



Appendices



Appendix A – CFOC Guide Crosswalk to Procedures Manual

CFOC Implementation Guide		VA Implementation Guide	
Activity	Page Number	Phase	Activity
Step 1: Planning	6-23		
• 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.9: Integrate and coordinate with other control-related activities
• Determine Scope of Significant Financial Reports	15	I. Planning	I.2: Determine scope of significant reports
• Determine Materiality	16	I. Planning	I.3: Determine Materiality
• Determine Key Processes Supporting Material Line Items	18	I. Planning	I.4: Determine key processes supporting material line items
• Financial Reporting Assertions	19	I. Planning	I.5: Identify financial reporting assertions
• Risk Assessment	19	I. Planning	I.6: Conduct 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.11: Plan for an updated assurance statement in the Performance and Accountability Report (PAR)
Step 2: Evaluating Internal Control at the Entity Level	24-26	II. Evaluating	II.1: Evaluate Internal Controls at the Entity Level
Step 3: Evaluating Internal Control at the Process Level	27-34		
• Understanding Key Financial Reporting Processes	27	II. Evaluating	II.2: Evaluate internal control at the process level
• 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

CFOC Implementation Guide		VA Implementation Guide	
Activity	Page Number	Phase	Activity
• 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: Implement a risk-based approach
• Testing Key Controls	36	III. Testing	III.2: Test key controls
Step 5: Concluding, Reporting, and Correcting Deficiencies and Weaknesses	38-45		
• Concluding on Effectiveness	38	IV. Concluding, Reporting, and Correcting	IV.1: Conclude on control effectiveness
• Reporting	39	IV. Concluding, Reporting, and Correcting	IV.2: Report control weaknesses
• Correcting Deficiencies or Weaknesses	41	IV. Concluding, Reporting, and Correcting	IV.3: Correcting deficiencies and weaknesses

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
NoF	Notification of Findings
NoV	Notification of Validation
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 following¹:

- 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 ²

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 categories³:

- 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

¹ PCAOB AS 2.

² OMB Circular A-123, page 22.

³ 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 process. 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
Completeness	<ul style="list-style-type: none"> • All recorded transactions are accepted by the system (only once) • Duplicate postings are rejected by the system • Any transactions that are rejected are addressed and fixed
Accuracy	<ul style="list-style-type: none"> • Key data elements for transactions (including standing data) that are recorded and input to the computer are correct • Changes in standing data are accurately input
Validity	<ul style="list-style-type: none"> • Transactions, including the alteration of standing data, are authorized • Transactions, including standing data files, are not fictitious and they relate to the organization
Restricted Access	<ul style="list-style-type: none"> • Unauthorized amendments of data are barred from the system • The confidentiality of data is ensured • Entity assets are physically protected from theft and misuse • The segregation of duties is ensured

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 process/sub-process 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 ⁴

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

⁴ 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.⁵

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.⁶

Internal Control Standards ⁷

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

⁵ Adapted from PCAOB AS 2.

⁶ OMB Circular, A-123, Appendix A, page 22.

⁷ 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 Assertions⁸

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.

Materiality⁹

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 Control¹⁰

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.

⁸ OMB Circular, A-123, Appendix A, page 29.

⁹ OMB Circular, A-123, Appendix A, page 23.

¹⁰ GAO/PCIE Financial Audit Manual, Sec. 500.38.

Potential Misstatement

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

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.

Process or Cycle

A process or cycle 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).

Process/Cycle Risk Assessment

As part of the scoping exercises, management should identify the primary processes/cycles. In order to evaluate the extent of documentation and testing over each process/cycle, management should perform a risk assessment of each process/cycle. This risk assessment involves the identification of relevant risks to achieving the financial reporting objectives related to each account affected by each process/cycle. Higher risk processes/cycles 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 ¹¹

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 ¹²

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

¹¹ GAO/PCIE Financial Audit Manual, Sec. 500.49.

¹² OMB Circular, A-123, Appendix A, page 24.

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

A sub-process or sub-cycle 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 process 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 significant process, 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”¹³. 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 remediated 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 control¹⁴. 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 environment¹⁵.

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.¹⁶ Abuse is distinct from fraud. When abuse occurs, no law or regulation is violated. Rather, the

¹³ [Standards for Internal Control in the Federal Government, GAO Report # GAO/AIMD-00-21.3.1 \(11/99\)](#).

¹⁴ *Ibid.*

¹⁵ PCAOB AS 2.

¹⁶ *Ibid.*

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.¹⁷

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

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.¹⁸

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.¹⁹

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.

¹⁷ Adopted from the GAO Government Auditing Standards commonly referred to as the "Yellow-Book", paragraph 4.19.

¹⁸ Adopted from the *Standards for Internal Control in the Federal Government*, GAO Report # GAO/AIMD-00-21.3.1 (11/99),

¹⁹ Ibid

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 accountability for stewardship of government resources and achieving effective results.²⁰ 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	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. 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.

²⁰ 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.²¹

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.²²

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.

