

STATE OF *[NAME]*

THE INTERNAL CONTROL GUIDEBOOK

[DATE]

THIS PAGE LEFT BLANK INTENTIONALLY

PREFACE

The *Internal Control Guidebook* was developed based on the principle that the effectiveness of internal control depends on how well employees perform their control-related responsibilities. Because every individual in an organization has some role in effecting internal control, one objective of the *Guidebook* is to help managers and employees better understand the elements of their jobs that contribute to the internal control structure and to improve their performance.

The second tenet of this *Guidebook* is the belief that, given the proper tools, state agency personnel can conduct their own internal control review. Contained in the appendices to the *Guidebook* are a variety of hands-on tools that can be used *right now, starting today* to conduct an internal control assessment.

The material contained in the *Guidebook* is comprehensive. However, it is not a textbook and it does not address every potential control weakness or deficiency that may exist in an agency's internal control system. Instead, the *Guidebook* should be considered a work-in-progress that will be added to and modified in the months and years ahead. In fact, agencies are encouraged to adapt the questionnaires, flowcharts, and other tools to fit their specific circumstances.

The *[Name of Agency/Division]* is always interested in hearing feedback from its customers. Please send any comments or suggestions to *[Name of Internal Control Officer]* at *[email address]* or fax to *[phone number]*.

[Name of Administrator]
[Name of Agency/Division]

THIS PAGE LEFT BLANK INTENTIONALLY

ACKNOWLEDGEMENTS

The *[Name of Agency/Division]* wishes to acknowledge *[Names]*.

THIS PAGE LEFT BLANK INTENTIONALLY

**THE INTERNAL CONTROL GUIDEBOOK
TABLE OF CONTENTS**

CHAPTER ONE: INTERNAL CONTROLS – WHO NEEDS THEM?	1
A. The Role of the <i>[Agency/Division]</i>	1
B. Applicability of <i>[Internal Control Policy XXXX – Title]</i>	1
C. What is Internal Control over Financial Reporting?	2
D. Why Do We Need Internal Controls?	3
E. Effect of Information Technology on Internal Control	4
F. Limitations of Internal Control	5
CHAPTER TWO: THE FIVE HORSEMEN OF INTERNAL CONTROL	6
A. Control Environment	6
B. Risk Assessment	7
C. Control Activities	9
D. Information and Communication	10
E. Monitoring	11
CHAPTER THREE: ACTIVITIES FOR THE CONTROLLING MIND	12
A. Transaction Processing Errors and Frauds	12
B. Control Methods and Techniques	13
CHAPTER FOUR: ALL SYSTEMS GO	19
A. Potential Benefits of Using IT in the Financial Reporting Process	19
B. Potential Risks of Using IT in the Financial Reporting Process	19
C. General Controls Versus Application Controls	20
D. The Role of the IT Specialist	21
CHAPTER FIVE: “THE PLAN”	23
CHAPTER SIX: TESTING, TESTING, 1-2-3	27
A. Document Review	27
B. Surveys and Inquiries	28
C. General Computer Controls	29
A. Using Focus Groups	30

- B. Observation.....31**
- C. Re-performing Control Procedures31**
- D. Reconciliations32**
- E. Application Controls32**
- F. Summary33**

- CHAPTER SEVEN: THE BOTTOM LINE 34**
- A. Judging the Severity of Internal Control Deficiencies34**
- B. Reporting Guidelines36**

CHAPTER ONE: INTERNAL CONTROLS – WHO NEEDS THEM?

A. The Role of the [Agency/Division]

[Statute/regulation/policy] states that the [Agency] under the direction of the Governor and as provided by law, is responsible generally for the administration and coordination of internal accounting and other affairs, controls, procedures and services of a fiscal nature of the state government and agencies thereof. [Statute/regulation/policy] empowers [Agency] to direct and control the accounting for all the fiscal affairs of the state government and agencies thereof and to provide for the maintenance of the accounting records for those fiscal affairs. [Agency] is also responsible for establishing and maintaining systems of accounting and for prescribing the principles, standards and related requirements of those systems. Under [Statute/regulation/policy], [Agency] is to control and supervise the acquisition, installation and use of all electronic or automatic data processing equipment to be used primarily for the purposes of the accounting records and system referred to in [Statute/regulation/policy].

Within [Agency], the [State Controller's Division] has primary responsibility for carrying out these directives. In particular, the [State Controller's Division] is responsible for providing reliable and efficient statewide accounting and payroll systems, protecting the accuracy and integrity of statewide financial information, and promoting fiscal accountability, compliance and sound financial management. The [State Controller's Division] communicates its support of these objectives through publication of the [State Accounting Manual]. The policies and procedures contained in the [State Accounting Manual] are intended to enhance internal controls and promote financial discipline. Appropriately, the focus of this document is the applicability of [Internal Control Policy XXXX].

B. Applicability of [Internal Control Policy XXXX]

[Internal Control Policy XXXX] is the first policy in the [State Accounting Manual] chapter devoted to "Internal Control." It focuses on management's responsibilities for establishing and maintaining agency internal controls. Essentially, internal control is defined as a coordinated set of policies and procedures used by managers to ensure that their agencies, programs, or functions operate efficiently and effectively in conformance with applicable laws and regulations, and that the related transactions are accurate, properly recorded and executed in accordance with management's directives.

Throughout the year, management is expected to conduct reviews, tests and analyses of internal controls to ensure their proper operation. Agency management is responsible for the extent of the efficiency and effectiveness of internal controls, as well as any deficiencies. When weaknesses are identified, including any internal or external audit findings, a plan and schedule for corrective action should be prepared.

The purpose of this *Guidebook* is to provide a tool that agencies can use in performing internal control evaluations. The *Guidebook* is consistent with the internal control model developed by the [Committee of Sponsoring Organizations of the Treadway Commission](#) (COSO) discussed in [Internal Control Policy XXX].

