

**STATE OF GEORGIA
IMPROVE
GUIDANCE MANUAL**

OVERVIEW OF THE IMPROVE APPROACH

	PAGE
1. INTRODUCTION	
1.1 What is IMPROVE?	5
1.2 What is the purpose of IMPROVE?.....	6
1.3 Program Expectations and Timeline.....	6
1.4 Guidance Manual and Training Program.....	7
2. OVERVIEW OF INTERNAL CONTROLS OVER FINANCIAL REPORTING	
2.1 Introduction.....	8
2.2 Definition of Internal Control	8
2.3 COBIT.....	11
2.4 Responsibility for Internal Control System	13
2.5 Conclusion	14
3. TOP-DOWN, RISK-BASED APPROACH	
3.1 Introduction.....	15
3.2 Risk Identification.....	17
3.3 Controls Identification	18
3.4 Execution and Evaluation	20
3.5 Implementation	21
4. IDENTIFYING RISK	
4.1 Introduction.....	22
4.2 Performing the Risk Assessment	23
5. INTRODUCTION TO PROCESSES AND CONTROLS	
5.1 Introduction.....	24
5.2 Understanding Processes	24
5.3 Understanding Controls	27
5.4 Understanding IT Control Concepts	30
6. DOCUMENTATION OF PROCESSES AND CONTROLS	
6.1 Introduction.....	34
6.2 Gathering Information	34
6.3 Documenting an Understanding of Processes.....	36
6.4 Creating the Risk and Control Matrix.....	38
6.5 Reviewing Understanding with the Process Owner.....	42
6.6 Walkthroughs.....	42
6.7 Controls Residing with a Third-Party Service Provider	44

7. TESTING THEORY AND STRATEGY	
7.1 Introduction.....	48
7.2 Developing Control Testing Strategies.....	48
7.3 Documenting Testing.....	55
7.4 Evaluating Results	59
7.5 Communicating Results	60
8. FRAUD CONCEPTS	
8.1 Introduction.....	62
8.2 Fraud Defined	63
8.3 Who Commits Fraud and Why is Fraud Committed	64
8.4 Responsibility to Detect Fraud and Developing an Appropriate Oversight Process ...	65
8.5 Other Resources	68
9. CONCLUSION	
9.1 IMPROVE Program.....	69
9.2 Contact Information	69

APPENDICES

4.1	Materiality Template.....	71
4.2	Risk Assessment Templates.....	72
5.1	IT General Controls	74
5.2	End-User Computing Controls	91
6.1	Narrative Example	93
6.2	Flowchart Example	94
6.3	Walkthrough Example	95
6.4	Risk and Control Matrix Template	97
6.5	Third-Party Service Provider Inventory Template	98
6.6	Reliance on the Work of Others Templates	101
7.1	Determining Factors for Sample Size	109
7.2	Sample Size Guidance	110
7.3	Test Plan Template	111
7.4	Testing Leadsheet Example	112
7.5	Document Request Template.....	113
7.6	Issue Summary Template.....	114

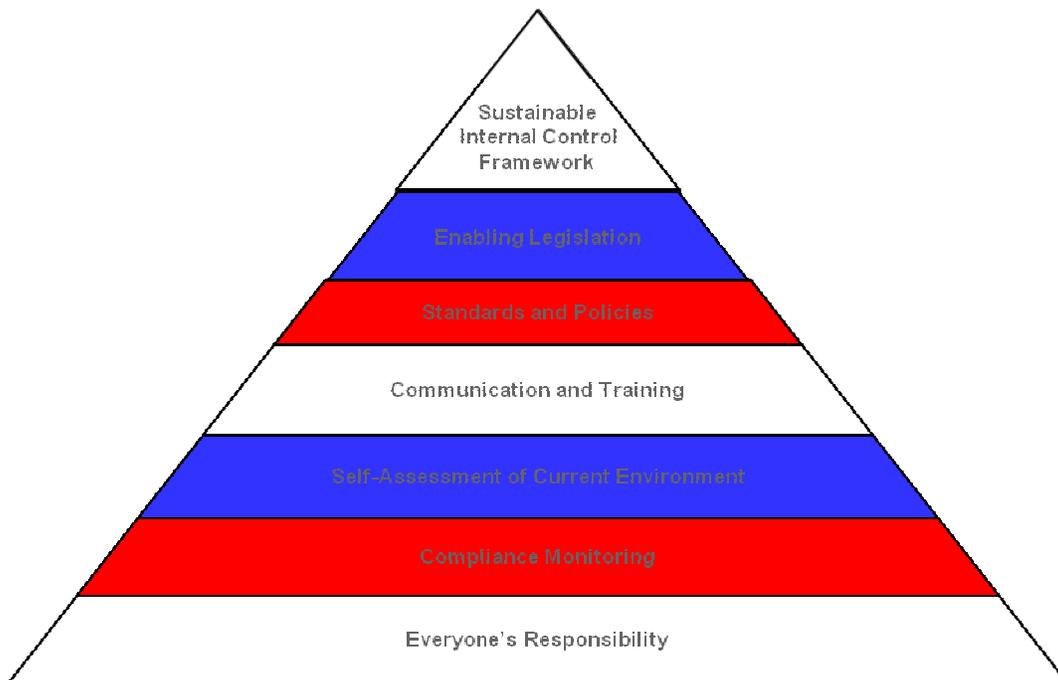
1. INTRODUCTION

1.1 WHAT IS IMPROVE?

The current business environment has significantly heightened the expectations of stakeholders regarding the adequacy and effectiveness of an organization's internal controls that support its financial, operational, and compliance objectives. Effective internal controls are the foundation for managing risk and creating a safe and sound operating environment. While emphasis in the past has been on regulating for-profit public companies, internal controls are becoming more important in the Government and Not-for-Profit Sectors. This is driven primarily by inquiries from stakeholders including the federal government, Compliance and Internal Audit functions, and bond rating agencies as well as enhanced public accountability to key stakeholders, namely taxpayers of the State of Georgia.

Internal controls, Monitoring, Process review, Risk assessment, Operational improvement, Validation and efficiency, and Effectiveness ("IMPROVE") is the State's new internal control program that was introduced by the State Accounting Officer ("SAO"). This framework is very similar to other states that have enacted a formal internal controls mandate to all their respective state agencies.

The Georgia statewide internal control program defines the vision of an effective system of internal controls for Georgia State government.



The statewide internal control framework is supported by:

- Enabling Common Framework - ensuring the vision of effective controls is properly applied

- Standards and Policies - expanding existing policies and promulgating new standards to fully implement the vision of effective internal controls
- Communication and Training - connecting with State Government and relaying the vision
- Self-Assessment of Current Environment - assessing risk and identifying areas for improvement
- Compliance Monitoring - assisting State of Georgia Government in proactively mitigating risks
- Everyone's Responsibility - An effective system of internal control can only be preserved by the diligence of every person involved in State of Georgia Government.

1.2 WHAT IS THE PURPOSE OF IMPROVE?

The purpose of the IMPROVE Program is not only to establish adequate internal control but also to increase fiscal accountability within State government.

To accomplish this effort, the SAO instituted a framework to accomplish the following:

1. Establish comprehensive standards, policies, and procedures to serve as a foundation for strong and effective internal controls
2. Make appropriate education efforts to inform state agencies of these standards, policies, and procedures which shall include training courses, manuals and other information sources to promulgate a strong and effective system of internal control over financial reporting in state agencies

Additionally, SAO will provide ongoing assistance and monitoring to support State agencies in their efforts. Via the IMPROVE website, located on the website of the SAO (http://sao.georgia.gov/00/channel_createdate/0,2095,39779022_161308762,00.html), SAO will provide general communication concerning the IMPROVE Program as well as resources including the internal control guidance manual, assessment templates, policies and procedures, calendar, contact information, and responses to Frequently Asked Questions (FAQ) to assist State agencies in performing their assessments.

SAO will provide recommended completion dates for each milestone on the IMPROVE website and will periodically distribute surveys to gauge effectiveness of the IMPROVE Program. This program will be rolled out in phases and will be communicated by SAO.

1.3 PROGRAM EXPECTATIONS AND GUIDELINES

Program Expectations

Under the IMPROVE Program, each agency will be required to perform an annual assessment of internal control over financial reporting. By performing this assessment, agencies can identify risks and compensating controls that reduce the possibility of material misstatements and misappropriation of assets. The assessment also will indicate opportunities to increase efficiency and control effectiveness in business processes and operations.

Each State agency will be asked to upload to the IMPROVE website all required internal control assessment documents in accordance with the milestone schedule as well as all significant changes, issues, corrective actions and resolutions. Agencies will also complete an annual self-assessment checklist in order to assist SAO in assessing the efficiency and effectiveness of the IMPROVE Program.

Training and Implementation

The IMPROVE pilot program is deployed in October 2010 and will be rolled out thereafter. SAO will provide a formal deployment schedule to the state agencies in early 2011.

1.4 GUIDANCE MANUAL AND TRAINING PROGRAM

This manual has been prepared with assistance from Ernst & Young to assist SAO in its efforts to inform State agencies on establishing standards, policies, and procedures necessary for an effective internal control system. This manual serves as a supplement to the one-day training program and is designed as a flexible set of principles, guidelines, and tools that can be followed to help each agency in performing its own internal control assessment.

2. OVERVIEW OF INTERNAL CONTROLS OVER FINANCIAL REPORTING

2.1 INTRODUCTION

One commonly used and understood framework for evaluating internal controls over financial reporting is contained in the report of The Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO is a voluntary organization originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent initiative that studied the causal factors that can lead to fraudulent financial reporting and developed recommendations. The National Commission was jointly sponsored by five major professional associations in the United States: the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Internal Auditors, and the National Association of Accountants (now the Institute of Management Accountants). The Commission was wholly independent of each of the sponsoring organizations and included representatives from industry, public accounting, investment firms and the New York Stock Exchange.

The COSO report, *Internal Control—Integrated Framework*, established a broad definition of internal control extending to all objectives of an organization.

2.2 DEFINITION OF INTERNAL CONTROL

In order to assess an organization's internal control environment, one must first identify the criteria against which the assessment will be made. Therefore, it is important to appropriately identify internal control early in the evaluation process. The COSO report contains the most widely accepted definition of internal control.

Internal control is broadly defined as a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following three COSO categories:

- Reliability of financial reporting - This item is related to the preparation of reliable published financial statements, including interim and condensed financial statements, such as earning releases, reported publicly or Comprehensive Annual Financial Report ("CAFR").
- Compliance with applicable laws and regulations - This item deals with complying with those laws and regulations to which the entity is subject.
- Effectiveness and efficiency of operations - This item addresses an entity's basic business objectives, including performance and profitability goals and safeguarding of resources.

In assessing the design and operating effectiveness of internal controls over financial reporting (ICFR), under the COSO framework, management also considers the five components of internal control as depicted in the COSO "Cube". If designed and operating effectively, controls within these five components in totality provide a framework for internal control.



The COSO internal control framework consists of the following five interrelated components:

1. Control Environment

- a. The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include:
 - i. Integrity, ethical values and competence of the entity’s people,
 - ii. Management’s philosophy and operating style,
 - iii. Commitment to competence,
 - iv. Organizational structure and assignment of authority and responsibility,
 - v. Board of Directors and/or audit committee participation in governance and oversight, and
 - vi. Human resources’ policies and practices.

2. Risk Assessment

- a. Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and usually internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change. Some factors to consider in understanding the risk assessment process are:
 - i. Whether entity-level objectives have been established and communicated,
 - ii. Whether a risk assessment process, including estimating the significance of risks, assessing the likelihood of their occurrence, and determining needed actions, has been established,
 - iii. Whether mechanisms are in place to anticipate, identify, and react to changes that may have a dramatic and pervasive effect on the entity, and
 - iv. Whether the accounting department has processes in place to identify significant changes in generally accepted accounting principles

promulgated by relevant authoritative bodies and/or changes in the operating environment, including regulatory changes.

3. Control Activities

- a. Control activities are the policies and procedures that help determine if management directives are carried out. They help facilitate the necessary actions required to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties. In understanding control activities at the entity level, some factors to consider are:
 - i. Whether the necessary policies and procedures exist with respect to each of the entity's activities,
 - ii. The extent to which controls called for by policy are being applied,
 - iii. Whether management has clear objectives in terms of budget, profit, and other financial and operating goals, and whether these objectives are clearly written, communicated and monitored,
 - iv. Whether planning and reporting systems are in place to identify variances from planned performance and communicate variances to appropriate levels of management,
 - v. Whether the appropriate level of management investigates variances and takes appropriate timely and corrective action,
 - vi. To what extent duties are divided logically through appropriate set up of information technology applications,
 - vii. Whether adequate safeguards are in place to prevent unauthorized access to or destruction of documents, records, and assets, and
 - viii. Whether access security software, operating system software, and/or application software is used to control access to data and programs.

4. Information and Communication

- a. Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external reporting. Effective communication must also occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders. In gaining an understanding of information and communication at the entity level, some factors to consider are:
 - i. Whether the information system provides the necessary reports to management to assess the entity's performance,
 - ii. To what extent information systems are developed or revised based on a strategic plan that is interrelated with the entity's overall information

- systems, and is responsive to achieving the entity-level and process/application level objectives,
- iii. Whether management commits the appropriate human and financial resources to develop the necessary information systems,
 - iv. How management verifies and monitors user involvement in the development and testing of programs,
 - v. Whether a disaster recovery plan has been established for all primary data centers,
 - vi. Whether management communicates employees' duties and control responsibilities in an effective manner,
 - vii. Whether communication channels have been established for people to report suspected improprieties, and
 - viii. Whether the agency is subject to monitoring and compliance requirements imposed by legislative and regulatory bodies.

5. Monitoring

- a. Internal control systems need to be monitored (a process that assesses the quality of the system's performance over time). This effort is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board (if applicable).

In September 2004, COSO issued the *Enterprise Risk Management – Integrated Framework*. The framework addresses internal control within enterprise risk management. Internal control is encompassed within and is an integral part of enterprise risk management. Enterprise risk management is broader than internal control, however, expanding and elaborating on internal control to form a more robust conceptualization focusing more fully on risk. The framework expanded from three objectives to four and expanded from five components into eight (it also changed one of the components from “Control Environment” to “Internal Environment”). The new objective is “Strategic” which deals with an organization’s high-level goals, aligned with and supporting its mission. The additional components are “Objective Setting”, “Event Identification” and “Risk Response”.

Internal Control – Integrated Framework remains in place for organizations and others reviewing internal control on a standalone basis and should continue to be used. However, in the future, organizations may decide to look to the enterprise risk management framework both to satisfy their internal control needs and to move toward a more robust risk management process.

2.3 COBIT

While COSO is commonly accepted as the internal control framework for organizations, COBIT is the accepted internal control framework for the information technology (IT) environment. Control Objectives for Information and related Technology (COBIT) was first released by the Information Systems Audit and Control Foundation (ISACF) in 1996 and has been updated to

include current IT governance principles and emerging international, technical, professional, regulatory and industry specific standards. The resulting control objectives have been developed for application to organization-wide information systems. Now in Edition 4.1, COBIT is intended to meet the multiple needs of management by bridging gaps between business risks, control needs and technical issues.

The COBIT framework is based on the following principle:

To provide the information the organization requires to achieve its objectives, the organization needs to invest in, manage and control IT resources using a structured set of processes to provide the services that deliver the required organization information.

The COBIT framework identifies 34 IT processes and an approach to control over these processes. It provides a generally applicable and accepted standard for sound IT security and control practices to support management's needs in determining and monitoring the appropriate level of IT controls for their organizations.

Four Sections of the COBIT 34 IT Processes

The COBIT framework is structured in four principle domains. Each domain includes unique processes which sum to the 34 IT processes discussed above. This structure serves as a process model for an enterprise to manage IT activities.

1) Plan and Organize (PO)

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. The realization of the strategic vision needs to be planned, communicated and managed for different perspectives. A proper organization as well as technological infrastructure should be put in place. This domain addresses the following processes:

- PO1 Define a Strategic IT Plan
- PO2 Define the Information Architecture
- PO3 Determine Technological Direction
- PO4 Define the IT Processes, Organization and Relationships
- PO5 Manage the IT Investment
- PO6 Communicate Management Aims and Direction
- PO7 Manage IT Human Resources
- PO8 Manage Quality
- PO9 Assess and Manage IT Risks
- PO10 Manage Projects

2) Acquire and Implement (AI)

To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives. This domain addresses the following processes:

- AI1 Identify Automated Solutions
- AI2 Acquire and Maintain Application Software
- AI3 Acquire and Maintain Technology Infrastructure
- AI4 Enable Operation and Use
- AI5 Procure IT Resources
- AI6 Manage Changes
- AI7 Install and Accredite Solutions and Changes

3) Deliver and Support (DS)

This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and operational facilities. It addresses the following processes:

- DS1 Define and Manage Service Levels
- DS2 Manage Third-Party Services
- DS3 Manage Performance and Capacity
- DS4 Ensure Continuous Service
- DS5 Ensure Systems Security
- DS6 Identify and Allocate Costs
- DS7 Educate and Train Users
- DS8 Manage Service Desk and Incidents
- DS9 Manage the Configuration
- DS10 Manage Problems
- DS11 Manage Data
- DS12 Manage the Physical Environment
- DS13 Manage Operations

4) Monitor and Evaluate (ME)

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and governance. It addresses the following processes:

- ME1 Monitor and Evaluate IT Performance
- ME2 Monitor and Evaluate Internal Control
- ME3 Ensure Compliance with External Requirements
- ME4 Provide IT Governance

2.4 RESPONSIBILITY FOR INTERNAL CONTROL SYSTEM

Responsibility for the establishment and monitoring of the internal control system resides with the following personnel:

- Management – The chief executive officer is ultimately responsible and should assume “ownership” of the system. More than any other individual, the chief executive sets the “tone at the top” that affects integrity, ethics, and other factors of a positive control environment. Also of significance are the financial officers and their staff, whose control activities cut across, as well as up and down, the operating and other units of an agency.
- Internal Auditors – Internal auditors play an important role in evaluating the effectiveness of control systems and contribute to ongoing effectiveness. Because of organizational position and authority in an entity, an internal audit function often plays a significant monitoring role.
- Other Personnel – Internal control is, to some degree, the responsibility of everyone in an organization and, therefore, should be an explicit or implicit part of everyone’s job description. Virtually all employees produce information used in the internal control system or take other actions needed to affect control. Also, all personnel should be responsible for communicating upward problems in operations, noncompliance with the code of conduct, or other policy violations or illegal actions.

2.5 CONCLUSION

This manual focuses on controls over financial reporting. However, there are many similarities and common considerations among controls related to financial reporting and controls related to compliance with laws and regulations as well as effectiveness and efficiency of operations. Much of this manual would be useful in an evaluation of controls over compliance with laws and regulations or operations.

The following chapters of the manual are designed to assist management by providing a methodology for transforming the COSO and the COBIT conceptual frameworks into a detailed, meaningful evaluation of internal controls over financial reporting.

3. TOP-DOWN, RISK-BASED APPROACH

3.1 INTRODUCTION

Definition

A top-down, risk-based approach is an approach to conducting an internal control assessment that identifies the risks related to reliable financial reporting, the combination of controls that effectively and efficiently addresses those risks, and evaluates the evidence necessary to conclude on the effectiveness of such controls. The approach rests on the premise that not all risks are equal, and management's effort should be tailored according to the nature (i.e., likelihood and magnitude) of the identified level of risk.

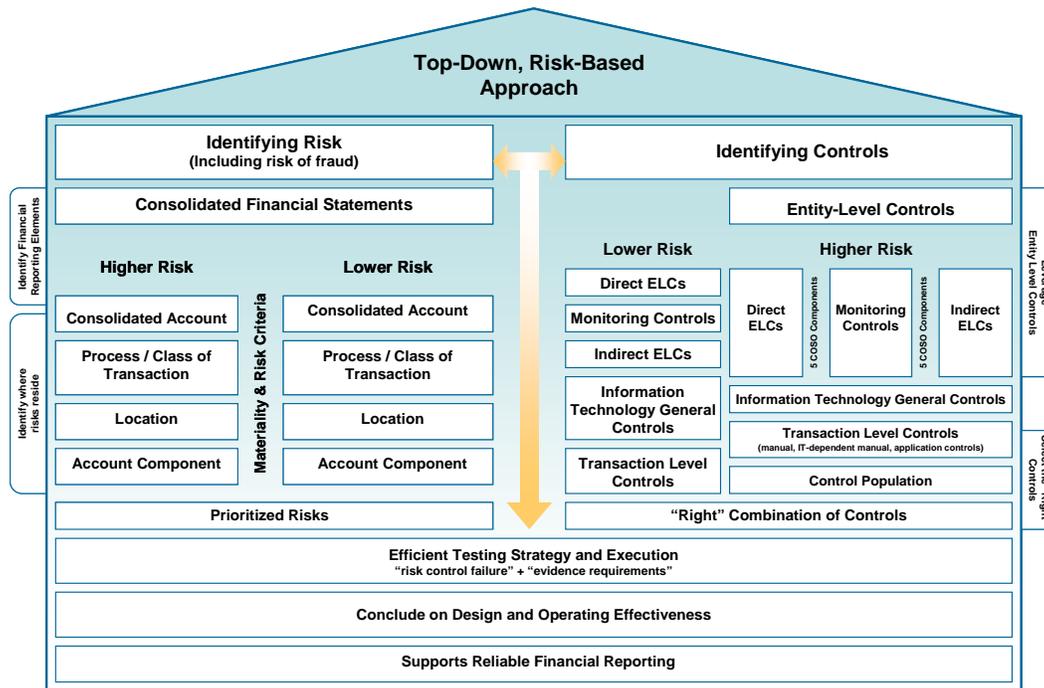
Overview

The goal of the assessment process is to determine whether there is a reasonable possibility that the agency's internal control over financial reporting (ICFR) will fail to prevent or detect, in a timely manner, a material misstatement in the financial statements and disclosures. This goal can be achieved more efficiently with a top-down, risk-based approach. The top-down, risk-based approach represents a thought process – a management perspective – that focuses on the organization as a whole and drives allocation of more resources to the areas of highest risk to reliable financial reporting and effective ICFR.

The top-down, risk-based approach encourages management to identify those accounts, financial statement assertions and business processes which have a higher likelihood of posing a material weakness, and to adjust the nature, extent, and timing of control testing efforts in those particular areas. Numerous benefits of this process include: focusing more effort on areas of higher financial reporting risk; reducing the effort expended on lower risk areas; and leveraging strong entity-level controls to reduce the amount of detailed transactional-level testing.

Model Diagram

To help explain the top-down, risk-based concept, a "house" diagram (as shown on the following page) can be used to depict the elements management should consider in assessing internal controls.



The 3 main activities that serve as the foundation of the “house” are:

1. Risk identification (Chapter 4)
2. Controls identification (Chapters 5 and 6)
3. Execution and evaluation (Chapters 7 and 8)

The risk identification activity, or “risk assessment,” involves identifying and assessing material financial reporting risks. The controls identification activity involves defining the “right” combination of controls to sufficiently address the risks identified in the risk assessment. Once the controls have been selected, the model is supported by a well-designed execution plan and evaluation that includes a testing strategy for identified controls that supports management’s assessment.

These activities, when undertaken together, provide management with a path to achieving reasonable assurance regarding the reliability of its financial reporting. The entire model rests on the premise of prioritized areas of risk and the “right” combination of internal controls. One of the critical success factors in implementing a top-down, risk-based approach is the availability of information and data pertaining to financial reporting elements and processes. Organizations that have a clear understanding of how their financial reporting elements are supported by relevant information systems are generally better positioned to successfully implement this guidance.

Each of these activities is necessary for successful implementation of the top-down, risk-based approach, and is described in further detail below.

3.2 RISK IDENTIFICATION

Risk identification is a continuous element in planning the overall assessment and is the cornerstone to an efficient and effective internal control program. Management should use its knowledge and understanding of the business, its organization, operations and processes to consider the sources and potential likelihood of misstatement in financial reporting and identify those sources that could result in a material misstatement to the financial statements. Included in this understanding is consideration for the generally accepted government auditing standards (GAGAS) that apply to its agency and the related risks to fair presentation of the financial statements.

Successful top-down risk assessments often identify the accounts, financial statement assertions, and business processes with a greater likelihood and larger magnitude of potential material financial misstatements. As one of the first steps in analyzing the potential risk of a material misstatement at the consolidated financial statement account (or caption) level, the risk assessment helps management determine, using both quantitative and qualitative risk factors, which accounts pose a greater risk of having a material financial misstatement.

