit and Accounting Guide, *Audit Sampling*.

### 1 Box 1

All exceptions should be evaluated quantitatively and qualitatively. A thorough understanding of the cause of the exception is important in evaluating whether a test exception represents a control deficiency. This evaluation should consider the potential implications with regard to the effectiveness of other controls.

In concluding whether the test objective was met, considerations include:

- The deviation rate in relation to the frequency of performance of the control (e.g., absent extending the test, there is a presumption that an exception in a control that operates less frequently than daily is a control deficiency)
- Qualitative factors, including exceptions that are determined to be systematic and recurring
- Whether the exception is known to have resulted in a financial statement misstatement (e.g., there is a presumption that an exception that results in a financial statement misstatement in excess of the level of precision at which the control is designed to operate is a control deficiency)

A control objective may be achieved by a single control or a combination of controls. A test of controls may be designed to test a single control that alone achieves the control objective or a number of individual controls that together achieve the control objective.

### 2 Box 2

If the test objective is not met, consideration should be given to whether additional testing could support a conclusion that the deviation rate is not representative of the total population. For example, if observed exceptions result in a non-negligible deviation rate, then the test objective initially is not met. In a test designed to allow for finding one or more deviations, the test objective is not met if the actual number of deviations found exceeds the number of deviations allowed for in the plan.

### 3 Box 3

If the test objective initially is not met, there are two options:

- If the observed exceptions and resulting non-negligible deviation rate are not believed to be representative of the population, the test may be extended and re-evaluated
- If the observed exceptions and resulting non-negligible deviation rate are believed to be representative of the population, the exceptions are considered to be a control deficiency and its significance is assessed

## Chart 2 – Evaluating Process/Transaction-Level Control Deficiencies

This decision tree is to be used for evaluating the classification of control deficiencies from the following sources:

- Design effectiveness evaluation
- Operating effectiveness testing (from Chart 1)
- Deficiencies that resulted in a financial statement misstatement detected by management or the auditor in performing substantive test work.

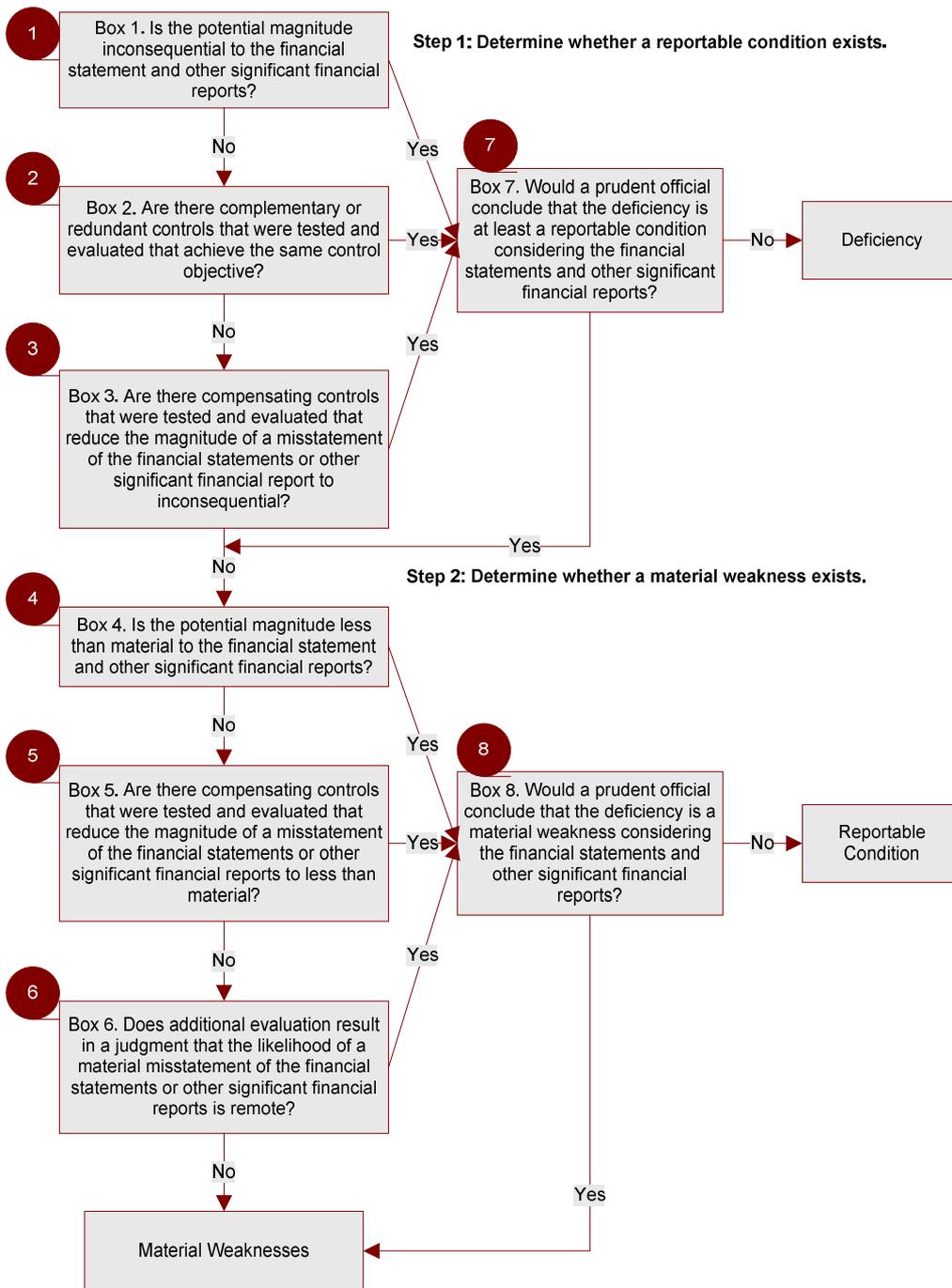


Chart 2

## Step 1. Determine whether a reportable condition exists:

---

### 1 Box 1

When evaluating deficiencies, potential magnitude (inconsequential, more than inconsequential, or material) is based on the potential effect on the financial statements or other significant financial reports. Potential magnitude of misstatement may be based on gross exposure, adjusted exposure, or other appropriate methods that consider the likelihood of misstatement.

### 2 | 3 Boxes 2 & 3

If there are controls that effectively mitigate a control deficiency, it is classified as only a deficiency, absent any qualitative factors. Such controls include:

- Complementary or redundant controls that achieve the same control objective
- Compensating controls that operate at a level of precision that would result in the prevention or detection of a *more than inconsequential* misstatement of the financial statements or other significant financial reports

Boxes 1, 2, and 3 should be considered separately. Adjusted exposure should not be reduced by the quantitative impact of the compensating and complementary or redundant controls.

### 3 Box 3

An unmitigated deficient control that results in a control objective not being met related to a significant account or disclosure generally results in a more-than-remote likelihood of a *more than inconsequential* misstatement of the financial statements or other significant financial reports and, therefore, is at least a reportable condition.

## Step 2. Determine whether a material weakness exists:

---

### 4 Box 4

The potential magnitude of a misstatement of the financial statements or other significant financial report that is less than material results in the deficient control being classified as only a reportable condition, absent any qualitative factors. Potential magnitude may be based on gross exposure, adjusted exposure, or other appropriate methods that consider the likelihood of misstatement.

## 5 Box 5

Compensating controls that operate at a level of precision that would result in the prevention or detection of a *material* misstatement may support a conclusion that the deficiency is not a material weakness.

## 6 Box 6

In evaluating likelihood and magnitude, related factors include but are not limited to the following:

- The nature of the financial statement accounts, disclosures, and assertions involved; for example, suspense accounts and intra-Departmental transactions involve greater risk
- The susceptibility of the related assets or liability to loss, waste, abuse or fraud; that is, greater susceptibility increases risk
- The subjectivity, complexity, or extent of judgment required to determine the amount involved; that is, greater subjectivity, complexity, or judgment, like that related to an accounting estimate, increases risk
- The cause and frequency of known or detected exceptions in the operating effectiveness of a control; for example, a control with an observed non-negligible deviation rate is a deficiency
- The interaction or relationship with other controls; that is, the interdependence or redundancy of controls
- The possible future consequences of the deficiency
- An indication of increased risk evidenced by a history of misstatements, including misstatements identified in the current year
- The adjusted exposure in relation to overall materiality

This framework recognizes that in evaluating deficiencies, the risk of misstatement might be different for the maximum possible misstatement than for lesser possible amounts.

As a result of this additional evaluation, determine whether the likelihood of a material misstatement is remote. In extremely rare circumstances, this additional evaluation could result in a judgment that the likelihood of a more than inconsequential misstatement is remote.

## 7 | 8 Boxes 7 & 8

When determining the classification of a deficiency, the Senior Assessment Team should also consider the level of detail and degree of assurance that would satisfy prudent officials in the conduct of their own affairs, such that they have reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles.<sup>43</sup> If the Senior Assessment Team determines that the deficiency would prevent prudent officials in the conduct of their own affairs from concluding that they have reasonable assurance, the auditor should deem the deficiency to be at least a reportable condition. Having determined in this manner that a deficiency represents a reportable condition, the Senior Assessment Team should further evaluate the deficiency to determine whether individually, or in combination with other deficiencies, the deficiency is a material weakness.