The COSO framework, which is well accepted by accounting authorities and professionals, identifies three categories of internal control objectives:

- Efficiency and effectiveness of operations
- Financial reporting
- Compliance with laws and regulations

Although an agency's internal control plan may address objectives in each of these categories, not all of the objectives and related controls are relevant to financial reporting. Generally, the focus of the *[State Controller's Division]* is on internal control objectives and activities that pertain to financial reporting. However, since some controls may achieve objectives in more than one category, *all* controls that could materially affect financial reporting shall be considered for purposes of this *Guidebook* as part of *internal control over financial reporting*.

Because agencies in state government vary in size, complexity, and degree of centralization, no single method of internal controls is universally applicable. This *Guidebook* provides a general framework. It is management's responsibility to develop the detailed internal control policies, procedures, and practices that best fit each agency's business needs.

C. What is Internal Control over Financial Reporting?

For purposes of this document, internal control over financial reporting is defined as follows:¹

Internal Control over Financial Reporting

Internal control over financial reporting is defined as a process designed by, or under the supervision of the entity's principal executive and principal financial officers, or persons performing similar functions, and effected by the entity's governing board, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

1. Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the entity;
2. Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the entity are being made only in accordance with authorizations of management and directors of the entity; and
3. Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the entity's assets that could have a material effect on the financial statements.

¹ This definition was adapted from the definition of internal control set forth in Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 5: *An Audit of Internal Control over Financial Reporting That is Integrated with an Audit of Financial Statements*, June 12, 2007.

This definition reflects certain fundamental concepts:

- Internal control is a process. It is a means to an end, not an end in itself.
- People are what make internal control work. Internal control is not just the policies and procedures contained in an accounting manual. Personnel play an important role in making internal control happen.
- No matter how well designed and operated, internal control can provide only reasonable (not absolute) assurance that all agency objectives will be met.

When designing and implementing internal control activities, managers should consider the following four basic principles:

- Internal control should benefit, rather than hinder, the organization. Internal control policies and procedures are not intended to limit or interfere with an agency's duly granted authority related to legislation, rule-making or other discretionary policy-making.
- Internal control should make sense within each agency's unique operating environment.
- Internal control is not a set of stand-alone practices. Internal control is woven into the day-to-day responsibilities of managers and their staff.
- Internal control should be cost effective.

Internal control is not a separate, static system. Instead, it should be viewed as a continuous series of actions and activities that are interwoven throughout an entity's operations. In a sense, internal control is management control built into the entity as part of its infrastructure to help managers run the entity and achieve their goals on an ongoing basis.

D. Why Do We Need Internal Controls?

Accountability

Agency managers are responsible for managing the resources entrusted to them to carry out government programs. A major factor in fulfilling this responsibility is ensuring that adequate controls exist. Adequate internal controls allow managers to delegate responsibilities to subordinate staff and contractors with reasonable assurance that what they expect will happen, actually does.

The concept of accountability is intrinsic to the governing process. Public officials, legislators, and taxpayers are entitled to know whether government funds are handled properly and in compliance with applicable laws and regulations. They need to know whether government organizations, programs, and services are achieving the objectives for which they were authorized and funded. A key factor in achieving these objectives and minimizing operational problems is the implementation of appropriate internal control.

Encourage Sound Financial Management Practices

Management's role is to provide the leadership that an agency needs to achieve its goals and objectives. Part of that responsibility encompasses establishing internal control policies and

procedures designed to safeguard agency assets, check the accuracy and reliability of financial data, promote operational efficiency, and encourage adherence to prescribed managerial policies and compliance with applicable laws and regulations. The exact plan of internal control will depend, in part, on management's estimation and judgment of the benefits and related costs of control procedures, as well as on available resources.

Effective internal control helps managers cope with shifting environments and evolving demands and priorities. As programs change and as agencies strive to improve operational processes and implement new technologies, management must continually evaluate its internal control to ensure that the control activities being used are effective and updated when necessary.

Facilitate Preparation for Audits

Each agency is periodically subject to audit by the *[Name of financial statement auditors]*, federal auditors and; in some cases, by internal auditors. These audits are conducted to ensure the following:

- Public funds are administered and expended in compliance with applicable laws and regulations;
- Agency programs are achieving the objectives for which they were authorized and funded;
- Programs are managed economically and efficiently;
- Financial statements accurately represent the financial position of the State of *[Name]*; and
- Information system controls exist and provide a reasonable basis for relying on system results.

Only in rare instances, where audit procedures are developed to accomplish very limited objectives, will an audit not include an assessment of an agency's system of internal control.

Fraud Prevention

Managers are accountable for the adequacy of the internal control systems in their agencies. Weak or insufficient internal controls may result in audit findings and, more importantly, can lead to theft, shortages, operational inefficiency, or a breakdown in the control structure.

E. Effect of Information Technology on Internal Control²

The use of information technology (IT) affects the fundamental manner in which transactions are initiated, recorded, processed, and reported. In a manual system, an entity uses manual procedures to record transactions in a paper format. Internal controls are also manual and may include such procedures as approvals and reviews of activities, reconciliations and follow-up of reconciling items.

² This subsection on the effect of IT on internal control was adapted from AICPA Professional Standards, AU Section 319.17, *Consideration of Internal Control in a Financial Statement Audit*.

Alternatively, computerized information systems use automated procedures to initiate, record, process and report transactions. As a result, records are stored in electronic formats that may replace paper documents. Controls for computerized systems generally consist of a combination of automated controls (e.g., controls embedded in the computer programs) and manual controls. The manual controls may be independent of IT; they may use information produced by IT; or they may be limited to monitoring the information systems and automated controls and handling exceptions. The mix of manual and automated controls will vary with the nature and complexity of an entity's use of IT.

F. Limitations of Internal Control³

Internal controls, no matter how well designed and operated, can provide only *reasonable assurance* to management regarding the achievement of an entity's objectives, the reliability of reports, and compliance with laws and regulations. Certain limitations are inherent in all internal control systems.