In conjunction with assessing the consolidated financial statement account risk, management may find it helpful to assess the relevance of each of the financial statement assertions related to each account (e.g., existence and occurrence; completeness; valuation and measurement/allocation; rights and obligations; and presentation and disclosure). This will focus management's attention on identifying specific areas of risk within an account. Business processes can be assessed in much the same manner. Documenting the level of risk associated with an organization's business processes can allow management to study the accounts to determine what specific business processes and locations are driving the higher-risk activities. Management can then focus its efforts accordingly.

The following discussions outline some of the key areas within risk assessment activities where management may identify opportunities to focus efforts on specific risks identified through the process:

1. Materiality decisions

Materiality thresholds are an important consideration for management's assessment. While overall, materiality is, in large part, a quantitative consideration based on key financial measures (e.g., income or revenues), it is also important to consider inherent risks of misstatement, the expectations of key stakeholders, and other qualitative factors. The key insight here is that management should challenge whether the levels of materiality used to identify in-scope financial reporting elements and risks appropriately reflect both **quantitative** and **qualitative** factors.

2. Identification of financial reporting elements

Typically, management breaks down consolidated financial statement line items and disclosures into individual **financial reporting elements** to determine those that are material to the organization. This exercise is very important as individual consolidated accounts (or captions) can be made up of many components, each with different levels of materiality and risk. This is where management exercises judgment and uses its knowledge of the business to determine risks specific to the organization. For example, an account may be of high monetary value yet still be

determined to be low risk due to the low probability of a material misstatement associated with the account. On the other hand, there are some accounts that might be of low monetary value, and yet should be included in scope due to their higher risk of material misstatement based on qualitative factors.

3. Development of financial reporting risk assessment criteria

Once “in scope” risks are identified, management should prioritize these risks. This prioritization will be important for future activities such as facilitating better risk-based control identification and developing testing strategies. Leading practices indicate that once financial reporting elements and related assertions have been identified, management should develop customized risk assessment criteria, including the risk of fraud. Management should consider fraud risk factors at the account, assertion and process levels as part of its approach to evaluating internal controls. The likelihood of fraud occurring generally increases when one or more fraud risks are present, particularly in an environment where significant pressure exists to meet financial or operational targets. Refer to Chapter 9 for more information on Fraud concepts.

Risk rating and prioritization are *judgmental processes* and, therefore, highly dependent on the experiences of participants involved in the process. Validating risk criteria and prioritization outcome is crucial. Refer to Chapter 4 for recommended criteria for the risk assessment.

4. Consideration of significant processes

To understand risks within financial reporting elements, management is encouraged to identify the major classes of transaction affecting those elements and related significant processes. By “significant processes” and “classes of transactions,” we mean those that materially affect the financial reporting elements. Different types of transactions have varying levels or risk and likelihood of errors. For example, classes of transactions might be routine and involve frequently recurring financial data. Other classes of transactions might be non-routine or involve estimation or numerous judgments and assumptions and, therefore, represent higher risk (significant processes will be discussed further in Chapter 5).

3.3 CONTROLS IDENTIFICATION

Typically, management first considers entity-level controls (ELCs) and then transaction-level controls (TLCs). The premise behind this approach is that, in general, ELCs that are pervasive in nature may be more efficient and effective in addressing risk across the organization. Information technology (IT) also plays a vital role in an organization’s system of internal control and impacts an organization’s financial reporting processes and, by extension, its internal control program. As such, management must also consider IT controls when determining the “right” combination of controls.

Entity Level Controls

Entity-Level Controls (ELCs) set the tone of an organization’s overall system of internal control and generally have a wide scope impact on the achievement of the organization’s objectives for internal control. Management’s evaluation process must include not only controls over particular areas of financial reporting risk, but also the entity-wide and other pervasive elements of internal

control defined by its selected control framework. Therefore, an effective system of internal control includes a balance of ELCs and Transaction-Level Controls (TLCs) that work in combination.

ELCs are organized in categories consistent with the COSO framework: monitoring, information and communication, control activities, risk assessment and control environment. In the past, ELCs have been under-leveraged. Now, however, leading organizations realize they can test fewer TLCs when effectively utilizing ELCs. When ELCs are operating effectively, management can enjoy a higher level of confidence that the TLCs will continue to function effectively over time.

There are three primary types of ELCs:

1. Indirect controls are those controls that are cross-functional and which affect the achievement of the organization's control objectives in indirect, but important ways. *Examples include such control environment controls as a code of conduct or code of ethics as well as communication and training efforts.*
2. Direct controls are controls that operate directly at the process, transaction, or application level and are designed to timely prevent or detect material misstatements in one or more financial reporting elements. *Examples include period-end financial reporting activities such as monthly reconciliations and analytics such as margin or variance analyses.*
3. Monitoring controls are those that monitor the effectiveness of other controls and identify possible breakdowns among lower-level controls, though not in a manner that would, by themselves, sufficiently address the risk that material misstatements in financial reporting will be timely prevented or detected. *Examples include activities of the internal audit function.*

Information Technology Controls

There are three primary types of IT Controls:

1. Application controls (also known as automated process controls) are configurable controls within a business application designed to prevent or detect and correct errors or anomalies in the inputs, processes, or outputs. In addition, application controls consist of controls designed around interfaces between business applications and access to specific functionality, such as the setup of the chart of accounts or the configuration of three-way match. In other words, an application control is a specific process control that is dependent upon a computer application to function.
2. IT-dependent manual controls are performed by an individual who relies on some type of automated output. When testing IT-dependent controls, the tester typically performs two separate tests: the IT portion, to validate the accuracy and completeness of the system-generated report, and the manual portion, to test the effectiveness of the manual portion of the control the same way they would test any other manual control.

3. IT General Controls (ITGCs) set the tone within the IT control environment by supporting the functioning of application controls and IT-dependent manual controls. ITGCs are typically broken out into the following three areas:
 - a. Access to programs and data (e.g., the process of granting access to an organization's data to modify, delete, or enhance it)
 - b. Program change and development (e.g., looking at the software development life cycle and asking such questions as who modifies the programs, what are the controls surrounding those changes, is there a rigorous change management process in place?)
 - c. Computer operations (e.g., how does the organization run its IT department?)

Transaction-Level Controls

Transaction-level controls include:

1. Manual controls
2. IT-dependent manual controls
3. Application controls
4. End-user computing controls

Management identifies only those transaction-level controls that address identified risks and has the discretion to not identify controls that are not important to achieving the objectives of internal controls. In addition, in identifying the “right” combination of controls, management has the discretion to select controls for which evidence of operating effectiveness can be attained more efficiently.

3.4 EXECUTION AND EVALUATION

After documenting processes and identifying the “right” combination of controls, a testing strategy may be designed to focus efforts on those controls that have been designed to prevent or detect errors of the highest risk processes.

“Testing” refers to the procedures performed to obtain evidence about the operating effectiveness of controls. The evidence that management evaluates comes from direct test of controls, ongoing monitoring, or a combination of both. Management is in the best position to determine the character and quality of evidence required to support its assessment about the operating effectiveness of internal controls.

Determining the nature, extent, and timing of control testing is a matter of management judgment. Leading organizations determine their testing strategy considering the risk of control failure or the level of risk. There is no requirement to test every control in a process. What to test is a matter of management judgment.

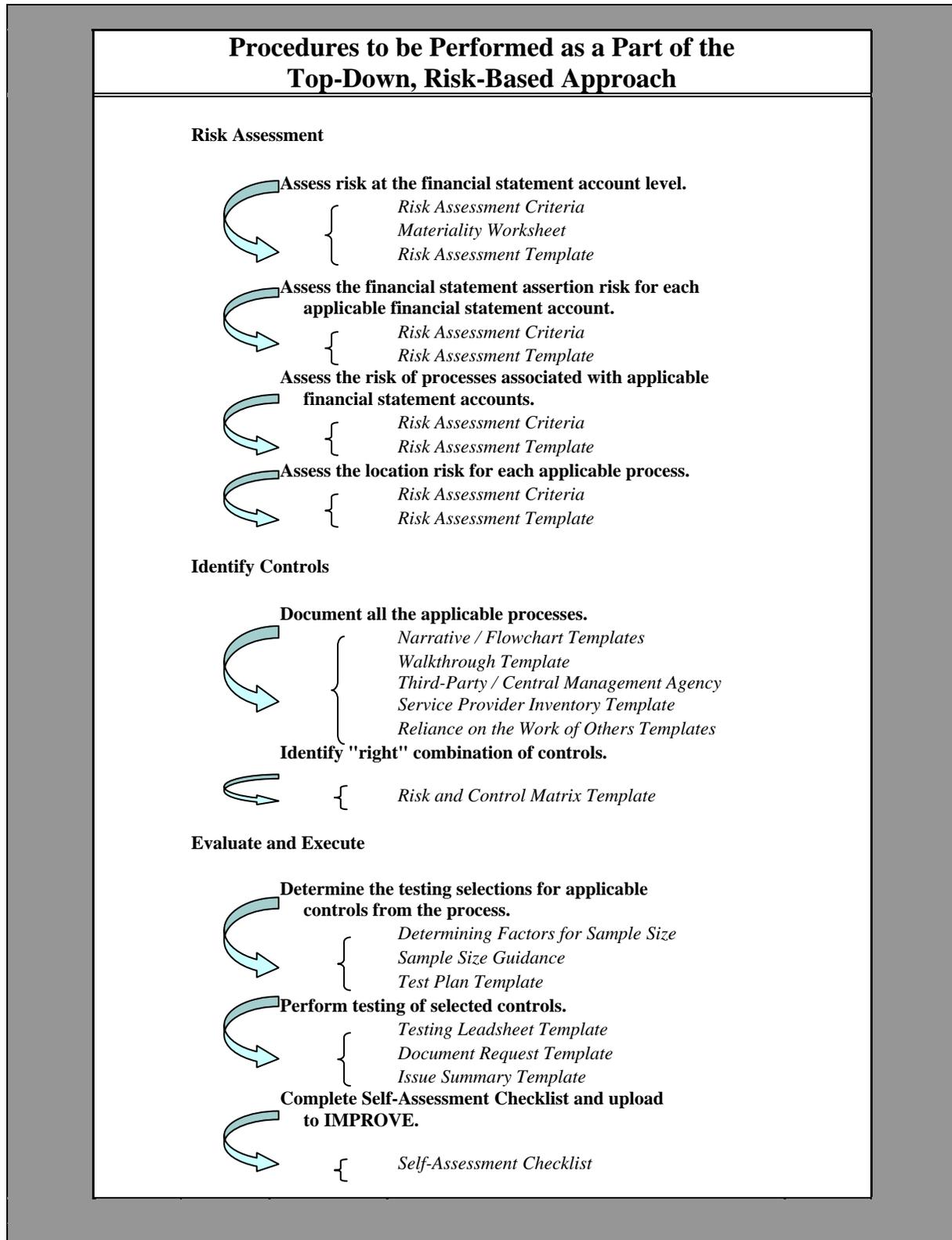
That judgment will depend on considerations related to the following:

1. What to test (whether the controls reside among transaction-level, entity-level, or both).
2. How to test, relates to the level of evidence needed to adequately assess the operating effectiveness of the control.
3. When to test, depending on the nature of the control and the judgment required.

Refer to Chapter 7 for further detail on Testing Theory and Strategy.

3.5 IMPLEMENTATION

While the discussion above focuses on three high-level activities involved in implementing a top-down, risk-based approach to internal controls evaluation, the following depicts a more detailed roadmap for the evaluation of internal controls. Each activity listed in this diagram is discussed in more detail in subsequent chapters (4-8).



4. IDENTIFYING RISK

4.1 INTRODUCTION

Top-down risk assessments are performed to identify the accounts, financial statement assertions, business processes, and locations with a greater likelihood and larger magnitude of potential material financial misstatements. As the first step in analyzing the potential risk of a material misstatement at the consolidated financial statement account level, the risk assessment helps management to determine, using both quantitative and qualitative risk factors, which accounts pose a greater risk of having a material financial misstatement.

The risk assessment activities involve identifying and assessing material financial reporting risks. Management uses its knowledge and understanding of the business, its organization, operations, and processes to consider the sources and potential likelihood of misstatement in financial reporting and identifies those sources that could result in a material misstatement to the financial statements. Internal and external risk factors impacting the business, including the nature and extent of any changes in those risks, may give rise to financial reporting risks. Financial reporting risks may also arise from sources such as the initiation, authorization, processing and recording of transactions and other adjustments that are reflected in the financial reporting elements. Management's evaluation of financial reporting risks should also consider the vulnerability of the agency to fraudulent activity (for example, fraudulent financial reporting, misappropriation of assets and corruption) and whether any of those exposures could result in a material misstatement to the financial statements.

Assessment of financial reporting risks begins with the identification of financial reporting elements; namely, the individual accounts, notes and disclosures that make up the consolidated financial statements. The agency defines the material financial reporting elements and then prioritizes them using risk assessment criteria. Next, the agency will identify the processes relating to the material accounts and relevant assertions, and determine the locations where the processes are performed, if applicable. Agencies will then gain an understanding of what could go wrong in those processes (which may differ by location) to help further define the financial reporting risk. Finally, the agency will prioritize the financial reporting risks. This process is facilitated by the use of management's judgment to determine what is material to the consolidated financial statements and considers the characteristics of individual financial reporting elements and the likely sources of misstatement within the significant processes within an agency.

A financial statement risk assessment is composed of four components:

1. Account risk - Account risk considers the underlying risk associated with the financial statement account, from its size and materiality to the complexity and subjectivity of transactions it represents.
2. Process risk - Process risk takes the information gained in the Account risk stage and applies it to the individual processes that constitute the financial statement accounts. This provides a more detailed analysis that is later used to assist in the determination of the organization's testing effort.

3. Financial Statement Assertion risk - Financial Statement Assertion risk focuses on the risk associated with the five financial statement assertions for each of the financial statement accounts.
4. Location risk - Location risk helps management to understand which locations represent the highest risk for each financial statement account and consequently require the most effort to test.

Each of the four components of risk uses a series of quantitative and qualitative factors as part of the risk assessment. Some of these are relatively simple to obtain, such as the size and composition element of the Account Risk criteria. Others require management to exercise judgment in defining the criteria for High, Moderate and Low risk and the application of these criteria to the accounts.

Impact on Information Technology

Application scoping is an output of the risk assessment process, and IT general controls, IT application controls, and IT dependent manual controls serve as a large part of an entity's control environment. These will be discussed in later chapters in more detail.

4.2 PERFORMING THE RISK ASSESSMENT

The financial statement risk assessment is based around the four risk components previously introduced. Criteria are developed for each component, and are based around risk factors that can be tailored by the organization. Information to develop the risk assessment criteria is obtained from a number of sources to understand the organizational structure, strategy, management, fraud prevention and operational issues faced by the organization. Each criteria is developed with key stakeholders and is then validated with senior personnel.

5. INTRODUCTION TO PROCESSES AND CONTROLS

5.1 INTRODUCTION

A strong understanding of processes and controls is necessary when conducting an internal control assessment. This chapter is devoted to identifying the types of processes and their components, identifying the types and nature of controls, and describing basic IT process and control concepts. The different types of processes include executive processes, operating processes, and support processes; and the process components consist of process boundaries, process inputs, process activities, and process outputs. Controls may be prevent or detect, and there are three main types of controls: manual, IT-dependent manual, and IT application. IT general controls protect the systems that support the relevant processes and allow for reliance on IT application and IT-dependent manual controls. Additionally, end-user computing controls should be a consideration when conducting an internal control assessment.

5.2 UNDERSTANDING PROCESSES

A **process** is a group of logically related activities that, when performed, use the resources of an organization to produce definitive results or transform input through a series of activities into a product or service. More simply stated, a process is a group of logically related activities that transform inputs into outputs.

Significant processes are major processes where significant classes of transactions are initiated, recorded, processed and/or reported (e.g. financial close process). Within processes, one may identify a variety of types or classes of transactions. **Classes of transactions** are data, information, or account detail of a common nature within the financial or other processes of a business (e.g., sales, purchase of goods or services, recording depreciation expense). A transaction is generally considered to be of a separate class if its processing differs from other classes of transactions in any significant respect and, therefore, is susceptible to different inherent and/or control risks.

Transaction types can be distinguished if they are processed differently during part or all of their flow through the system and, in particular, if they are subject to different controls. If different transaction types are *not* properly distinguished, later testing of internal controls may be based on incorrect assumptions about the underlying population of items and may produce misleading results.

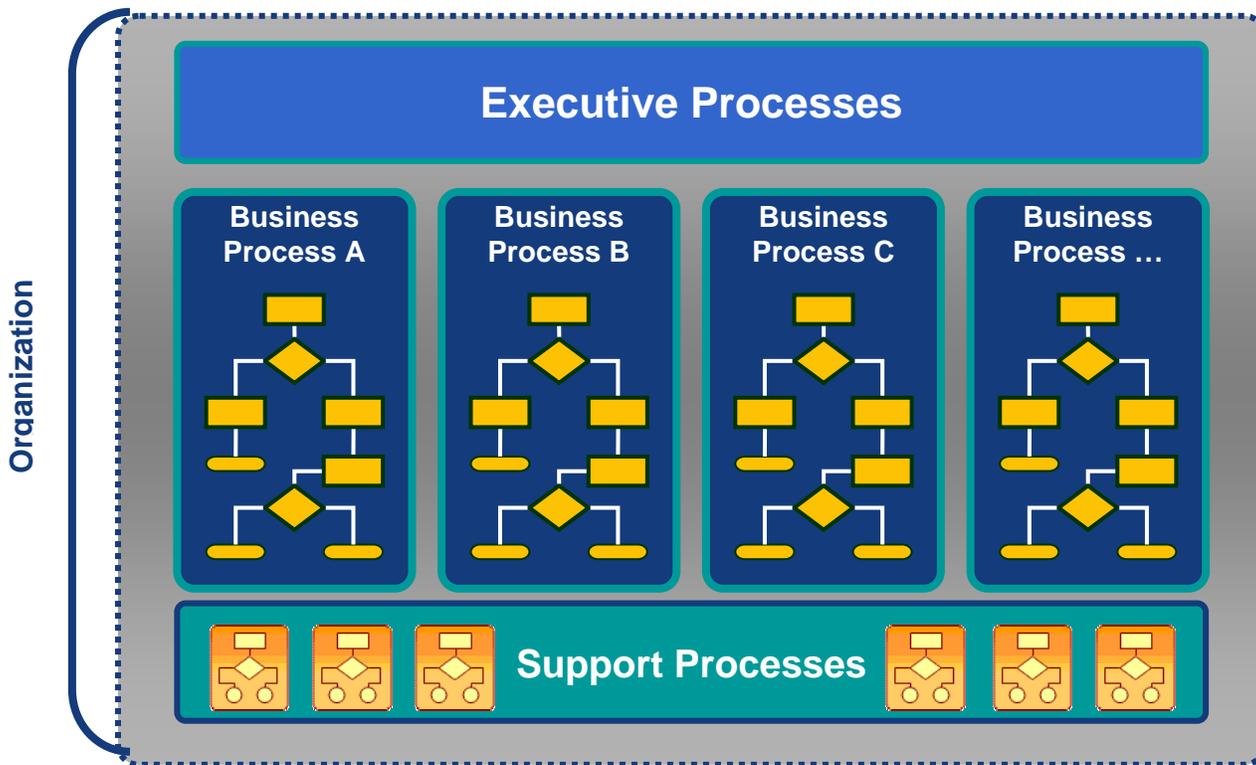
Transactions are classified by the following types:

1. Routine
2. Non-routine
3. Estimation

Process Types

In every organization there are three types of processes: executive, operating and support. **Executive processes** define and monitor the strategy and activities necessary to achieve the defined objectives of an organization, such as strategic planning or corporate governance. **Operating processes** are those processes that drive an organization's core business, such as sales or production. **Support processes** are non-core business processes necessary to operate an organization. Examples of support processes include corporate accounting, payroll and human resources.

Depending on the organization, some processes (e.g., purchasing) may be classified as operating or support. For example, at a manufacturing organization, purchasing is an operating process as it is core to manufacturing operations. Purchasing may be a support process at, for example, a university as it does not relate to its core business.



Process Components

Process boundaries include the logical beginning and ending of a process. These may be different for different organizations. It is important to understand process boundaries as they impact the scope of process review. Boundaries determine what is included in the process as well as what is excluded. Boundaries define sources of inputs to the process and the destination of outputs from the process. An agency's review of a process may not always examine the entire process from beginning to end, or alternatively, may extend beyond the process boundaries.



One should be aware of the scope of the process in question, which should provide details relating to the point in the process where the review begins. For example, an organization may need to document a payroll process, with the exception of the new hire set-up process, which is performed by another organization. As a result the process documentation might begin with the time entry process for hourly employees.

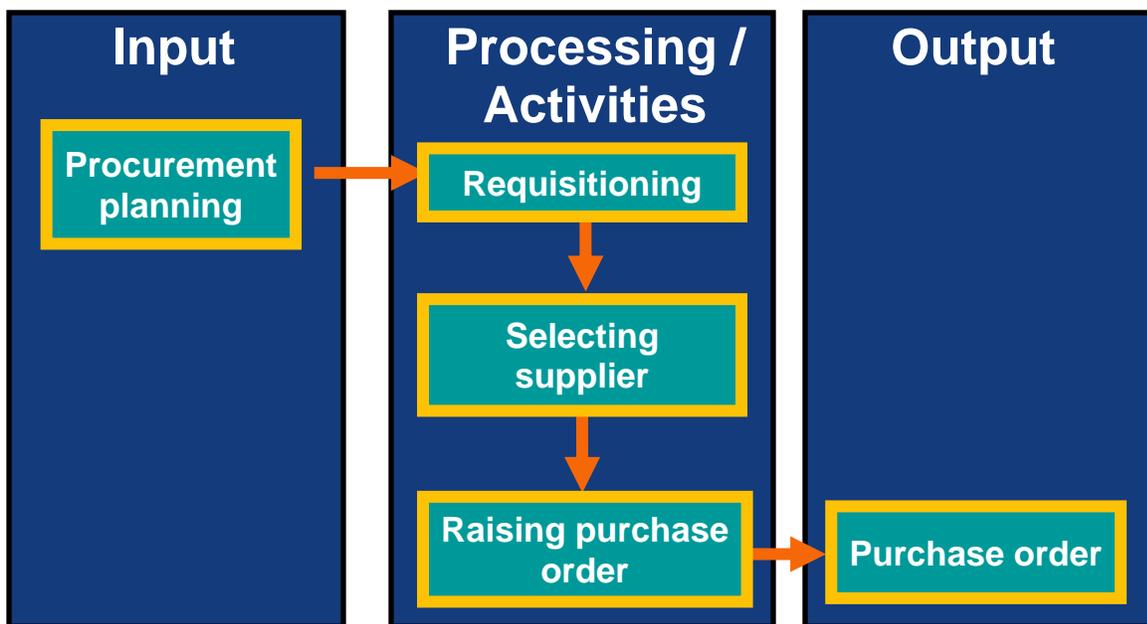
A process has three main components: inputs, activities and outputs. It is important to understand the difference between the different components. They can be defined as follows:

Process Inputs are the material, capital, human resources and information that a business process receives and acts upon in order to transform it into its output.

A **Process Activity** is a specific deed, action or function designed on its own or with other related activities to turn input into output.

Process Outputs are those things transformed by a process for the benefit of the customer or for use as an input in a later process or activity.

The following diagram depicts example process inputs, activities and outputs for a purchasing process:



5.3 UNDERSTANDING CONTROLS

Prevent vs. Detect

Prevent controls, as the name implies, are those used to prevent errors from occurring (e.g., to prevent the wrong source documents from being entered into the system or to prevent an irregularity from taking place). Examples include use of approval matrices, automated validity and edit checks, sequential pre-numbering of checks and logical access security.

Detect controls are those used to detect any error or irregularity after it has occurred. These include independent checking and review, exception monitoring routines and reconciliations.

Prevent controls are usually easy to identify, since they generally operate on every transaction of a given type and are often automated. Where effective prevent controls exist, the likelihood of errors is low and the need for extensive detect controls is reduced.