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:

²¹ Adopted from the *Standards for Internal Control in the Federal Government*, GAO Report # GAO/AIMD-00-21.3.1 (11/99),

²² Ibid

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

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

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

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 process/sub-process 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 process. The purpose of the flowcharts is to identify control points in the process 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 process. Specific process activity, decision point or reference is described within the shape. The movement of a process model travels from left to right in a timeline fashion.

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

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

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

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

Flowchart Legend

	Terminator: Marks the beginning or end of a process. Usually contains the word "start" or "end".
	On-page connector: Indicates that the flow continues on the same page where a matching symbol containing the same number has been placed
	Off-page connector: Indicates that the process continues on another (different) page where a matching symbol containing the same number has been placed
	General process: Denotes a general task that should be done. It can represent a single step or an entire sub-process within a larger process.
	Manual process: Denotes a task that is performed using manual means
	Document: Denotes a printed document or report
	Prepare: Typically denotes a task that requires a user to complete a form or document or assemble a package
	Decision: 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.
	Input/Output: Represents material or information entering or leaving the system, such as a customer order (input) or a product (output)

	Manual Input: Denotes a step requiring manual entry of data (such as keying in values on a spreadsheet)
	Stored Data: Indicates a general step where data gets stored
	Direct Data: Another term for "random access" or hard disk storage (as opposed to "sequential data" which is stored in a structure)
	Sequential Data: Denotes data stored on tape
	Display: Indicates a step that displays data to the end user
	Flow-Line: Lines that indicate the sequence of steps and the direction of the flow
	Transfer of Control: Denotes that the control of the process has been transferred from one Process Owner or organization to another
	Control: Denotes that the step in the process contains a non-key internal control
	Key Control: Denotes that the step in the process contains a key internal control
	Annotation: 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
SMC	Involved	I. Planning	1, 11
		IV. Concluding, Reporting, and Correcting	4
CFO	Involved	I. Planning	1
SAT	Responsible	IV. Concluding, Reporting, and Correcting	1, 2.1
	Involved	I. Planning	1-11
		II. Evaluating	1.4
		III. Testing	1
		IV. Concluding, Reporting, and Correcting	2.2, 4.1, 4.2
OBO/ICS	Responsible	I. Planning	1-11
		II. Evaluating	1-3
		III. Testing	1-2
		IV. Concluding, Reporting, and Correcting	2.2, 4
		IV. Concluding, Reporting, and Correcting	1, 2.1, 3
VA personnel	Involved	II. Evaluating	2.1.1-2.1.3, 2.4, 3
		IV. Concluding, Reporting, and Correcting	4
PO Liaisons	Responsible	II. Evaluating	2.1.5
	Involved	II. Evaluating	2.1.1-2.1.3
		IV. Concluding, Reporting, and Correcting	4
Process Owners	Responsible	II. Evaluating	2.1.5-2.1.6
		IV. Concluding, Reporting, and Correcting	3
	Involved	II. Evaluating	2.1.1-2.1.4, 2.2-2.4, 3
		III. Testing	2.4

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: ²³

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.

²³ 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.²⁴

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.²⁵

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.

²⁴ Definition adapted from the GAO/PCIE [Financial Audit Manual](#), section 350.

²⁵ Ibid.

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 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.