Cost will prevent management from installing an ideal system and, for this reason, management will choose to take certain risks because the cost of preventing such risks cannot be justified. In addition, *more* is not necessarily *better* in the case of internal controls. Not only does the cost of excessive or redundant controls exceed the benefits, but a negative perception may also result. If employees consider internal controls to be "red tape," this viewpoint can adversely affect their regard for internal controls in general.

A second limitation to internal control is the reality that the process is subject to *human judgment* which can be faulty. Breakdowns can also occur because of simple errors or mistakes. Management may fail to anticipate certain risks and, thus, does not design and implement appropriate controls. Controls can also be circumvented by the collusion of two or more people and/or by management's improper override of the system.

These limitations apply to information technology (IT) as well. For example, errors may occur in designing, maintaining, or monitoring automated controls. If an organization's IT personnel do not completely understand how an order entry system processes sales transactions, they may erroneously design changes to the system that impact the wrong product line. Conversely, these changes may be correctly designed but misunderstood by the people responsible for translating the design into program code. Errors also occur in the use of information produced by IT. Automated controls may be designed to report transactions over a specified dollar limit for management review. However, if individuals responsible for the review do not understand the purpose of the reports, they may fail to review them and, as a result, will fail to investigate unusual items.

³ The discussion on the limitations of IT controls was adapted from AICPA Professional Standards, AU Section 319.21, *Consideration of Internal Control in a Financial Statement Audit*.

CHAPTER TWO: THE FIVE HORSEMEN OF INTERNAL CONTROL

Each agency's and each business unit's internal controls and internal control plan will be unique; however, the internal control components set forth in this chapter should be incorporated into all systems of internal control. Using the COSO model, referred to in *Chapter One*, the internal control process can be broken down into five interrelated components that are derived from and integrated with the management process. These five components, which are the necessary foundation for an effective internal control system, include:⁴

- Control environment
- Risk assessments
- Control activities
- Information and communication
- Monitoring

A. Control Environment

The *control environment* of a state agency sets the tone of the organization and influences the effectiveness of internal controls within the agency. The control environment is an intangible factor. Yet, it is the foundation for all other components of internal control, providing discipline and structure and encompassing both technical competence and ethical commitment. Managers must evaluate the internal control environment in their own business unit and agency as the first step in the process of analyzing internal controls. Many factors determine the control environment, including the following:

- **Management's attitude, actions, and values** set the tone of an organization, influencing the control consciousness of its people. Internal controls are likely to function well if management believes that those controls are important and communicates that view to employees at all levels through policy statements, codes of conduct and by behavioral example.

Management demonstrates a positive attitude toward internal control by providing appropriate training and including internal control in performance evaluations, discussing internal controls at management and staff meetings, and by rewarding employees for

⁴ The information presented in this chapter is based on the principles set forth in *Internal Control—Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission (COSO), American Institute of Certified Public Accountants, USA, 1992.

good internal control practices. Management supports good internal controls by emphasizing the value of internal auditing and being responsive to information developed through internal and external audits.

- **Commitment to competence and human resources policies and practices.** Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Managers are required to comply with established personnel policies and practices for hiring, training, evaluating, promoting, and compensating employees, and to provide employees the resources necessary to perform their duties. Hiring and staffing decisions include pertinent verification of education and experience and, once on the job, the employee is given the necessary formal and on-the-job training.

Management should provide candid and constructive counseling and performance appraisals. Promotions driven by periodic performance appraisals demonstrate commitment to the advancement of qualified personnel to higher levels of responsibility.

- **Assignment of authority and responsibility; organizational structure.** This factor includes management's responsibility for defining key areas of authority and responsibility and establishing appropriate lines of reporting. Management should provide policies and direct communications so that all personnel understand the agency's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

In addition to organizational hierarchies, a proper segregation of duties is a necessary condition to make control procedures effective. Management should ensure adequate separation of the following responsibilities: authorization of transactions, recording of transactions, custody of assets, and periodic reconciliation of existing assets to recorded amounts.

- **Advisory board participation.** The involvement of an agency's governing board in a review of internal controls and audit activities can be a positive influence on the agency's control environment.

B. Risk Assessment

Organizations exist to achieve some purpose or goal. Goals, because they tend to be broad, are usually divided into specific targets known as objectives. A *risk* is anything that endangers the achievement of an objective.

Risk assessment, the second internal control component, is the process used to identify, analyze, and manage potential risks. Over the course of time, situations can occur which prevent a business unit or an agency from fulfilling its responsibilities and meeting its goals and objectives. Because of this possibility, successful managers continually identify and analyze potential risks to their organizations.

- What circumstances might endanger future funding of agency programs?
- What practices are being questioned by auditors and other oversight agencies?

- What information is critical to the agency's operations and how vulnerable is it?
- What activities are regulated by the federal government?
- Which areas are most susceptible to fraud?
- Are assets (cash, inventory, fixed assets) adequately protected?

When beginning a risk assessment, managers should start by analyzing the two circumstances most likely to create problems: *change* and *inherent risk*.

Periods of Change

The risk that objectives will not be achieved increases dramatically during a time of change. Some examples of circumstances that expose an agency to increased risk are listed below:

- Changes in management responsibilities
- Disruption of information systems processing due to new or revamped systems
- Rapid growth and/or new technology
- New programs or services
- Re-engineering agency operating processes
- Downsizing agency operations
- Early retirements that reduce workforce and knowledge base

Inherent Risks

The second risk category involves activities, which due to their nature, have a greater potential for loss from fraud, waste, unauthorized use, or misappropriation. Cash handling, for example, has a much higher inherent risk for theft than data entry activities do.

Other examples of activities where inherent risk is high include the following:

- Situations and systems that involve great *complexity* increase the risk that a program or activity will not operate properly or comply fully with applicable regulations.
- *Third party beneficiaries* are more likely to fraudulently attempt to obtain benefits when those benefits are similar to cash.
- *Decentralization* increases the likelihood that problems will occur. However, a problem in a centralized system may be more serious than a problem in a decentralized system because, if a problem does exist, it could affect the entire agency.
- A *prior record of control weaknesses* often indicates a higher level of risk because bad situations tend to repeat themselves.