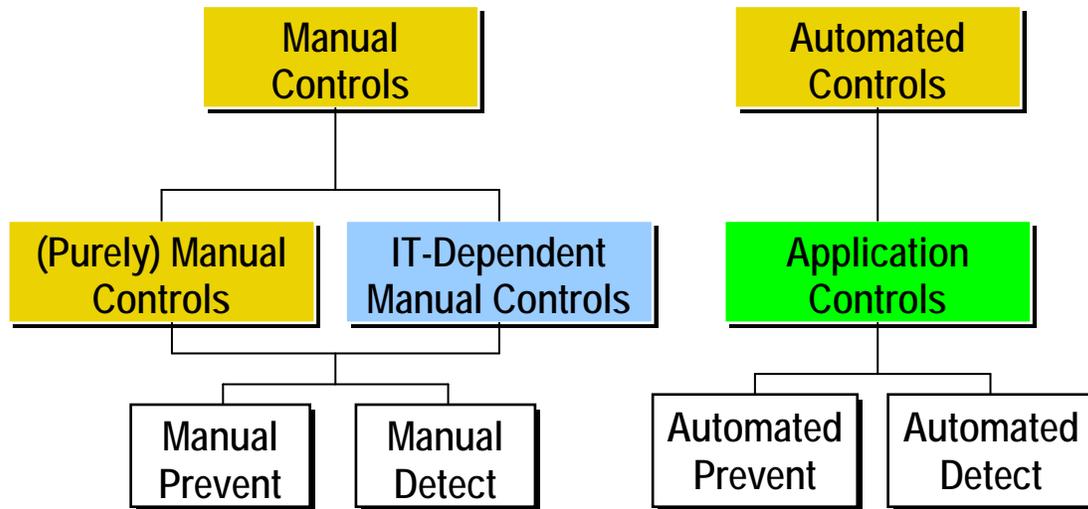
Conversely, where prevent controls are not sufficient, there is a greater need for particularly sensitive and effective detect controls. Detect controls are less likely to be applied to every transaction during the normal flow of processing and may only be performed at intervals. They are also less likely to be fully automated, may be less formalized and may be more difficult to identify.

Good detect controls can sometimes compensate for the absence of adequate prevent controls. Even if informal, controls can be effective if they capture all relevant data completely and accurately, identify all potentially significant errors, are performed on a consistent and regular basis and include timely follow-up of errors and problems detected. Consequently, care must be taken to understand all of the relevant controls before developing conclusions and recommendations on the control system.

Nature of Controls

At the transaction level, there are three types of controls:

1. Manual Controls as the name implies, are those controls that are manually performed by an individual. Examples include the independent review of general ledger reconciliations or the authorization of employee expense reports.
2. IT-Dependent Manual Controls are those controls that are manually performed, but require input based upon the results of computer-produced information. Examples of IT-dependent manual controls include management's review of a monthly variance report and follow up with significant variances. Management relies on the computer-produced report to identify and generate variances.
3. IT Application Controls are performed entirely by a computer or computer-based system. Examples of IT application controls include an automated three-way match, data input validation checks and restricted user access.



It is important to understand the nature of a control in order to properly design effective testing methods to determine if the control is designed and operating effectively. (For more information on Testing Theory and Strategy, refer to Chapter 7.)

Control Frequency

It is important to understand the frequency at which a control is performed, as this helps in determining the design effectiveness of a control as well as what sample size is appropriate for testing the operation of the control. (Sample sizes are discussed further in Chapter 7.)

Controls may be performed at any one of the following frequencies:

Frequency	Example
Ongoing	Firewall
Daily / Multiple times per day	Three-way Match
Weekly	Weekly timesheet review and approval
Monthly	Review of general ledger reconciliations
Quarterly	Review of access to IT systems
Annually	Review of accounting policies
Ad hoc / As required	Authorization of termination payment to employee

Control Owner

Understanding who owns the control assists in the determination of effective control design. For example, general ledger reconciliations are performed by the accountant rather than the goods receiving clerk. It is also important to understand who is responsible for the custody, authorization and recording of transactions in order to determine if appropriate segregation of duties exists. Finally, identifying the control owner identifies whom to contact to understand and test the control.

How to Write a Control

When writing a control, it is important to document the following:

1. Who performs the control activity?
2. What is the control activity (not the process)?
3. When is the control activity performed?
4. How is the control activity documented?

A good control description clarifies how a control is to be tested. The following control description answers each of the four questions posed above:

“Before processing each invoice (3), the Accounts Payable supervisor (1) reconciles the quantity on the goods receipt to the quantity on the invoice (2). Any discrepancies are followed up with the receiving personnel in the warehouse and documented on the invoice (4). The Accounts Payable supervisor also reconciles the quantity and price on the approved purchase order to the invoice (2). If there are differences, the Accounts Payable supervisor further investigates and resolves with the assistance of the procurement department (2). The payment is then processed in the Accounts Payable system.”

Determining Key Controls

Even where controls, taken as a whole, are likely to be effective, the contribution of individual controls to that result is likely to be unequal. When using process flowcharts and a Risk and Control Matrix (discussed in Chapter 6), one should carefully consider the role that each control plays in the control system. Judgment needs to be used to determine which individual controls to consider as significant in preventing or detecting each type of error (i.e., each statement or question of “what could go wrong”).

Controls should be identified as significant if they contribute to the evaluation of overall control effectiveness in precluding errors and achieving control objectives. In general, controls will be subjected to further tests later. Consequently, one should consider the incremental value and costs associated with further testing as secondary factors in designating controls.

Identifying Redundant or Inefficient Controls

Throughout the evaluation of the control system, it is important to be conscious of the cost and inefficiency of unnecessary controls. Where individual controls do not contribute materially to the overall control system, are redundant with other existing controls, or could be productively replaced by a more efficient control, management should reconsider testing or evaluating these controls.

NOTE: Although all controls are not necessarily tested, this does not diminish or remove the need for the sound internal controls throughout an agency. Controls not tested should continue to be performed to contribute to the overall control environment of an agency.

5.4 UNDERSTANDING IT CONTROL CONCEPTS

When evaluating how well risk is managed within a process, it is important to understand the IT environment and IT controls that may be relied upon in order to develop appropriate test plans. Virtually all processes use IT systems; with that in mind, consider the IT environment an “umbrella” over an agency’s infrastructure. If the IT environment acts as the “umbrella” over an agency’s infrastructure, the agency needs controls in place to mitigate the risk of information being processed incorrectly and the risk of unauthorized access.

The relationship between processes and transactions and the computer applications that support them is often complex. Processes are frequently dependent on more than one computer application. In order to avoid duplication of effort in gaining an understanding of these systems, one should limit attention to those applications which are significant to the processes under review. (Refer to Chapter 6 for further discussion of IT processes which may not be under the control of an agency.)

An **application** is a software program that supports the processing of transactions and maintenance of an organization’s records on electronic media. An application typically consists of programmed procedures, files and databases. A **database** is a repository for storing data in a format that can be accessed by applications for calculations and reporting. Most databases are considered pertinent to financial statement reporting because they are the location where financial data resides and could potentially be manipulated.

In order to properly restrict applications, agencies should consider the importance of IT controls. IT controls can be generally categorized as application controls, IT-dependent manual controls, End-User computing controls and IT general controls.

Application Controls

Application controls are automated controls that apply to the processing of individual transactions to provide reasonable assurance that all transactions are valid, properly authorized and recorded, and are processed completely, accurately and on a timely basis. This includes controls such as edit checks, validations, calculations, interfaces and reporting.

The following components of application controls should be considered:

- Configuration settings and custom automated controls
- Master data controls and access
- Control overrides
- Segregation of duties and function access
- Interface control

IT-Dependent Manual Controls

IT-dependent manual controls are specific process controls that are manually performed, but require input based upon the results of computer-produced information. Typical IT-dependent manual controls are computer generated reports that are used to either input key financial information, or review for exception reporting.

Some examples of IT-dependent manual controls are:

- Review and follow up of exceptions on a payroll exception report.
- Review and follow up of exceptions on a customer billing cycle report.
- Hourly time summary report is manually entered into payroll system.

End-User Computing Controls

End-User Computing introduces a different level of risk to an organization's information technology and operational environment. End-User Computing generally involves the use of department-developed spreadsheets and databases, which are frequently used as tools in performing daily work. To the extent these spreadsheets are in place, they are an extension of the IT environment, and results generated from them may, in assessing their impact, have an effect on the organization's financial statements.

End-User Computing can be monitored and controlled by manual processes; using automated tools; or by the ideal method of eliminating the need for End-User Computing, i.e., by adding the computations to systems controlled by information technology.

End-User Computing monitoring typically includes:

- Identifying any and all spreadsheets and/or databases that are in use and form the basis for reports, data used in performing duties, or assist in creating financial data and transactions.
- Locating the spreadsheet and/or database on the network, including the drive and server location; or if on a desktop, locating the personnel who use the spreadsheet in conducting their duties.
- Determining personnel with access to the spreadsheet or database. Identifying controls in place (i.e., version control, change control, password access, etc.) and what computer security is in place for these files.

In order to mitigate the risk introduced by End-User Computing, it is pertinent to confirm adequate controls are in place for those high risk spreadsheets, databases and other user-developed programs as they are equivalent to any other system. These controls should allow for processing integrity, and validate the tool's ability to sort, summarize and report accurately. Some example End-User controls are as follows:

- Access control
 - Controls that limit access to specific rights within a particular system object, such as a file directory or individual file. The most common access control is to restrict the ability to write, delete or execute a file or directory.
- Version or Change control
 - Controls or techniques, especially in an automated environment, to control access to and modification of documents and to track versions of a document when it is revised.
- Review for completeness, accuracy and processing integrity
 - Controls that confirm the data housed via spreadsheets or databases are complete and accurate.
- Backup
 - A control that makes copies of data so that these additional copies may be used to restore the original after a data loss event. The greater the importance of the data

that is stored on the computer, the greater the necessity for data backup procedures.

Note: Spreadsheets are equivalent to any other system; therefore, it is pertinent to confirm adequate controls are in place around those 'key' or high risk spreadsheets (i.e. password protection, version control, etc.).

Refer to Appendix 5.2 for an illustrative list of End-User Computing controls to provide guidance in identifying typical controls in an agency. These lists are not all-inclusive; each project team will need to consider the unique End-User Computing environment of its agency.

IT General Controls

IT general controls confirm that all changes to the supporting application(s) are properly requested, authorized, tested and approved before being implemented into production. This includes:

- Change Management
 - Changes are authorized, tested and approved to confirm application controls operate effectively through the period of intended reliance.
 - Changes are monitored on a regular basis for unauthorized changes.
- Logical Access
 - Access to key systems and files is approved, appropriate and monitored to confirm data generated by the applications is reliable.
 - Application Security: Higher-level logins and parameter change restrictions confirm applications are secure.
- Computer Operations
 - Data supporting the key financial information is backed-up, such that data can be accurately and completely recovered if there is a system outage or data integrity issue.
 - Programs are executed as planned, with deviations from scheduled processing being identified and investigated, including controls over job scheduling, processing, and error monitoring.

To review, business processes are supported by applications; for example, procure to pay – purchasing application, accounts payable application, etc. The applications reside on a database (for example, Oracle DB) which houses the data, and the database resides on an operating system (platform) which is on a network which sits on a physical box in a data center.

IT general controls support reliance on IT application controls and IT-dependent manual controls within business processes. When performing control testing, agencies should also test the database, operating system and network (at the general controls level) to a sufficient extent to conclude that the overall control environment effectively mitigates risk. For further discussion of Control Testing, refer to Chapter 7.

Refer to Appendix 5.1 for an illustrative list of IT general controls considered relevant to support financial reporting objectives. This list is not all-inclusive, and each project team will need to consider the unique IT environment of its agency.

6. DOCUMENTATION OF PROCESSES AND CONTROLS

6.1 INTRODUCTION

Within its financial statements, an organization implicitly makes claims regarding its financial position, results of operations and cash flows. Such claims are known as financial statement assertions. It is important to note that assertions are indicators of where risk could occur towards financial misstatements. Prioritization of the assertions for each financial reporting element assists in determining the need for controls to mitigate risks related to the assertions. If the risk of an assertion to an account is significant, a more thorough set of direct transaction and/or monitoring controls are needed to satisfy the assertion.

An account balance can generally be misstated under three conditions: missing entries, erroneous entries, and the presence of entries that do not belong in the account. Testing an account balance will, therefore, require verifying that the recorded transactions have occurred during a given period (existence or occurrence), searching for omitted items or transactions that should have been recorded in the account (completeness), testing whether the entries have been recorded for the correct amounts (valuation/measurement(allocation)), and considering whether the assets and liabilities of the agency are accurately presented (rights and obligations, presentation and disclosure).

Financial statement assertions are classified into the following five categories:

- Existence or Occurrence:
- Completeness
- Valuation or Allocation
- Rights and Obligations
- Presentation and Disclosure

6.2 GATHERING INFORMATION

In order to begin documentation, one must first gather all available background information. This information may be obtained in the form of existing documentation, policies and procedures or interviews. Existing documentation often provides a starting point from which to begin. It allows the reader to gain a precursory understanding of the process and identify areas where more information is required. If existing documentation does not exist, often policies and procedures will be of some assistance.

A policy details the principles that guide the actions and decisions in an organization. Policies do not tell “how” to do something, but specify what is acceptable, unacceptable, right and wrong. An organization usually has policies addressing each of its functional areas. A compilation of these policies is a policy manual. The manual might contain the policies of the entire organization, or separate manuals may house policies for each functional department.

Procedures (also known as Standard Operating Procedures [SOPs]) address “how things are to be done.” Procedures define the steps to be taken in various business situations that are typical to

the organization. An organization may have the same processes established at various locations. Procedures help bring uniformity (standardization) in action across the organization.

Interviews

After reviewing existing documentation and policies and procedures in order to gain a basic understanding of a process, it is recommended that interviews be conducted to capture and retain the specific details of a current process. Interviews are conducted with process owners in order to inform them of the scope and approach of the assessment, obtain the process owner's preliminary assessment of key risks and controls and to understand planned changes (if any) to processes and controls. A good interview will result in an understanding of the process and transaction flow as well as validate any additional information gathered prior to the interview.

When conducting an interview, consider the following:

- What are the beginning and end points of the process?
- What are the specific activities within the process?
- What are the key inputs and outputs of the process?
- What types of controls are included in the process, i.e. Automated vs. Manual, Detect vs. Prevent?
- What are the decision points and alternative paths? It is important for the assessment team to identify all decision points within a process, as there may be alternative paths that transactions can take. If all the alternative paths are not identified, it may not be possible to identify all of the key risks and controls.
- What are the integration points with other areas of the organization? Because risks are present at integration points with other areas of the organization, it is important to understand where these integration points are. If required, identify contacts for additional information.
- What are the key IT systems supporting the process? The supporting IT systems may determine how transactions are processed and recorded, as well as the types of risks and controls included.
- Who are the responsible personnel within a process? Identify positions and names. Names alone are not sufficient, because there may be changes over time.
- What is the time frame of the process? It is important to understand both the actual and elapsed time for tasks in the process.
- What is the impact on the financial statements? What general ledger accounts are affected?
- What are the key performance measures, monitoring controls and reporting controls?
- What are the Process Owner's key concerns (risk areas)?
- Is there a history of problems with key controls or process areas?
- Are there any potential compensating controls within the process?
- What is the impact of control breakdowns (if known)?

A successful interview will answer these types of questions. If all of the questions cannot be answered in one interview, it is possible to request and complete a follow-up interview.

6.3 DOCUMENTING AN UNDERSTANDING OF THE PROCESS

After the interview has been completed, it is important to record an understanding of the transaction flow for significant processes and transaction types. This may be accomplished through a flowchart, process narrative, or both.

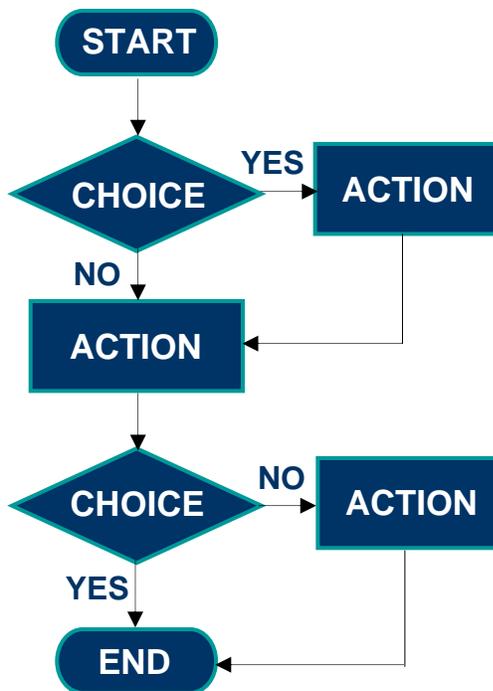
Flowcharts

A **flowchart** is a diagram that shows step-by-step progression through a procedure or system, especially using connecting lines and a set of conventional symbols. Flowcharts provide a concise, efficient and rigorous means of depicting the sequential flow of documents and information, the interaction with key files, and the relevant processing procedures and control points. Properly done, they are easy to read and understand, and easy to update. (Refer to Appendix 6.2 for a flowchart example.)

Flowcharts are ultimately utilized to break down processes into individual events and activities which help identify interdependencies across the organization by linking system and manual activities. Additionally, the flowchart helps identify gaps, weaknesses, segregation of duties problems and potential inefficiencies in a process.

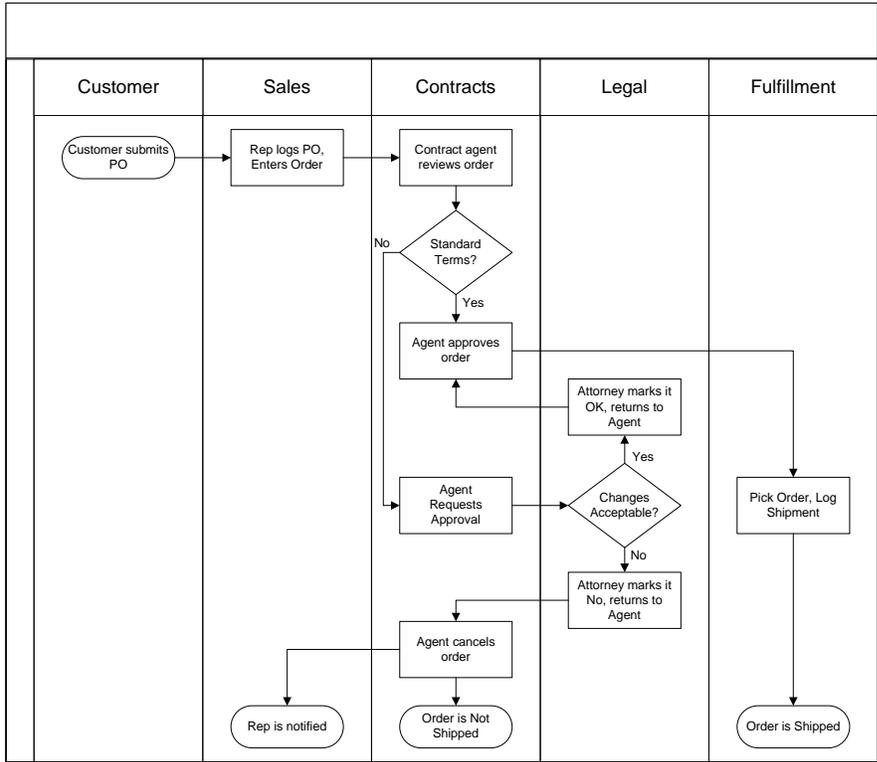
Types of Flowcharts

- **Linear Flowchart** - a diagram that displays the sequence of work steps that make up a process. This tool can help identify rework and redundant or unnecessary steps within a process. This type is the most commonly used.



- **Deployment Flowchart** (often called a **swim-lane flowchart**) - shows the actual process flow and identifies the people or groups involved at each step. This type

of chart depicts where the people or groups fit into the process sequence, and how they relate to one another throughout the process.



Flowchart Components

The flowchart for specific processes will depict a start-to-finish diagram flow with key controls highlighted in the body of the map. The process map uses symbols to illustrate various parts of the process flow.

- Rectangles typically represent each step within the process.
- Triangles typically represent additional information relevant to the process.
- Diamonds typically represent each decision point within the process.

When documenting a process using a flowchart, one should consider the following information:

- Title
- Legend
- Start and End points
- Process Steps
- Decisions and all relevant decision paths
- Responsible Parties
- Key Risk and Controls
- On and off page connectors (where appropriate)
- Notes – to provide additional detail to describe process/control

Narratives

Narrative descriptions of the transaction flow may be used as a supplement to flowcharts or as stand-alone documentation. In general, the assessment team should choose the form of documentation that is most efficient and effective for the current assessment, without losing sight of the longer-term benefits of creating automated flowcharts that can be updated quickly for future changes. (Refer to Appendix 6.1 for an example narrative.)

A narrative may be used either in lieu of a flowchart to document the process, or as a complement to a flowchart (to capture additional detail). A narrative is a document that describes a process or transaction flow using words rather than a pictorial representation. When documenting a narrative, one must also consider information useful in creating process flows.

Narratives evidence understanding of a process and help identify and document key risks and controls as well as control gaps in a process while helping confirm understanding with the process owner. Narratives provide knowledge that can be used in future years or for other means.

When completing a narrative, consider the following:

- Date – the date the narrative was prepared and reviewed
- Agency name and location
- Process name (e.g., Financial Statement Close Process)
- Source of information (e.g. process owner’s name and title)
- Purpose (e.g., to document the accounts payable process)
- Background
- Systems used
- Process overview or summary
- Start and end points
- Risks and controls
- Cross-reference to flowchart or Risk and Control Matrix (RACM)
- Control weaknesses or improvement opportunities

6.4 CREATING THE RISK AND CONTROL MATRIX

The **Risk and Control Matrix** is a common format for documenting the assessment team’s analysis of “what could go wrong” and subsequently, the controls in place to prevent or detect those risks.

The Risk and Control Matrix is designed to capture, for each significant process (or transaction type, if necessary), the following information:

- The key processes impacting the account
- The team’s questions or statements for each objective of what could go wrong
- Relevant controls in place to prevent those errors or detect and correct them
- A cross-reference to the flowchart, narrative or other workpaper describing the control
- Control type

- Financial statement assertion covered
- How often the control is performed
- Whether the control was tested

To assist in the preparation and maintenance of the Risk and Control Matrix, a standard template is available in Excel (see Appendix 6.4, Risk and Control Matrix Template).

Identifying Controls

After completion of process interviews and documentation of process flows and narratives, the agency should consider controls over each significant process that address the “what can go wrong” questions for the relevant assertions. The objective is to identify the controls that provide reasonable assurance that errors relating to each of the relevant financial statement assertions are prevented, or that any errors that occur during processing are detected and corrected.

For each “what could go wrong” question, relevant controls should be recorded on the Risk and Control Matrix. Controls can be incorporated by description or by reference to flowcharts/narratives; controls frequently apply to more than one question/risk, and can be cross-referenced within the Risk and Control Matrix as well.

Management generally designs, and places in operation, controls over processes to confirm that the operating, financial reporting, and compliance objectives of each process are achieved. **However, for purposes of evaluating the effectiveness of internal control over financial reporting, the agency is concerned with controls that address the financial reporting objective.** Therefore, the agency should identify controls related to the initiation, recording, processing, and reporting of transactions.

In some situations, the agency may identify entity-level controls that are relevant to both operating and financial reporting objectives. If these entity-level controls are sufficiently sensitive to prevent or detect errors of importance for one or more assertions, the agency may identify and evaluate them. While entity-level controls may be present, the assessment team should not focus solely on such controls because they generally are dependent on controls over processes or activities at the transaction level. The assessment team should also understand processes or activities at the transaction level in order to identify and understand controls that address all relevant assertions. The agency’s conclusions about the effectiveness of the related controls may be based on a combination of entity-level controls and controls at the transaction level (refer to Chapter 5 – Introduction to Processes and Controls).

The assessment team should keep in mind that, to be effective, internal controls often have to include strong prevent controls in addition to detect controls. For example, where there is a high volume of transactions, the lack of prevent controls significantly increases the risk of errors and accordingly increases the need for particularly sensitive detect controls. In the absence of prevent controls, a high number of errors can render detect controls ineffective in detecting and correcting errors in a timely manner. The categorization of a control by the assessment team may depend on how and for what purpose it is used, and the way in which the agency views it. Ultimately, what matters is not the categorization but whether the control is effective in reducing the risk of errors of importance or fraud.