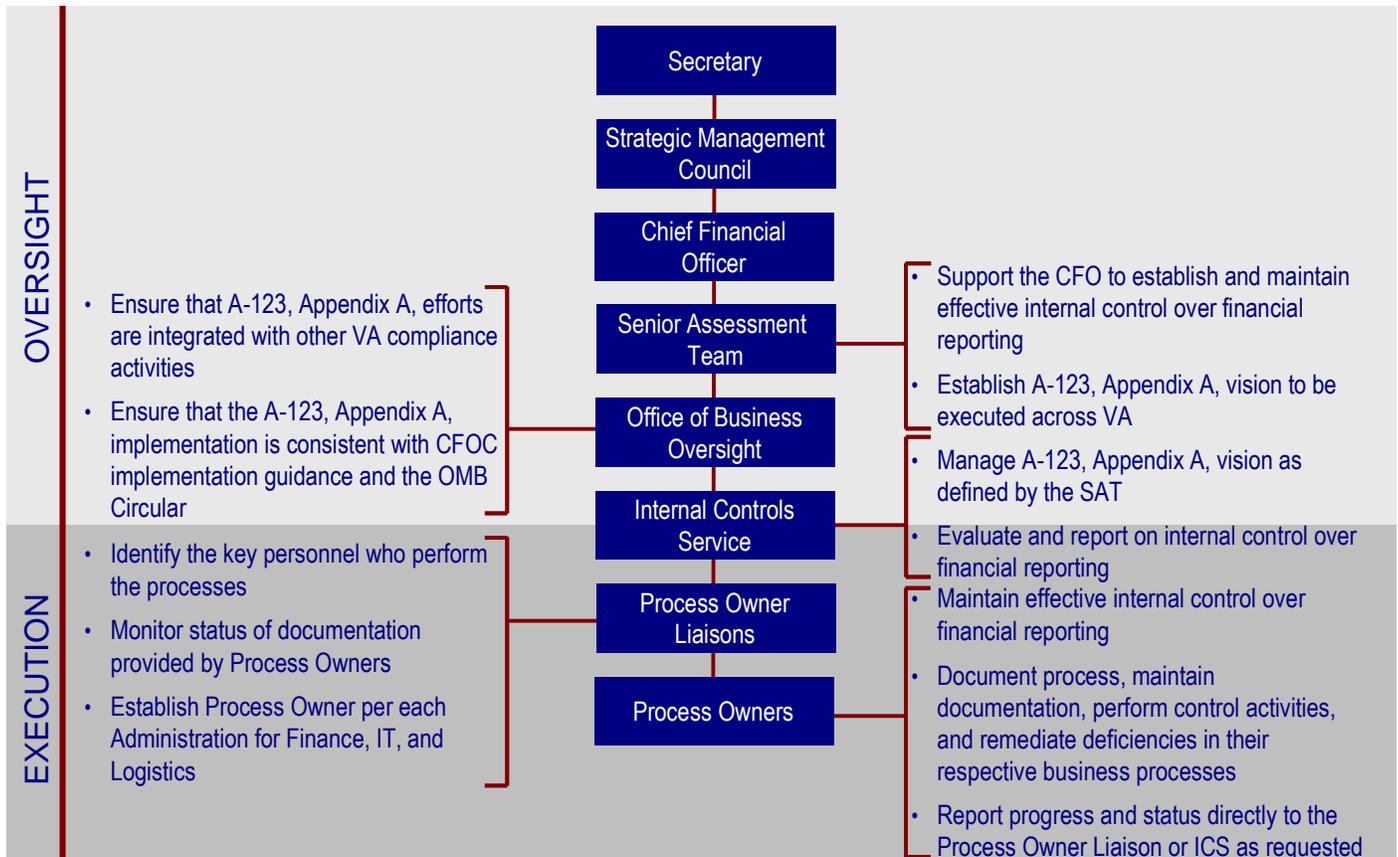
Re-performance

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

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

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.²⁶

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.

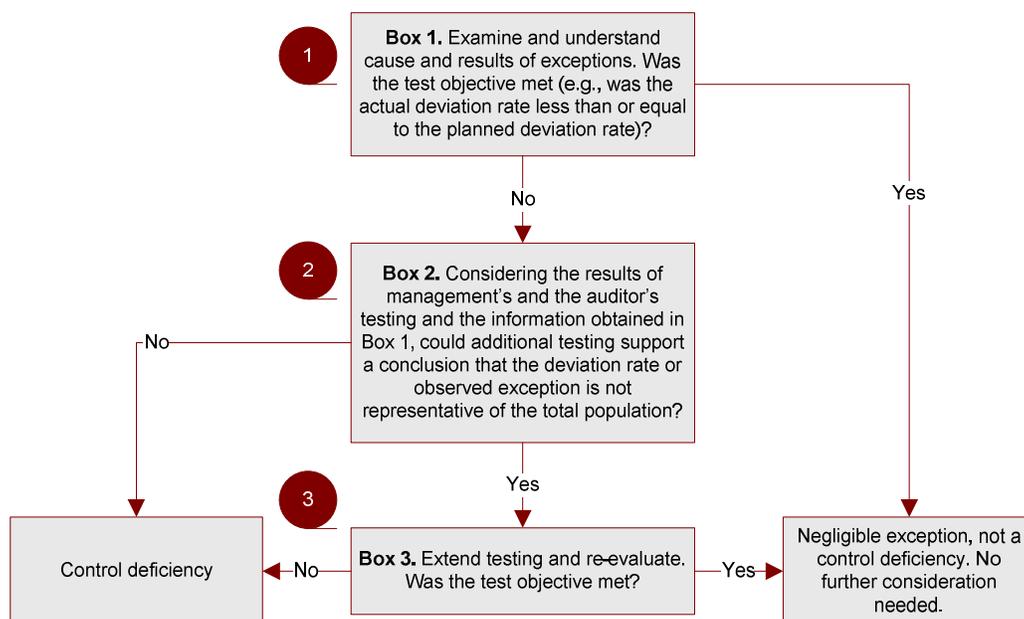


Chart 1

²⁶ 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.