- A *lack of corrective actions* in response to control weaknesses identified in prior audits often indicates that future problems are likely to occur.

Evaluate Identified Risks

Once potential risks are identified, they should be analyzed for their possible effect.

- *How important is this risk?*
- *How likely is it that this risk will occur?*
- *How large is the dollar amount involved?*
- *To what extent does the risk potential of one activity affect other activities?*
- *Are existing controls (policies and procedures) sufficient to manage this risk?*
- *To what degree are secondary controls in place?*

Both quantitative and qualitative ranking activities ([link to Risk Assessment Form??](#)) should be used to evaluate the severity of identified risks and the likelihood of their occurrence. A moderate loss that is likely to occur may pose as much danger as a more serious loss that is less likely to occur.

Risk Response

Many risks are accepted or avoided by implementing effective control activities ahead of time. Other risks, beyond our control (e.g. a severe weather event or power outage that prevents access to financial systems) should also be identified. Managers must be ready to respond to these with a set of activities (e.g. disaster recovery plan).

C. Control Activities

Once managers identify and assess risks, the next step is to develop methods to minimize the risks. These methods are referred to collectively as *control activities*, the third component of internal control. By control activities, we mean the *policies, procedures, techniques, and mechanisms* that enforce management's directives. Control activities occur at all levels and functions. They include a wide range of diverse activities such as approvals, authorizations, verifications, reconciliations, performance reviews, security measures, and the creation and maintenance of appropriate documentation. In short, these activities represent basic management practices. See example below.

ACCOUNTS PAYABLE UNIT

OBJECTIVE No. 1: Compliance with statewide bill paying policies.

- RISK No. 1:** A/P staff does not have required knowledge, skills and ability.

- i. **MITIGATING CONTROL NO. 1:** All A/P employees receive training within 2 weeks of hire.
 - ii. **MITIGATING CONTROL NO. 2:** The A/P accounting manager designates staff for cross-training.
- b. **RISK NO. 2:** Payments are made too late to take vendor discounts.
- i. **MITIGATING CONTROL NO. 1:** All invoices are date-stamped upon receipt in the Financial Services office.
 - ii. **MITIGATING CONTROL NO. 2:** Monthly reports are generated that help A/P identify and investigate reasons for late payments.

Managers should be careful to avoid excessive control, recognizing that absolute assurance is generally not achievable and would be prohibitively expensive and impede productivity. When a problem arises, before implementing a new policy or procedure, managers should make sure that a relevant policy does not already exist that simply needs to be enforced.

Chapter Three presents a detailed discussion of the control methods and techniques commonly used by managers to mitigate risks.

D. Information and Communication

An agency's control structure must provide for the identification, capture and exchange of information both within the agency and with external parties. For example, management relies on the information system, including the accounting system, for reporting on agency or program activities to the Legislature, oversight agencies, and federal grantors. Accurate information communicated in a timely manner is, therefore, the focus of the fourth component of internal control.

Within the organization, communication must be up, as well as down. Supervisors must communicate duties and responsibilities to their staff. Staff and middle management must be able to alert upper management to potential problems. Administrative and program staff must communicate requirements and expectations to each other. Well-designed internal controls outline the specific authority and responsibility of individual employees in carrying out their day-to-day activities. They also serve as a point of reference for employees seeking guidance when unusual situations arise.

Sending information electronically allows management to immediately distribute new procedures and other information to a large staff. Agencies should consider conducting in-house training sessions upon releasing new or revised internal control policies and procedures. Internal control concepts should be emphasized as a part of the orientation for new employees. Managers should reinforce policies and procedures through their own actions and words.

Effective communication also encourages employee involvement. Agencies should consider establishing a process that supports recommendations from employees for quality improvement and acknowledges good suggestions with meaningful recognition. Employees should also feel

they can report suspected improprieties without fear of reprisal and that their anonymity and confidentiality will be respected.

E. Monitoring

After risks have been identified, policies and procedures put into place and information on control activities communicated, managers must implement the fifth component of internal control, *monitoring*. Monitoring assesses the quality of internal controls over time, making adjustments as necessary. Like the other four components, monitoring is a basic management practice that involves activities such as performance evaluations; ongoing supervisory activities, reviews and analyses; and independent evaluations of internal controls performed by management or other parties outside of the process. Proper monitoring ensures that controls continue to be adequate and to function properly.

Monitoring allows a manager to identify whether controls are being followed before problems occur. For example, a business unit's internal control plan may identify situations where cross-training is required. If the manager does not monitor the plan to ensure that cross-training occurs on a regular basis, he or she may discover too late that the back-up staff will not be able to handle the operations when circumstances change.

The monitoring process should also include policies and procedures designed to ensure that the findings of audits and other reviews are promptly resolved. Managers should determine the proper remedies in response to audit findings and complete, within established time frames, all actions needed to correct identified deficiencies.

Control activities help ensure that management directives are carried out. They include (1) performance reviews, such as an analysis and follow-up of budget variances; (2) transaction processing controls, including approvals, verifications and reconciliations; (3) physical controls designed to ensure safeguarding and security of assets and records; and (4) segregation of duties designed to reduce opportunities for a person to be in a position to perpetrate and conceal errors and frauds when performing normal duties.

A. Transaction Processing Errors and Frauds

Control activities (both computerized and manual) are imposed on the accounting system for the purpose of preventing and detecting errors and frauds that might enter and flow through to the financial statements.

Seven Categories of Errors and Frauds

1. *Invalid transactions are recorded:* Fictitious revenue transactions are recorded and charged to nonexistent customers.
2. *Valid transactions are omitted from the accounts:* Shipments of merchandise to customers are not recorded.
3. *Unauthorized transactions are executed and recorded:* A customer's order is not approved for credit, yet the goods are shipped and/or the service is provided and billed to the customer without requiring payment or an advance deposit.
4. *Transaction amounts are inaccurate:* A customer is billed and the sale is recorded in the wrong amount because the quantity shipped and quantity billed are not the same and the unit price is for a different product.
5. *Transactions are classified in the wrong accounts:* Expenditures for capital acquisitions are coded and charged to an operating supplies object.
6. *Transaction accounting and posting are incorrect:* Sales are posted in total to the accounts receivable GL control account, but not all of them are posted to the individual customer account records in the subsidiary ledger.
7. *Transactions are recorded in the wrong period:* Purchases made in one fiscal year (June) are recorded as expenditures in the next fiscal year when the invoice is received (July). Revenues attributable to July are recorded as transactions occurring in June.