IT Control Considerations

Prevent and detect controls can reside both within and outside of computerized environments. Within the computerized environment, prevent and detect controls are often referred to collectively as “application controls” in that their implementation and ongoing effectiveness depends on the consistent application of an embedded software program or application to transactions processed by that application. Programmed controls usually are either programmed control procedures (e.g., edit, matching, or reconciliation routines) or computer processes (e.g., calculations, on-line entries, automatic interfaces between systems). Identifying controls may require collaboration with both process owners and IT personnel.

If the agency determines that management is relying on programmed controls or that identified controls are dependent on IT-generated data (i.e., electronic evidence), it should ask a second question: “What ensures that programmed controls are operating effectively?” The response may be:

1. User procedures verify the accuracy of the processing (e.g., manually recomputed complex calculations or reconcile IT reports to manual batch totals) and/or
2. Management relies on the IT system to effectively execute the control or produce the data.

When (2) is the response, the agency should consider the effect of IT general controls in evaluating the effectiveness of controls that are dependent on the IT system or IT-generated data. IT general controls are IT processes and related controls that generally are applied above the computer application level; however, they can be performed on a single platform for a single application. IT general controls, or IT process controls, are designed to: confirm that changes to applications are properly authorized, tested, and approved before they are implemented, and confirm that only authorized personnel and applications have access to data, and then only to perform specifically defined functions (e.g., inquire, execute, update). Except in certain rare instances, agencies will find it necessary to document IT general controls. Many prevent controls are programmed controls residing in computer applications, and detect controls often rely on information produced by computers. Therefore, the documentation and evaluation of IT general controls is important because those controls provide a basis for concluding that prevent controls residing in computer applications continue to function over time and provide, in part, a basis to rely on the output from computerized applications (i.e., electronic evidence) used in the performance of detect controls.

Most prevent controls residing in computer applications should have been tested prior to implementation. If this is the case and the earlier tests results were retained (and IT General controls prove to be effective), assessment teams generally will be able to document the prevent controls without extensive additional effort.

Considerations for Documenting Controls

The assessment team’s documentation of controls should provide evidence that appropriate controls have been established and are effectively designed to prevent or detect errors of importance or fraud. It is recommended the documentation include a description of each control, including how the control is performed, who performs the control, what data reports, files, or other materials are used in performing the control, and what physical evidence, if any, is produced as a result of performing the control. This documentation will be helpful in subsequent

phases of the process, particularly in designing procedures to verify the operating effectiveness of those controls. In addition, this documentation will be useful in:

- Identifying whether controls have changed over time.
- Identifying situations where there is a potential lack of segregation of duties.
- Considering whether controls have been designed so that they are not easily overridden and, if they are overridden, whether policies and programs (e.g., fraud programs) exist to detect and report such overrides.

The following questions should be considered when documenting controls:

- How?
 - How is the control performed?
 - How does one know when the control is not working? (Be specific and include details of report names or systems used)
- What?
 - What does the control seek to do?
 - What is the frequency of the control (e.g. daily, annually)?
 - What is the evidence that the control is working?
- Who?
 - Who performs the control? (Use job titles)
 - Who performs the control in the person's absence?
- When?
 - When is the control performed? (Are there any dependencies which must be performed prior to the control operating? Can the control be bypassed and processing continues?)

Determining the “Right Combination of Controls”

A Top-Down, Risk-Based approach first considers entity-level controls and then transaction-level controls. When selecting the “right combination of controls”, agencies should select a combination of prevent and detect controls that were clearly understood and preliminarily evaluated to mitigate the risks for relevant financial statement assertions. When considering the “right combination of controls”, it is important to select those prevent and detect controls that are sufficiently sensitive by themselves or in combination with other controls to mitigate the risks of a material misstatement.

From a testing perspective, selecting the “right combination of controls” can be very important. Typically, manual prevent controls can be difficult to test because agencies will need to test a higher number of occurrences in order to determine that the controls operated effectively. However, when selecting controls to test, agencies should keep in mind that detect controls often work in combination with prevent controls to mitigate the risks of material misstatement (i.e., rely on the accuracy of underlying data, which is the result of effective prevent controls). Therefore, agencies need to test the most efficient combination of both prevent and detect controls, whether manual, IT-dependent manual, application or related IT general controls. Testing application controls, however, may be more efficient because agencies may only have to test a sample of one of each applicable transaction type to determine that they operated effectively, provided the agency can conclude that IT General Controls supporting the application controls are functioning effectively.

The level of financial reporting risk identified by management can have a direct influence on how persuasive the evidence needs to be for identified controls in each area. By using this top-down, risk-based approach, and identifying the “right combination of controls”, testing efforts can be varied to direct increased levels of testing to higher risk areas and related controls, thus reducing the need for more extensive testing and documentation of lower risk areas and related controls (see Chapter 7 – Testing Theory and Strategy for further discussion).

6.5 REVIEWING UNDERSTANDING WITH THE PROCESS OWNER

Once the assessment team has completed its detailed control evaluation, the results of the analysis should be reviewed with the process owner. The purpose of this review is two-fold:

1. To confirm that the assessment team’s understanding of the process and controls is accurate and complete.
2. To improve the process owner’s awareness and understanding of key risks and the effectiveness of the controls in reducing risk.

Depending on the process owner’s experience and perspective, it may be helpful for the assessment team to provide some general background on internal controls. The team should generally share flowcharts and control analyses with process owners, confirming the team’s understanding and discussing the team’s views on the effectiveness of the control system and opportunities for its improvement. The results of the meetings should be documented in the work papers, and any questions or issues arising from them resolved to the assessment team’s satisfaction.

6.6 WALKTHROUGHS

Perform Walkthroughs to Confirm Understanding of Process and Controls

A **walkthrough** traces one representative transaction through a process from beginning to end. It is recommended that the assessment team perform a walkthrough of each process in order to confirm the team’s understanding of the process and the related risks and controls. These walkthroughs should be performed from the point at which the major classes of transactions are initiated to the end of the recording process, to confirm (1) the understanding of the processing procedures, (2) the correctness of the information obtained about the relevant prevent and/or detect controls in the process, and (3) that these controls have, in fact, been placed in operation. For non-routine and estimation transactions, generally the assessment team can gain an understanding of the transaction, identify and understand controls, and conduct walkthroughs simultaneously.

A walkthrough is normally performed using documents that the assessment team believes are typical of the process being reviewed. It is recommended to perform a walkthrough for at least one transaction within each major class of transactions previously identified, unless additional walkthroughs are needed to confirm the assessment team’s understanding. When there have been significant changes in the process and/or the supporting computer applications during the period under evaluation, the assessment team should consider the need to walk through transactions that

were processed both before and after the change. The need to do this depends on the nature of the change and how it affects the likelihood of errors of importance or fraud in the related accounts.

During the walkthrough, the assessment team should question personnel at each point where important processing controls or procedures are prescribed (i.e., those most relevant to the accuracy of the financial statements). The questions should focus on the personnel's understanding of what is required and whether the processing procedures and controls are performed on a regular basis.

The assessment team may also attempt to corroborate information obtained at various points in the walkthrough by asking personnel to describe their understanding of the previous and succeeding processing or control activities and to demonstrate what they do. Furthermore, during the walkthrough it is recommended to attempt to identify exceptions to the prescribed processing procedures and controls as well as any differences between what the assessment team understands is required and what is actually done. If the control is an employee review, for example, and the employee is required to initial a document as evidence of having reviewed it, it is recommended to inquire about the nature of the review performed and ascertaining whether the documents subject to the walkthrough have been initialed by an appropriate employee. Furthermore, it is important to ask what the person does if the review process reveals an error or other discrepancy in the document, and if appropriate, examine documents where problems were detected to confirm that appropriate actions were taken. If the control consists of the preparation and analysis of a periodic reconciliation, it is recommended that one should:

- Review one or more of the reconciliations to determine whether all the relevant data are accurately and promptly included.
- Note the disposition of any unusual items.
- Inquire about the actions taken when the reconciliation reveals actual or potential errors.
- Inquire how the errors occurred.
- Whenever practicable, obtain evidence of the correction of the errors that were noted during the reconciliation process.
- Determine whether the reconciliation is performed by or relies on information processed by a computer system. If the reconciliation relies on an automated process, the agency should consider the results of procedures performed related to IT general controls.

In addition to walking through the physical flow of documents and forms, the assessment team should also follow the flow of data (flowchart) and information through the automated processes (at a system level, not a detailed logic level). These procedures may include inquiry of independent and knowledgeable personnel, review of user manuals, observation of a user processing transactions at a terminal in the case of an online application, and review of documentation such as output reports.

Performing Walkthroughs of IT General Controls

IT general controls are designed to (1) confirm that changes to applications are properly authorized, tested, and approved before they are implemented and (2) confirm that only authorized persons and applications have access to data, and then only to perform specifically defined functions (e.g., inquire, execute, update). The assessment team should perform walkthroughs of the IT general controls (or equivalent procedures) to confirm the team's

understanding of the IT general controls' design and determine that the controls have been placed in operation. In addition, the assessment team should also obtain evidence about whether the controls are operating as designed. The means of gathering evidence during the walkthroughs or equivalent procedures may include:

- Corroborating the understanding obtained from the IT process owner.
- Selecting an item over which the controls are designed to operate (e.g., a request for a program change) and inspecting evidence of the operation of the controls on that item.
- Using judgment to determine the adequacy of the evidence collected.
- Examining documentation of the control's design.
- Examining reports of key performance indicators or other information that is used to monitor the controls.
- Observing whether the IT process owner or others act upon the results of the controls.

Considerations for Documenting Walkthroughs

Walkthroughs of processes and the related controls are generally documented in brief memos describing the procedures performed by the assessment team to confirm its understanding of the process design and related controls and whether they have been placed in operation (refer to Appendix 6.3 for an example walkthrough).

6.7 CONTROLS RESIDING WITH A THIRD-PARTY SERVICE PROVIDER

Because agencies may use service organizations to hold assets, execute transactions and maintain related accountability, or record transactions and process related data, the assessment team may identify parts of the process and/or controls related to significant accounts or groups of accounts that are performed by service organizations. Additionally, because agencies use central management agencies to provide services that impact the agency's internal control environment, the assessment team may identify parts of the process and/or controls that are performed specifically by the central management agency as part of their services.

Determining Controls Residing Outside the Agency

Service Organizations are third-party service providers performing specific tasks or replacing entire business units or functions of an entity. Some examples of service organizations are:

- Payroll Services (ADP, Ceridian)
- Data Center Hosting (Cimco)

Central Management Agencies are agencies within the State of Georgia, providing services that impact other agencies' (user agencies) internal control environment. Typically, there are two main types of central management agencies:

- Agencies that assist other agencies with initiating, authorizing, recording, and processing transactions.
- Agencies that host or support other agencies' hardware and/or software.

An example of central management agencies would be the State Accounting Office. SAO is considered to be central management agencies because it provide services for other agencies that ultimately affect their internal control environment.

When determining the controls residing outside of the agency, it is important to inventory critical outsourced processes, applications, and IT systems. This inventory will act as a starting point in determining the amount of information needed from the specific service organization or central management agency. Refer to Appendix 6.5, for the third-party/central management agency service provider inventory template. This template will assist the agency in identifying these outsourced items. After the agency completes the inventory document of relevant third-party service organizations and central management agencies, the agency would need to understand how the relevant central management agencies' processes, applications, and systems are controlled. Additionally, the agency would need to understand how any relevant third-party service organizations control their processes, applications, and systems in order to determine if a SAS 70 is needed (refer to Evaluating Use of Work of Others section below for more information).

SAS 70, or Statement on Auditing Standards No. 70, established requirements for examinations of controls at Service Organizations that may be part of a User Organization's information system in the context of an audit of financial statements. In other words, SAS 70's should be performed for third-party service organizations that execute transactions and/or maintain accountability for clients, record transactions and process related data of clients, or develop and sell / lease software that processes transactions of financial significance.

SAS 70 reports consist of two types:

- Type I Report
 - Description of controls that may be relevant to a user organization in the context of a financial statement
 - Controls suitably designed to meet stated control objectives
 - Controls placed in operation (walkthroughs only)
 - Bridge to Type II report
- Type II Report
 - Controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified.
 - Should cover at least a six-month period
 - The as-of date should be sufficiently close to the user organization's year-end to provide assurance as to the effectiveness of controls at year-end.

Note: Type II reports are required in the majority of situations, as Type I reports do not include testing of operating effectiveness for the defined service organization controls.

Agencies should consider the following factors when determining the significance of the Service Organization:

- The nature and materiality of the transactions or accounts affected by the service organization.

- Even if not material to financial statements, the user agency may still need to gain an understanding of the nature of the processes in place at the service organization.
- The degree of interaction between internal control at the user agency and the controls of the service organization.
 - If the user agency has implemented effective internal control over the processing performed by the service organization, the user agency may not need to gain an understanding of the processes in place at the service organization.
- Determine if services provided by the service organization are significant to the user agency's internal control over financial reporting.

The user agency should first determine whether the user agency has implemented effective internal control over the processing performed by the service organization. In situations where this is the case, the assessment team may not need to gain an understanding of the flow of the transactions or the controls at the service organization because the agency has the ability to, and has, placed effective controls in operation (e.g., comparison of input to output).

When determining controls residing outside of the agency, but within the State of Georgia, it is important to maintain direct communication with the applicable central management agency to discuss scope and reliance of controls. It is important for the agency to determine all services that would be considered part of the user agency's transaction processing / information system, because these services would be included within the central management's scope of internal control testing. Additionally, the central management agency should prepare a description of all applicable controls with sufficient detail for the user agency to plan its own control approach, i.e., help the user agency determine what controls can be relied upon and what controls need to be independently tested.

Evaluating Use of Work of Others

When an agency uses a service organization, transactions that affect its financial statements are subjected to controls that are, at least in part, physically and operationally separate from the agency. The significance of the controls of the service organization to those of the agency depends on the nature of the services provided by the service organization, primarily the nature and materiality of the transactions it processes for the agency and the degree of interaction between its activities and those of the agency. In order for the agency to place effective controls over the service organization's activities into operation, the agency would need to gain an understanding of the flow of transactions and the controls at the service organization, as well as at the agency. For relevant third-party service organizations, the assessment team should obtain, read, and evaluate an appropriate service auditor's report (i.e., SAS 70 report) that describes the service organization's processes, identifies the related controls, including describing tests of their operating effectiveness performed by the service auditor, and specifies the period covered by the report. The agency should document its conclusions as to how the controls at the service organization support the relevant financial statement assertions (similar to how it documents other controls). In order to evaluate that the service organizations have effective internal control over the processing performed, the agency should obtain and review the applicable SAS 70.

The user organization (agency) should then evaluate the obtained SAS 70 for appropriateness. In order to properly evaluate the obtained SAS 70, the agency should complete the Reliance of the Work of Others – Third-Party Service Provider template (refer to Appendix 6.6) and look for the following in the report:

- Applications and locations covered by the report
- Flow of significant transactions through the service organization
- What could go wrongs (WCGWs)
- Description of controls
- Service auditor understanding of subject matter
- Timing of service auditor's report
- Service auditor's opinion
- Nature of exceptions noted

After the agency evaluates its third-party service organizations, they should then determine whether the agency has implemented effective internal control over the processing performed by the relevant central management agencies. In order to evaluate the internal controls of the central management agency, the user agency should obtain test results from the central management agency and map the central management agency's internal controls to the user agency's controls. After the user agency performs this mapping, they should determine if any additional controls may be needed at the user agency to achieve an appropriate level of control. Once the user agency determines that no additional controls are needed and that the central management agency has an effective internal control environment, the agency should then complete the Reliance of the Work of Others – Central Management Agency template (refer to Appendix 6.6). Once this template is completed, the agency can move on to finalizing the documentation of controls.

Note: All control testing documentation would include control activities, test results, and complimentary controls at the user organization. All exceptions noted (on the applicable SAS 70 for third-party service organizations or on the issue summary report for central management agencies) should be maintained and documented by the user agency and identified within their issue summary template (refer to Chapter 7 for more information on documenting issues).

7. TESTING THEORY AND STRATEGY

7.1 INTRODUCTION

The objectives in performing tests of controls generally include determining all of the following:

- The control is operating as understood and as designed.
- The control is operating throughout a period of time.
- The procedure is applied on a timely basis.
- The procedure is applied consistently, on all applicable transactions.
- Errors identified by a control are corrected.

Tests of controls are directed toward confirming that key controls operated in an effective manner, as designed, and consistently throughout the period under review. Controls should be tested by someone other than the individual who performs the control (process owner).

When testing controls, the following steps are performed:

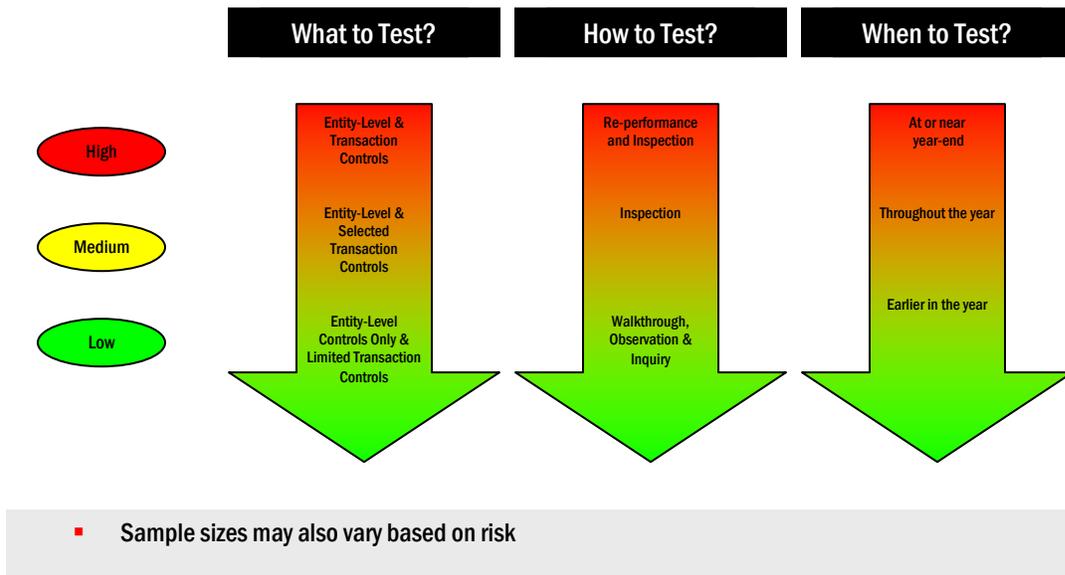
- Determine “**NET**” - the **nature, extent, and timing** of testing of key controls as part of the testing strategy.
- Execute tests of controls and document in the test plan and detailed work papers.
- Discuss and document any issues arising from testing and conclude on results.

7.2 DEVELOPING CONTROL TESTING STRATEGIES

The first step in developing the control testing strategy is to determine which controls to test. When selecting controls to test, the agency should consider which controls must operate together to mitigate those risks and whether each control needs to be tested or whether there is a primary control which should be tested. Note too, that each key control need not be tested *individually*, particularly if more than one control covers the same risk or if a single test can provide evidence with respect to more than one control. Redundant controls should be discussed further with management. Some level of redundant controls may be considered in the event that the originally tested control fails.

The level of identified risk will help influence the appropriate nature, timing and extent of the testing to be performed on identified controls. The control testing strategy is a critical step in the top-down, risk-based approach. The level of financial reporting risk identified by management can have a direct influence on how persuasive the evidence needs to be for testing identified controls in each area. As the risk associated with a control increases, management may need to obtain more persuasive evidence in support of their assessment. The persuasiveness of evidence is not only a function of the quantity of evidence generated, but of its quality. Quantity relates to the sample sizes, which can be varied based on risk when direct testing is performed. Quality of evidence is a function of many factors, including the objectivity and competence of those performing the control, nature of testing performed and time period covered. By using this top-down, risk-based approach, testing efforts can be varied to direct increased levels of testing to higher risk areas and related controls, thus reducing the need for more extensive testing and documentation of lower risk areas and related controls. This offers management an opportunity to adopt an effective testing strategy

that considers the benefits, costs and desired return. The graphic below illustrates how the testing strategy can be varied based on the outcome of the risk assessment.



To develop the testing strategy, the agency should consider “How to Test” (i.e. nature – “N”), “What to Test” (i.e. extent – “E”), and “When to Test” (i.e. timing – “T”). The nature of testing refers to how to test (i.e. the testing method that most effectively achieves the level of persuasiveness of evidence required to support management’s assessment). The extent of testing refers to how much to test and varies according to a variety of factors described in subsequent chapter sections. The timing of test of controls refers to when to test, depending on the nature of the control and the judgment required. Specific details on each of these concepts (NET) are described below.

It should be noted that professional literature provides a great deal of information on testing techniques. This guidance manual includes a limited discussion of key testing considerations as well as recommended practices. It assumes a basic familiarity with testing principles and statistical methods. If necessary, agency members should refer to other reference materials for a more thorough discussion of the underlying principles and related methods.

Determine “N”: Nature of Testing

Once the “right” combination of controls has been selected for testing, the second step in developing the control testing strategy is to determine the nature of testing.

The agency can choose from a variety of different and often complementary techniques in obtaining sufficient and competent evidence. These techniques are summarized below:

1. **REPERFORMANCE:** This test method refers to the repetition of a control performed by an employee or system and provides the strongest level of evidence that the control is operating effectively. It is the reperformance of a control using the original data to verify that the result or outcome mirrors the result of the original operation of the control. Reperformance is particularly useful in testing the accuracy of calculations or counts, but

is also useful in evaluating internal controls.

2. **INSPECTION AND EXAMINATION:** This technique involves inspecting documentation, records, or reports that provide evidence that the control has operated effectively. This may include counting securities or cash to verify existence and proper posting, or tracing certain amounts on reconciliations to gain assurance that they were actually performed.
3. **OBSERVATION:** Actual observation includes direct visual viewing of employees performing their work, as well as other facts and events. Although the tester must consider the impact of his or her presence, observation can provide important evidence that employees are properly trained and actually execute a process or control as designed.
4. **INQUIRY:** Employees, management, and third parties are asked about performance of procedures, controls, etc. A tester may ask who prepares a reconciliation, how often it is performed, and how corrections are made. Management may be asked how they verify that reconciliations are performed in an accurate and timely manner. Inquiry by itself is often less reliable than other forms of evidence, and may need to be used in combination with other testing techniques.
5. **ANALYTICAL REVIEW PROCEDURES:** This technique involves evaluations of financial and operational information made by a study and use of predictable relationships among data points. These procedures can also be used during the planning process to gain a better understanding of the specific account area.

Through earlier work in the assessment process, the tester will have conducted some testing of each key control, through inquiry, observation, and one or more walkthroughs. In determining the nature of testing to conduct at this stage, the tester must consider the evidence already gathered, the nature and importance of the control, and its objectives in further testing. In general, inquiry and observation do not provide sufficient evidence that a control operated consistently throughout a period of time. For most key controls, it will be appropriate to obtain additional evidence through inspection or reperformance.

In addition, the tester must consider the type of control being tested when considering the nature of testing to be performed. There are two basic types of controls: prevent and detect. Somewhat different testing considerations may apply to prevent than to detect controls.

Prevent Controls

In some cases, **prevent controls** will provide limited evidence indicating whether or not they were performed, by whom, or how well. In other cases, there will be evidence that a control was performed (e.g., a signature on a document), but the tester may need to test the validity of the data or reperform the checking routine involved to obtain sufficiently persuasive evidence that the control was effective.

Automated prevent controls often provide better evidence and are more easily tested than manual controls. In some cases, the tester may be able to rely on testing performed during

application or pre-implementation reviews; in others, reperformance of the control can be done efficiently using test transactions or other computer assisted techniques. An example of a prevent control is restricting user access to IT systems.

Detect Controls

In contrast, **detect controls** are usually supported by physical evidence of their performance, such as monthly reconciliations. The tester should examine evidence that the reconciliation was properly completed and that review and follow-up procedures were carried out.

Detect controls, which are generally applied to groups of transactions, are typically performed less frequently than prevent controls. A high degree of reliability can often be obtained by examining comparatively small amounts of evidence. An example of a detect control is performing a monthly bank reconciliation.

Determine “E”: Extent of Testing

The first step in determining the extent of testing has already been completed by identifying the “right” combination of controls to test (i.e. what combination of entity-level controls and transaction-level controls is appropriate based on the risk assessment). There are other factors to consider in determining the extent of testing as discussed below.