### **Additional considerations related to misstatements identified:**

A greater than de minimis misstatement identified by the Senior Assessment Team or by the auditor during a test of controls or during a substantive test is ordinarily indicative of a deficiency in the design and/or operating effectiveness of a control, which is evaluated as follows:

- The design and/or operating deficiency(ies) that did not prevent or detect the misstatement should be identified and evaluated based on Chart 2 – Evaluating Process/Transaction-Level Control Deficiencies, applying the following:
  - A known or likely (including projected) misstatement that is inconsequential is at least a deficiency
  - A known or likely (including projected) misstatement that is more than inconsequential is a strong indicator of a reportable condition
  - A known or likely (including projected) misstatement that is material is at least a reportable condition and a strong indicator of a material weakness
- The implications on the effectiveness of other controls, particularly compensating controls, also should be considered

---

<sup>43</sup> AS 2.137.

## Chart 3 – Evaluating General Computer Control Deficiencies

This decision tree is to be used for evaluating the classification of general computer control (GCC) deficiencies from the following sources:

- GCC design effectiveness evaluation
- GCC operating effectiveness testing (from Chart 1)
- GCC design or operating deficiencies identified as a result of application control testing (from Chart 2)

### General

Deficiencies in GCCs are evaluated in relation to their effect on application controls.

- GCC deficiencies do not directly result in misstatements
- Misstatements may result from ineffective application controls

There are three situations in which a GCC deficiency can rise to the level of a material weakness:

- An application control deficiency related to or caused by a GCC deficiency is classified as a material weakness
- The pervasiveness and significance of a GCC deficiency leads to a conclusion that there is a material weakness in the entity's control environment
- A GCC deficiency classified as a reportable condition remains uncorrected after some reasonable period of time

In evaluating whether a GCC deficiency affects the continued effective operation of application controls, it is not necessary to contemplate the likelihood that an effective application control could, in a subsequent year, become ineffective because of the deficient GCC.

### Relationship between GCCs and application controls

An understanding of the relationship among applications relevant to internal control over financial reporting, the related application controls, and GCCs is necessary to appropriately evaluate GCC deficiencies. GCCs may affect the continued effective operation of application controls. For example, an effective security administration function supports the continued effective functioning of application controls that restrict access. As another example, effective program change controls support the continued effective operation of programmed application controls, such as a three-way match. GCCs also may serve as controls at the application level. For example, GCCs may directly achieve the control objective of restricting access and thereby prevent initiation of unauthorized transactions.

Similarly, GCC deficiencies may adversely affect the continued effective functioning of application controls; in the absence of application controls, GCC deficiencies also may represent control deficiencies for one or more relevant assertions.

### Evaluating GCC deficiencies

GCC deficiencies are evaluated using Chart 3. Additionally, if a GCC deficiency also represents a deficiency at the application level because it directly relates to an assertion, the GCC deficiency is also evaluated using Chart 2. In all cases, a GCC deficiency is considered in combination with application controls to determine whether the combined effect of the GCC deficiency and any application control deficiencies is a deficiency, reportable condition, or material weakness.

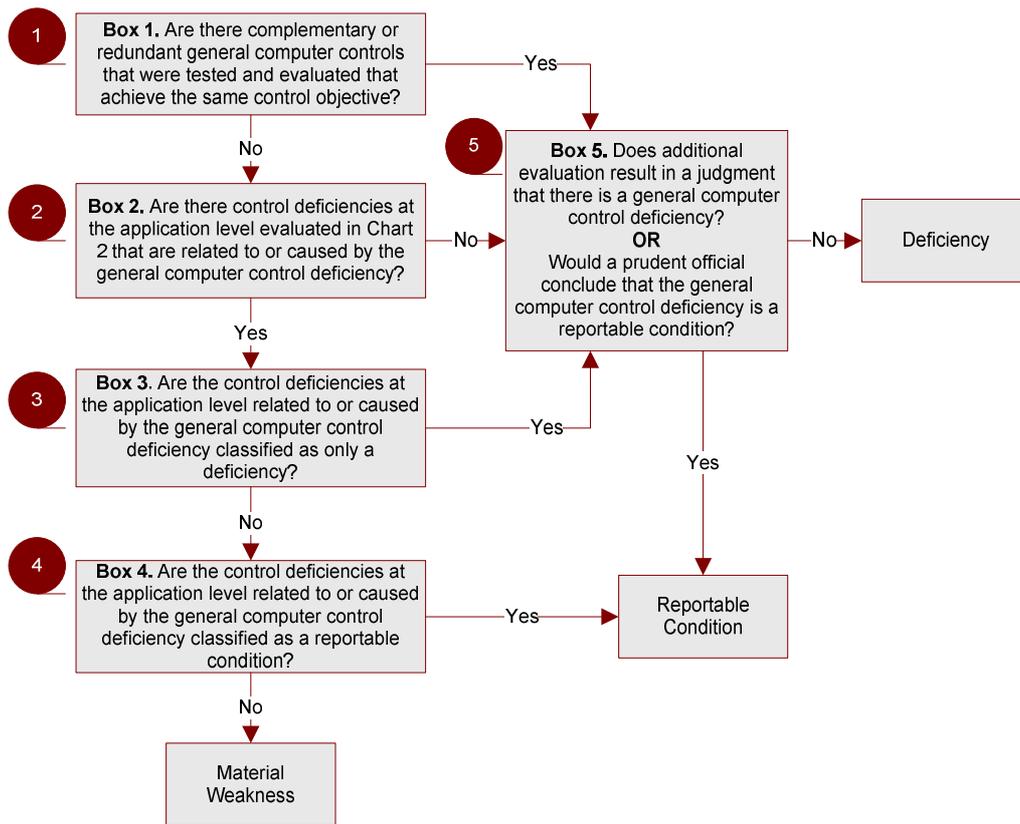


Chart 3

### 1 Box 1

Controls that effectively mitigate a control deficiency result in the deficiency being classified as only a deficiency, absent any qualitative factors. Such controls include complementary or redundant controls that achieve the same control objective. A GCC deficiency identified as a result of an application control deficiency indicates that other GCCs could not have achieved the same control objective as the deficient GCC.

### 2 Box 2

If no deficiencies are identified at the application level (as evaluated in Chart 2), the GCC deficiency could be classified as only a deficiency. (Refer to Box 5.)

### 3 | 4 Boxes 3 & 4

If there is a control deficiency at the application level related to or caused by a GCC deficiency, the GCC deficiency is evaluated in combination with the deficiency in the underlying application control and generally is classified consistent with the application control deficiency. As a result:

- A material weakness in an application control related to or caused by a GCC deficiency indicates that the GCC deficiency also is a material weakness
- A reportable condition in an application control related to or caused by a GCC deficiency indicates that the GCC deficiency also is a reportable condition
- An application control deficiency (that is only a deficiency) related to or caused by a GCC deficiency generally indicates that the GCC deficiency is only a deficiency

## 5 Box 5

Notwithstanding the guiding principles relating to Boxes 1 through 4, the classification of a GCC deficiency should consider factors including, but not limited to, the following:

- The nature and significance of the deficiency, e.g., does the deficiency relate to a single area in the program development process or is the entire process deficient?
- The pervasiveness of the deficiency to applications and data, including:
  - The extent to which controls related to significant accounts and underlying processes are affected by the deficiency
  - The number of application controls that are related to the deficiency
  - The number of control deficiencies at the application level that are related to or caused by the deficiency
- The complexity of the entity's systems environment and the likelihood that the deficiency could adversely affect application controls
- The relative proximity of the control to applications and data
- Whether a deficiency relates to applications or data for accounts or disclosures that are susceptible to loss or fraud
- The cause and frequency of known or detected exceptions in the operating effectiveness of a GCC; for example, (1) a control with an observed non-negligible deviation rate, (2) an observed exception that is inconsistent with the expected effective operation of the GCC, or (3) a deliberate failure to apply a control
- An indication of increased risk evidenced by a history of misstatements relating to applications affected by the deficiency, including misstatements in the current year

When determining the classification of a deficiency, the Senior Assessment Team should determine the level of detail and degree of assurance that would satisfy prudent officials<sup>44</sup> in the conduct of their own affairs. The Senior Assessment Team then can have reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles. If the Senior Assessment Team determines that the deficiency would prevent prudent officials in the conduct of their own affairs from concluding that they have reasonable assurance, the deficiency should be deemed to be at least a reportable condition.

### Additional consideration

GCCs support the proper and consistent operation of automated application controls. Therefore, consideration should be given to the nature, timing, and extent of the testing of related application controls affected by, or manual controls dependent on, the deficient GCC.

---

<sup>44</sup> The idea of "prudent official" and related discussion is based off of AS 2.137.