Management's task is to design control activities that prevent, detect and correct these and other potential errors and other frauds. Front-end, or *preventive*, controls are performed before an action takes place. For example, a supervisor or manager must approve an invoice before it is processed for payment. Back-end, or *detective*, controls examine transactions after they have been processed to ensure they are appropriate. An example would be the month-end reconciliation of cash account balances to the bank statement to ensure that all payments have been recorded. Sometimes, the existence of detective controls can also serve to prevent irregularities. An individual tempted to use agency funds inappropriately may be deterred by the knowledge that the bank account is regularly reconciled.

B. Control Methods and Techniques

Control activities can be automated or manual, have various objectives and are performed at various organizational and functional levels. Generally, control activities that pertain to financial reporting can be grouped into the following categories.

Segregation of Duties

Segregation of duties is one of the most important features of an internal control plan. The fundamental premise of segregated duties is that an individual or small group of individuals should not be in a position to initiate, approve, undertake and review the same action. These are called incompatible duties when performed by the same individual. Examples of incompatible duties include situations where the same individual (or small group of people) is responsible for:

- Managing both the operation of and recordkeeping for the same activity.
- Managing custodial activities and recordkeeping for the same assets.
- Authorizing transactions and managing the custody or disposal of the related assets or records.

Stated differently, there are four kinds of functional responsibilities that should be performed by different work units, or at a minimum, by different persons within the same unit:

- *Authorization to execute transactions:* This duty belongs to persons with authority and responsibility to initiate and execute transactions.
- *Recording transactions:* This duty refers to the accounting or recordkeeping function, which in most organizations, is accomplished by entering data into a computer system.
- *Custody of assets involved in the transactions:* This duty refers to the actual physical possession or effective physical control/safekeeping of property.
- *Periodic reviews and reconciliation of existing assets to recorded amounts:* This duty refers to making comparisons at regular intervals and taking appropriate action to resolve differences.

The advantage derived from an appropriate segregation of duties is twofold:

- Fraud is more difficult to perpetrate because it would require collusion of two or more persons, and most people hesitate to seek the help of others to conduct wrongful acts.
- By handling different aspects of the transaction, innocent errors are more likely to be found and flagged for correction.

At a minimum, an agency's plan of internal control should ensure that the following activities are properly segregated:

1. Personnel and Payroll Activities

- Individuals responsible for hiring, terminating and approving promotions should not be directly involved in preparing payroll or personnel transactions or inputting data.
- Managers should review and approve payroll deductions and time sheets before data entry, but should not be involved in entering payroll transactions.
- Individuals involved in payroll data entry should not have payroll approval authority. Individuals who are part of the payroll staff should not enter changes to their own data files.
- An individual who is not involved in the payroll process should periodically verify all personnel salaries and wage rates.
- Unless otherwise approved, dual update access to the central payroll processing system and the human resources personnel database should not be permitted.
- Gross pay adjustment reports should be received and reviewed by an individual outside of the payroll function.

2. Other Expenditure Activities

- Individuals responsible for cash disbursement functions should be segregated from those responsible for cash receipts.
- Individuals responsible for data entry of encumbrances and payment vouchers should not be responsible for approving these documents, nor batch release.
- A department should not delegate expenditure transaction approval to the immediate supervisor of data entry staff or to data entry personnel.
- Delegated expenditure authority must be in writing and approved by the appointing authority.
- Individuals responsible for acknowledging the receipt of goods or services should not also be responsible for purchasing or accounts payable activities.

3. Inventories

- Individuals responsible for monitoring inventories should not have the authority to authorize withdrawals of items maintained in inventory.
- Individuals performing physical inventory counts should not be involved in maintaining inventory records.

4. Check Writing Activities

- Individuals who prepare/record checks should not sign the checks.
- Individuals who prepare/record checks should not reconcile the checking account.

5. Revenue Activities

- Individuals responsible for cash receipts functions should be segregated from those responsible for cash disbursements.
- Individuals who receive cash into the office should not be involved in preparing bank deposits.
- Individuals who receive cash or make deposits should not be involved in reconciling the bank accounts.
- Individuals responsible for issuing agency billings should not be involved in estimating, budgeting, collecting or processing cash receipts and should not be directly involved in maintaining accounts receivable.
- Individuals responsible for maintaining accounts receivable records should not be directly involved in the billing process or cash receipting.

If agencies do not have sufficient staff to accomplish an optimum division of duties, management will need to be more actively involved in reviewing reports and reconciliations and ensuring transactions are adequately documented and properly authorized.

Access Controls

Control over physical access refers to the physical security of assets. Physical safeguards include secured facilities; limited access to assets and important records, documents and blank forms; and periodic physical counts that are compared with amounts shown on control records. Inventories of items held for sale and stocks of materials and supplies should not be available to persons who have no need to handle them. Likewise, access to accounts receivable records and payroll data should be denied to people who do not have a recordkeeping responsibility for them.

Access control over information systems means that access to program documentation, data files, programs and computer hardware is limited to the extent required by individual job duties. Access controls should include the use of multilevel security, user identifications coupled with

regularly changed passwords, limited access rooms, call backs and dial-up systems, use of file attributes and firewalls, and encryption of confidential information.

Periodic Reconciliations

Managers should provide for periodic comparison of recorded amounts with independent evidence of existence and valuation. Internal auditors and/or other members of the accounting staff can perform such comparisons on a regular basis. These individuals, however, should not also have responsibility for authorization of the related transactions, accounting or recordkeeping, or custodial responsibility for the assets.