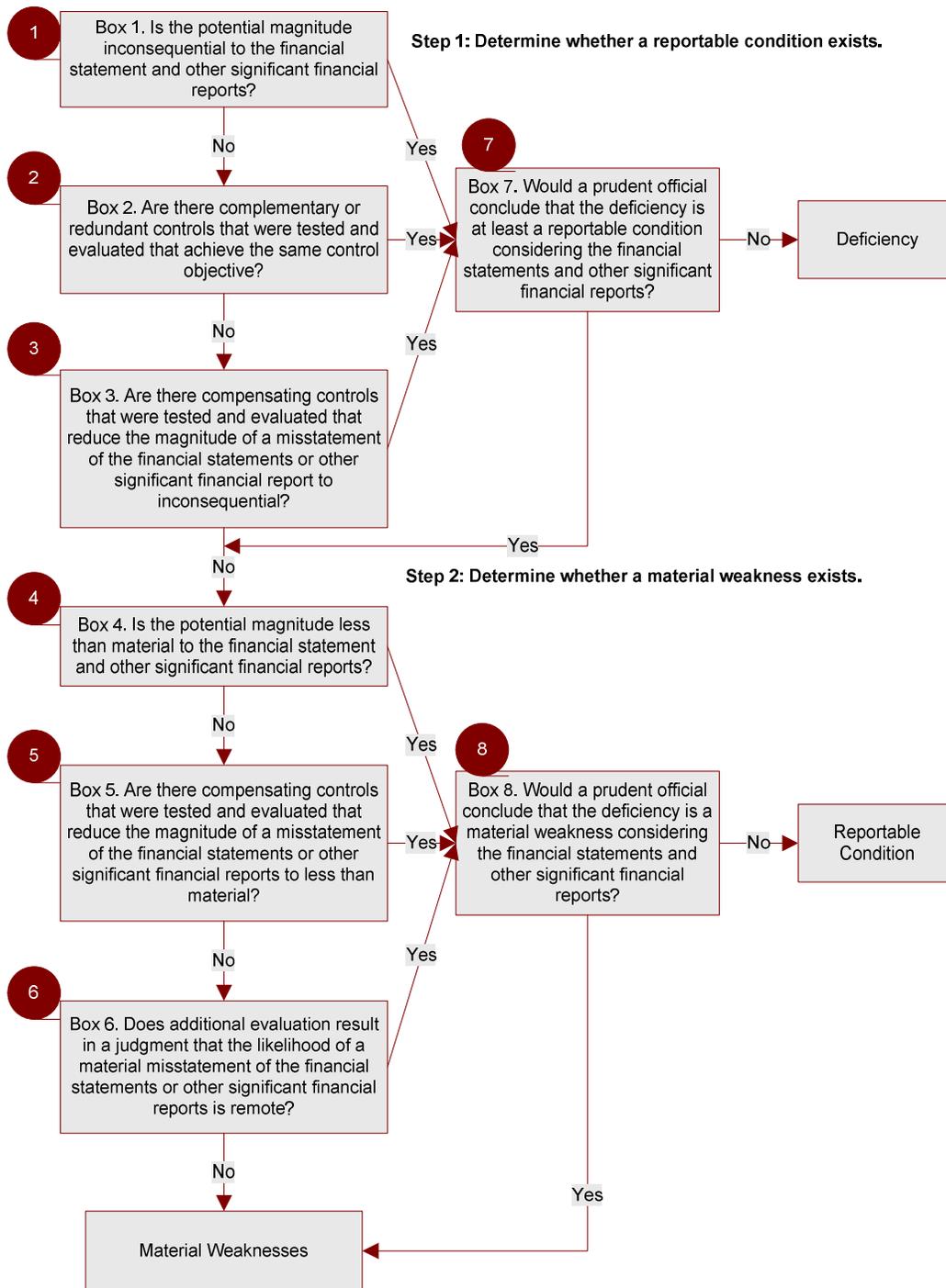


Chart 2

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.²⁷ 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

²⁷ 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.