It is critical to note that judgment should be used to determine the extent of testing. At a high-level, the tester should consider the following factors in this determination:

1. The relative importance of the “key risk” question from the Risk and Control Matrix, considering transaction volumes and materiality, transaction complexity, regulatory and statutory considerations, and other factors that the tester may determine to be relevant.
2. How often the control is performed. Fewer monthly reconciliations need to be tested than a control applied separately to each transaction. For a monthly control, it may be sufficient to perform a detailed test of one month and a review of documentation for other months for any unusual issues and evidence the control was applied.
3. Persuasiveness of the evidence produced by the control. If it can be determined with direct evidence that the control was in effect, fewer items may need to be tested.
4. The need to be satisfied that the control operated as intended throughout the period of reliance. When the tester needs to gain assurance that the control operated over a longer period of time, the tester may need observations and evidence produced at different times throughout the period.
5. The purpose of the test. If the primary purpose of the test is to detect errors and the tester expects the population to be nearly error-free, sample sizes will be based on an expected error rate of zero and will generally be small. If the primary purpose to estimate the extent of errors with greater precision, sample sizes will be larger. As an example, for controls where the number of occurrences ranges from 50 to 250 during the

year, the minimum sample size is approximately 10% of the number of occurrences. As such, the sample size typically seen for a manual control performed daily is 25.

6. Other factors that relate to the effective operation of the control. These include the competence of the person performing the control, the quality of the control environment, changes in the system of controls during the period, and unexplained variances and fluctuations in related accounts.

Use of Sampling

Sampling is a broad term that refers to the application of a procedure to less than 100 percent of a total population (total population being either all items within an account balance or class of transactions) for the purpose of evaluating some characteristic of the balance or class. Sampling may be **statistical** or **nonstatistical**. Conceptually, the same principles apply in either case; the tester must exercise judgment in planning, performing and evaluating a sample and in relating the results from the sample to other evidential matter in forming a conclusion.

For each test, the tester has two initial decisions to make in considering sampling:

1. Is sampling an appropriate strategy?
2. If so, should the sampling be statistical or nonstatistical?

The use of sampling (statistical or nonstatistical) is not required by professional standards or this methodology. However, it is generally the most efficient approach to gathering sufficient, competent evidence about populations where extended testing is needed and 100% testing is not appropriate.

Sampling carries an inherent risk (often referred to as sampling risk) that the tester may reach a different conclusion than would result from testing every item. This risk is inversely related to the size of the sample.

Statistical vs. Nonstatistical Sampling

As noted above, both methods are fundamentally similar in principle and in the steps followed. They differ in that statistical sampling requires the tester to quantify certain factors and to select items randomly; in turn, statistical sampling allows the tester to express the results quantitatively and to measure and manage sampling risk quantitatively as well.

Nonstatistical sampling uses samples which are selected either informally (i.e., without conscious bias in selection) or judgmentally (i.e., the tester decides which items to select based on judgment as to their relevance to the test objective). Results of nonstatistical sampling are not measurable with respect to precision and confidence, although informal samples may be evaluated as though they were randomly selected.

In general, the recommended practice is to use statistical methods for sampling whenever practical to do so. Although the tester should use his or her judgment as to the most cost-effective testing strategy in each instance, **statistical sampling** should be used when:

- The population of items is large (greater than 500 items, for example).
- Measurability of precision and confidence level are required or desired to extend results to the whole population (e.g., in order to estimate the financial impacts of a control weakness).
- The individual sampling unit and sampling “frame” (or representation of the population, such as a listing, file drawer, etc.) can be defined.
- Random selection of test items is practical (i.e., every item must have an equal or calculable chance of selection).

Conversely, **nonstatistical sampling** may be preferable if:

- The population is small (less than 500 items).
- Measurability is not required or desired.
- Other evidence indicates that errors are highly unlikely or the tester has prior information as to which items are likely to be erroneous.
- Definition of a suitable frame is impractical.

In some cases, it may be useful to combine statistical sampling with either nonstatistical sampling or 100% testing. For example, if the tester expects more errors or higher risk in one subset of the population, he or she might judgmentally sample that portion and use statistical methods to test the rest.

General Steps in Sampling

The following steps should be followed in the design and execution of testing using samples, whether statistical or nonstatistical:

- Step 1: **DETERMINE THE OBJECTIVE OF THE TEST.** The objective of every extended test must be clearly specified.
- Step 2: **DEFINE THE POPULATION.** The population defined by the tester must include all items that are related to the objective of the test. The population is made up of individual sampling units that may be individual transactions, documents, customer or vendor balances, or an individual entry. The tester must consider the objective of the test (what am I going to test?) and, secondarily, the efficiency of the test (how are the records maintained?) when defining the sampling unit. In general, a more elementary sampling unit will produce more reliable test results.

The **sampling frame** is a representation of the whole population as defined for purposes of the test. It may be, for example, a listing of all items, a file drawer of documents, or a computer data file. The sample results may only be projected to the frame from which the sample was selected. If the frame differs from the

population (intentionally, as a result of stratification, or unintentionally), test results will be meaningful only for the frame tested. In addition, the sampling frame should be complete in all respects and consistent with the objective of the test. For example, if the tester is concerned with all cash disbursements made during a period, the sampling frame should also include all canceled checks from the period rather than just recorded disbursements.

Step 3: CHOOSE A SAMPLING TECHNIQUE. As discussed above, the tester must initially determine whether a nonstatistical or statistical sampling approach will be used for the test. A variety of specific sampling techniques are available to support tests of controls.

Step 4: DETERMINE THE SAMPLE SIZE. Judgment is necessary in determining the sample size. The decision process for determining the sample size is similar for both statistical and nonstatistical sampling. In statistical sampling, the tester will quantify the relevant factors; in nonstatistical sampling, the factors will be described in a less structured manner.

Sample size is a function of the variability of the population (expressed as an expected error rate in certain sampling techniques), the acceptable level of risk (i.e., reliability or confidence level), the level of tolerable error, and the population size (refer to Appendix 7.1 for detail on Determining Factors for Sample Size).

Below is table describing OSC recommended sample sizes which can be used based on level of risk:

Frequency of Control	Estimated Population	Range of Sample Size	Risk		
			Low	Medium	High
More than daily	More than 250	25-40	25	30	40
Daily	61-250	15-25	15	20	25
Weekly	40-60	5-10	5	7	10
Bi-Weekly	20-30	3-7	3	5	7
Monthly	12	2-4	2	3	4
Quarterly	4	2	2	2	2
Annually	1	1	1	1	1
Automated	N/A	1	1	1	1

Refer to Appendix 7.2 for further detail on sample size guidance.

Step 5: DETERMINE THE METHOD OF SELECTING THE SAMPLE. The tester's objective is to select a sample that can be expected to be representative of all items in the population. For a sample to be statistically valid, sampling units must be selected from the defined population so that each sampling unit has an equal (or calculable) chance of being selected.

- Step 6: **PERFORM THE SAMPLING PLAN.** Once the sample has been selected, the tester should perform the test, applying appropriate procedures.
- Step 7: **EVALUATE THE SAMPLE RESULTS.** After the sample units have been tested, the sample results should be evaluated to determine whether the controls operated effectively.
- Step 8: **DOCUMENT THE SAMPLING PROCEDURES.** Sampling procedures should be documented in workpapers.

Determine “T”: Timing of Testing

The period of time over which controls should be evaluated is a matter of the tester’s judgment. However, it should vary with the nature of the controls being evaluated, the frequency with which specific controls operate and the specific policies that are applied. Some controls operate continuously, while others operate only at certain times. The tester should evaluate controls over a period of time that is adequate to determine whether the controls are operating effectively.

Management has the flexibility to test controls during the year, and to perform update testing if necessary at year-end based on consideration of the risk of control failure and risk that a material misstatement will occur in the event of a control failure. Ongoing monitoring assists in determining that controls continue to function effectively even though time has passed since the controls were subject to direct testing. The timing and frequency of the direct testing should reflect the risks associated with the significant account and related assertions and the risk associated with the controls, the influence of entity-level controls, and the strength of ongoing monitoring procedures and the evidence they provided.

7.3 DOCUMENTING TESTING

As can be seen from the preceding material in this chapter, testing requires the tester to make thoughtful decisions and judgments. In general, documentation of testing must be sufficient to achieve two purposes:

- Guiding those performing testing in the execution of the test procedures.
- Providing an adequate record of the tester’s work in planning, performing, and evaluating the tests for subsequent use including management’s overall assessment of internal control over financial reporting.

To guide the tester in conducting testing, a test plan should be prepared prior to test execution, although test plans may be revised as needed to reflect any changes in test plans that prove necessary. The tester should develop test plans specifically for each process. Test plans should provide enough detail to guide the execution of the test, without necessarily containing all of the detailed information used in planning the test (e.g., considerations of tolerable error, expected error, reliability level, and other determinants of sample size).

A test plan should be created for each process. The test plan should be organized to make test execution as efficient as possible, so that tests related to a common sample are grouped together, for example. As tests are completed, results should be recorded on the test program by individuals and cross-referenced to test leadsheets or to other detailed test documentation elsewhere in the workpapers. The elements of a test plan include:

- Objectives of the test
- Source of sample (reports or data) used – source documents include specific reports used to perform the testing, including a description of the sampled items (e.g., “select aged items over 30 days from the monthly accounts receivable aging report). Also, it is beneficial to include the contact name for obtaining the information.
- Time period subject to sampling – identify the period of time over which the sample size is selected (e.g. last three months).
- Population – determine the population size for the time period being sampled. This documents the number of transactions where the control should have occurred. When the population consists of different transaction types, it may be appropriate to describe the risk characteristics of each type to help determine the sampling strategy.
- Sample approach to be applied – sample size, sampling method, strategy or source of sample, relevant population information to describe the population and its risk characteristics. Is the population comprised of one transaction type, or several types? If more than one transaction, is each type subjected to the same control procedure? If not, this impacts whether you may need two samples or one.
- Test Attributes– identify the specific attributes or characteristics of the items selected (i.e., aged items older than 30 days). It is important to keep the project scope in mind when selecting attributes for testing so that only attributes relevant to the scope are tested. Frequently, there are other attributes that could be tested, but are unrelated to the risks included in your scope.

Preparation and completion of the test plans are the responsibility of the tester, with the guidance and active participation of the assessment team. When testing must address some unusual or difficult issues, the assessment team should guide the tester in selecting an appropriate testing approach.

Before the tester completes the extended testing phase, the assessment team should carefully review the test plans again to make sure that all necessary tests have been appropriately completed and that all objectives for testing have been achieved.

Test plans may be discussed with the responsible process owner after the test plans have been prepared, and before commencing testing. This will increase process owners’ buy-in to the testing phase and may identify controls that the process owners know will fail the testing phase. These tests can be recorded as having failed testing and remediation actions agreed without the tests having been performed. This will save a significant amount of time in the testing phase and enable remediated controls to be designed more quickly. Refer to Appendix 7.3 for an example test plan template.

In addition, a testing leadsheet and testing summary may also be created for each control being tested. The testing leadsheet serves as the workpaper to evidence testing performed for each control. There can be one testing leadsheet for each control or, if testing procedures can be combined, one testing leadsheet can include multiple controls. The testing summary serves to

assist the process owner in monitoring the controls to be tested and which controls have been tested to date. There can be one testing summary for each significant process. The testing summary can be included on the test plan (refer to Appendix 7.3).

The following is specific information that may be included on the testing leadsheet before the test is performed:

- Control reference, description, and process in which control resides
- Test strategy (i.e., “Examination of Evidence”, “Reperformance”, etc.)
- A detailed description of the test procedures performed and attributes tested
- Period from which the sample has been chosen
- Sample size and the rationale behind the determination of this figure, along with a justification of the risk assessment
- Sample selection method

The following is specific information that may be included on the testing leadsheet after the test is performed:

- Evidence obtained from testing (i.e., source test documents)
- Details of any exceptions identified
- Root cause analysis of exceptions identified
- Conclusion
- Review and sign off

Refer to Appendix 7.4 for an example testing leadsheet.

To aid in obtaining the necessary source documents in order to test controls, a document request template can assist in gathering information. This request can be sent to the necessary process owners to obtain requested evidence. Refer to Appendix 7.5 for a document request template.

Documentation Standards

Workpapers can be utilized to document the evidence of the work performed. Workpapers should be designed so that someone with minimal knowledge of the process can follow the work performed.

The objectives of workpapers are to:

- Provide the principal support for observations and conclusions.
- Document the planning, performance, and review of work.
- Document whether the objectives and scope were achieved.
- Provide support for the work procedures.

Workpaper Elements

Typically, workpapers contain standard elements which are discussed further below:

Heading

Each workpaper should include a heading, consisting of the name of the organization or activity being examined, the title or description of the area, and date or period covered by the project.

Example: Department of XXX
 Purchase to Pay
 06/30/XX

Cross-Referencing

Cross-referencing on manual workpapers is used to agree a specific number or fact to another workpaper. Cross-referencing is used to make sure:

- The information on one workpaper agrees with another workpaper.
- Each test procedure was performed and documented.

Cross-referencing is done by indicating the workpaper reference of the relating workpapers next to the information being cross-referenced. Cross-referencing should only be done for key information within workpapers.

Source

The source of the information should always be indicated. In many cases, this will become key to facilitate future follow-up of assessments. For example:

Source: Jane Doe, Senior Vice President

Purpose

Each workpaper should include its nature or purpose. This provides the reviewer with an understanding as to the purpose of the workpaper.

Sign-Off

Each working paper should be signed (or initialed) and dated by the individual preparing the workpapers. The tester, if applicable, should also initial and date the workpapers reviewed. In cases where subsequent adjustments are made, additional sign-offs may be made.

Tickmarks

Testing results should be shown in a standard manner to allow further review and analysis. Generally, this can be completed by using standard tickmarks. Each workpaper should have a legend indicating the tickmarks used and the related meaning. In the legend, be specific when defining the tickmarks being used. For example, “Agreed to supporting documentation” is not specific enough. A better tickmark would be, “Agreed to Report XX, which was generated from System X on xx/xx/xx.”

Evidence of Work Performed

The workpapers should record the information obtained, the analyses made and the conclusion reached. The documentation can take several forms. It may include an attribute worksheet (i.e. testing leadsheet) which indicates the testing performed in the columns and the items tested in the rows. It may consist of an observation or scanning memo which indicates the work

performed but does not detail the items. For example, if the tester reviewed all expense accounts for the first quarter of the year for unusual expenses, it is not necessary to detail every expense account reviewed. It is necessary to indicate clearly the scope of the documentation reviewed and any exceptions.

Statements necessary to summarize the nature and extent of work performed should be consistent with the objectives of the workstep. For example:

- “Based on testing performed to validate the existence and accuracy of [ABC process], we noted no exceptions.”
- “We selected 25 invoices out of 1,000 prepared for fiscal year 20XX and noted no exceptions with respect to the procurement process.”

The workpaper should provide enough documentation for a third party to reconstruct the work performed.

Conclusions

A conclusion should be documented on each workpaper based on testing results and/or work performed. The conclusion should be designed so that someone with minimal knowledge of the process can arrive at the same results.

Types of Workpapers

Workpapers may be electronically or manually prepared. In either case, they can consist of flowcharts, process models, and Word or Excel documents.

7.4 EVALUATING RESULTS

The tester should evaluate the results of each test against its objectives. If control exceptions have been found (that is, instances in the sample where the control was not applied as intended), each one should be investigated regardless of sample size. It is important to note that once an exception has been identified, it is critical to gain an understanding of the nature of the exception to help determine the root cause. Factors to consider when gaining an understanding of the exception include:

- Is the exception systematic or a one time occurrence? For example, is the open purchase order report missing approval because the purchasing manager forgot to evidence the approval or because the purchasing manager is new and does not know the need to review and approve the open purchase order report?
- Does the control exception apply to the whole population or particular segments? For example, particular locations or departments do not document the goods received from suppliers.
- When did the exception occur (e.g., during the year or 13th month)?
- Is the control exception one of performance or documentation (e.g., the purchasing manager reviews the changes to the vendor master list but does not evidence approval of the report)?

The tester must be very careful not to dismiss exceptions as random or unique occurrences. With the small sample sizes typically used for tests of controls, every exception must be considered important.

If the tester is satisfied with the results of the test, no further testing should be required to assess the control as effective. “Effective” implies that the internal controls exist that would prevent or detect a control weaknesses in a timely period by employees in the normal course of performing their assigned functions.

If the test does not achieve the desired objectives several options exist:

- Extend testing (in anticipation of not finding another control exception) – In some cases, it may be appropriate to extend testing at the request of management as to the extent and impact of an error. This should be done sparingly and only after prior discussion with the assessment team. Note that, when statistically valid tests have been performed, the tester should be able to project error rates or balances with sufficient accuracy for management. The tester should always document discussions with management of matters arising from testing.
- Consider whether a compensating control is available to test. If another control (or group of controls) can be identified that achieves the same control objective, it should be tested even if not previously considered key.
- Deem the control ineffective. If other controls do not achieve the same objective, the tester should consider the need for procedures to determine or quantify the impact of the exception.
- Consider control remediation and retest the control. Depending on the timing of when the control exception was identified, there may be time to remediate the control and retest in order to achieve a clean sample.

Once control exceptions have been confirmed, they should be clearly documented and communicated to management.

7.5 COMMUNICATING RESULTS

Communicating Exceptions

As in every phase of the IMPROVE Program, the tester should promptly review results of the testing work and communicate to management. This is particularly important when exceptions have been found, both to inform management of the potential issues and to direct the tester in considering any factors which might help in evaluating the error.

The tester should use an Issue Summary Template to document control exceptions. The template should include the following information:

- Finding or observation
- Implication of the control exception
- Recommendation for improvement or remediation plan
- Management’s response to the control exception and recommendations

See Appendix 7.6 for an issue summary template.

Once testing is completed, it is recommended that the tests hold a closing meeting to review all open findings with management and the assessment team to reach final agreements on issues, and obtain management action plans for all control issues that may be documented in management's assessment.

Issues raised in testing – whether related to ineffective operation of controls or misstatement of balances – are often significant and should be discussed on a timely basis.

Identifying Matters for Improvement

Over the course of the evaluation process, it is likely the agency will identify areas where controls may require modification or where the assessment team determines certain processes require control enhancements to respond to new services or emerging risks. The agency might also identify areas where automating manual controls may improve both efficiency and compliance with management's policies or areas where the agency's evaluation of processes and controls identify redundant controls or other procedures that are no longer necessary. The agency should consider the concept of reasonable assurance when evaluating whether suggested improvements should be implemented.

8. FRAUD CONCEPTS

8.1 INTRODUCTION

The importance of fraud should be a factor in planning, executing, and evaluating the assessment of the internal control program. Elements of an anti-fraud program include: setting the proper tone within the organization, proactively identifying fraud risks and monitoring internal controls to prevent or detect fraud, and establishing reactive protocols in the event that fraud is suspected.

The risk of fraud can be reduced through a combination of prevention, deterrence, and detection measures. However, fraud can be difficult to detect because it often involves concealment through falsification of documents or collusion among management, employees, or third parties. Therefore, it is important to place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals not to commit fraud because of the likelihood of detection and punishment. Moreover, prevention and deterrence measures are much less costly than the time and expense required for fraud detection and investigation.

An agency's management has both the responsibility and the means to implement measures to reduce the incidence of fraud. The measures an organization takes to prevent and deter fraud also can help create a positive workplace environment that can enhance the agency's ability to recruit and retain high-quality employees.

Through documentation of processes and controls as well as test of controls, evidence should be provided that appropriate controls have been established and are effectively designed to prevent or detect errors of importance or fraud. Specifically, management should consider whether its controls sufficiently address identified risks of material misstatement due to fraud and the risk of management override of other controls. Controls that might address these risks include:

- Controls over significant, unusual transactions, particularly those that result in late or unusual journal entries;
- Controls over journal entries and adjustments made in the 13th month financial reporting process;
- Controls over related party transactions;
- Controls related to significant management estimates; and
- Controls that mitigate incentives for, and pressures on, management to falsify or inappropriately manage financial results.

As such, management's evaluation of the risk of misstatement should include consideration of the vulnerability of the agency to fraudulent activity (e.g., fraudulent financial reporting, misappropriation of assets and corruption, and whether any such exposure could result in a material misstatement of the financial statements).

8.2 FRAUD DEFINED

Misstatements in the financial statements can arise from fraud or error. The distinguishing factor between fraud and error is whether the underlying action that results in the misstatement of the financial statements is intentional or unintentional.

The term “fraud,” according to Statement on Auditing Standards (SAS) 99, *Consideration of Fraud in a Financial Statement Audit*, is defined as an intentional act performed by one or more individuals among management, employees, or third parties that result in a material misstatement in the financial statements that are the subject of an audit. Although fraud is a broad legal concept, an internal control framework is established to help prevent or detect fraud that may cause a material misstatement in the financial statements. Fraud involving one or more members of management or those charged with governance is referred to as “management fraud;” fraud involving only employees of an organization is referred to as “employee fraud.” In either case, there may be collusion within an organization or with third parties outside of an organization.

The term “error” refers to an unintentional misstatement in financial statements, including the omission of an amount or a disclosure, such as the following:

- A mistake in gathering or processing data from which financial statements are prepared.
- An incorrect accounting estimate arising from oversight or misinterpretation of facts.
- A mistake in the application of accounting principles relating to measurement, recognition, classification, presentation or disclosure.

Types of Fraud

The two primary types of intentional misstatements relevant to an internal control framework are misstatements resulting from misappropriation of assets and misstatements resulting from fraudulent financial reporting. Corruption is sometimes described as a third type of fraud to highlight the abusing influence and power within an organization to obtain a benefit at an organization’s expense. Examples might include kickbacks or conflicts of interest.

Misappropriation of assets involves the theft of an agency’s assets and is often perpetrated by employees in relatively small and immaterial amounts. However, it can also involve management who are usually more able to disguise or conceal misappropriations in ways that are difficult to detect. Misappropriation of assets can be accomplished in a variety of ways including:

- Embezzling cash receipts (for example, misappropriating collections on accounts receivable or diverting receipts in respect of written-off accounts to personal bank accounts).
- Stealing physical assets or intellectual property (for example, stealing inventory for personal use or for sale, stealing scrap for resale, colluding with a competitor by disclosing technological data in return for payment).
- Causing an agency to pay for goods and services not received (for example, payments to fictitious vendors, kickbacks paid by vendors to the agency’s purchasing agents in return for inflating prices, payments to fictitious employees).
- Using an agency’s assets for personal use (for example, using the agency’s assets as collateral for a personal loan or a loan to a related party).

Misappropriation of assets is often accompanied by false or misleading records or documents in order to conceal the fact that the assets are missing or have been pledged without proper authorization.

Fraudulent financial reporting involves intentional misstatements including omissions of amounts or disclosures in financial statements to deceive financial statement users. Fraudulent financial reporting may be accomplished by the following:

- Manipulation, falsification (including forgery), or alteration of accounting records or supporting documentation from which the financial statements are prepared.
- Misrepresentation in, or intentional omission from, the financial statements of events, transactions or other significant information.
- Intentional misapplication of accounting principles relating to amounts, classification, manner of presentation, or disclosure.

Fraudulent financial reporting often involves management override of controls that otherwise may appear to be operating effectively. Fraud can be committed by management overriding controls using such techniques as:

- Recording fictitious journal entries, particularly close to the end of an accounting period, to manipulate operating results or achieve other objectives;
- Inappropriately adjusting assumptions and changing judgments used to estimate account balances;
- Omitting, advancing or delaying recognition in the financial statements of events and transactions that have occurred during the reporting period;
- Concealing, or not disclosing, facts that could affect the amounts recorded in the financial statements;
- Engaging in complex transactions that are structured to misrepresent the financial position or financial performance of the agency; and
- Altering records and terms related to significant and unusual transactions.

8.3 WHO COMMITS FRAUD AND WHY IS FRAUD COMMITTED

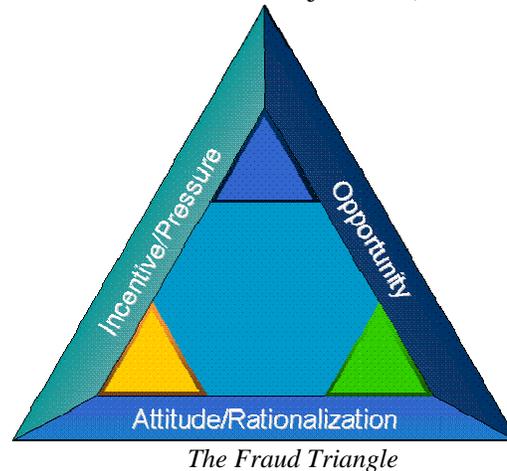
Fraud can occur at any level of the organization. Management might commit fraud via manipulation of the accounting records. Management fraud is typically committed through fraudulent financial reporting. Employees might commit fraud by stealing an organization's assets such as cash, inventory, etc. Employee fraud is fraud perpetrated by employees against the organization.