Periodic comparisons may include reconciliation of bank statements, inventory counting, confirmation of accounts receivable and accounts payable. The more frequent the comparisons, the greater the opportunity to detect errors. The results of nightly processing in the central accounting system for example, should be compared the next morning to the agency's detail summary records. Cash account balances per the central accounting system should be reconciled monthly to monthly bank statements (and to the agency's internal subsystem if one is involved). For other records, the frequency of periodic comparisons must be balanced against the costs and benefits.

Subsequent action to correct differences is also important. Together, periodic comparisons and actions to correct errors lower the risk that material misstatements in the financial statements will occur.

Periodic Performance Comparisons

This category of controls includes periodic reviews of actual performance versus budgets, forecasts and prior period performance. Operating (activity-based) data is compared to financial data. The relationship of the two data sets is analyzed, with the differences investigated and corrective action taken if necessary. This type of control activity is usually performed by management employees that have no recordkeeping or custodial responsibilities.

Authority

Evidence must be maintained to demonstrate that only persons acting within the scope of their authority are allowed to authorize and execute transactions. Agencies need to document which persons have expenditure authority and the extent of that authority. The signature of authorized personnel is a matter of record and should be readily available for comparison when the underlying documents are audited. Periodically, the agency chief fiscal officer or delegate should perform reviews to ensure compliance.

Transfer transactions and adjusting entries, particularly year end financial statement entries, require special control to avoid errors and possible misstatement. Management oversight is critical. The supporting documentation should provide clear evidence that these transactions have been properly reviewed and authorized *before* they are entered into the accounting system.

Documentation Control

Internal control systems, all transactions and other significant events should be clearly documented, and the documentation should be readily available for examination at each agency.

- *Detailed written evidence of the internal control system*, its objectives and activities, is essential. This documentation is valuable to managers in controlling their operations and is useful to auditors or others involved in analyzing and reviewing operations. Written documentation facilitates job training by communicating specific responsibilities. The documentation should appear in management directives, administrative policy, and accounting procedure manuals. Many documentation tools are available such as checklists, flow charts, narratives, and software packages. These tools may be particularly helpful in documenting complex information systems and the related control activities.
- *Internal control reviews and risk analyses* should be documented. Supporting documentation for conclusions should be kept on file for [XXX] years.
- *Documentation of transactions* and other significant events should be timely, complete and accurate and should allow tracing the transaction or event from the source documents, while it is in process, through to the financial reports. It is important that each step in the transaction process is documented and the appropriate control accounts, ledgers and files are updated.

Regardless of format, the supporting documentation should indicate the purpose or reason for the transaction and that the transaction was properly authorized. The transaction amount should be clearly evident or easily verified upon recalculation. In addition, the documentation should fully support the information entered into the following data: fund number and/or project identifier, general ledger account, comptroller object; and vendor name/number, if applicable.

Adjusting entries, which include reclassifications, error corrections and year end financial statement adjustments must be fully documented. In cases where estimates are used, the estimates must be reasonable, based on relevant information and sufficiently documented. For system-generated transactions, documentation that clearly describes the methodology, formulas and calculations, and the applicable system links and processes should be maintained.

Finally, transaction documentation should be archived in accordance with state archival rules.

Supervision

The effectiveness of any system of internal control depends on continuous, qualified supervision of all staff. It is management's primary means of monitoring and maintaining a system of internal control. In fulfilling their responsibilities, managers and supervisors should:

- Assign tasks and establish written procedures for completing assignments.
- Systematically review each staff member's work.
- Approve work at critical points to ensure quality and accuracy.

- Provide guidance and training when necessary.
- Provide documentation of supervision and review (e.g., initialing examined work).

Adequate and timely supervision is especially important in small departments, where limited personnel make it difficult to establish a complete segregation of duties. Accounting and payroll reports are vital tools that managers can use in carrying out their supervisory responsibilities. The reports provide managers with timely information for transaction verification, analysis and forecasting, and reference purposes.

CHAPTER FOUR: ALL SYSTEMS GO

Because the accuracy and timeliness of financial reporting is to a large extent dependent on a well-controlled systems environment, more and more attention is being focused on the role of information technology (IT) in the financial reporting process. For most agencies, the role of information technology is critical to achieving an agency's financial objectives. Whether transactions are processed directly in central accounting system, or transmitted to the central accounting system from independent agency subsystems, IT systems are deeply embedded in the initiation, recording, processing and reporting of financial transactions.

A. Potential Benefits of Using IT in the Financial Reporting Process⁵

IT provides the following potential internal control benefits because it enables an agency to:

- Consistently apply predefined business rules and perform complex calculations in processing large volumes of transactions or data.
- Enhance timeliness, availability and accuracy of information.
- Facilitate additional analysis of information.
- Enhance the ability to monitor the performance of the agency's activities and its policies and procedures.
- Reduce the risk that control will be circumvented.
- Enhance the ability to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems.

B. Potential Risks of Using IT in the Financial Reporting Process

IT also poses specific risks to an agency's internal control, such as:

- Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.
- Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or nonexistent transactions or inaccurate recording of transactions.
- Unauthorized changes to data in master files.

⁵ The subsections on the potential benefits and risks of IT on internal controls were adapted from AICPA Professional Standards, AU Section 319.18 -319.19, *Consideration of Internal Control in a Financial Statement Audit*.

- Unauthorized changes to systems or programs.
- Failure to make necessary changes to systems or programs.
- Inappropriate manual intervention.
- Potential loss or compromise of data.

The use of computer systems to process financial transactions, store data, and perform statistical and other analysis does not change the internal control objectives already discussed. However, extensive use of computer systems may change the techniques used to meet control objectives. For example, when IT is used in an information system, segregation of duties may be achieved or enhanced by implementing access security controls.

C. General Controls Versus Application Controls

In an automated environment there are two broad categories of controls: *general controls* and *application controls*.