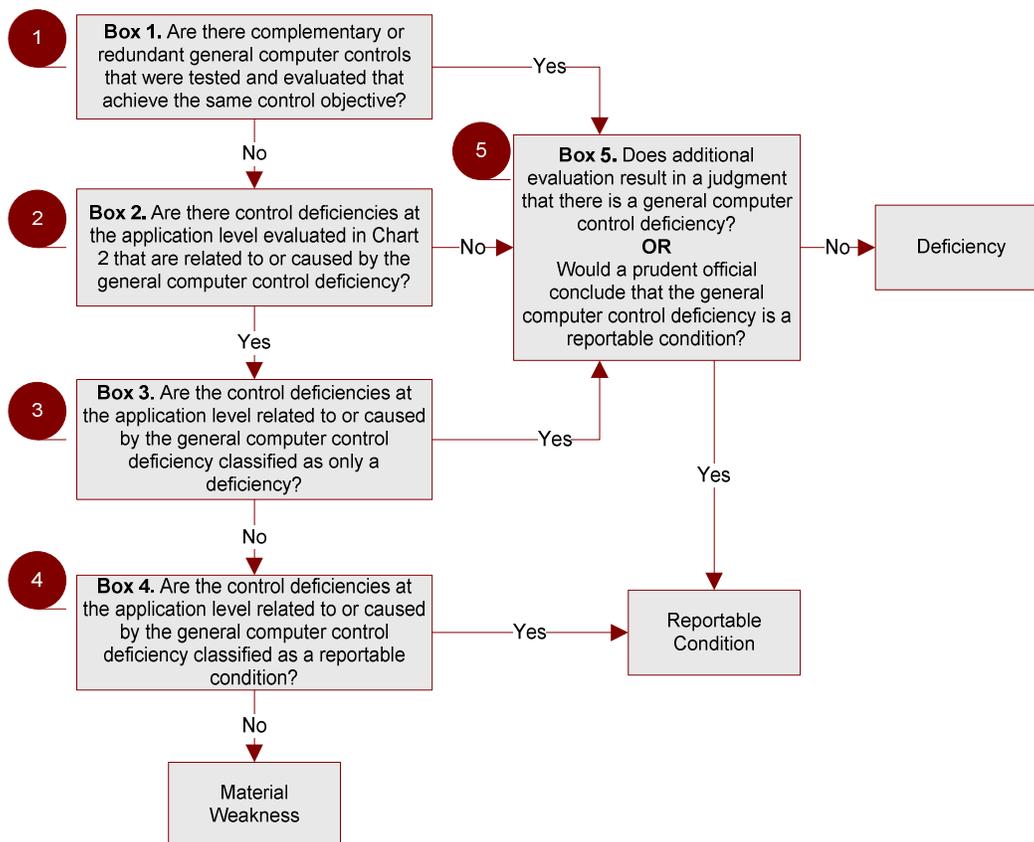


Chart 3

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 officials²⁸ 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.

²⁸ 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.

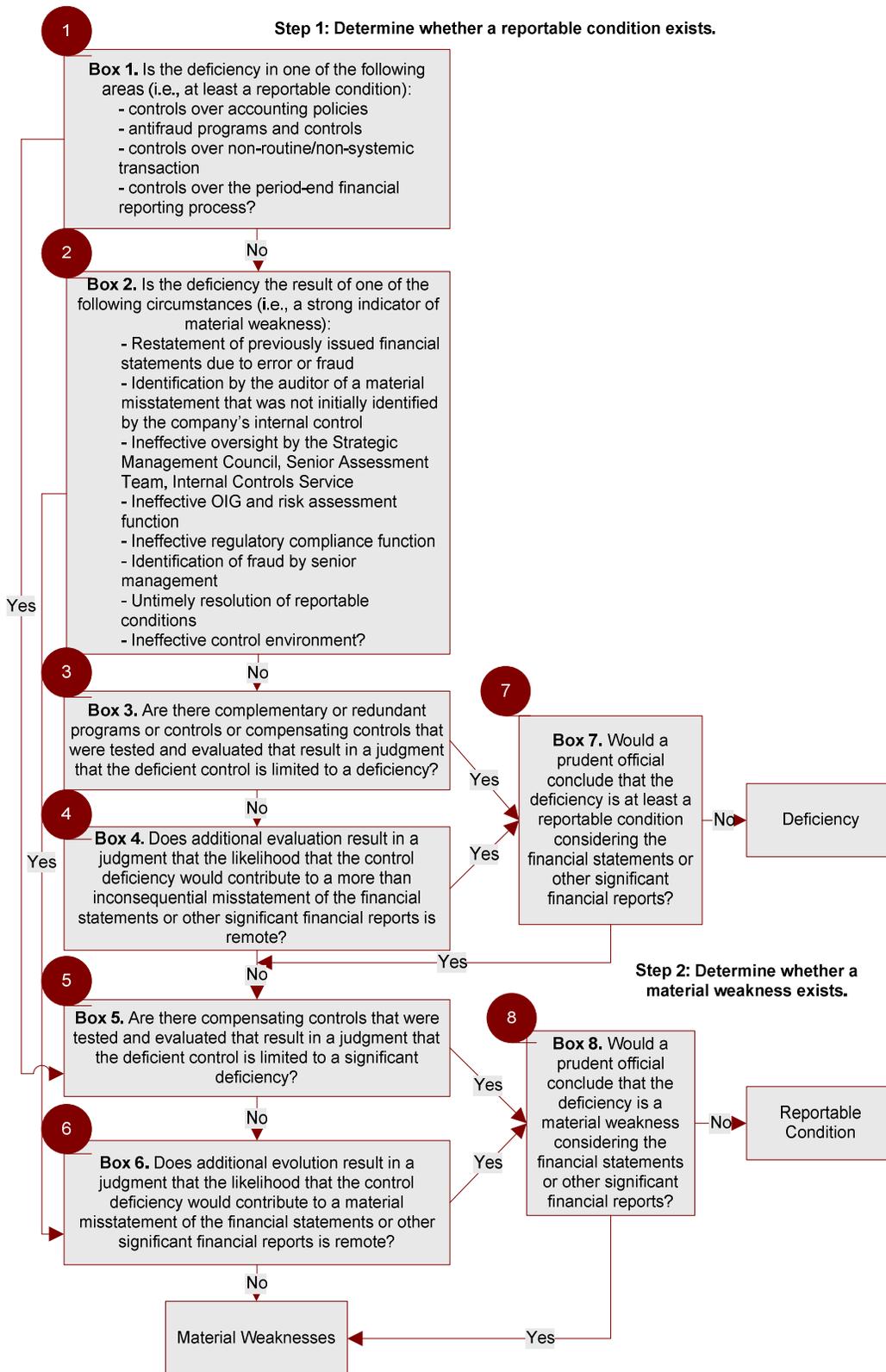


Chart 4

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.²⁹

- 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 weakness³⁰:

- 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:

²⁹ Based on guidance provided in AS 2.139.