## **Chart 4 – Evaluating Control Deficiencies in Pervasive Controls Other than GCC**

This decision tree is to be used for evaluating the classification of control deficiencies in pervasive controls other than GCC from the following sources:

- Design effectiveness evaluation
- Operating effectiveness testing (from Chart 1)

### **General**

Deficiencies in pervasive controls generally do not directly result in a misstatement. However, they may contribute to the likelihood of a misstatement at the process level. Accordingly, evaluation of a deficiency in a pervasive control other than GCC is based on the likelihood that such deficiency would contribute to circumstances that could result in a misstatement. Quantitative methods generally are not conducive to evaluating such deficiencies.

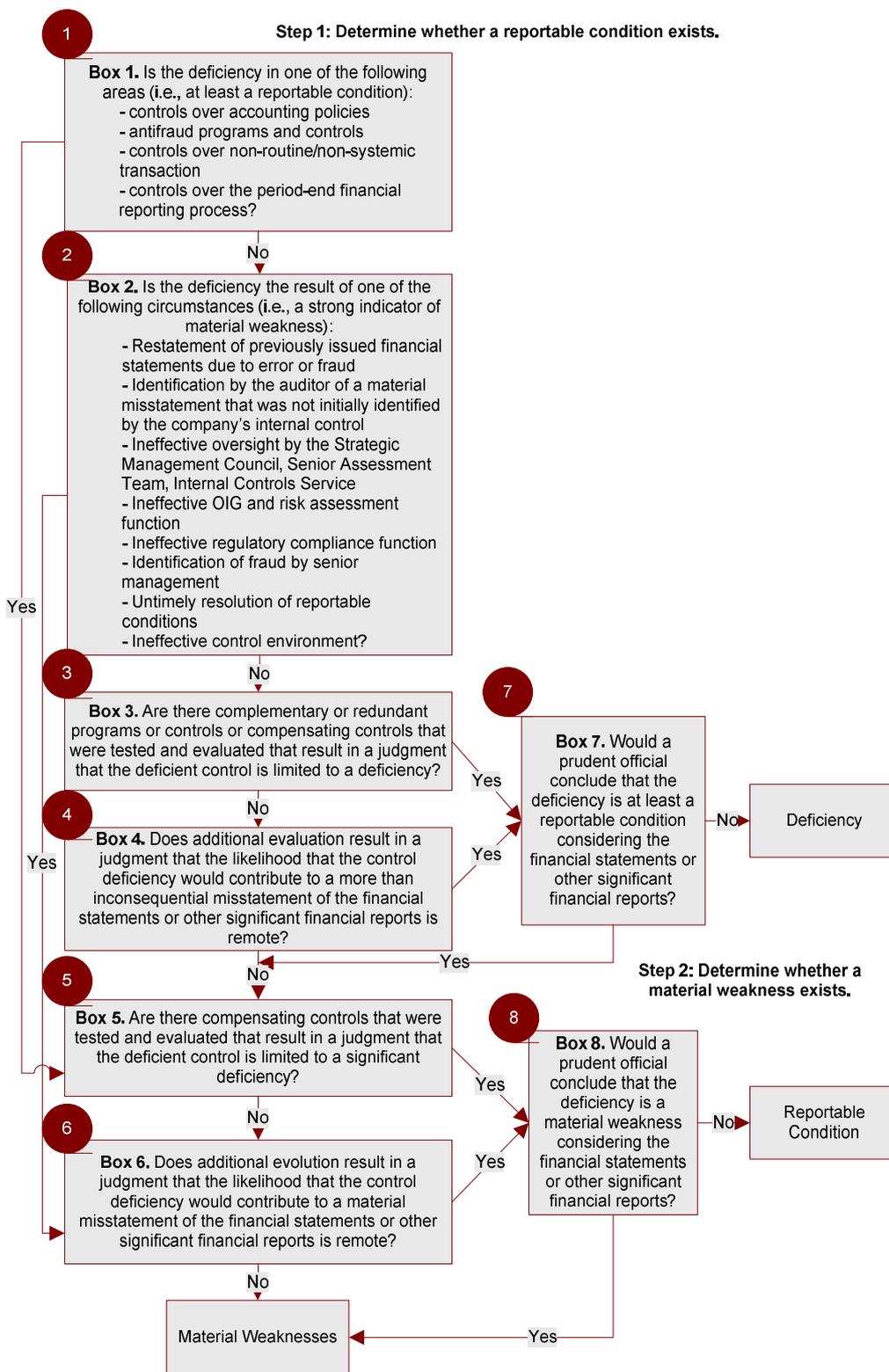


Chart 4

## Step 1. Determine whether a reportable condition exists:

---

### 1 | 2 Boxes 1 & 2

A deficiency in one of the following areas ordinarily results in deficiencies being at least a reportable condition.<sup>45</sup>

- Controls over the selection and application of accounting policies that are in conformity with generally accepted accounting principles
- Anti-fraud programs and controls
- Controls over non-routine and non-systematic transactions
- Controls over the period-end financial reporting process, including controls over procedures used to enter transaction totals into the general ledger; initiate, authorize, record, and process journal entries into the general ledger; and record the recurring and nonrecurring adjustments to the financial statements

The circumstances in which an evaluation would lead to the deficiency not being classified as a reportable condition are rare. The following circumstances should be regarded as at least a reportable condition and as a strong indicator of a material weakness<sup>46</sup>:

- Restatement of previously issued financial statements due to error or fraud to reflect the correction of a misstatement
- Identification by the auditor of a material misstatement in financial statements in the current period that was not initially identified by the entity's internal control over financial reporting. This is a strong indicator of a material weakness even if management subsequently corrects the misstatement.
- Oversight of the external financial reporting and internal control over financial reporting by the Senior Management Council, Senior Assessment Team, or Internal Control Committee is ineffective
- The OIG function or the risk assessment function is ineffective in the monitoring Component or risk assessment Component
- An ineffective regulatory compliance function that is solely related to those aspects of ineffective regulatory compliance in which associated violations of laws and regulations could have a material effect on the reliability of financial reporting
- Identification of fraud of any magnitude on the part of senior management
- Reportable Conditions that have been communicated to the Senior Management Council and Senior Assessment Team remain uncorrected after a reasonable period of time
- An ineffective control environment

### 3 Box 3

Certain controls could result in a judgment that the deficient control is limited to a deficiency and classified as only a deficiency, considering qualitative factors. Such controls include:

---

<sup>45</sup> Based on guidance provided in AS 2.139.

<sup>46</sup> Based on guidance provided in AS 2.140.

- Complementary or redundant programs or controls
- Compensating controls within the same or another Component

#### 4 **Box 4**

A deficiency with a more-than-remote likelihood that the deficiency would contribute to a more-than-inconsequential misstatement is a reportable condition. Such judgment considers an evaluation of factors such as:

- The pervasiveness of the deficiency across the entity
- The relative significance of the deficient control to the location
- An indication of increased risks of error (evidenced by a history of misstatement)
- An increased susceptibility to fraud (including the risk of management override)
- The cause and frequency of known or detected exceptions for the operating effectiveness of a control
- The possible future consequences of the deficiency

### Step 2. Determine whether a material weakness exists:

---

#### 5 **Box 5**

The evaluation of certain controls could result in a judgment that the deficient control is limited to a reportable condition and classified as such, considering qualitative factors. Such controls include compensating controls within the same or another Component.

#### 6 **Box 6**

A deficiency with a more-than-remote likelihood that the deficiency would contribute to a material misstatement is a material weakness. Such judgment considers an evaluation of factors such as:

- The pervasiveness of the deficiency across the entity
- The relative significance of the deficient control to the location
- An indication of increased risks of error (evidenced by a history of misstatement)
- An increased susceptibility to fraud (including the risk of management override)
- The cause and frequency of known or detected exceptions for the operating effectiveness of a control
- The possible future consequences of the deficiency

A deficiency of the type described in **Box 2** is generally a material weakness; in limited circumstances, it may be appropriate to conclude the deficiency is only a reportable condition. The only circumstance that would likely occur is<sup>47</sup>:

- The auditor initially identified a material misstatement in the financial statements but, given the circumstances, determined that management ultimately would have found the misstatement.

---

<sup>47</sup> Based on guidance provided in AS2 Appendix E99.

The auditor could determine that the circumstance was a reportable condition, but not a material weakness.

In this case, the deficiency would be a reportable condition.

## **7** | **8** **Boxes 7 & 8**

When determining the classification of a deficiency in internal control over financial reporting, the Senior Assessment Team should also consider the level of detail and degree of assurance that would satisfy prudent officials in the conduct of their own affairs, such that they have reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles.<sup>48</sup> If the Senior Assessment Team determines that the deficiency would prevent prudent officials in the conduct of their own affairs from concluding that they have reasonable assurance, the Senior Assessment Team should deem the deficiency to be at least a reportable condition. Having determined in this manner that a deficiency represents a reportable condition, the Senior Assessment Team should further evaluate the deficiency to determine whether individually, or in combination with other deficiencies, the deficiency is a material weakness.