The Fraud Triangle

The fraud triangle concept is relevant in identifying and understanding the importance of fraud risk factors that may be present. The three conditions typically present when fraud exists are:

- Incentives or pressures on management to perpetrate fraud to achieve desired financial results.
- Opportunity (i.e., control weaknesses) to carry out fraud without being detected.

- Attitude of personnel who are able to rationalize to themselves a need for the fraud (i.e., they convince themselves that the fraud is justified).



Fraud involves incentive or pressure to commit fraud, a perceived opportunity to do so and some rationalization of the act. Individuals may have an incentive to misappropriate assets, for example, because the individuals are living beyond their means. Fraudulent financial reporting may be committed because management is under pressure, from sources outside or inside the agency, to achieve an expected (and perhaps unrealistic) earnings or operational target – particularly since the consequences to management for failing to meet financial or operating goals can be significant. A perceived opportunity for fraudulent financial reporting or misappropriation of assets may exist when an individual believes internal control can be overridden, for example, because the individual is in a position of trust or has knowledge of specific weaknesses in internal control. Individuals may be able to rationalize committing a fraudulent act. Some individuals possess an attitude, character or set of ethical values that allow them knowingly and intentionally to commit a dishonest act. However, even otherwise honest individuals can commit fraud in an environment that imposes sufficient pressure on them.

It is important to be aware of the incentives or pressures that might lead someone to commit fraud and be alert for indication(s) for potential fraudulent activity. The likelihood of fraud increases when one or more fraud risks have been identified, particularly in an environment where significant pressure exists to meet financial or operational targets. Identifying one or more fraud risk factors does not necessarily mean that internal control at the agency level is ineffective. However, the presence of numerous fraud risk factors should heighten awareness. Particular attention should be paid to risk factors relating to attitudes of management or oversight boards, or opportunities resulting from inappropriate attention to, or disregard for, internal control.

8.4 RESPONSIBILITY TO DETECT FRAUD AND DEVELOPING AN APPROPRIATE OVERSIGHT PROCESS

Responsibility to Detect Fraud / Oversight Process

The primary responsibility for the prevention and detection of fraud rests with both those charged with governance of the agency and with management. The respective responsibilities of those charged with governance and of management may vary by agency. In some entities, the

governance structure may be more informal as those charged with governance may be the same individuals as management of the agency.

It is important that management, with the oversight of those charged with governance, place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals not to commit fraud because of the likelihood of detection and punishment. This involves a culture of honesty and ethical behavior. Such a culture, based on a strong set of core values, is communicated and demonstrated by management and by those charged with governance. It provides the foundation for employees as to how the agency conducts its business. Creating a culture of honesty and ethical behavior includes setting the proper tone; creating a positive workplace environment; hiring, training and promoting appropriate employees; requiring periodic confirmation by employees of their responsibilities; and taking appropriate action in response to actual, suspected or alleged fraud.

Setting the Tone at the Top

Directors and officers of agencies set the “tone at the top” for ethical behavior within any organization. Research in moral development strongly suggests that honesty can best be reinforced when a proper example is set. The management of an agency cannot act one way and expect others in the agency to behave differently.

Creating a Positive Workplace Environment

Research results indicate that wrongdoing occurs less frequently when employees have positive feelings about an employer than when they feel abused, threatened, or ignored. Without a positive workplace environment, there are more opportunities for poor employee morale, which can affect an employee’s attitude about committing fraud against an employer.

Employees should be empowered to help create a positive workplace environment and support the agency’s values and code of conduct. They should be given the opportunity to provide input to the development and updating of the agency’s code of conduct, to make certain that it is relevant, clear, and fair. Involving employees in this fashion may also effectively contribute to the oversight of the agency’s code of conduct and an environment of ethical behavior.

Employees should be given the means to obtain advice internally before making decisions that appear to have significant legal or ethical implications. They should also be encouraged and given the means to communicate concerns, anonymously if preferred, about potential violations of the agency’s code of conduct, without fear of retribution. Many organizations have implemented a process for employees to report on a confidential basis any actual or suspected wrongdoing, or potential violations of the code of conduct or ethics policy. For example, some organizations use a telephone “hotline” that is directed to or monitored by an ethics officer, fraud officer, general counsel, internal audit director, or another trusted individual responsible for investigating and reporting incidents of fraud or illegal acts.

Hiring, Training and Promoting Appropriate Employees

Each employee has a unique set of values and personal code of ethics. When faced with sufficient pressure and a perceived opportunity, some employees will behave dishonestly rather than face the negative consequences of honest behavior. The threshold at which dishonest

behavior starts, however, will vary among individuals. If an agency is to be successful in preventing fraud, it must have effective policies that minimize the chance of hiring or promoting individuals with low levels of honesty, especially for positions of trust.

Confirmation

Management needs to clearly articulate that all employees will be held accountable to act within the agency's code of conduct. All employees within senior management and the finance function, as well as other employees in areas that might be exposed to unethical behavior (for example, procurement, sales and marketing) should be required to sign a code of conduct statement annually, at a minimum.

Requiring periodic confirmation by employees of their responsibilities will not only reinforce the policy but may also deter individuals from committing fraud and other violations and might identify problems before they become significant. Such confirmation may include statements that the individual understands the agency's expectations, has complied with the code of conduct, and is not aware of any violations of the code of conduct other than those the individual lists in his or her response. Although people with low integrity may not hesitate to sign a false confirmation, most people will want to avoid making a false statement in writing. Honest individuals are more likely to return their confirmations and to disclose what they know (including any conflicts of interest or other personal exceptions to the code of conduct). Thorough follow-up by internal auditors or others regarding non-replies may uncover significant issues.

Discipline

The way an agency reacts to incidents of alleged or suspected fraud will send a strong deterrent message throughout the agency, helping to reduce the number of future occurrences. The following actions should be taken in response to an alleged incident of fraud:

- A thorough investigation of the incident should be conducted.
- Appropriate and consistent actions should be taken against violators.
- Relevant controls should be assessed and improved.
- Communication and training should occur to reinforce the agency's values, code of conduct, and expectations.

Expectations about the consequences of committing fraud must be clearly communicated throughout the agency. For example, a strong statement from management that dishonest actions will not be tolerated, and that violators may be terminated and referred to the appropriate authorities, clearly establishes consequences and can be a valuable deterrent to wrongdoing. If wrongdoing occurs and an employee is disciplined, it can be helpful to communicate that fact anonymously in an employee newsletter or other regular communication to employees. Seeing that other people have been disciplined for wrongdoing can be an effective deterrent, increasing the perceived likelihood of violators being caught and punished. It also can demonstrate that the agency is committed to an environment of high ethical standards and integrity.

Evaluate Antifraud Processes and Controls

Neither fraudulent financial reporting nor misappropriation of assets can occur without a perceived opportunity to commit and conceal the act. Organizations should be proactive in reducing fraud

opportunities by (1) identifying and measuring fraud risks, and (2) implementing and monitoring appropriate prevent and detect internal controls and other deterrent measures.

Identifying and Measuring Fraud Risks

Management has primary responsibility for establishing and monitoring all aspects of the agency's fraud risk assessment and prevention activities. Fraud risks often are considered as part of an enterprise-wide risk management program, though they may be addressed separately. The fraud risk assessment process should consider the vulnerability of the agency to fraudulent activity (fraudulent financial reporting, misappropriation of assets, and corruption) and whether any of those exposures could result in a material misstatement of the financial statements or material loss to the organization. In identifying risks, organizations should consider organizational and industry-specific characteristics that influence the risk of fraud.

The nature and extent of management's risk assessment activities should be proportionate to the size of the agency and complexity of its operations. For example, the risk assessment process is likely to be less formal and less structured in smaller entities. However, management should recognize that fraud can occur in organizations of any size or type, and that almost any employee may be capable of committing fraud given the right set of circumstances. Accordingly, management should develop a heightened "fraud awareness" and an appropriate fraud risk management program, with oversight from an appropriate governing body.

Implementing and Monitoring Appropriate Internal Controls

Some risks are inherent in the environment of the agency, but most can be addressed with an appropriate system of internal control. Once a fraud risk assessment has occurred, the agency can identify the processes, controls, and other procedures that are needed to mitigate the identified risks. Effective internal control will include a well-developed control environment, an effective and secure information system, and appropriate control and monitoring activities. Because of the importance of information technology in supporting operations and the processing of transactions, management also needs to implement and maintain appropriate controls, whether automated or manual, over computer-generated information.

In particular, management should evaluate whether appropriate internal controls have been implemented in any areas management has identified as posing a higher risk of fraudulent activity, as well as controls over the agency's financial reporting process.

8.5 OTHER RESOURCES

To obtain more information on fraud and implementing antifraud programs and controls, please go to the following Web sites where additional materials, guidance, and tools can be found:

American Institute of Certified Public Accountants - www.aicpa.org

Association of Certified Fraud Examiners - www.cfenet.com

Financial Executives International - www.fei.org

Government Accounting Standards Board - www.gasb.org

Government Finance Officers Association - www.gfoa.org

Information Systems Audit and Control Association - www.isaca.org

The Institute of Internal Auditors - www.theiia.org

9. CONCLUSION

9.1 IMPROVE PROGRAM

Effective internal controls are the foundation for managing risk and creating a safe and sound operating environment. The IMPROVE Program was created to establish adequate internal control and to increase fiscal accountability within State government.

Under the IMPROVE Program, each agency is required to perform an annual assessment of internal control over financial reporting. By performing this assessment, agencies can identify risks and compensating controls that reduce the possibility of material misstatements and misappropriation of assets. The assessment will also indicate opportunities for increased efficiency and control effectiveness in agency processes and operations.

10.2 CONTACT INFORMATION

For further information on the IMPROVE Program or for assistance, agencies may use the following resources:

IMPROVE Program Website through SAO:

http://sao.georgia.gov/00/channel_createdate/0,2095,39779022_161308762,00.html

APPENDICES

- 4.1 [Materiality Template](#)
- 4.2 [Risk Assessment Templates](#)
- 5.1 [IT General Controls Normative Model](#)
- 5.2 [End-User Computing Controls](#)
- 6.1 [Narrative Example](#)
- 6.2 [Flowchart Example](#)
- 6.3 [Walkthrough Example](#)
- 6.4 [Risk and Control Matrix Template](#)
- 6.5 [Third-Party / Central Management Agency Service Provider Inventory Template](#)
- 6.6 [Reliance on the Work of Others Templates](#)
- 7.1 [Determining Factors for Sample Size](#)
- 7.2 [Sample Size Guidance](#)
- 7.3 [Test Plan Template](#)
- 7.4 [Testing Leadsheet Example](#)
- 7.5 [Document Request Template](#)
- 7.6 [Issue Summary Template](#)

APPENDIX 4.1

MATERIALITY TEMPLATE

State Accounting Office Materiality Threshold Guide						
Materiality Threshold			Legend			
Low	1%		Auto Calculating Field			
Moderate	1% - 5%		User Entry Field			
High	5%					
Balance Sheet Materiality Determination						
Total Assets	Capital Assets	Total Assets less Capital Assets	Low Threshold	High Threshold	Low Materiality	High Materiality
		\$ -	1%	5%	\$ -	\$ -
Income Statement Materiality Determination						
Total Revenues	Greater of Revenues or Expenditures	Low Threshold	High Threshold	Low Materiality	High Materiality	
	No Value Entered	1%	5%	\$ -	\$ -	
Total Expenditures						
Account Type	Account Balance	Materiality				
Balance Sheet						
Income Statement						

APPENDIX 4.2

RISK ASSESSMENT TEMPLATE – ACCOUNT RISK

Agency Name
Account Risk Assessment
June 30, 20XX

Caption / Account Description	06/30/XX Account Balance	Size and Composition	Transaction Volume	Transaction Complexity	Subjectivity and Estimation	Inherent Risk	Total Score
STATEMENT OF NET ASSETS							
XXXX							

STATEMENT OF REVENUES, EXPENSES, AND CHANGES IN NET ASSETS

Expenses
XXXX

Financial Statement Assertion Risk

STATEMENT OF NET ASSETS
XXXX

C	E/O	V/M	R&O	P&D

C - Completeness
 E/O - Existence / Occurrence
 V/M - Valuation / Measurement (Allocation)
 R&O - Rights and Obligations
 P&D - Presentation and Disclosure

APPENDIX 4.2

RISK ASSESSMENT TEMPLATE – PROCESS RISK

EXAMPLE
Agency Name
Process Risk Assessment
June 30, 20XX

Account Description	Account Risk	Related Significant Processes	Size and Composition	Susceptibility due to error / fraud	Transaction Complexity	Homogeneity of transactions	IT dependency / manual intervention	Degree of subjectivity / estimation	Total Score
<i>Accounts payable</i>	High	<i>New Vendor Setup</i>	2	2	1	1	2	1	9
		<i>Purchasing</i>	3	2	2	2	1	1	11
		<i>Receiving</i>	2	2	1	2	3	2	12
		<i>Processing Invoices</i>	3	3	2	3	2	2	15
		<i>Payments</i>	3	3	2	3	2	2	15
		<i>Update to G/L</i>	3	2	2	2	1	2	12
		<i>AP Applications and Data Access</i>	3	3	2	2	2	1	13

Note: Completed portion for example purposes only.

APPENDIX 5.1

IT GENERAL CONTROLS

Providing information to enable management's reporting to key stakeholders is a life cycle of collecting complete and accurate information and reporting it on a timely basis. As one might expect, this life cycle is highly dependent on information systems, such as applications, databases and other tools used to enhance the efficiency and effectiveness of data processing. The balance of this appendix is dedicated to providing guidance on IT controls that are specifically designed to support financial reporting objectives. These controls are not intended to be an exhaustive list. However, they do provide a starting point as agencies determine which IT controls are necessary for their environment. Consideration should also be given to IT controls that may not be included below, but which an agency considers relevant nonetheless. The most relevant internal controls applicable to financial statement assertions can be defined to include activities that prevent or detect and correct a significant misstatement in the financial reporting or other required disclosures, including those over recording amounts into the general ledger and recording journal entries (standard, nonstandard and consolidation). The most relevant controls may be manual or automated, and preventive or detective in nature.

As noted previously, this guidance is not intended to be authoritative. Professional judgment needs to be applied when determining the necessary controls that should be included in the compliance program, including some which may not be highlighted as most relevant controls in this document.

Note: The documentation noted below is from the IT Governance Institute (ITGI), IT Control Objectives For Sarbanes Oxley – “THE ROLE OF IT IN THE DESIGN AND IMPLEMENTATION OF INTERNAL CONTROL OVER FINANCIAL REPORTING (2ND EDITION)”.

Acquire and Maintain Application Software (AI2)

Control Objective: Controls provide reasonable assurance that application and system software is acquired or developed that effectively supports financial reporting requirements.

Rationale: The process of acquiring and maintaining software includes the design, acquisition/building and deployment of systems that support the achievement of business objectives. This process includes major changes to existing systems. This is where controls are designed and implemented to support initiating, recording, processing and reporting financial information and disclosure. Deficiencies in this area may have a significant impact on financial reporting and disclosure. For instance, without sufficient controls over application interfaces, financial information may not be complete or accurate.

IT General Controls supporting control objective:

IT General Control (Bold controls are considered most relevant for IMPROVE compliance)	Tests of Controls	COBIT References (4.1)
The organization has a system development life cycle (SDLC) methodology, which includes security and processing integrity requirements of the organization.	Obtain a copy of the organization's SDLC methodology to determine that it addresses security and processing integrity requirements. Consider whether there are appropriate steps to determine if these requirements are considered throughout the development or acquisition life cycle, e.g., security and processing integrity are considered during the requirements phase.	PO8.3 AI2.3 AI2.4
The organization's SDLC policies and procedures consider the development and acquisition of new systems and major changes to existing systems.	Review the organization's SDLC methodology to determine if it considers both the development and acquisition of new systems and major changes to existing systems.	PO6.3 AI2 AI6.2
The SDLC methodology includes requirements that information systems be designed to include application controls that support complete, accurate, authorized and valid transaction processing.	Review the SDLC methodology to determine if it addresses application controls. Consider whether there are appropriate steps so that application controls are considered throughout the development or acquisition life cycle, e.g., application controls should be included in the conceptual design and detail design phases.	AI1 AI2.3 AC
The organization has an acquisition and planning process that aligns with its overall strategic direction.	Review the SDLC methodology to determine if the organization's overall strategic direction is considered, e.g., an IT steering committee should review and approve projects so that a proposed project aligns with strategic business requirements and will utilize approved technologies.	PO4.3 AI3.1
To maintain a reliable environment, IT management involves users in the design of applications, selection of packaged software and testing thereof.	Review the SDLC methodology to determine if users are appropriately involved in the design of applications, selection of packaged software and	AI1 AI2.1 AI2.2 AI7.2

	testing.	
Post implementation reviews are performed to verify that controls are operating effectively.	Determine if post implementation reviews are performed on new systems and significant changes reported.	AI7.12
The organization acquires/develops application systems software in accordance with its acquisition, development and planning process.	Select a sample of projects that resulted in new financial systems being implemented. Review the documentation and deliverables from these projects to determine if they have been completed in accordance with the acquisition, development and planning processes.	AI2

Acquire and Maintain Technology Infrastructure (AI3)

Control Objective: Controls provide reasonable assurance that technology infrastructure is acquired so that it provides the appropriate platforms to support financial reporting applications.

Rationale: The process of acquiring and maintaining technology infrastructure includes the design, acquisition/building and deployment of systems that support applications and communications. Infrastructure components, including servers, networks and databases, are critical for secure and reliable information processing. Without an adequate infrastructure there is an increased risk that financial reporting applications will not be able to pass data between applications, financial reporting applications will not operate, and critical infrastructure failures will not be detected in a timely manner.

IT General Control	Tests of Controls	COBIT References (4.1)
Documented procedures exist and are followed so that infrastructure systems, including network devices and software, are acquired based on the requirements of the financial application they are intended to support.	Select a sample of technology infrastructure implementations. Review the documentation and deliverables from these projects to determine if infrastructure requirements were considered at the appropriate time during the acquisition process.	AI3

Enable Operations (PO6, PO8, AI6, DS13)

Control Objective: Controls provide reasonable assurance that policies and procedures that define required acquisition and maintenance processes have been developed and are maintained, and that they define the documentation needed to support the proper use of the applications and the technological solutions put in place.

Rationale: Policies and procedures include the SDLC methodology and the process for acquiring, developing and maintaining applications as well as required documentation. For some organizations, the policies and procedures include service level agreements, operational practices and training materials. Policies and procedures support an organization’s commitment to perform business process activities in a consistent and objective manner.

IT General Control	Tests of Controls	COBIT References (4.1)
The organization has policies and procedures regarding program development, program change, access to programs and data, and computer operations, which are periodically reviewed, updated and approved by management.	<p>Confirm that the organization has policies and procedures that are reviewed and updated regularly for changes in the business. When policies and procedures are changed, determine if management approves such changes.</p> <p>Select a sample of projects and determine that user reference and support manuals, systems documentation and operations documentation were prepared. Consider whether drafts of these manuals were incorporated in user acceptance testing. Determine whether any changes to proposed controls resulted in documentation updates.</p>	PO6.1 PO6.3 PO8.1 PO8.2 PO8.3 AI6.1 D13.1
The organization develops, maintains and operates its systems and applications in accordance with its supported, documented policies and procedures.	Obtain the policies and procedures and determine if the organization manages its IT environment in accordance with them.	PO6.1 PO6.3 PO8.1 PO8.2 AI6.1 DS13.1

Install and Accredit Solutions and Changes (AI7)

Control Objective: Controls provide reasonable assurance that the systems are appropriately tested and validated prior to being placed into production processes and that associated controls operate as intended and support financial reporting requirements.

Rationale: Installation testing and validating relate to the migration of new systems into production. Before such systems are installed, appropriate testing and validation should be performed to determine if the systems are operating as designed. Without adequate testing, systems may not function as intended and may provide invalid information, which could result in unreliable financial information and reports.

IT General Control	Tests of Controls	COBIT References (4.1)
A testing strategy is developed and followed for all significant changes in applications and infrastructure technology, which addresses unit, system, integration and user acceptance-level testing so that deployed systems operate as intended.	Select a sample of systems development projects and significant system upgrades (including technology upgrades). Determine if a formal testing strategy was prepared and followed. Consider whether this strategy considered potential development and implementation risks and addressed all the necessary components to address these risks, e.g., if the completeness and accuracy of system interfaces are essential to the production of complete and accurate reporting, these interfaces were included in the testing strategy. (Note: Controls over the final move to production are addressed in <i>Manage Changes</i>)	AI7.2 AI7.4 AI7.6 AI7.7
Load and stress testing is performed according to a test plan and established testing standards.	Select a sample of system development projects and system upgrades that are significant for financial reporting. Where capacity and performance were considered of potential concern, review the approach to load and stress testing. Consider whether a structured approach was taken to load and stress testing and the approach taken adequately modeled the anticipated volumes, including types of transactions being processed and the impact on performance of other services that would be running concurrently.	AI7.2
Interfaces with other systems are tested to confirm that data transmissions are complete, accurate and valid.	Select a sample of system development projects and system upgrades that are significant for financial reporting. Determine if interfaces with other systems were tested to confirm that data transmissions are complete, e.g., record totals are accurate and valid. Consider whether the extent of testing was sufficient and included recovery in the event of incomplete data transmissions.	AI7.5
The conversion of data is tested between their origin and their destination to confirm that the data are complete, accurate and valid.	Obtained a sample of system development projects and system upgrades that are significant for financial reporting. Determine if a conversion strategy documented. Consider whether it included strategies to “scrub” the data in the old system before the conversion, or to “run down” data in the old system before conversion. Review the conversion testing plan.	AI7.5

Manage Changes (AI6, AI7)

Control Objective: Controls provide reasonable assurance that system changes of financial reporting significance are authorized and appropriately tested before being moved to production.

Rationale: Managing changes addresses how an organization modifies system functionality to help the business meet its financial reporting objectives. Deficiencies in this area could significantly impact financial reporting. For instance, changes to the programs that allocate financial data to accounts require appropriate approvals and testing prior to the change so that proper classification and reporting integrity is maintained.

IT General Control	Tests of Controls	COBIT References (4.1)
<p>Requests for program changes, system changes and maintenance (including changes to system software) are standardized, logged, approved, documented and subject to formal change management procedures.</p>	<p>Determine that a documented change management process exists and is maintained to reflect the current process.</p> <p>Consider if change management procedures exist for all changes to the production environment, including program changes, system maintenance and infrastructure changes.</p> <p>Evaluate the process used to control and monitor change requests.</p> <p>Consider whether change requests are properly initiated, approved and tracked.</p> <p>Determine whether program change is performed in a segregated, controlled environment.</p> <p>Select a sample of changes made to applications/systems to determine whether they were adequately tested and approved before being placed into a production environment. Establish if the followed are included in the approval process: operations, security, IT infrastructure management and IT management.</p> <p>Evaluate procedures designed to determine that only authorized/approved changes are moved into production.</p> <p>Trace the sample of changes back to the change request log and supporting documentation.</p> <p>Confirm that these procedures address the timely implementation of patches to system software. Select a sample to</p>	<p>AI6.1 AI6.2 AI6.4 AI6.5 AI7.3 AI7.8 AI7.9 AI7.10 AI7.11</p>

	determine compliance with the documented procedures.	
Emergency change requests are documented and subject to formal change management procedures.	<p>Determine if a process exists to control and supervise emergency changes.</p> <p>Determine if an audit trail exists of all emergency activity and verify that it is independently reviewed.</p> <p>Determine that procedures require emergency changes to be supported by appropriate documentation.</p> <p>Establish that backout procedures developed for emergency changes.</p> <p>Evaluate procedures ensuring that all emergency changes are tested and subject to standard approval procedures after they have been made. Review a sample of changes that are recorded as “emergency” changes, and determine if they contain the needed approval and the needed access was terminated after a set period of time. Establish that the sample of changes was well documented.</p>	AI6.3 AI7.10
Controls are in place to restrict migration of programs to production by authorized individuals only.	<p>Evaluate the approvals required before a program is moved to production. Consider approvals from system owners, development staff and computer operations.</p> <p>Confirm that there is appropriate segregation of duties between the staff responsible for moving a program into production and development staff. Obtain and test evidence to support this assertion.</p>	AI7.8
IT management implements system software that does not jeopardize the security of the data and programs being stored on the system.	<p>Determine that a risk assessment of the potential impact of changes to system software is performed. Review procedures to test changes to system software in a development environment before they are applied to production. Verify that backout procedures exist.</p>	AI6.2 AI7.4 AI7.9

Define and Manage Service Levels (DS1)

Control Objective: Controls provide reasonable assurance that service levels are defined and managed in a manner that satisfies financial reporting system requirements and provides a common understanding of performance levels by which the quality of services will be measured.