General Controls

General controls apply to all information systems—mainframe, minicomputer, network, and end-user environments; they impact the entire data processing environment, including application systems. General controls address data center and network operations; system software acquisition and maintenance; physical security, environmental protection, disaster recovery, hardware maintenance and computer operations. Other examples include program change controls; controls that restrict access to programs or data; controls over implementation of packaged software or development of new software applications; and controls over system software that monitors the use of system utilities that could change financial data without leaving an audit trail.

Application Controls

Application controls, on the other hand, are more specific to individual application systems. They include both computerized and manual controls and are designed to help ensure the completeness, accuracy, and validity of all information processed. Application controls should be installed at an application's interfaces with other systems to ensure that all inputs are received and are valid and outputs are correct and properly distributed.

- **Input control activities:** Input controls are designed to provide reasonable assurance that data received for computer processing have been properly authorized and converted into machine-sensible form, and that the data have not been lost, suppressed, added, duplicated, or improperly changed. Computerized input controls include validation procedures such as check digits, record counts, hash totals and batch financial totals. Computerized edit routines include valid character tests, missing data tests, sequence tests and limit or reasonableness tests – all designed to detect data conversion errors.
- **Processing control activities:** Processing controls are designed to provide reasonable assurance that data processing has been performed as intended without any omission or double-counting. Many processing controls are the same as the input controls, but

they are used during the actual processing phases. These controls include run-to-run totals, control total reports, file and operator controls, such as external and internal labels, system logs of computer operations, and limit or reasonableness tests.

- **Output control activities:** Output controls are designed to provide reasonable assurance that processing results are accurate and distributed to authorize personnel only. Control totals produced as output during processing should be compared and reconciled to input and run-to-run control totals produced during processing. Computer-generated change reports for master files should be compared to original source documents for assurance that data are correct.

General and application controls over computer systems are interrelated. General control supports the functioning of application control, and both are needed to ensure complete and accurate information processing. If general controls are inadequate, the application controls are unlikely to function properly and could be overridden.

The checklists developed in conjunction with this *Guidebook* contain questions that relate to IT general and application control objectives from a financial systems perspective. Large agencies with internal audit functions may have already addressed most of these questions, particularly those agencies that operate in highly complex data processing environments and have large IT organizations. All agencies, however, will find that answering these questions provides the following benefits:

- Assurance that the agency's IT operations and investment strategies, as they relate to financial systems, are well planned, properly staffed and executed in accordance with the agency and statewide IT strategies and security and control policies.
- Documentation that the agency has conducted a review of IT general and applications controls over financial systems, which can be incorporated into the agency's internal control plan.
- A tool that agencies, who are contemplating replacement of existing financial systems or who are currently in the implementation phase, can use to monitor and control the acquisition/development software project.

D. The Role of the IT Specialist⁶

When evaluating controls over computer processing, the presence of one or more of the following conditions may require the expertise of an IT specialist:

- Technology is an integral part of the agency's business processes, involving both its primary, customer-oriented activities and its support activities, such as general management, planning, finance and accounting.
- The agency has recently implemented a new IT financial system or made significant modifications to an existing financial system.

⁶ This subsection was adapted from the example on project team organization presented by Mr. Michael Ramos in his book entitled, *How to Comply with Sarbanes-Oxley Section 404 – Assessing the Effectiveness of Internal Control*, John Wiley & Sons, Inc., Hoboken, NJ, 2004.

- The agency is engaged in significant e-commerce activity.
- Data is shared extensively between computer applications.

The IT specialist can help the evaluation team identify risks related to the IT system, document and test controls, design and assist in implementing missing controls, and monitor the continued effectiveness of IT controls.

The successful completion of the IT component of the evaluation project will largely depend on (1) how well the evaluation team leader and agency financial management understand the risks inherent in IT systems, and (2) IT management's understanding of the financial reporting process and its supporting systems. Ideally, senior IT management should be well-informed concerning the types of IT controls needed to support reliable financial information processing.

CHAPTER FIVE: “THE PLAN”

[Internal Control Policy XXXX – Title] requires each agency head to designate one senior manager as the agency’s internal control officer. This person shall be responsible for the agency’s overall internal control review. Working with agency managers and other personnel, the internal control officer’s mission is to develop a cost effective approach that best fits the agency’s size, staff and budget.

To get started, agencies are encouraged to create an internal control team. The team will need to formulate a strategy, establish timelines and set milestones, assign tasks to key personnel and keep the agency head informed of progress. Certain activities that should be undertaken in conjunction with the internal control review include:

- Updating/creating policies and procedures to reflect current processes
- Updating organization charts
- Identifying and listing electronic files
- Identifying financial data reports/data warehouse queries, where they are located and how they are accessed (central accounting system, accounting data mart, central payroll processing system; payroll data mart, PC based)
- Reviewing the organization of paper filing systems and archiving procedures
- Completing an inventory of fixed assets

There is no single prescribed methodology for conducting an evaluation of internal controls. Agencies that have an internal audit unit may already have adopted one of several risk assessment models. These models generally involve an assessment of administrative controls, as well as fiscal controls. For those agencies that do not have an internal audit function, the balance of this chapter presents a plan to evaluate fiscal internal controls, using a six-step approach.

1. Identify who does what; obtain copies of agency governance documents (mission statement, charter of governing boards, code of conduct, human resource policies and personnel handbook, accounting manuals, etc.).
2. Determine what business cycles/processes/activities to evaluate.
3. Document the transaction processing cycles and related controls. Supplement written sources through inquiries and surveys.
4. Test the controls (how is the work being done versus how *should* the work be done).

5. Evaluate findings and report the results.
6. Monitor controls on a continuous basis.

AN INTERNAL CONTROL EVALUATION AND MONITORING PLAN

STEP 1: IDENTIFY WHO DOES WHAT

- a. **Introduction:** In this section of the internal control plan, identify the agency's internal control officer and his/her responsibilities for providing technical support and assistance. Include brief statements that address the frequency of internal control evaluations, the agency's commitment to maintaining an effective internal control system, and how recommendations for improvement are handled, including those based on the findings of the Secretary of State, Audits division and federal auditors, if applicable. Identify other internal control contacts/team members.
- b. **Agency Mission:** State the agency's mission and mandate and cite applicable statutory references.
- c. **Organizational Structure:** Include names and titles of executive management. Discuss agency programs, number of employees, internal plan of organization, etc. Insert an organizational chart.
- d. **Management's Key Internal Control Concepts:** Discuss the key internal control concepts, philosophies and actions already put into effect that significantly strengthen the agency's overall control environment. Incorporate the agency's governance documents.