### **Consider and Evaluate Deficiencies in the Aggregate**

Deficiencies are considered in the aggregate by significant account balance, disclosure, and Internal Control Standards Component to determine whether they collectively result in reportable conditions or material weaknesses. Aggregation of control activities deficiencies by significant account balance and disclosure is necessary since the existence of multiple control deficiencies related to a specific account balance or disclosure increases the likelihood of misstatement. Aggregation by the control environment, risk assessment, information and communication, and monitoring Components of Internal Control Standards is more difficult and judgmental. For example, unrelated control deficiencies relating to design ineffectiveness in other Internal Control Standards Components could lead to the conclusion that a reportable condition or material weakness in the risk assessment Component exists. Similarly, unrelated control deficiencies in other Internal Control Standards Components could lead to a conclusion that a reportable condition or material weakness in the control environment or monitoring Component exists.

---

<sup>48</sup> AS 2.137.

## Appendix M – Templates and Checklists

The following table lists the templates referenced in this manual, their purpose, and the users of the templates.

Template/Checklist	Purpose	User
Corrective Action Plan Template	<ul style="list-style-type: none"> <li>Provides a format for Process Owners to document corrective action status</li> </ul>	<ul style="list-style-type: none"> <li>Process Owners</li> <li>ICS</li> </ul>
Documentation Quality Review checklist	<ul style="list-style-type: none"> <li>Helps ICS check for accuracy and consistency across outputs (narratives, flowcharts and RCMs)</li> </ul>	<ul style="list-style-type: none"> <li>Process Owners</li> <li>Process Owner Liaisons</li> <li>ICS</li> </ul>
Documentation template	<ul style="list-style-type: none"> <li>Breaks down KFPs into individual, granular control activities</li> <li>Includes narratives, significant accounts, policies and procedures, interfaces with other KFPs, significant documents, sources of information and flowcharts</li> </ul>	<ul style="list-style-type: none"> <li>ICS</li> <li>Process Owners</li> </ul>
Evidence Request List template	<ul style="list-style-type: none"> <li>Lists the evidence that Process Owners must prepare for the testing of internal controls</li> <li>Includes forms and reports referenced in the documentation and KFP-level test plans</li> </ul>	<ul style="list-style-type: none"> <li>ICS</li> <li>Process Owners</li> </ul>
Exception Log template	<ul style="list-style-type: none"> <li>Assists ICS and the SAT in assessing and classifying internal control deficiencies during the Concluding, Internal Reporting, and Correcting Phase of the A-123, Appendix A, effort</li> </ul>	<ul style="list-style-type: none"> <li>ICS</li> <li>OBO</li> <li>SAT</li> </ul>
Financial Statement Assertions template	<ul style="list-style-type: none"> <li>Documents the financial statement assertions for each line item</li> </ul>	<ul style="list-style-type: none"> <li>ICS</li> </ul>
Finding Outline Worksheet	<ul style="list-style-type: none"> <li>Documents the five elements of the finding, the finding classification, and management/SAT review of the finding</li> </ul>	<ul style="list-style-type: none"> <li>Process Owners</li> <li>ICS</li> <li>SAT</li> </ul>
Flowchart template	<ul style="list-style-type: none"> <li>Depicts the sequential flow of a KFP through events as objects, using a number of shapes</li> <li>Ties back to the KFP narratives through "node numbers" that are placed on each object, directly corresponding to each control activity number in the narrative</li> </ul>	<ul style="list-style-type: none"> <li>ICS</li> <li>Process Owners</li> </ul>
General Computer Controls template	<ul style="list-style-type: none"> <li>Facilitates documentation of General Computer Controls (GCCs), which are categorized by FISCAM area</li> </ul>	<ul style="list-style-type: none"> <li>ICS</li> </ul>

Template/Checklist	Purpose	User
KFP-Level Test Plan template	<ul style="list-style-type: none"> <li>Documents the elements of the test including sample size, test steps and key attributes</li> </ul>	<ul style="list-style-type: none"> <li>ICS</li> </ul>
Location Selection Recommendations template	<ul style="list-style-type: none"> <li>Documents the rationale for in-scope sites</li> </ul>	<ul style="list-style-type: none"> <li>ICS</li> <li>SAT</li> </ul>
Risk/Control Matrix template	<ul style="list-style-type: none"> <li>Lists all controls (both key and non-key) and captures risks, control objectives, frequency and design assessment</li> </ul>	<ul style="list-style-type: none"> <li>Process Owners</li> <li>ICS</li> </ul>
SAS 70 Assessment Checklist template	<ul style="list-style-type: none"> <li>Assists ICS in reviewing and documenting SAS 70 assessments for cross-servicing organizations</li> </ul>	<ul style="list-style-type: none"> <li>ICS</li> </ul>
Test Sheet template	<ul style="list-style-type: none"> <li>Assists ICS in conducting the tests specified in the KFP-level test plans and documenting test results</li> </ul>	<ul style="list-style-type: none"> <li>ICS</li> </ul>
Testing Quality Review Checklist template	<ul style="list-style-type: none"> <li>Provides a framework for the Supervisor to review the test procedures and results</li> </ul>	<ul style="list-style-type: none"> <li>ICS</li> </ul>

## Appendix N – Sample Narrative and Flowchart

This sample narrative and flowchart are based on the Property, Plant, and Equipment Management Process Narrative Section 6 dated February 1 2007. For more information on these examples, refer to the Documentation Package Template and Process Flow Template.

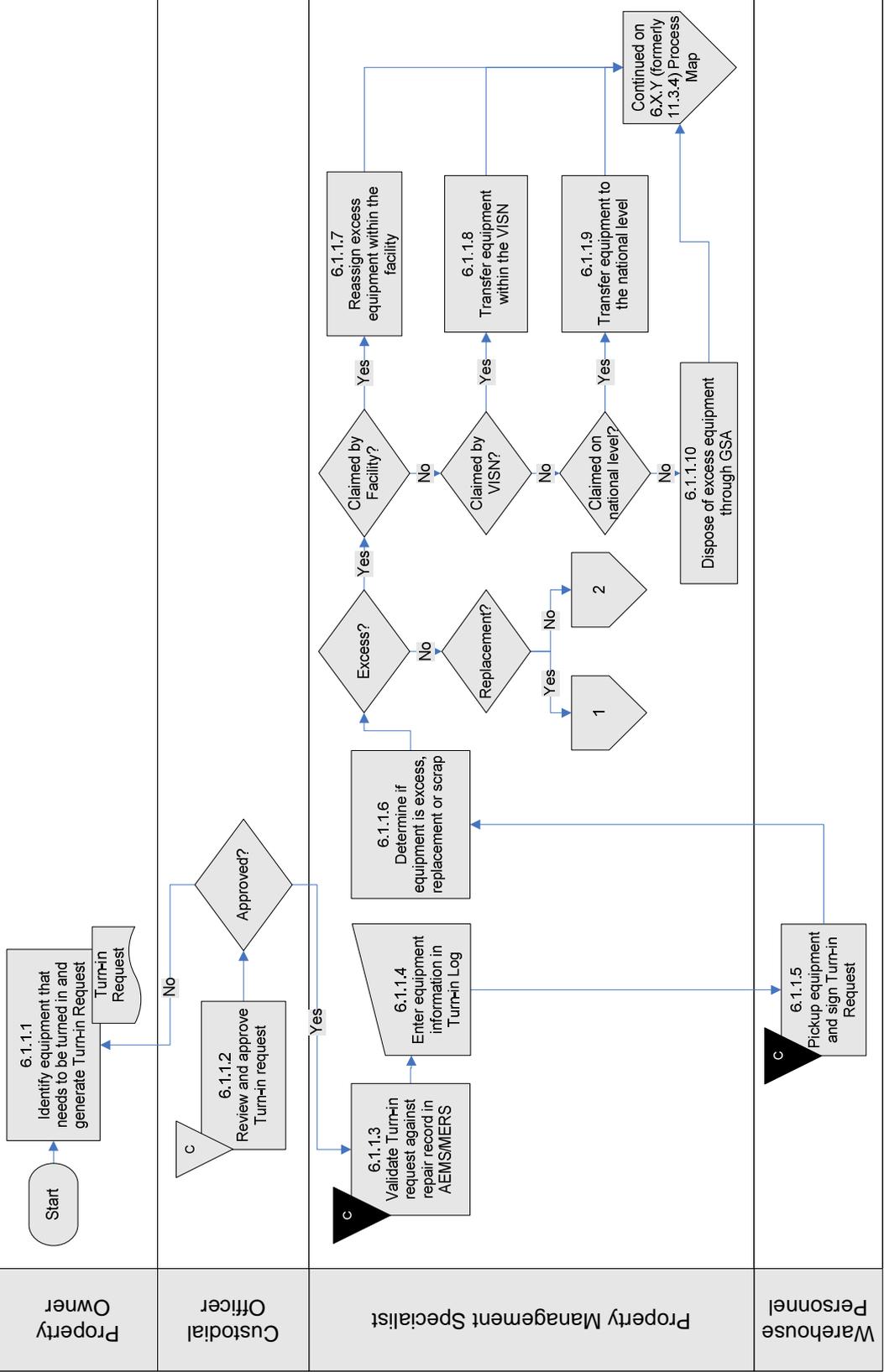
Process Narrative	
<b>6 Property, Plant and Equipment Management</b> <b>6.1 Personal Property</b> <b>6.1.1 Disposal</b>	
Process Verification	
Verified By: _____ Title: _____	Signature: _____ Date: _____
Signature confirms that this process and its controls have been accurately documented.	