³⁰ 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 is³¹:

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

³¹ 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.³² 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.

³² AS 2.137.

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.

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
Documentation Quality Review checklist	<ul style="list-style-type: none"> Helps ICS check for accuracy and consistency across outputs (narratives, flowcharts and RCMs) 	<ul style="list-style-type: none"> Process Owners Process Owner Liaisons ICS
Documentation template	<ul style="list-style-type: none"> Breaks down processes into individual, granular control activities Includes narratives, significant accounts, policies and procedures, interfaces with other processes, significant documents, sources of information and flowcharts 	<ul style="list-style-type: none"> ICS Process Owners
Evidence Request List template	<ul style="list-style-type: none"> Lists the evidence that Process Owners must prepare for the testing of internal controls Includes forms and reports referenced in the documentation and process-level test plans 	<ul style="list-style-type: none"> ICS Process Owners
Flowchart template	<ul style="list-style-type: none"> Depicts the sequential flow of a process through events as objects, using a number of shapes Ties back to the process narratives through "node numbers" that are placed on each object, directly corresponding to each control activity number in the narrative 	<ul style="list-style-type: none"> ICS Process Owners
General Computer Controls template	<ul style="list-style-type: none"> Facilitates documentation of General Computer Controls (GCCs), which are categorized by FISCAM area 	<ul style="list-style-type: none"> ICS
Financial Statement Assertions template	<ul style="list-style-type: none"> Documents the financial statement assertions for each line item 	<ul style="list-style-type: none"> ICS
Implementation Plan template	<ul style="list-style-type: none"> Helps management document its assessment approach and communicate to stakeholders both within and outside of VA 	<ul style="list-style-type: none"> ICS SAT
Issue Log template	<ul style="list-style-type: none"> Assists ICS and the SAT in assessing and classifying internal control deficiencies during the Concluding, Reporting, and Correcting Phase of the A-123, Appendix A, effort 	<ul style="list-style-type: none"> ICS OBO SAT

Template/Checklist	Purpose	User
Location-based Risk Assessment template	<ul style="list-style-type: none"> Assists in determining the risks present at each location 	<ul style="list-style-type: none"> ICS SAT
Location Selection template	<ul style="list-style-type: none"> Documents the rationale for in-scope sites 	<ul style="list-style-type: none"> ICS SAT
Mapping template	<ul style="list-style-type: none"> Maps the significant financial statement line items to the key processes 	<ul style="list-style-type: none"> ICS
Process-Level Test Plan template	<ul style="list-style-type: none"> Documents the elements of the test including sample size, test steps and key attributes 	<ul style="list-style-type: none"> ICS
Remediation Plan Template	<ul style="list-style-type: none"> Provides a format for Process Owners to document corrective action status 	<ul style="list-style-type: none"> Process Owners ICS
Risk/Control Matrix template	<ul style="list-style-type: none"> Lists all controls (both key and non-key) and captures risks, control objectives, frequency and design assessment 	<ul style="list-style-type: none"> Process Owners ICS
SAS 70 Assessment Checklist template	<ul style="list-style-type: none"> Assists ICS in reviewing and documenting SAS 70 assessments for cross-servicing organizations 	<ul style="list-style-type: none"> ICS
Testing Quality Review Checklist template	<ul style="list-style-type: none"> Provides a framework for the Supervisor to review the test procedures and results 	<ul style="list-style-type: none"> ICS
Test Sheet template	<ul style="list-style-type: none"> Assists ICS in conducting the tests specified in the process-level test plans and documenting test results 	<ul style="list-style-type: none"> ICS

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.