Rationale: The process of defining and managing service levels addresses how an organization meets the functional and operational expectations of its users and, ultimately, the objectives of

the business. Roles and responsibilities are defined and an accountability and measurement model is used to determine if services are delivered as required. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, if systems are poorly managed or system functionality is not delivered as required, financial information may not be processed as intended.

IT General Control	Tests of Controls	COBIT References (4.1)
Service levels are defined and managed to support financial reporting system requirements.	<p>Obtain a sample of service level agreements and review their content for clear definition of service descriptions and expectations of users.</p> <p>Discuss with members of the organization responsible for service level management and test evidence to determine whether service levels are actively managed.</p> <p>Obtain and test evidence that service levels are being actively managed in accordance with service level agreements.</p> <p>Discuss with users whether financial reporting systems are being supported and delivered in accordance with their expectations and service level agreements.</p>	DS1.2 DS1.3 DS1.5 DS1.6
A framework is defined to establish appropriate performance indicators to manage service-level agreements, both internally and externally.	<p>Obtain service-level performance reports and confirm that they include key performance indicators.</p> <p>Review the performance results, identify performance issues and assess how service-level managers are addressing these issues.</p>	DS1.1 DS1.3

Manage Third-party Services (DS2)

Control Objective: Controls provide reasonable assurance that third-party services are secure, accurate and available; support processing integrity; and are defined appropriately in performance contracts.

Rationale: Managing third-party services includes the use of outsourced service providers to support financial applications and related systems. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, insufficient controls over processing accuracy by a third-party service provider may result in inaccurate financial results.

IT General Control	Tests of Controls	COBIT References (4.1)
A designated individual is responsible for regular monitoring and reporting on the	Determine if the management of third-party services has been assigned to	DS2.2

achievement of the third-party service-level performance criteria.	appropriate individuals.	
Selection of vendors for outsourced services is performed in accordance the organization's vendor management policy.	<p>Obtain the organization's vendor management policy and discuss with those responsible for third-party service management if they follow such standards.</p> <p>Obtain and test evidence that the selection of vendors for outsourced services is performed in accordance with the organization's vendor management policy.</p>	PO1.4 PO6.3 DS2
IT management determines that, before selection, potential third parties are properly qualified through an assessment of their capability to deliver the required service and a review of their financial viability.	<p>Obtain the criteria and business case used for selection of their-party service providers.</p> <p>Assess whether these criteria include a consideration of the third party's financial stability, skill and knowledge of the systems under management, and controls over security and processing integrity.</p>	DS2.3
Third-party service contracts address the risks, security controls and procedures for information systems and networks in the contract between the parties.	Select a sample of third-party service contracts and determine if they include controls to support security and processing integrity in accordance with the company's policies and procedures.	DS2.3
Procedures exist and are followed that include requirements that for third-party services a formal contract be defined and agreed to before work is initiated, including definition of internal control requirements and acceptance of the organization's policies and procedures.	<p>Review a sample of contracts and determine whether:</p> <ul style="list-style-type: none"> • There is definition of services to be performed • The responsibilities for the controls over financial reporting systems have been adequately defined. • The third party has accepted compliance with the organization's policies and procedures, e.g., security policies and procedures. • The contracts were reviewed and signed by appropriate parties before work commenced. • The controls over financial 	DS2.3

	<p>reporting systems and subsystems described in the contract agree with those required by the organization.</p> <p>Review gaps, if any, and consider further analysis to determine the impact on financial reporting.</p>	
<p>A regular review of security and processing integrity is performed by third-party service providers (e.g., SAS 70, Canadian 5970, and ISA 402).</p>	<p>Inquire whether third-party service providers perform independent reviews of security and processing integrity, e.g., a service auditor report. Obtain a sample of the most recent review and determine if there are any control deficiencies that would impact financial reporting.</p>	ME2.6

Ensure System Security (DS5)

Control Objective: Controls provide reasonable assurance that financial reporting systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.

Rationale: Managing systems security includes both physical and logical controls that prevent unauthorized access. These controls typically support authorization, authentication, nonrepudiation, data classification and security monitoring. Deficiencies in this area could significantly impact financial reporting. For instance, insufficient controls over transaction authorization may result in inaccurate financial reporting.

IT General Control	Tests of Controls	COBIT References (4.1)
<p>An information security policy exists and has been approved by an appropriate level of executive management.</p>	<p>Obtain a copy of the organization’s security policy and evaluate the effectiveness. Points to be taken into consideration include:</p> <ul style="list-style-type: none"> • Is there an overall statement of the importance of security to the organization? • Have specific policy objectives been defined? • Have employee and contractor security responsibilities been addressed? • Has the policy been approved by 	<p>PO6.3 PO6.5 PO5.2</p>

	<p>an appropriate level of senior management to demonstrate management's commitment to security?</p> <ul style="list-style-type: none"> • Is there a process to communicate the policy to all levels of management and employees? 	
A framework of security standards has been developed that supports the objectives of the security policy	<p>Obtain a copy of the security standards. Determine whether the standards framework effectively meets the objectives of the security policy. Consider whether the following topics, which are often addressed by security standards, have been appropriately covered:</p> <ul style="list-style-type: none"> • Security organization • Roles and responsibilities • Physical and environmental security • Operating system security • Network security • Application security • Database security <p>Determine if there are processes in place to communicate and maintain these standards</p>	PO8.2 DS5.2
An IT security plan exists that is aligned with overall IT strategic plans	Obtain a copy of security plans or strategies for financial reporting systems and subsystems and assess their adequacy in relation to the overall company plan.	DS5.2
The IT security plan is updated to reflect changes in the IT environment as well as security requirements of specific systems.	Confirm that the security plan reflects the unique security requirements of financial reporting systems and subsystems.	DS5.2
Procedures exist and are followed to authenticate all users of the system (both internal and external) to support the existence of transactions.	Assess the authentication mechanisms used to validate user credentials for financial reporting systems and subsystems and validate that user sessions time-out after the predetermined period of time. Validate that no shared user profiles (including administrative profiles) are used.	DS5.3 AC
Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., regular password changes)	Review the security practices to confirm that authentication controls (passwords, IDs, two-factor, etc.) are used appropriately and are subject to common confidentiality requirements (IDs and passwords not shared, alphanumeric passwords used, etc.).	DS5.3 DS5.4
Procedures exist and are followed relating to timely action for requesting, establishing, issuing, suspending and closing user account. (Include procedures for authenticating transactions originating outside the	Confirm that procedures for the registration, change and deletion of users from financial reporting systems and subsystems on a timely basis exist and are followed.	DS5.4

<p>organization.)</p>	<p>Select a sample of new users and determine if management approved their access and the access granted agrees with the access privileges that were approved.</p> <p>Select a sample of terminated employees and determine if their access has been removed, and the removal was done in a timely manner.</p> <p>Select a sample of privileged and current users and review their access for appropriateness based upon their job functions.</p>	
<p>A control process exists and is followed to periodically review and confirm access rights.</p>	<p>Inquire whether access controls for financial reporting systems and subsystems are reviewed by management on a periodic basis.</p> <p>Assess the adequacy of how exceptions are reexamined, and if the follow-up occurs in a timely manner.</p>	<p>DS5.4</p>
<p>Where appropriate, controls exist so that neither party can deny transactions, and controls are implemented to provide nonrepudiation of origin or receipt, proof of submission, and receipt of transactions.</p>	<p>Determine how the organization established accountability for transaction initiation and approval.</p> <p>Test the use of accountability controls by observing a user attempting to enter an authorized transaction.</p> <p>Obtain a sample of transactions, and identify evidence of the accountability or origination of each.</p>	<p>DS11.6 AC</p>
<p>Appropriate controls, including firewalls, intrusion detection and vulnerability assessments, exist and are used to prevent unauthorized access via public networks.</p>	<p>Determine the sufficiency and appropriateness of perimeter security controls, including firewalls, and intrusion detection systems.</p> <p>Inquire whether management has performed an independent assessment of controls within the past year (e.g., ethical hacking, social engineering).</p> <p>Obtain a copy of this assessment and review the results, including the appropriateness of follow-up on identified weaknesses.</p> <p>Determine if antivirus systems are used to protect the integrity and security of financial reporting systems and subsystems.</p> <p>When appropriate, determine if encryption techniques are used to support the confidentiality of financial</p>	<p>DS5.10</p>

	information sent from one system to another.	
IT security administration monitors and logs security activity at the operating systems, application and database levels and identified security violations are reported to senior management.	<p>Inquire whether a security office exists to monitor for security vulnerabilities at the application and database levels and related threat events.</p> <p>Asses the nature and extent of such events over the past year and discuss with management how they have responded with controls to prevent unauthorized access or manipulation of financial systems and subsystems.</p> <p>Validate that attempts to gain unauthorized access to financial reporting systems and subsystems are logged and follow up on a timely basis.</p>	DS5.5
Controls relating to appropriate segregation of duties over requesting and granting access to systems and data exist and are followed.	Review the process to request and grant access to systems and data and confirm that the same person does not perform these functions.	DS5.3 DS5.4
Access to facilities is restricted to authorized personnel and requires appropriate identification and authentication.	<p>Obtain policies and procedures as they relate to facility security, key and card reader access, and determine if those procedures account for proper identification and authentication.</p> <p>Observe the in-and-out traffic to the organizations facilities to establish that proper access is controlled.</p> <p>Select a sample of users and determine if their access is appropriate based upon their job responsibilities.</p>	DS12.2 DS12.3

Manage the Configuration (DS9)

Control Objective: Controls provide reasonable assurance that IT components, as they relate to security and processing, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.

Rationale: Configuration management includes procedures such that security and processing integrity controls are set up in the system and maintained through its life cycle. Insufficient configuration controls can lead to security exposures that may permit unauthorized access to systems and data and impact financial reporting. An additional potential risk is corruption to data integrity caused by poor control of the configuration when making system changes or by the introduction of unauthorized system components.

IT General Control	Tests of Controls	COBIT References (4.1)
Only authorized software is permitted for use by employees using company IT	Determine if procedures are in place to detect and prevent the use of	DS9.2

assets.	<p>unauthorized software. Obtain and review the company policy as it related to software use to see that it is clearly articulated.</p> <p>Consider reviewing a sample of applications and computer to determine if they are in conformance with organization policy.</p>	
System infrastructure, including firewalls, routers, switches, network operating systems, servers and other related devices, is properly configured to prevent unauthorized access.	<p>Determine if the organization's policies require the documentation of the current configuration, as well as the security configuration, settings to be implemented.</p> <p>Review a sample of servers, firewalls, routers, etc., to consider if they have been configured in accordance with the organization's policy.</p>	DS5.3 DS5.4 DS5.10
Application software and data storage systems are properly configured to provision access based on the individual's demonstrated need to view, add, change or delete data.	<p>Conduct an evaluation of the frequency and timeliness of management's review of configuration records.</p> <p>Assess whether management has documented the configuration management procedures.</p> <p>Review a sample of configuration changes, additions or deletions, to consider if they have been properly approved based on a demonstrated need.</p>	DS5.4
IT management has established procedures across the organization to protect information systems and technology from computer viruses.	<p>Review the organization's procedures to detect computer viruses.</p> <p>Verify that the organization has installed and is issuing virus software on its networks and personal computers.</p>	DS5.9
Periodic testing and assessment is performed to confirm that the software and network infrastructure is appropriately configured.	Review the software and network infrastructure to establish that it has been appropriately configured and maintained, according to the organization's documented process.	AI3.2 AI3.3

Manage Problems and Incidents (DS8, DS10)

Control Objective: Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution.

Rationale: The process of managing problems and incidents addresses how an organization identifies, documents and responds to events that fall outside of normal operations. Deficiencies in this area could significantly impact financial reporting.

IT General Control	Tests of Controls	COBIT References (4.1)
---------------------------	--------------------------	-------------------------------

<p>IT management has defined and implemented an incident and problem management system such that data integrity and access control incidents are recorded, analyzed, resolved in a timely manner and reported to management.</p>	<p>Determine if an incident management system exists and how it is being used. Review how management has documented how the system is to be used.</p> <p>Review a sample of incident reports, to consider if the issues were addressed (recorded, analyzed and resolved) in a timely manner.</p>	<p>DS8</p>
<p>The problem management system provides for adequate audit trail facilities, which allow tracing from problem or incident to underlying cause.</p>	<p>Determine if the organization's procedures include audit trail facilities – tracking of the problems or incidents.</p> <p>Review a sample of problems recorded on the problem management system to consider if a proper audit trail exists and is used.</p>	<p>DS10.2</p>
<p>A security incident response process exists to support timely response and investigation of unauthorized activities.</p>	<p>Verify that unauthorized activities are responded to in a timely fashion, and there is a process to support proper disposition.</p>	<p>DS5.6 DS8.3 DS10.1 DS10.3</p>

Manage Data (DS11)

Control Objective: Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.

Rationale: Managing data includes the controls and procedures used to support information integrity, including its completeness, accuracy, authorization and existence. Controls are designed to support initiating, recording, processing and reporting financial information. Deficiencies in this area could significantly impact financial reporting. For instance, without appropriate authorization controls over the initiation of transactions, resulting financial information may not be reliable.

<p>IT General Control</p>	<p>Tests of Controls</p>	<p>COBIT References (4.1)</p>
<p>Policies and procedures exist for the distribution and retention of data and reporting output.</p>	<p>Review the policies and procedures for the distribution and retention of data and reporting output. Determine whether the policies and procedures are adequate for the protection of data and the timely distribution of the correct financial reports (including electronic reports) to appropriate personnel.</p> <p>Obtain and test evidence that the controls over the protection of data and timely distribution of financial reports (including electronic reports) to appropriate personnel are operating effectively.</p>	<p>DS11.1 DS11.2 DS11.6</p>
<p>Management protects sensitive information – logically and physically, in storage and during transmission – against unauthorized access or modification.</p>	<p>Review the results of security testing. Determine if there are adequate controls to protect sensitive information – logically and physically, in storage and</p>	<p>DS11.6</p>

	during transmission – against unauthorized access or modification.	
Retention periods and storage terms are defined for documents, data, programs, reports and messages (incoming and outgoing), as well as the data (keys, certificates) used for their encryption and authentication.	<p>Obtain the procedures dealing with distribution and retention of data.</p> <p>Confirm that the procedures define the retention periods and storage terms for documents, data, programs, reports and messages (incoming and outgoing), as well as the data (keys, certificates) used for their encryption and authentication.</p> <p>Confirm that the retention periods are in conformity with Sarbanes-Oxley Act.</p> <p>Confirm that the retention periods of previously archived material are in conformity with the Sarbanes-Oxley Act. Select a sample of archived material and test evidence that archived material is being archived in conformance with the requirements of the Sarbanes-Oxley Act.</p>	DS11.2
Management has implemented a strategy for cyclical backup of data and programs.	Determine if the organization has procedures in place to back up data and programs based on IT and user requirements. Select a sample of data files and programs and determine if they are being backed up as required.	DS11.5
The restoration of information is periodically tested.	<p>Inquire whether the retention and storage of messages, documents, programs, etc., have been tested during the past year.</p> <p>Obtain and review the results of testing activities.</p> <p>Establish whether any deficiencies were noted and whether they have been reexamined. Obtain the organization’s access security policy and discuss with those responsible whether they follow such standards and guidelines dealing with sensitive backup data.</p>	DS11.5
Changes to data structures are authorized, made in accordance with design specifications and implemented in a timely manner.	Obtain a sample of data structure changes and determine whether they adhere to the design specifications and were implemented in the time frame required.	AI6

Manage Operations (DS13)

Control Objective: Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing and error monitoring.

Rationale: Managing operations addresses how an organization maintains reliable application systems in support of the business to initiate, record, process and report financial information.

Deficiencies in this area could significantly impact an entity's financial reporting. For instance, lapses in the continuity of application systems may prevent an organization from recording financial transactions and thereby undermine its integrity.

IT General Control	Tests of Controls	COBIT References (4.1)
<p>Management has established, documented and follows standard procedures for IT operations, including job scheduling and monitoring and responding to security and processing integrity events.</p>	<p>Determine if management has documented its procedures for IT operations, and operations are reviewed periodically for compliance.</p> <p>Review a sample of events to confirm that response procedures are operating effectively. When used, review the job scheduling process and the procedures in place to monitor job completeness.</p>	<p>DS13.1 DS13.2</p>
<p>System event data are sufficiently retained to provide chronological information and logs to enable the review, examination and reconstruction of system and data processing.</p>	<p>Determine if sufficient chronological information is being recorded and stored in logs, and it is usable for reconstruction, if necessary. Obtain a sample of the log entries, to determine if they sufficiently allow for reconstruction.</p>	<p>DS13.3</p>
<p>System event data are designed to provide reasonable assurance as to the completeness and timeliness of system and data processing.</p>	<p>Inquire as to the type of information that is used by management to determine the completeness and timeliness of system and data processing.</p> <p>Review a sample of system processing event data to confirm the completeness and timeliness of processing.</p>	<p>DS11.1 SA13.3</p>

APPENDIX 5.2

END-USER COMPUTING CONTROLS

The following illustrative controls for End-User Computing are presented to address the characteristics of a typical End-User Computing environment. Appropriate COBIT processes apply to this environment.

End-User Computing Control	Test of Controls
End-User Computing policies and procedures concerning security and processing integrity exist and are followed.	Obtain a copy of the End-User Computing policies and procedures and confirm that they address security and processing integrity controls.
End-User Computing, including spreadsheets and other user-developed programs, are documented and regularly reviewed for processing integrity, including their ability to sort, summarize and report accurately.	<p>Inquire as to management’s knowledge of End-User programs in use across the agency.</p> <p>Inquire as to the frequency and approaches followed to review End-User programs for processing integrity, and review a sample of these to confirm effectiveness.</p> <p>Review user-developed systems and test their ability to sort, summarize and report in accordance with management intentions.</p>
User-developed systems and data are regularly backed up and stored in a secure area.	Inquire how End-User systems are backed up and where they are stored.
User-developed systems, such as spreadsheets and other end-user programs, are secured from unauthorized use.	<p>Review the security used to protect unauthorized access to use-developed systems.</p> <p>Consider observing a user attempting to gain unauthorized access to user-developed systems.</p> <p>Inquire how management is able to detect unauthorized access and what follow-up procedures are performed to assess the impact of such access.</p> <p>Select a sample of user-developed systems and determine who has access and if the access is appropriate.</p>

End-User Computing Control	Test of Controls
<p>Inputs, processing and outputs from user-developed systems are independently verified for completeness and accuracy.</p>	<p>Inquire how management verifies the accuracy and completeness of information processed and reported from user-developed systems.</p> <p>Inquire as to who review and approves outputs from user-developed systems prior to their submission for further processing or final reporting.</p> <p>Consider reperforming or reviewing the logic used in user-developed systems and conclude on their ability to process completely and accurately.</p>

APPENDIX 6.1

NARRATIVE EXAMPLE

Process: Purchase to Pay

Supporting Application: Application XYZ

This document provides a description of the Purchase to Pay Process as performed by Agency ABC as of 6/30/XXXX.

The following processes form part of the Purchase to Pay process at AGENCY ABC.

- New Vendor Setup: This is as a prerequisite to the Purchase to Pay Process (P2P), since one cannot start the process without having vendors set up on the system.
- Purchasing (Purchase Request (PR) and Purchase Orders (PO):
 - PR - This initiates the P2P process, since anyone in the agency can request an item to be used in his or her daily activities.
 - PO - This is where the purchasing department transforms related purchase requests to orders.
- Receiving: This is where the requester and/or receiving clerk receives the goods ordered.
- Processing Invoices: This is where Agency ABC receives the vendor's invoice, performs a verification process on the invoice, and makes it ready for payment.
- Payments: This is where the vendor's payment is created and delivered. The account payable (AP) is maintained here.
- Update the General Ledger (GL)/Accrual: This is where the above transaction is reflected in the GL.

New Vendor Setup

Inputs: Vendor information (name, address, bank details, payment terms, discounts, matching principal, accounting, etc.)

Output: Vendor in system

A formal process exists to add or modify vendors. Note that Application XYZ does not permit the deletion of vendors; it will only allow a vendor to be altered or disabled. This process consists of the following activities:

- The Supplier Maintenance Form is filled out by the buyer. This form details the vendor's name, address, bank details, payment terms, discounts, matching principal, accounting information, etc.
- The form must be signed by the buyer's supervisor, who checks the details for accuracy.
- The form is then sent to the AP department where it is reviewed and entered into the system.

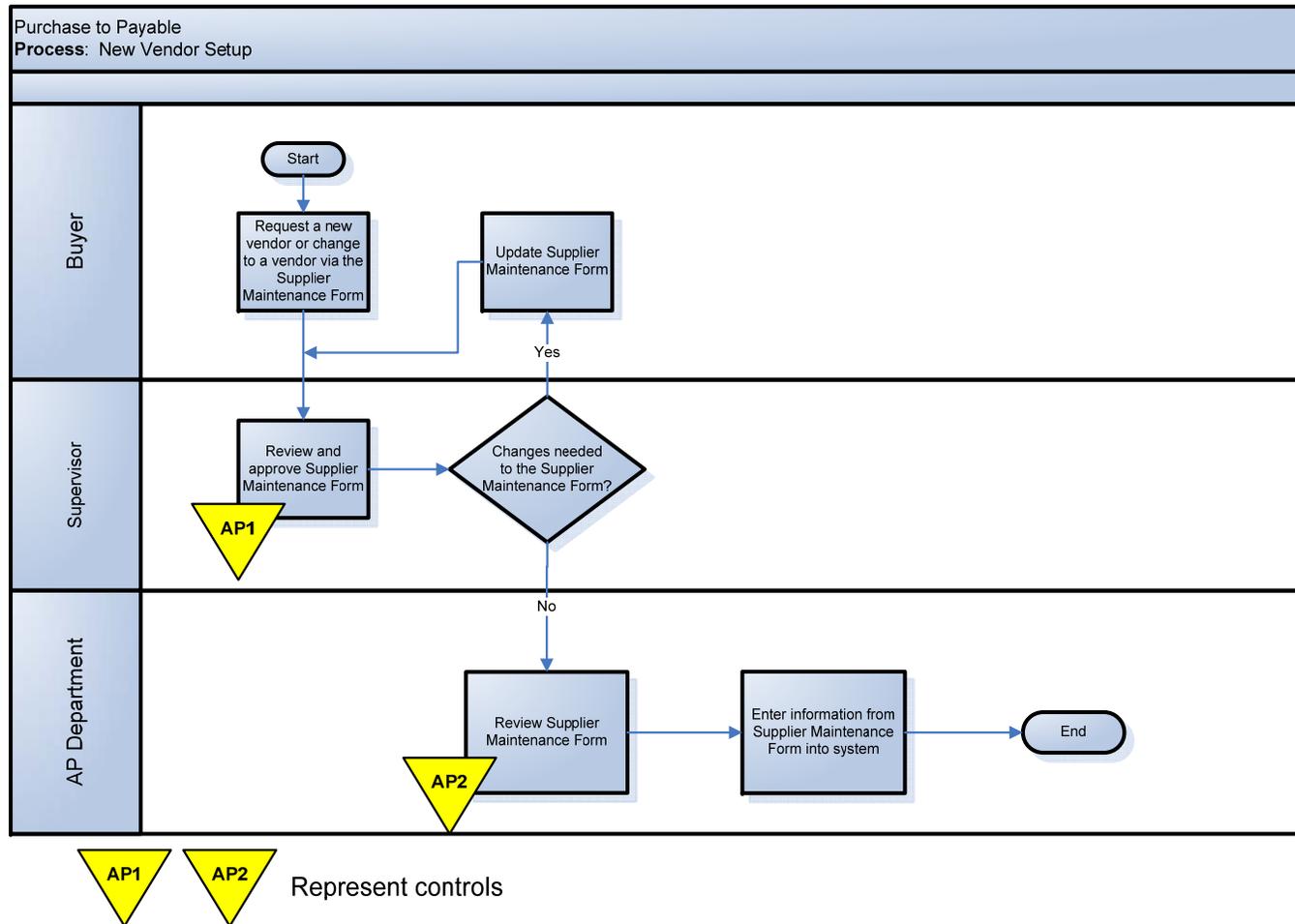
Additional Notes:

- Application XYZ does not allow duplicate supplier names to reside in the system.