Key Financial Process Activity	Process Owner	Control Matrix Reference
Background: The disposal sub-process encompasses activities used by VA to timely remove Fixed Assets from the Property, Plant and Equipment accounts, as well as from service. It encompasses the activities used to initiate, authorize, record, process and report on the retirement, sale, donation or transfer of fixed assets. VA directives and handbooks 7125 and 7127 establish Materiel Management policies and procedures for VA. The KFP for Fixed Asset Accounting is documented in X.Y.Z (formerly 11.3.4).		
<b><u>6.1.1.1 Identify equipment that needs to be turned in and generate Turn-in Request</u></b> The property owner (with the assistance of the Facility Engineer or the Biomedical Technician) identifies the specific equipment that needs to be turned in. The VA employee uses the VISTA system to generate an online Turn-in Request (VA form 2237). The VA employee enters the following data onto the Turn-in Request: serial number, make, model, year purchased, purchase order number, the reason for the turn-in (i.e. asset damaged and needs replacement; biomedical technician determines that the asset is not serviceable, Report of Survey for missing assets; retirement, etc). The employee submits the Turn-in Request to the Custodial Officer.	Property Owner	
<b><u>6.1.1.2 Review and approve Turn-in request</u></b> The designated Custodial Officer reviews the Turn-in Request for completeness and accuracy of the request. If the Custodial Officer approves the Turn-in Request, the Custodial Officer sends the approved Turn-in Request to Property Management Specialist. If the Custodial Officer rejects the request, the Custodial Officer sends the Turn-in Request back to the assigned VA employee.	Custodial Officer	C - 6.1.1.2

Key Financial Process Activity	Process Owner	Control Matrix Reference
<p><b><u>6.1.1.3 Validate Turn-in request against repair record in AEMS/MERS</u></b>  The Property Management Specialist reviews the Turn-in Request and compares the information on the Turn-in Request to the equipment preventive maintenance and repair record in AEMS/MERS to ensure the information is accurate and complete, and that the facility owns the item.</p>	Property Management Specialist	C - 6.1.1.3
<p><b><u>6.1.1.4 Enter equipment information in Turn-in Log</u></b>  The Property Management Specialist enters the equipment information in the Turn-in Log and notifies the Warehouse Personnel that the equipment is ready for pickup.</p>	Property Management Specialist	
<p><b><u>6.1.1.5 Pickup equipment and sign Turn-in Request</u></b>  The Warehouse Personnel picks up the equipment from the Custodial Officer, signs the Turn-in Request for receipt of equipment, gives a copy of the Turn-in Request to the Custodial Officer, brings the equipment to the holding area, and notifies the Property Management Specialist.</p>	Warehouse Personnel	C - 6.1.1.5
<p><b><u>6.1.1.6 Determine if equipment is excess, replacement, or scrap</u></b>  The Property Management Specialist inspects the equipment and determines the state of the equipment as either excess, replacement (trade-in) or scrap.</p>	Property Management Specialist	
<p><b><u>6.1.1.7 Reassign equipment within the facility</u></b>  If the equipment is designated as excess, the Property Management Specialist notifies other departments via email within that facility that the equipment is available. If the equipment is claimed within the facility it is reassigned to a new EIL in the AEMS/MERS system and will continue in service.</p>	Property Management Specialist	
<p><b><u>6.1.1.8 Transfer equipment within the VISN</u></b>  If the excess equipment is not claimed by the facility, the Property Management Specialist offers the equipment as excess within the Veterans Integrated Service Network {(VISN) (group of medical centers within a certain geographic area)}. If the equipment is claimed by a VISN it is taken off the books at that facility and transferred to the new VISN facility.</p>	Property Management Specialist	
<p><b><u>6.1.1.9 Transfer equipment to the national level</u></b>  If the excess equipment is not claimed by the VISN, the Property Management Specialists offers the equipment as excess at the national level; meaning the equipment is available agency wide. The Property Management Specialist notifies other VA facilities via email regarding the availability of the equipment and the offer remains open for 10 days. If another VA facility requests the equipment, it is transferred to the facility.</p>	Property Management Specialist	

Key Financial Process Activity	Process Owner	Control Matrix Reference
<p><b><u>6.1.1.10 Dispose of excess equipment through GSA</u></b>            If no VA facility requests the excess equipment within the allotted time frame, the Property Management Specialist reports the item to General Service Administration (GSA). GSA conducts an external screening on the GSA website to identify other Federal Agencies that may be interested in the equipment. GSA makes the equipment available for 21 days to other Federal Agencies. If another Federal agency is interested in the equipment, it is transferred to the agency without reimbursement and the transfer is coordinated by GSA. The Warehouse Personnel and the GSA official sign the 2237 acknowledging the transfer as well other as other appropriate GSA forms. If no other Federal agency is interested in the equipment, the Property Management Specialist instructs GSA to sell the equipment to external interested parties.</p>	Property Management Specialist	
<p><b><u>6.1.1.11 Transfer replacement equipment to GSA</u></b>            If the equipment is designated as replacement, the Property Management Specialist determines if the equipment is a trade-in as part of the replacement. If not the Property Management Specialist converts the Turn-in Request to a Request for Sale (Exchange Sale, GSA -126) and sends the approved Request for Sale to GSA. The Warehouse Personnel coordinates the removal and the transfer of the equipment to GSA.</p>	Property Management Specialist	
<p><b><u>6.1.1.12 Report equipment as scrap to GSA</u></b>            If the equipment is designated as scrap by the biomedical technician, the Property Management specialist reports to GSA using the GSA FED system to sell the equipment. If GSA cannot sell the equipment within 45 days, then GSA considers the equipment as scrap.</p>	Property Management Specialist	
<p><b><u>6.1.1.13 Dispose of scrap equipment</u></b>            The Property Management Specialist then disposes of the equipment at the local recycle center or by using an outside company to scrap the equipment. The Property Management Specialist logs the time to dispose of the equipment, prepares a bill for the scrap dealer and sends the bill to the Account Technician.</p>	Property Management Specialist	

6 Property, Plant and Equipment  
 6.1 Personal Property  
 6.1.1 Disposal



<p>6 Property, Plant and Equipment          6.1 Personal Property          6.1.1 Disposal</p>			<pre> graph TD     Start1{{1}} --&gt; Step1[6.1.1.11 Transfer replacement equipment to GSA]     Step1 --- ReqSale[Request for Sale]     Step1 --&gt; ContMap[Continued on 6.X.Y (formerly 11.3.4) Process Map]     Start2{{2}} --&gt; Step2[6.1.1.12 Report equipment as scrap to GSA]     Step2 --&gt; Step3[6.1.1.13 Dispose of scrap equipment]     Step3 --&gt; ContMap         </pre>	
	Property Owner	Custodial Officer	Property Management Specialist	Warehouse Personnel

## Appendix O – Risks and Control Objectives

During the Evaluating Phase, ICS will identify risks and control objectives for each in-scope KFP. These risks/objectives will then be put in the RCMs and matched with controls to determine if the KFP has any gaps. The table below lists suggested risks and control objectives for selected KFPs. It is not an all-inclusive list; ICS will modify this list based on information gathered during interviews with Process Owners.