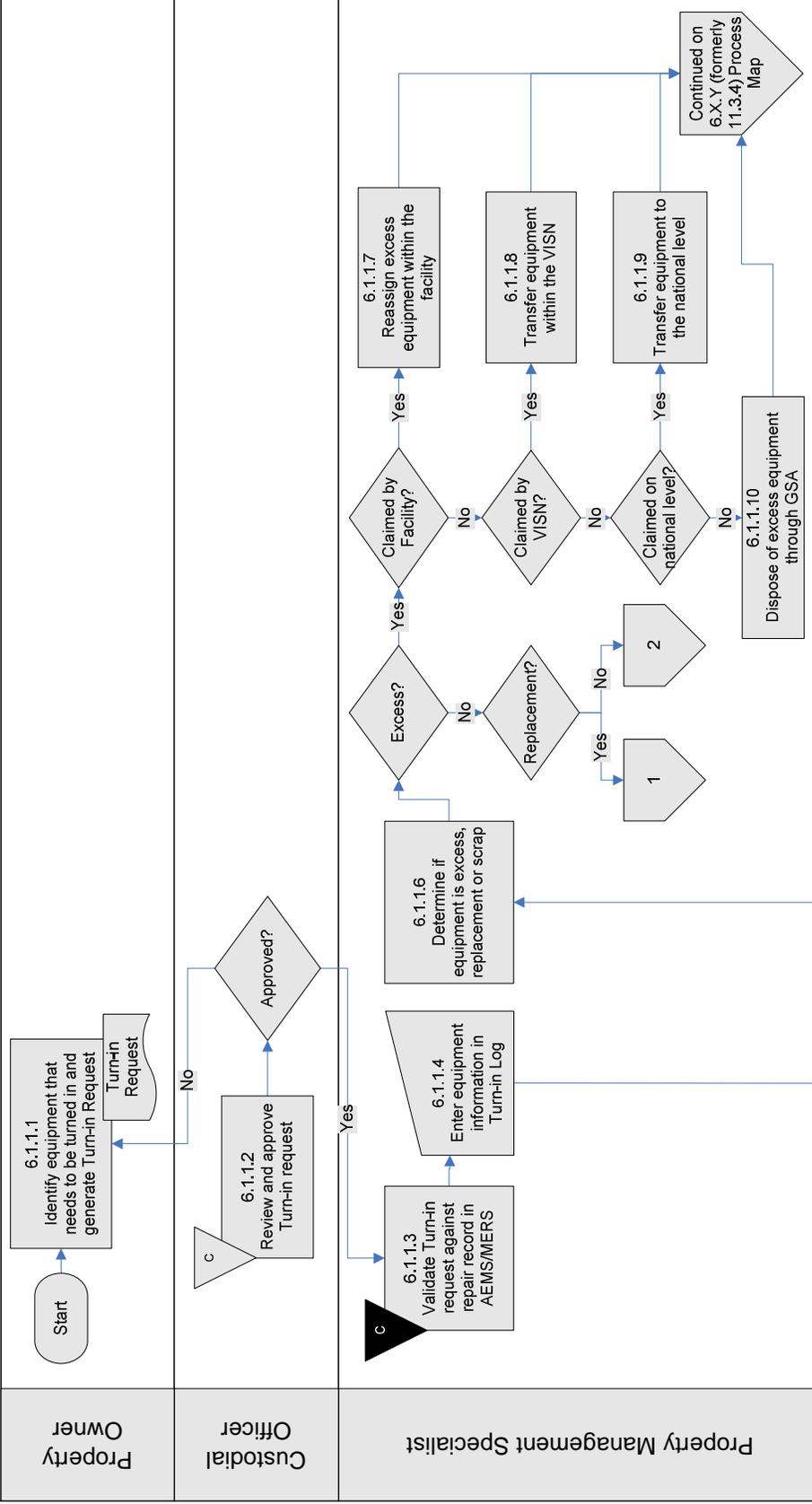
Process Narrative	
6 Property, Plant and Equipment Management 6.1 Personal Property 6.1.1 Disposal	
Process Verification	
Verified By: _____	Signature: _____
Title: _____	Date: _____
1. Confirms that this process and its controls have been accurately documented.	

Key Process Activity	Process Owner	Control Matrix Reference
<p>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 process for Fixed Asset Accounting is documented in 6.X.Y (formerly 11.3.4).</p>		
<p><u>6.1.1.1 Identify equipment that needs to be turned in and generate Turn-in Request</u> 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.</p>	Property Owner	
<p><u>6.1.1.2 Review and approve Turn-in request</u> 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.</p>	Custodial Officer	C - 6.1.1.2

Key Process Activity	Process Owner	Control Matrix Reference
<p><u>6.1.1.3 Validate Turn-in request against repair record in AEMS/MERS</u> 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><u>6.1.1.4 Enter equipment information in Turn-in Log</u> 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><u>6.1.1.5 Pickup equipment and sign Turn-in Request</u> 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><u>6.1.1.6 Determine if equipment is excess, replacement, or scrap</u> 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><u>6.1.1.7 Reassign equipment within the facility</u> 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><u>6.1.1.8 Transfer equipment within the VISN</u> 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><u>6.1.1.9 Transfer equipment to the national level</u> 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 Process Activity	Process Owner	Control Matrix Reference
<p><u>6.1.1.10 Dispose of excess equipment through GSA</u> 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><u>6.1.1.11 Transfer replacement equipment to GSA</u> 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><u>6.1.1.12 Report equipment as scrap to GSA</u> 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><u>6.1.1.13 Dispose of scrap equipment</u> 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



Property Owner

Custodial Officer

Property Management Specialist

Warehouse Personnel

<p>6 Property, Plant and Equipment 6.1 Personal Property 6.1.1 Disposal</p>			<pre> graph TD 1{{1}} --> 6.1.1.11[6.1.1.11 Transfer replacement equipment to GSA] 2{{2}} --> 6.1.1.12[6.1.1.12 Report equipment as scrap to GSA] 6.1.1.11 --> 6.1.1.13[6.1.1.13 Dispose of scrap equipment] 6.1.1.12 --> 6.1.1.13 6.1.1.13 --> Map{Continued on 6.X.Y (formerly 11.3.4) Process Map} </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 process. These risks/objectives will then be put in the RCMs and matched with controls to determine if the process has any gaps. The table below lists suggested risks and control objectives for selected key processes. It is not an all-inclusive list; ICS will modify this list based on information gathered during interviews with process owners.