Narratives for remaining processes have been intentionally omitted

APPENDIX 6.2

FLOWCHART EXAMPLE



APPENDIX 6.3

WALKTHROUGH EXAMPLE

Process: Purchase to Pay
Sub-process: New Vendor Setup
Supporting Application: Application XYZ
Title: New Vendor Setup Walkthrough

This walkthrough template assists in documenting our understanding of the design of controls. We document the procedures performed, evidence obtained and conclusions as to the effective design of the underlying controls and whether the controls have been implemented.

Process Owner Name / Title: Jane Smith, AP Buyer
Interview Date: January 1, 20XX
Selection: South Telephone (Vendor #101)

Procedures Performed:

To perform a walkthrough of the New Vendor Setup process, we obtained the Vendor Report listing all current vendors as of the walkthrough date. We randomly selected vendor #100, South Telephone. We then performed the procedures below.

- The Supplier Maintenance Form is filled out by the buyer. This form details the vendor's name, address, bank details, payment terms, discounts, matching principal, accounting information, etc.
-Walkthrough procedures: We obtained the Supplier Maintenance Form for South Telephone vendor and noted that all the form details were filled out (refer to w/p [API.1](#)).
- The Supplier Maintenance Form must be signed by the buyer's supervisor, who checks the details for accuracy (**Control AP1**).
-Walkthrough procedures: We noted the approval by the buyer's Supervisor on the Supplier Maintenance Form (refer to w/p [API.1](#)).
- The Supplier Maintenance Form is then sent to the AP department where it is reviewed and entered into the system (**Control AP2**).
-Walkthrough procedures: We noted the form details including the vendor's name, address, bank details, payment terms, and discounts and agreed these to the system (refer to w/p [API.2](#)).
- Application XYZ does not allow duplicate supplier names to reside in the system (**Control AP3**).
-Walkthrough procedures: We obtained a listing of suppliers report from the system and noted that our selected vendor, South Telephone, resides within the system. We requested that the Buyer enter the same vendor name into the system. We noted that the system appropriately rejected the vendor (refer to w/p [API.3](#)).

- Vendor maintenance is performed by the AP department and limited to supervisors. Role-based security is utilized in Application XYZ, such that individuals having access to perform vendor maintenance do not also have access to perform other AP functions such as processing vouchers and printing checks (**Control AP4**).
 - Walkthrough procedures: We obtained a user access log for Application XYZ for vendor maintenance and noted that there are excessive users with access. Additionally, we noted that a few of the users with access to vendor maintenance had the ability to perform other AP functionality (refer to w/p **API.4**; also refer to **Issue Summary Log** for details on the exception noted)*

APPENDIX 6.4

RISK AND CONTROL MATRIX TEMPLATE

Document:	Risk and Control Matrix (RACM)
Entity:	<i>Agency Name</i>
Reporting Date:	
Process:	
Financial Statement Accounts:	
Systems / Applications:	

Prepared by:	
Reviewed by:	

Process	Process Risk	Financial Statement Assertions	Risks	Control Description	Control Ref.	Control Owner	Automated, Manual or Both?	Prevent or Detect?	Frequency of Control Activity
<i>New Vendor Setup</i>	<i>Low</i>	<i>Existence Rights & Obligations</i>	<i>Unauthorized or incorrect changes are made to the vendor master file, increasing the risk of fraudulent payment transactions.</i>	<i>The Supplier Maintenance Form is reviewed and approved by the buyer's Supervisor.</i>	<i>AP1</i>	<i>Buyer's Supervisor</i>	<i>Manual</i>	<i>Prevent</i>	<i>More than daily</i>
				<i>The Supplier Maintenance Form is sent to the AP department where it is reviewed and entered into the system.</i>	<i>AP2</i>	<i>AP Clerk</i>	<i>Manual</i>	<i>Prevent</i>	<i>More than daily</i>
				<i>Application XYZ does not allow duplicate supplier names to reside in the system.</i>	<i>AP3</i>	<i>XYZ</i>	<i>Automated</i>	<i>Prevent</i>	<i>Continuous</i>
				<i>Vendor maintenance is performed by the AP department and limited to supervisors. Role-based security is utilized in Application XYZ, such that individuals having access to perform vendor maintenance do not also have access to perform other Accounts Payable functions - process vouchers and print checks.</i>	<i>AP4</i>	<i>XYZ</i>	<i>Automated</i>	<i>Prevent</i>	<i>Continuous</i>

Note: Line 1 for example purposes only

APPENDIX 6.5

THIRD-PARTY / CENTRAL MANAGEMENT AGENCY SERVICE PROVIDER INVENTORY TEMPLATE

Agency:

Date:

<p>Purpose: The purpose of this form is to document the third-party service organizations and service agencies that are used to support the various business processes for the specified agency.</p>

I. Third Parties and Service Agencies Supporting Significant Classes of Transactions within Significant Processes

We identify the significant classes of transactions within significant processes that affect the significant accounts and assertions as part of our review strategy. These significant processes are those major processes where significant classes of transactions are initiated, recorded, processed and/or reported. When understanding the relationship between processes, classes of transactions, and significant accounts, we also consider the parties that are responsible for performing those processes and transactions, as well as the controls associated with those processes. We document the third party resources related to significant classes of transactions within significant processes in the Third-Party/Central Management Agency Service Provider Inventory Template.

Significant Classes of Transactions within Significant Processes

To complete the Third-Party/Central Management Agency Service Provider Inventory Template, the assessment team (or designee) considers the significant classes of transactions within significant processes associated with their respective agency. These are recorded in the column **Significant Class of Transactions/Process**.

Internal or External Process Owner

Each process owner that is used by the agency to support the significant classes of transactions within significant processes is identified and listed in the column **Class of Transactions/ Process Owner**. In the column **Internal or External Process Owner**, a designation should be provided to indicate if the owner is internal or external. More than one agency may own or support each significant class of transactions/process.

**THIRD-PARTY / CENTRAL MANAGEMENT AGENCY SERVICE PROVIDER
INVENTORY TEMPLATE**

II. Other Significant Information

Use the space below to provide any explanation that may be needed to supplement the information contained in Section I.

--

APPENDIX 6.6

RELIANCE ON THE WORK OF OTHERS TEMPLATES

Reliance on the Work of Others – Central Management Agency Template

Agency	_____	Workpaper Ref.	_____
Location	_____	Assessed by	_____
Financial Statement Date	_____		
Name of Service Agency	_____		
Significant Classes of Transactions/Accounting Records:	_____		

Instructions

When an agency (i.e. user agency) uses a service agency (central management agency or other service-providing agency), transactions that affect the agency's financial statements are subjected to controls that are, at least in part, physically and operationally separate from the agency. The significance of the service agency's controls to those of the user agency depends on the nature of the services provided by the service agency, primarily the nature and materiality of the transactions it processes for the user agency and the degree of interaction between its activities and those of the user agency.

During the documentation phase of IMPROVE, the assessment team uses this form to assist in documenting consideration of the effect of a service agency on the user agency's internal control over financial reporting. The form should be completed if transactions affected by the service agency relate to one or more significant processes that are being evaluated for IMPROVE compliance.

Workpaper documentation includes those controls that have been implemented at the service agency that prevent or detect and correct potential errors that could occur in the flow of transactions affected by the service agency. When the controls implemented at the service agency have been evaluated and tested, the assessment team documents that evaluation and testing in the workpapers by cross-referencing to the service agency's results.

1. Describe the transaction processing and related accounting records that are affected by the services provided by the service agency. Describe the aspects of the services in sufficient detail to identify what portions of the transaction flow or related accounting records are affected by the outsourced services. Be sure to include related information technology services which are outsourced to a service agency.

2. If the service agency makes their assessment results available, agencies will need to evaluate that information and its adequacy in addressing the flow of information, the design of the processing procedures and controls at the service agency, and any tests of the operating effectiveness of those controls that in effect represent a component of the user agency's overall system of internal control over financial reporting. We need to consider whether these results provide sufficient evidence to support their internal control environment.

Evaluate and describe the service agency's results.

- | | Yes | No |
|---|--------------------------|--------------------------|
| a. Is there sufficient documentation of processes, utilizing policies, procedures, narratives, and flowcharts, such that the user agency can understand the relevant processes at the service agency along with the flow of transactions through the service agency? Have relevant risks been identified?

If no, describe what is missing. _____ | <input type="checkbox"/> | <input type="checkbox"/> |
| b. Do the results describe in sufficient detail the controls that have been implemented to prevent or detect those possible risks, and do the controls appear to be suitably designed to meet those objectives? | <input type="checkbox"/> | <input type="checkbox"/> |
| c. Are the service agency's relevant controls documented within a risk and control matrix? | <input type="checkbox"/> | <input type="checkbox"/> |
| d. Is there testing evidence (walkthroughs, testing sheets) to support the design and operating effectiveness of the defined controls? | <input type="checkbox"/> | <input type="checkbox"/> |
| e. Has the nature of any noted exceptions been adequately | | |

described in an issue log?

Describe exceptions. _____

If, after review of the service agency's results, we conclude that additional evidence about the operating effectiveness of controls at the service agency is required, we will need to consider other potential sources of information, such as policies and procedures, processing descriptions, and manuals to gain the needed understanding of the controls at the service agency, which may include:

- Evaluating the procedures performed by management and the results of those procedures.
- Contacting the service agency to obtain specific information.
- Requesting that additional documentation and testing be conducted to supply the necessary information.

Describe the additional procedures performed, if applicable.

Conclusion

	Yes	No
Do we have a sufficient understanding of the effect of the service agency on the user agency's internal control over financial reporting, including an understanding of the controls placed in operation by the service agency whose services are part of the user agency's information system?	<input type="checkbox"/>	<input type="checkbox"/>

Is the control testing performed by the service agency relevant to and sufficient for purposes of our assessment of internal control over financial reporting?	<input type="checkbox"/>	<input type="checkbox"/>
--	--------------------------	--------------------------

Describe any additional procedures we will need to perform.

Reliance on the Work of Others - Third-Party Service Organization Template

Agency		Workpaper Ref.	
Location		Assessed by	
Financial Statement Date			
Name of Service Organization			
Significant Classes of Transactions/Accounting Records:			

Instructions

When an agency (i.e. user agency) uses a third-party service organization/provider, transactions that affect the agency's financial statements are subjected to controls that are, at least in part, physically and operationally separate from the agency. The significance of the third-party service organization's controls to those of the user agency depends on the nature of the services provided by the third-party service organization, primarily the nature and materiality of the transactions it processes for the user agency and the degree of interaction between its activities and those of the user agency.

During the documentation phase of IMPROVE, the assessment team uses this form to assist in documenting consideration of the effect of a third-party service organization on the user agency's internal control over financial reporting. The form should be completed if transactions affected by the third-party service organization relate to one or more significant processes that are being evaluated for IMPROVE compliance.

Workpaper documentation includes those controls that have been implemented at the third-party service organization that prevent or detect and correct potential errors that could occur in the flow of transactions affected by this provider. When the controls implemented at the third-party service organization have been evaluated and tested, the assessment team documents that evaluation and testing in the workpapers by cross-referencing to the service auditor's report (SAS 70).

1. Describe the transaction processing and related accounting records that are affected by the services provided by the third-party service organization. Describe the aspects of the services in sufficient detail to identify what portions of the transaction flow or related accounting records are affected by the outsourced services.

2. If the third-party service organization makes a SAS 70 report available, agencies will need to evaluate that information and its adequacy in addressing the flow of information, the design of the processing procedures and controls at the third-party service organization, and any tests of the operating effectiveness of those controls that in effect represent a component of the agency's overall system of internal control over financial reporting. We need to consider whether this report provides sufficient evidence to support their internal control environment.

Evaluate and describe the report's contents.

- | | Yes | No |
|--|--------------------------|--------------------------|
| a. Is the report a Type I?
If yes, what is the "as of" date? _____ | <input type="checkbox"/> | <input type="checkbox"/> |
| b. Is the report a Type II?
If yes, what is the time period covered?
_____ | <input type="checkbox"/> | <input type="checkbox"/> |
| c. Does the report address the applications and/or those service center locations used by the agency? | <input type="checkbox"/> | <input type="checkbox"/> |
| d. Does the report test period cover a sufficient time period for our reliance (e.g., 6 months)? Refer to Question 3 below when the service auditor's report significantly precedes the date of management's assessment.
Document our considerations. _____ | <input type="checkbox"/> | <input type="checkbox"/> |
| e. Does the report provide adequate information to understand the flows of transactions through the third-party service organization and the risks? | <input type="checkbox"/> | <input type="checkbox"/> |

If no, describe what is missing. _____

f. Does the report describe in sufficient detail the controls that have been implemented to prevent or detect those possible risks, and do the controls appear to be suitably designed to meet those objectives? Cross-reference our evaluation of the controls in our workpapers to the location in the service auditor's report where the controls have been identified and described.

Yes No

g. If the report does not provide adequate information (as described above) or does not describe in sufficient detail the controls that have been implemented to prevent or detect possible errors, is there sufficient information at the agency describing the flow of transactions and controls at the third-party service organization to supplement the service auditor's report? (If the response to e. and f. above are both "Yes," leave blank).

Describe the other information.

h. Has the nature of any noted exceptions been adequately described (for Type II reports only)?

Describe exceptions. _____

i. Are there any subservice providers identified in the report opinion?

If yes, have we obtained the additional SAS 70 Type II report(s)?

List. _____

If no, does the SAS 70 Type II report identify mitigating controls that address the controls covered by the subservice providers?

List. _____

Yes No

j. User control considerations are located on page(s): _____

Document below (or with the related program steps) our procedures performed to test relevant user controls, if any, and the related findings. Cross-reference the relevant user controls identified in the service auditor's report to the location in our workpapers where we document our testing of

them.

Describe. _____

- k. Is the service auditor's opinion sufficient for our purposes?

Describe the service auditor's opinion on the operating effectiveness of controls, i.e., unqualified or qualified.

Describe. _____

3. When a significant period of time has elapsed between the time period covered by the test of controls in the service auditor's report and the date of agency's assessment, additional procedures should be performed. We should inquire to determine whether any changes in the third-party service organization's controls subsequent to the period covered by the service auditor's report (such as changes communicated to the us from the third-party service organization, changes in personnel at the third-party service organization with whom the agency interacts, changes in reports or other data received from the third-party service organization, changes in contracts or service level agreements with the third-party service organization, or other errors identified in the service organization's processing). If such changes are identified, we should determine whether additional procedures need to be performed to evaluate the effect of such changes on the effectiveness of the agency's internal control over financial reporting.

If, after review of the SAS 70 report, we conclude that additional evidence about the operating effectiveness of controls at the third-party service organization is required, or if a SAS 70 report is not available, we will need to consider other potential sources of information, such as service contracts, processing descriptions, and manuals to gain the needed understanding of the controls at the third-party service organization, which may include:

- Evaluating the procedures performed by management and the results of those procedures.
- Contacting the third-party service organization to obtain specific information.
- Requesting that a service auditor be engaged to perform procedures that will supply the necessary information.
- Visiting the service organization and performing such procedures.

Describe the additional procedures performed, if applicable.

Conclusion

	<u>Yes</u>	<u>No</u>
Do we have a sufficient understanding of the effect of the third-party service organization on the agency's internal control over financial reporting, including an understanding of the controls placed in operation by the third-party service organization whose services are part of the agency's information system?	<input type="checkbox"/>	<input type="checkbox"/>
Is the control testing, if any, performed by the service auditor relevant to and sufficient for purposes of our assessment of internal control over financial reporting?	<input type="checkbox"/>	<input type="checkbox"/>

Describe any additional procedures we will need to perform.

APPENDIX 7.1

DETERMINING FACTORS FOR SAMPLE SIZE	
Variability of the Population	<p>The variability of the population has a direct effect on the required sample size. As variability (measured as the standard deviation of the population in statistical sampling) increases, the required sample size increases significantly. For highly variable populations, we generally stratify the population into two or more ranges, each of which represents a less diverse population which can be independently sampled. For tests of controls and monetary unit sampling, variability is addressed through an expected error rate.</p>
Expected Error Rate	<p>The expected error rate reflects the tester's assessment of the <i>probable</i> rate of noncompliance or amount of error. It is used for tests of controls that use monetary unit sampling. An estimate of the expected amount of error in a particular account balance or group of transactions is based on the following factors:</p> <ul style="list-style-type: none"> • Understanding of the entity's business • Prior years' tests of the population • Results derived from a small pilot sample
Desired Reliability Level	<p>In determining an acceptable level of risk, the Tester should consider the degree of audit risk that is appropriate and the reliance that can be placed on the internal control structure and other audit procedures. In statistical sampling, this is expressed as a reliability or confidence level that the results will provide correct information about the whole population. Reliability or confidence levels in the range of 90%-95% would be typical for many audit tests.</p>
Tolerable Error Rate	<p>The tolerable error is an estimate of the maximum rate of noncompliance or level of error that the Tester is willing to accept in an account balance or group of transactions. Viewed from a different perspective, it is the potential error rate that a given sample is designed to detect with a given level of confidence. Lower tolerable error requires larger sample sizes, all other things being equal.</p>
Population Size	<p>Although sample sizes increase for larger populations, the increase is not proportional and, for large populations (>5000 units), the impact is negligible. For example, all other factors held constant, if a population of 1000 required a statistical sample of 85, a population of 50 would require a sample of 33 and a population of 100,000 would require a sample of 93.</p>

APPENDIX 7.2

SAMPLE SIZE GUIDANCE

Below is the recommended sample size table to be used based on level of risk:

Frequency of Control	Estimated Population	Range of Sample Size	Risk		
			Low	Medium	High
More than daily	More than 250	25-40	25	30	40
Daily	61-250	15-25	15	20	25
Weekly	40-60	5-10	5	7	10
Bi-Weekly	20-30	3-7	3	5	7
Monthly	12	2-4	2	3	4
Quarterly	4	2	2	2	2
Annually	1	1	1	1	1
Automated	N/A	1	1	1	1

Note 1: The risk assessment of a specific process is based on the judgment of the tester and is a function of the process' level of complexity, routineness, centralization, and automation.

Note 2: For controls with a frequency of "As needed" or "Event Based", use the "Range of Sample Size" guidance above that is closest to the estimated population. For example, if a control occurs as needed and the actual or estimated population equals 45 occurrences, then our sample size guidance indicates we should follow the "Weekly" frequency which is the closest estimated population size noted above.

APPENDIX 7.3

TEST PLAN TEMPLATE

Document:	Test Plan
Entity:	Agency Name
Reporting Date:	
Process:	
Financial Statement Accounts:	

Prepared by:	
Reviewed by:	

Ref	Control Description	Control Reference	Process	Process Risk Rating	Objective of Test	Testing Procedures	Results	Conclusion	Issue Raised?	Testing w/p ref
1	All invoices are approved by the AP Clerk prior to validation.	AP8	Processing Invoices	High	Purchases are appropriately authorized.	Select invoices paid during the year. Confirm that approvals for all invoices paid are consistent with the signature log maintained by the AP Department.	Exceptions noted.	Ineffective	Y	P2P.Testing Leadsheet; Issue Summary Log

Note: Line 1 for example purposes only

APPENDIX 7.4

TESTING LEADSHEET EXAMPLE

Document:	Testing Leadsheet	Performed by:	XX Smith						
Entity:	Agency ABC	Reviewed by:	XX Thomas						
Reporting Date:	6/30/XX								
Process:	Purchase to Pay								
Control Reference:	AP13								
Control Description:	G/L accounts and AP subledgers are reconciled on a monthly basis by the AP Accountant. Reconciliations are reviewed and approved by the AP Supervisor.								
Sub-Process:	Update to GL	← The transaction or sub-process within which the control resides.							
Sub-Process Risk Rating:	Moderate	← The risk ranking associated with the sub-process based on the risk assessment.							
Control Owner:	AP Accountant	← The person responsible for performing the control.							
Control Type:	IT-dependent Manual	← Manual, IT-dependent Manual, or Automated							
Control Frequency:	Monthly	← How often the control is performed (i.e., daily, weekly, monthly, etc.)							
Sample Methodology:	Random	← How the sample was selected (i.e., random, judgmentally, haphazardly, etc.)							
Sample Size:	4	← Number of items selected based on Sample Size Guidance Table (refer to Handout 1)							
Source Test Documents:	Accounts Payable Reconciliations	← Documentation obtained as evidence for test.							
Procedures / Testing Discussion:	Randomly selected 4 months from 20XX and obtained reconciliation of AP subledger to G/L from AP Accountant.		← Procedures should start with how the sample was selected and state procedures performed for testing including who provided source documents.						
Definition of an Exception:	An exception will be noted under any of the following conditions: No evidence of AP Supervisor's sign-off on AP Reconciliation No evidence of reconciling items for significant/unexplained differences		← Define what an exception will be before testing.						
Sample #	Month	A	B	C	D	E	W/P ref	← List each sample item selected. For each test selection, include any unique identifiers such as month, check #, invoice #, etc. it and whether each attribute was satisfied or not.	
1	January	x	x	x	x	x			
2	February	x	x	x	x	x			
3	March	x	x	x	x	o, Note 2			
4	April	x	o, Note 1	x	x	x			
Attributes:	A	Reconciliation between AP subsidiary ledger to GL performed by AP Supervisor.							← Attributes section lists each attribute that was tested.
	B	Evidence of AP Supervisor sign-off.							
	C	Amount in AP Reconciliation ties to AP Subledger detail							
	D	Amount in AP Reconciliation ties to Trial Balance							
	E	Evidence of reconciling items for significant/unexplained differences							
Tickmark Legend:	x	Attribute satisfied without exception.							← Tickmark Legend section is used to explain tickmarks used in the testing matrix above.
	o	Attribute not satisfied.							
	n/a	Attribute not applicable.							
	Note 1	AP Supervisor did not sign-off on the AP Reconciliation.							
	Note 2	No evidence to support reconciling items.							
Results:	For one of the four selections, no evidence of review existed. For one of the four selections, no supporting documentation for reconciling items existed.							← The results section should summarize the results of testing, note any exceptions and describe any observations.	

APPENDIX 7.5

DOCUMENT REQUEST TEMPLATE

Document:	Document Request List
Entity:	<i>Agency Name</i>
Reporting Date:	
Process:	
Financial Statement Accounts:	

Prepared by:	
Reviewed by:	

Item	Control Reference	Agency Contact	Date Requested	Date Received

APPENDIX 7.6

ISSUE SUMMARY TEMPLATE

Agency Name
Issue Summary Log
June 30, 20XX

	Process	Control	Control Reference	Issue	Risk/Implication	Recommendation	Management's Response
1	<i>Purchase to Pay - New Vendor Set-Up</i>	<i>Vendor maintenance is performed by the AP department and limited to supervisors. Role-based security is utilized in Application XYZ, such that individuals having access to perform vendor maintenance do not also have access to perform other Accounts Payable functions - process vouchers and print checks.</i>	<i>AP4</i>	<i>We obtained a user access log for Application XYZ for vendor maintenance and noted that there are excessive users with access. Additionally, we noted that a few of the users with access to vendor maintenance had the ability to perform other AP functionality. Issue was noted during walkthrough.</i>	<i>Unauthorized or incorrect changes are made to the vendor master file, increasing the risk of fraudulent payment transactions.</i>	<i>We recommend that management review the listing of AP users and their access rights in detail to help ensure that access to perform vendor maintenance be restricted to only AP supervisors. Additionally, we recommend that those AP supervisors be restricted from performing other AP functions.</i>	<i>A listing of users with access to perform vendor maintenance will be reviewed for appropriateness by Joe Controller and restricted only to AP supervisors. Additionally, a segregation of duties review will be performed to further restrict access within the AP department.</i>

Note: Line 1 is for example purposes only