Risk	Control Objectives
<b>Financial Reporting</b>	
Inaccurate changes to the chart of accounts result in financial reporting errors	<ul style="list-style-type: none"> <li>• The chart of accounts is complete and accurate</li> <li>• Ability to modify chart of accounts is restricted to appropriate users</li> </ul>
Incorrect postings result in inaccuracies in subsidiary ledgers and the general ledger.	<ul style="list-style-type: none"> <li>• Postings from sub-ledger to GL are made completely, accurately and in the proper period</li> <li>• Suspense, invalid or other rejected or improper automated posting are analyzed and resolved on a timely basis</li> <li>• Resolution of suspense postings is approved</li> <li>• Ability to make direct postings to the GL is restricted</li> </ul>
Budgetary and Proprietary accounts do not balance causing an inaccuracy in the Statement of Budgetary Resources	<ul style="list-style-type: none"> <li>• Budgetary and proprietary accounts balance</li> </ul>
Adjustments are inaccurate, incomplete, and not made in the correct accounting period	<ul style="list-style-type: none"> <li>• Period-end closing adjustments are recorded completely and accurately</li> <li>• Quarterly reporting procedures are consistent across all business units and departments</li> <li>• Quarterly adjustments are approved</li> <li>• All journal entries balance</li> <li>• Ability to record closing adjustments is restricted to appropriate users</li> </ul>
Financial statements do not accurately report the accounting activities	<ul style="list-style-type: none"> <li>• Account balances, details, and supporting notes are presented in the financial statements completely and accurately</li> <li>• Financial statement data is restricted to appropriate users prior to submission</li> <li>• Financial statements are submitted accurately and completely</li> </ul>
Financial statements may not comply with applicable laws or regulations.	<ul style="list-style-type: none"> <li>• Policies and procedures that drive the financial activities appropriately address applicable laws, regulations, and requirements</li> </ul>

<b>Human Capital Management</b>	
Inaccurate data may be entered into the personnel files which may result in inaccurate payroll distribution	<ul style="list-style-type: none"> <li>• Personnel actions are authorized</li> <li>• Input of personnel records are complete, accurate, and made in a timely manner</li> <li>• Personnel actions are processed completely and accurately</li> </ul>
Personnel actions may be noncompliant with applicable laws and regulations	<ul style="list-style-type: none"> <li>• Employee benefit transactions and reporting are in compliance with laws and regulations</li> </ul>
Hours worked may be inadvertently recorded	<ul style="list-style-type: none"> <li>• Only legitimate and approved time and attendance information can be entered into the system</li> </ul>
Financial records may be inaccurate due to inaccurate payroll information	<ul style="list-style-type: none"> <li>• Payroll payments are processed completely and accurately</li> <li>• Adjustments are approved by the appropriate personnel and made to the correct accounts and in the proper period</li> </ul>
<b>Budgetary Resources</b>	
Transactions are not executed in accordance with laws governing the use of budget authority resulting in non-compliance with laws and regulations (e.g., Anti-Deficiency Act, Appropriations Law)	<ul style="list-style-type: none"> <li>• The recorded appropriation amount agrees with the amount made available in the appropriation or other appropriate legislation, including restrictions on amount, purpose and timing</li> <li>• The recorded apportionments agree with the OMB apportionments and the total amount apportioned does not exceed the amount appropriated</li> <li>• The total amount allotted does not exceed the total amount apportioned</li> <li>• Budget transactions are authorized</li> <li>• Budget transaction are recorded completely and accurately</li> <li>• Fixed appropriation accounts are identified by fiscal year after the end of the period in which they are available for obligation until they are closed</li> <li>• Fixed appropriation accounts are closed on the 5th fiscal year after the end of the period that they are available for obligation</li> <li>• The ability to record and authorize budgetary transactions are limited</li> </ul>

## Procurement Management

<p>Unauthorized and/or inappropriate goods or services may be procured resulting in non-compliance with VA policy and inappropriate use of funds</p>	<ul style="list-style-type: none"> <li>• Procurement of goods and services are authorized validating the need of the goods or service</li> <li>• Purchase tracking logs and procurement of goods and supplies are complete, accurate and in compliance with purchasing policy</li> <li>• Purchase orders are entered into the system accurately and completely</li> <li>• Long outstanding open purchase orders are investigated and resolved</li> <li>• Procurement is bid fairly to all eligible vendors</li> <li>• Contracting Officers, Cardholders, and Approving Officials have appropriate training and knowledge to make informed procurement decisions</li> <li>• The Department is compliant with applicable laws and regulations</li> <li>• Ability to enter purchase orders is restricted to appropriate users</li> </ul>
<p>VA may be non-compliant with the Prompt Payment Act</p>	<ul style="list-style-type: none"> <li>• Invoices are paid in accordance with the Prompt Payment Act</li> </ul>
<p>Improper payments may be made</p>	<ul style="list-style-type: none"> <li>• Payment is only made for the goods and services ordered and received</li> <li>• Payment is made only for the agreed upon amount per the terms of the contract</li> <li>• Invoices are only paid once</li> <li>• Electronic funds transfers are controlled</li> </ul>
<p>Inaccurate or incomplete payments may be processed</p>	<ul style="list-style-type: none"> <li>• Invoices are input for processing completely and accurately</li> <li>• Disbursements are input for processing completely and accurately</li> <li>• Total disbursements input equal to amounts updated to cash accounts and accounts payable</li> </ul>
<p>Payments may be recorded incompletely and inaccurately</p>	<ul style="list-style-type: none"> <li>• Periodic updates for batch processing are complete and accurate</li> <li>• Invoices are only recorded once</li> <li>• Input to payables sub-ledgers are restricted to appropriate users</li> </ul>

## Property, Plant & Equipment Management

<p>Inappropriate use of Capital Funds may result in improper selection of Capital Projects and misuse of funds</p>	<ul style="list-style-type: none"> <li>• Specific guidelines are available and utilized when selecting capital projects</li> <li>• Construction Projects are authorized by appropriate personnel</li> <li>• Funding for new capital projects are verified before they are authorized</li> </ul>
<p>Acquired capital assets are not captured in the Department's financial and asset tracking records resulting in an understatement of assets.</p>	<ul style="list-style-type: none"> <li>• PP&amp;E Acquisitions are recorded accurately and timely</li> <li>• Software Work In Progress is captured and properly accounted for in the financial records.</li> </ul>
<p>Acquisition and management of Capital Lease Projects may be inappropriately handled resulting in the misuse of appropriated funding</p>	<ul style="list-style-type: none"> <li>• Capital Lease Project submissions are complete and contain the necessary information including technical specifications and market surveys to ensure prospective vendors are qualified.</li> <li>• All Capital Lease needs are addressed and captured in the original planning of the project.</li> <li>• Contractor work is reviewed to verify completeness before payments are granted.</li> <li>• Invoices are authorized by appropriate personnel before payments are distributed.</li> <li>• Technical Specifications and contract requirements were adhered to by the vendor.</li> </ul>
<p>Selected contractors may not have adequate ability and technical expertise to meet project demands resulting in cost overruns and loss of time</p>	<ul style="list-style-type: none"> <li>• Solicitation of prospective vendors meet FAR guidelines</li> <li>• Project submissions of prospective contractors are reviewed to ensure technical competence before a selection is made</li> <li>• Potential vendors are financially capable of finishing the project</li> </ul>
<p>Lack of Contractor oversight may lead to cost overruns and project delays</p>	<ul style="list-style-type: none"> <li>• Capital Projects are monitored by appropriate personnel to verify that tasks are being performed by contractors in a timely manner</li> </ul>
<p>Fraudulent submission and/or improper processing of contractor payments may lead to financial losses.</p>	<ul style="list-style-type: none"> <li>• Invoices are reviewed and approved by the COTR and CO before disbursements are issued</li> <li>• Funding is verified before invoice payments are submitted</li> </ul>
<p>Inadequate tracking of inventory of assets results in the inability to detect fraud, theft, and/or misappropriation of assets</p>	<ul style="list-style-type: none"> <li>• PP&amp;E is tracked periodically by appropriate personnel</li> <li>• Lost/Stolen property is reported periodically and reviewed by appropriate personnel</li> <li>• Lost/stolen laptops are reported to appropriate authorities</li> <li>• Transfers of assets to other federal agencies are reviewed and approved by appropriate personnel.</li> </ul>

Disposal of capital assets may not be accurately and completely input into the Agency's financial management system.	<ul style="list-style-type: none"> <li>• Disposal of PP&amp;E are accurately and completely input into the Agency's financial management system</li> <li>• Disposal of assets are recorded timely</li> <li>• Appropriate personnel approve of the disposal of assets.</li> </ul>
Depreciation data of capital assets are not captured resulting in misstated financial statements.	<ul style="list-style-type: none"> <li>• Accurate and complete depreciation data of PP&amp;E is input into the property system</li> <li>• All capital assets that are capitalized have a depreciation rate assigned to it.</li> </ul>
Data manipulation within the property system may occur, causing unreliable data.	<ul style="list-style-type: none"> <li>• Capital asset financial data within property system can be relied upon</li> </ul>
<b>Funds Management</b>	
Fund Balance with Treasury (FBwT) is over/under stated	<ul style="list-style-type: none"> <li>• FBwT is accurate and complete</li> </ul>
VA is non-compliant with Treasury's reporting requirements	<ul style="list-style-type: none"> <li>• SF-224 is submitted timely and accurately</li> <li>• Differences are investigated and resolved timely</li> <li>• Adjustments to prior month SF-224 is reviewed and approved</li> <li>• Cash reconciliations are performed accurately and completely</li> <li>• Cash reconciliations are performed on a timely basis</li> </ul>
Data is manipulated and external reporting is incorrect	<ul style="list-style-type: none"> <li>• External reports are submitted accurately</li> </ul>
Fraud and error is undetected	<ul style="list-style-type: none"> <li>• Adequate segregation of duties exist</li> </ul>
<b>Revenue Management</b>	
Financial records may inaccurately reflect the payment terms and conditions as agreed on the Reimbursable Agreements resulting in overstatement of unfilled customer orders	<ul style="list-style-type: none"> <li>• Reimbursable agreements (RAs) are accurately and completely entered into the financial system</li> </ul>
Financial records may inaccurately reflect the payment terms and conditions as agreed on the Reimbursable Agreements resulting in overstatement of unfilled customer orders	<ul style="list-style-type: none"> <li>• Adjustments to the RAs are made to the appropriate vendor, completely, and in the correct accounting period</li> </ul>