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

Inaccurate data may be entered into the personnel files which may result in inaccurate payroll distribution	<ul style="list-style-type: none"> • Personnel actions are authorized • Input of personnel records are complete, accurate, and made in a timely manner • Personnel actions are processed completely and accurately
Personnel actions may be noncompliant with applicable laws and regulations	<ul style="list-style-type: none"> • Employee benefit transactions and reporting are in compliance with laws and regulations
Hours worked may be inadvertently recorded	<ul style="list-style-type: none"> • Only legitimate and approved time and attendance information can be entered into the system
Financial records may be inaccurate due to inaccurate payroll information	<ul style="list-style-type: none"> • Payroll payments are processed completely and accurately • Adjustments are approved by the appropriate personnel and made to the correct accounts and in the proper period

Budgetary Resources

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"> • The recorded appropriation amount agrees with the amount made available in the appropriation or other appropriate legislation, including restrictions on amount, purpose and timing • The recorded apportionments agree with the OMB apportionments and the total amount apportioned does not exceed the amount appropriated • The total amount allotted does not exceed the total amount apportioned • Budget transactions are authorized • Budget transaction are recorded completely and accurately • 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 • Fixed appropriation accounts are closed on the 5th fiscal year after the end of the period that they are available for obligation • The ability to record and authorize budgetary transactions are limited
---	--

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

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"> • Specific guidelines are available and utilized when selecting capital projects • Construction Projects are authorized by appropriate personnel • Funding for new capital projects are verified before they are authorized
<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"> • PP&E Acquisitions are recorded accurately and timely • Software Work In Progress is captured and properly accounted for in the financial records.
<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"> • Capital Lease Project submissions are complete and contain the necessary information including technical specifications and market surveys to ensure prospective vendors are qualified. • All Capital Lease needs are addressed and captured in the original planning of the project. • Contractor work is reviewed to verify completeness before payments are granted. • Invoices are authorized by appropriate personnel before payments are distributed. • Technical Specifications and contract requirements were adhered to by the vendor.
<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"> • Solicitation of prospective vendors meet FAR guidelines • Project submissions of prospective contractors are reviewed to ensure technical competence before a selection is made • Potential vendors are financially capable of finishing the project
<p>Lack of Contractor oversight may lead to cost overruns and project delays</p>	<ul style="list-style-type: none"> • Capital Projects are monitored by appropriate personnel to verify that tasks are being performed by contractors in a timely manner
<p>Fraudulent submission and/or improper processing of contractor payments may lead to financial losses.</p>	<ul style="list-style-type: none"> • Invoices are reviewed and approved by the COTR and CO before disbursements are issued • Funding is verified before invoice payments are submitted

Inadequate tracking of inventory of assets results in the inability to detect fraud, theft, and/or misappropriation of assets	<ul style="list-style-type: none"> • PP&E is tracked periodically by appropriate personnel • Lost/Stolen property is reported periodically and reviewed by appropriate personnel • Lost/stolen laptops are reported to appropriate authorities • Transfers of assets to other federal agencies are reviewed and approved by appropriate personnel.
Disposal of capital assets may not be accurately and completely input into the Agency's financial management system.	<ul style="list-style-type: none"> • Disposal of PP&E are accurately and completely input into the Agency's financial management system • Disposal of assets are recorded timely • Appropriate personnel approve of the disposal of assets.
Depreciation data of capital assets are not captured resulting in misstated financial statements.	<ul style="list-style-type: none"> • Accurate and complete depreciation data of PP&E is input into the property system • All capital assets that are capitalized have a depreciation rate assigned to it.
Data manipulation within the property system may occur, causing unreliable data.	<ul style="list-style-type: none"> • Capital asset financial data within property system can be relied upon
Funds Management	
Fund Balance with Treasury (FBwT) is over/under stated	<ul style="list-style-type: none"> • FBwT is accurate and complete
VA is non-compliant with Treasury's reporting requirements	<ul style="list-style-type: none"> • SF-224 is submitted timely and accurately • Differences are investigated and resolved timely • Adjustments to prior month SF-224 is reviewed and approved • Cash reconciliations are performed accurately and completely • Cash reconciliations are performed on a timely basis
Data is manipulated and external reporting is incorrect	<ul style="list-style-type: none"> • External reports are submitted accurately
Fraud and error is undetected	<ul style="list-style-type: none"> • Adequate segregation of duties exist
Revenue Management	
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"> • Reimbursable agreements (RAs) are accurately and completely entered into the financial system

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"> • Adjustments to the RAs are made to the appropriate vendor, completely, and in the correct accounting period
Data is manipulated, lost, or diverted resulting in inaccurate financial records	<ul style="list-style-type: none"> • Access to the financial systems are restricted • Reimbursable agreements (RAs) are accurately and completely entered into the financial system • Changes to the system are restricted and monitored • Periodic batch processing is made completely and accurately
Services are not provided but recorded resulting in over statement of accounts receivable	<ul style="list-style-type: none"> • Billings are recorded accurately and completely • Accounts receivable is recorded accurately and completely
Data may be manipulated, lost or diverted resulting in inaccurate financial records	<ul style="list-style-type: none"> • Access to financial system is restricted