Data is manipulated, lost, or diverted resulting in inaccurate financial records	<ul style="list-style-type: none"> <li>• Access to the financial systems are restricted</li> <li>• Reimbursable agreements (RAs) are accurately and completely entered into the financial system</li> <li>• Changes to the system are restricted and monitored</li> <li>• Periodic batch processing is made completely and accurately</li> </ul>
Services are not provided but recorded resulting in over statement of accounts receivable	<ul style="list-style-type: none"> <li>• Billings are recorded accurately and completely</li> <li>• Accounts receivable is recorded accurately and completely</li> </ul>
Data may be manipulated, lost or diverted resulting in inaccurate financial records	<ul style="list-style-type: none"> <li>• Access to financial system is restricted</li> </ul>

## Template Appendices





### Appendix 3 - Location Selection Recommendations Template

Department of Veterans Affairs							
Location Selection Recommendations							
In-Scope Key Financial Process	Organization				Program(s)	Recommended Locations	Comments/ Rationale
	VHA	VBA	NCA	Dept			
List In-Scope KFP	Mark each applicable administration/organization with an X				Indicate all program(s) each KFP impacts (i.e., Medical Research, Insurance, etc.)	List Recommended Location 1 List Recommended Location 2 List Recommended Location 3...	Rationale for Location 1 Rationale for Location 2 Rationale for Location 3
Funds Management	X	X	X	X	Med care	VACO	Provides 28% coverage
					Med care	Dallas VISN	Known Issues at this location
					Med care	Chicago VA Regional Office	Program has undergone significant personnel changes

# Appendix 4 - SAS 70 Assessment Checklist

Department of Veterans Affairs A-123, Appendix A, Assessment			
SAS 70 Assessment Checklist			
Cross-sponsoring organization			
Report Title			
Report Date			
Question	Y/N	Notes	
Are controls in place to provide reasonable assurance that physical and logical access to VA mainframe and client-server resources, using computer terminals at client locations, is restricted to authorized individuals?			
Are controls in place to provide reasonable assurance that designated individuals, at client locations, comply with VA security policies, standards, and procedures?			
Are controls in place to provide reasonable assurance that audit reports of system use made available by VA are reviewed?			
Are controls in place to provide reasonable assurance that VA receives prompt written notification of changes for individuals who are authorized to add, change, and delete user access to VA application production regions?			
Are controls in place to provide reasonable assurance that client custom programming changes are appropriately documented, reviewed, tested, and implemented?			
Are controls in place to provide reasonable assurance that comprehensive user acceptance testing for any fixes and enhancements are performed and communicated to the responsible individual(s)?			
Are controls in place to provide reasonable assurance that the record-retention (e.g., off-line storage) requirements for financial statements is documented and communicated to the responsible individual(s)?			
Are controls in place to provide reasonable assurance that on-line retention and archiving of VA data has been established and communicated to the responsible individual(s)?			
Are controls in place to provide reasonable assurance that Computer Incident Response procedures have been developed in coordination with the responsible individual(s)?			
Are controls in place to provide reasonable assurance that the production cycles are properly maintained and changes to them are timely communicated to the responsible individual(s)?			
Are controls in place to provide reasonable assurance that obligations are not incurred in excess of the available budgetary amounts?			
Are controls in place to provide reasonable assurance that appropriate users review output reports for completeness and accuracy?			
Are controls in place to provide reasonable assurance that the transactions processed are complete, accurate, and appropriately authorized and approved?			
Are controls in place to provide reasonable assurance that erroneous data is corrected and resubmitted?			
Are controls in place to provide reasonable assurance that incompatible job functions surrounding the processing of VA transactions are identified and pertinent policies and procedures are enforced to segregate these job functions?			
<b>Conclusion:</b>			
Completed by: _____			
Date: _____			
Reviewed by: _____			
Date: _____			

- Are controls in place to provide reasonable assurance that physical and logical access to VA mainframe and client-server resources, using computer terminals at client locations, is restricted to authorized individuals?
- Are controls in place to provide reasonable assurance that designated individuals, at client locations, comply with VA security policies, standards, and procedures?
- Are controls in place to provide reasonable assurance that audit reports of system use made available by VA are reviewed?
- Are controls in place to provide reasonable assurance that VA receives prompt written notification of changes for individuals who are authorized to add, change, and delete user access to VA application production regions?
- Are controls in place to provide reasonable assurance that client custom programming changes are appropriately documented, reviewed, tested, and implemented?
- Are controls in place to provide reasonable assurance that comprehensive user acceptance testing for any fixes and enhancements are performed and communicated to the responsible individual(s)?
- Are controls in place to provide reasonable assurance that the record-retention (e.g., off-line storage) requirements for financial statements is documented and communicated to the responsible individual(s)?
- Are controls in place to provide reasonable assurance that on-line retention and archiving of VA data has been established and communicated to the responsible individual(s)?
- Are controls in place to provide reasonable assurance that Computer Incident Response procedures have been developed in coordination with the responsible individual(s)?
- Are controls in place to provide reasonable assurance that the production cycles are properly maintained and changes to them are timely communicated to the responsible individual(s)?
- Are controls in place to provide reasonable assurance that obligations are not incurred in excess of the available budgetary amounts?
- Are controls in place to provide reasonable assurance that appropriate users review output reports for completeness and accuracy?
- Are controls in place to provide reasonable assurance that the transactions processed are complete, accurate, and appropriately authorized and approved?
- Are controls in place to provide reasonable assurance that erroneous data is corrected and resubmitted?
- Are controls in place to provide reasonable assurance that incompatible job functions surrounding the processing of VA transactions are identified and pertinent policies and procedures are enforced to segregate these job functions?

## Appendix 5 - GCC Template

Department of Veterans Affairs						
General Computer Controls Assessment						
Environment (Host Site):						
VACO						
FISCAM Reference	Element (Control Objective)	Description and Frequency of Control Activity	Control Techniques	P or D (1)	A or M (2)	Control Effective (Y/N)?
Five domains within FISCAM include: Security Management (SM), FISCAM Section 3.1; Access Control (AC), FISCAM Section 3.2; Configuration Management (CM), FISCAM Section 3.3; Segregation of Duties (SD), FISCAM Section 3.4; Contingency Planning (CP), FISCAM Section 3.5.	Describe the purpose of the control activity	Explain the actual activity being performed and how often the activity is performed, e.g., daily, weekly, monthly, annually	Describe the requirements associated with an effective control for this control activity	Indicate the control approach as either preventive or detective	Identify the control activity as automated (performed using a system or application) or manual (requires human intervention or judgment)	Indicate the control design as effective (Y) or not effective (N)
<i>AC-2.1</i>	<i>Resource owners have identified authorized users and their access is authorized.</i>	<i>Access authorizations are (a) documented on standard forms and maintained on file, and (b) evidence of management approval is retained. Daily activity.</i>	<i>1. Appropriate business owners periodically review current access levels and determine whether users and their associated access rights remain appropriate. Documentation of management review and corrective actions taken are retained. 2. Inactive users' accounts are monitored and removed after a predetermined period of inactivity (i.e., 120 days)</i>	<i>P</i>	<i>M</i>	<i>Y</i>

# Appendix 6 - Documentation Quality Control Checklist

Department of Veterans Affairs A-123, Appendix A, Assessment						
<b>Documentation Quality Review Checklist</b>						
Document Name						
Originator(s)						
Deliverable Due Date						
Date Provided						
Reviewers: Place check marks in each of the boxes to indicate review of the attribute. Initial and date the bottom of the column as evidence of your review.						
	Process Owner	Process Owner Liaison	ICS	Other:	Other:	
<b>Narrative</b>						
Describes the complete process as defined by VA						
Is formatted in accordance with template						
Contains clear descriptions of activities and controls						
Specifies Process Owners for each step						
Contains clear activity/step headings (Verb+object)						
Addresses all various scenarios (i.e. - What if the supervisor does <i>not</i> approve the JV?)						
Contains correct spelling, grammar, formatting						
<b>Flowchart</b>						
Displays consistent step names and numbers with narrative and RCM						
Uses correct shapes for each step						
Displays start and end points						
Includes yes/no options for all decision boxes						
Contains correct spelling, grammar, formatting						
<b>Risk Control Matrix</b>						
Is consistent with narrative and flowchart						
Contains all required fields						
Includes correct identification of objectives and risks						
Identifies key controls						
Identifies application name for all automated controls						
Contains correct spelling, grammar, formatting						
	Initials					
	Date					

## Appendix 7 - KFP-Level Test Plan Template

Department of Veterans Affairs											
Test Plan											
Key Financial Process:											
Reference Number	Location	Risk	Control Objective	Actual Control Activity	Process Owner	Frequency	Sample Size	Test Steps	Workpaper Reference Number	Test Result	Summary of Results
C - 6.1.1.2	VACO	Unauthorized disposal transactions	Disposals of fixed assets and removals from service are properly authorized	The designated Custodial Officer reviews the Turn-in Request for completeness and accuracy of the request. If the Custodial Officer approves the Turn-in Request, the Custodial Officer sends the approved Turn-in Request to Property Management Specialist. I	Custodial Officer	Continuous	45	A. Obtain a list of all equipment disposals between 10/1/07 to 5/31/08. B. For the sample selected obtain Turn-In Request (Form 2237) and print out the equipment preventative maintenance repair record from AEMS/MERS C. Verify that the Turn-In Request is approved (signed and dated) by the Custodial Officer D. Compare info on Turn-In Request to AEMS/MERS to verify accuracy.	X.Y.Z	Failed	Three of 45 Turn-In Requests were not signed by the Custodial Officer.
C - 6.1.1.3	VACO	Disposal of personal property is unauthorized or inaccurately input for processing resulting in an error on the financial statements	Disposals of fixed assets and removals from service are properly authorized	The Property Management Specialist reviews the Turn-in Request and compares the information on the Turn-in Request to the equipment preventive maintenance and repair record in AEMS/MERS to ensure the information is accurate and complete, and that the faci	Property Management Specialist	Continuous	45	A. Obtain a list of all equipment disposals between 10/1/07 to 5/31/08. B. For the sample selected obtain Turn-In Request (Form 2237) and print out the equipment preventative maintenance repair record from AEMS/MERS (signed and dated) C. Verify that the Turn-In Request is approved (signed and dated) by the Warehouse Personnel D. Compare info on Turn-In Request to AEMS/MERS to verify accuracy.	X.Y.Z	Passed	This control appears to be designed effectively and operating as intended.

## Appendix 8 - Evidence Request List Template

Department of Veterans Affairs									
Evidence Request List									
Date									
Key Financial Process									
Sub-Process									
As part of the A-123, Appendix A assessment, the Internal Control Service is beginning the testing phase of the assessment. We have identified below evidence that will be needed to allow us to test the operating effectiveness of controls identified during documentation. Upon compilation of the evidence, please group all appropriate Item Numbers together (in folders, binder clips, etc). Thank you for your continued help with our assessment.									
<u>Note:</u> Please be prepared with copies of all requested evidence. The assessment team will not be able to return original copies back to process owners.									
<u>Note:</u> If you are not the responsible party for the specific item, please forward this list onto the appropriate personnel/department.									
Sample Item Number	Location	Key Financial Process	Sub-process	Control Reference Number	Process Owner	Document Description	Evidence Requested	Date Due	Note
A unique ID number beginning with 1	Name of the site	Relevant key financial process	Relevant sub-process	Control reference number from the RCM	Name and Title of the Process Owner	Requested test sample/documentation including a description of all supporting documentation	Identifying information (dates, invoice numbers, etc) for selected sample	Date due to testing team	
1	VACO	Funds Management	Accounts Payable	C - 1.3.5.6	Joe Smith, Accountant	Approved invoices and all supporting documentation	Invoice numbers: 2533563 6786366 5678260	05/15/08	

# Appendix 9 - Test Sheet

<b>Department of Veterans Affairs</b>								
<b>Test Sheet Example</b>								
<b>Key Financial Process</b>								
<b>Reference Number</b>		C - 6.1.1.2						
<b>Actual Control Activity</b>		The designated Custodial Officer reviews the Turn-in Request for completeness and accuracy of the request. If the Custodial Officer approves the Turn-in Request, the Custodial Officer sends the approved Turn-in Request to Property Management Specialist. If the Custodial Officer rejects the request, the Custodial Officer sends the Turn-in Request back to the assigned VA employee.						
<b>Location</b>		Palo Alto, CA						
<b>Control Frequency</b>		Continuous						
<b>Sampling Unit</b>		Turn-In Request Forms 10/1/07 and 7/31/08						
<b>Sample Size</b>		45						
<b>Test Results</b>		Failed						
<b>Number of Deviations</b>		3						
<b>Exception(s) - if any</b>		Three of 45 Turn-In Requests were not signed by the Custodial Officer.						
<b>Cause of Exception(s) - if known</b>								
<b>Sampling Procedure Performed</b>		Explanation of how the sample was selected (i.e. Randomly selected a sample of 3 monthly Property Reconciliations)						
<b>Control Attribute Description:</b>		<p>A. Obtain a list of all equipment disposals between 10/1/07 to 5/31/08.</p> <p>B. For the sample selected obtain Turn-In Request (Form 2237) and print out</p> <p>C. Verify that the Turn-In Request is approved (signed and dated) by the Custodial Officer</p> <p>D. Compare info on Turn-In Request to AEMS/MERS to verify accuracy.</p>						
<b>Sample Number</b>	<b>Sample Identification</b>		<b>Control Attribute A</b>	<b>Control Attribute B</b>	<b>Control Attribute C</b>	<b>Control Attribute D</b>	<b>Work Paper Reference</b>	
	<b>Title</b>	<b>Date</b>						
1	HP Ultrasound	4/31/06	X	X	#1	X	X.Y.Z	
2								
3								
<b>Testing Tickmark Explanation:</b>		<p>X - Attribute Present; No Exception Noted</p> <p># - Attribute Not Present; Exception Noted</p>						
<b>Notes:</b>		<p>1. Turn-In Request was not signed by the Custodial Officer.</p> <p>2.</p> <p>3.</p>						
<b>Testing:</b>								
Performed By:								
Completed On:								
Reviewed By:								
Reviewed On:								

# Appendix 10 - Exception Log Template

Department of Veterans Affairs													
Exception Log													
Date													
ID Number	Key Financial Process	Sub-Process	Location	Key Control Number	Potential Risk	Control Activity	Frequency	Exception/Finding	Cause (if known)	Suggested Corrective Action	Management Response	Exception/Finding Type (Design Deficiency, Design Gap, Operating Deficiency)	Notes
Unique identifier	Relevant process	Relevant Sub-process	Location	Key control number from the RCM	Risk for the key control, as stated in the RCM	Control Activity, as stated in the RCM	As stated in the RCM	If a design gap, copy from the RCM under "design gap." If an operating deficiency, copy from the Test Plan under "summary test results."		What should be done to solve the problem.		Select appropriate finding type	
1	Property Management	Personal Property	VACO	C - 8.4.1.1.22	PP&E acquisitions were not authorized resulting in misappropriation of Capital funds.	The Branch Head reviewed the JV and reconciled the JV with the supporting documentation. If any discrepancies existed, he/she would return the JV to the Property Accountant to resolve the error. If no discrepancies exist, he/she would sign and date the JV and return to the Property Accountant. He/she printed and attached screenshots of the PO information (acquisition document control number) and costs.	Continuous	Four exceptions noted. One exception was due to posting prior to JV approval. One exception due to lack of JV approval date. One exception due to lack of supporting documentation. One exception due to inability to reconcile with supporting documentation.	Cause unknown.	Sign and date JV's prior to posting.	Agreed with corrective action	Operating Deficiency	

# Appendix 11 - Testing Quality Review Checklist

Department of Veterans Affairs A-123, Appendix A, Assessment			
<b>Testing Quality Review Checklist</b>			
Originator(s)			
Location			
Key Financial Process and Sub-Process			
Date Provided			
Reviewers: Place check marks in each of the boxes to indicate review of the attribute. Initial and date the bottom of the column as evidence of your review.			
	Associate Director	ICS Director	Other
<b>KFP-level test plan</b>			
Control reference number, control objective, risk, risk level, control activity, Process Owner and frequency correspond to data on RCM			
Sample size is correct based on frequency			
Test steps achieve test objective			
Workpaper reference number is correct			
Test result and summary matches data in test sheet			
<b>Test Sheet</b>			
Reference number matches KFP-level test plan and RCM			
Control activity matches KFP-level test plan and RCM			
Control frequency matches KFP-level test plan and RCM			
Sample size is correct based on frequency			
Test Results matches Exception			
Number of deviations matches test detail			
Exception description is clear and matches test results			
Test attributes achieve test objective and match KFP-level test plan			
All attributes are completed for each sample			
All exceptions are clearly documented			
Supporting documentation is provided for all exceptions			
Initials			
Date			

Page 1

## Appendix 12 - Finding Outline Worksheet

Department of Veterans Affairs  
FY20XX Finding Outline Worksheet

---

Identification Information	
Finding Reference:	
Source of Finding:	
Fiscal Year:	
Key Financial Process:	
Control Objective:	
Control Activity:	
Location(s):	
Related Internal Control Numbers: (optional)	

	Comments/ W/P Reference
Condition	
Criteria	
Cause	
Effect	
Recommendation	

Severity Rating	
-----------------	--



Review		
Title	Signature	Date
ICS Supervisor		
ICS Director		
SAT (SD and MW only)		

## Appendix 13 - Corrective Action Plan Template

This template will be inserted as part of Task K.