STEP 2: DETERMINE WHAT TO EVALUATE

- a. **Set priorities:** Focus first on high risk divisions, business units, programs or activities. Incorporate management's special concerns and knowledge. Consideration should be given to the following factors.
 - The degree of centralization versus decentralization
 - Competency and integrity of personnel
 - Dollar amount of budget
 - Degree to which public purpose may be affected
 - Safeguarding of resources
 - Organizational checks and balances that may provide a type of secondary control
 - Negotiability of the assets involved
 - Legal mandates

Once the high risk divisions, programs and/or activities have been evaluated, a systematic plan should be established to review all other risk areas.

b. Identify financial cycles and sub-cycles: Most agencies have the following basic transaction cycles.

- Expenditures
- Revenue
- Inventory
- Fixed Assets
- Payroll
- Automated transaction processing
- Agency specific programs and activities

STEP 3: DOCUMENT THE TRANSACTION PROCESSING CYCLES

In this section of the plan, document the types and the flow of transactions, the persons who process the transactions and the related control features, such as reviews and approvals, for each financial cycle identified above. Interview and involve other senior and line managers in the documentation phase, as necessary. Ask them to make the following records available to the members of the internal control team: Flowcharts

- Policies and procedure manuals, desk procedure manuals
- Job descriptions
- Business unit organizational charts
- Output reports

Agencies may find that the documentation phase is best accomplished by using a combination of documentation tools and formats, such as checklists, questionnaires, flow charts, narratives, and software packages. *Initially, focus on key processes and key check points.* With each successive review, more details can be added.

Review prior internal and external audit reports. If control weaknesses identified in prior audits have not been corrected, it may be an indicator of further problems.

STEP 4: TEST THE CONTROLS

Use a variety of techniques to test internal controls and gather evidence. For example, an agency's "control environment" may be verified through document reviews, employee surveys, and management inquiries. For transaction-oriented controls, use an employee focus group to help identify the various control points in a processing stream and then perform a "walk-through" to test prescribed procedures against actual operations. See *Chapter Six* for more details on testing procedures and example survey/inquiry tools.

STEP 5: EVALUATE FINDINGS AND REPORT THE RESULTS

The next step is to evaluate your findings and determine whether existing controls are sufficient to manage the risks. The risk questions presented in *Chapter Two* are repeated here:

- *How important is this risk?*

- *How likely is it that this risk will occur?*
- *How large is the dollar amount involved?*
- *To what extent does the risk potential of one activity affect other activities?*
- *Are existing controls (policies and procedures) sufficient to manage this risk?*
- *To what degree are secondary controls in place?*

Be certain to confirm your findings and evaluation by discussing them with appropriate business unit and agency managers. Ask them to develop corrective action plans and to submit a schedule for completion.

Finally, document your findings, both positive and negative, in a written report that is presented to senior management. Include recommendations for improvements, identify any redundant controls that should be modified or eliminated, and present the business unit's responses and corrective action plans.

STEP 6: CONTINUOUS MONITORING

Review internal controls for high risk divisions, business units and activities annually, more frequently if warranted. Review areas of lower risk annually by spot checking key controls, with full reviews every five years, unless there are significant changes in the operating environment. Situations involving new programs, changes in personnel, agency reorganizations or new systems increase the exposure to risk and, therefore, require more frequent review. Perform follow up for prior evaluations to make certain that corrective actions have been taken.

CHAPTER SIX: TESTING, TESTING, 1-2-3⁷

The COSO framework (described in *Chapter Two*) divides internal controls into two different levels, the general, entity-wide level and the specific, activity-level. The approach presented in this *Guidebook* is to test the effectiveness of entity-level controls first. By understanding entity-level controls, the agency's internal control team should be better able to develop tests at the activity-level.

ENTITY-LEVEL TESTS

Because entity-level controls are indirect and not transaction oriented, they are not easily verified through observation or by re-performing transaction related tests. As a result, the internal control team will need to use other techniques to gather evidence to support their evaluation of entity-wide controls.

A. Document Review

Governance Documents

To start, obtain copies of the agency governance documents. The team should review these documents to ensure it understands the agency's mission. Generally, the governance documents will describe the membership of the governing board, including number of members, their qualifications, independence requirements and selection process and their roles and responsibilities. Throughout this process, the internal control team should keep in mind the importance to the governing board of receiving reliable and accurate information on a timely basis. The team may want to explore and suggest changes to the ways in which information is gathered and communicated to the board.

Code of Conduct

A written code of conduct helps establish values, norms and shared beliefs. The form and content of a code of conduct may vary greatly from agency to agency. Nonetheless, a typical code of conduct will include a statement of values, identification of key behaviors that are accepted and not accepted in the workplace, examples of ethical situations that agency personnel are likely to encounter, and information on reporting violations of the code and how they will be investigated.

Other Documentation

Most agencies document their human resource policies and communicate them to their employees in the form of a *personnel handbook*. For purposes of an internal control evaluation, the internal control team should focus on those policies that demonstrate the agency's commitment to competence and address expectations regarding integrity and ethical behavior. The agency's *accounting manual* should include important information relating to the procedures used to capture and process accounting information, the documents required and

⁷ This information in this chapter was adapted from the testing strategies and techniques presented by Mr. Michael Ramos in his book entitled *How to Comply with Sarbanes-Oxley Section 404 – Assessing the Effectiveness of Internal Control*, John Wiley & Sons, Inc., Hoboken, NJ, 2004.

the related control procedures. This information is typically most useful in documenting activity-level controls. However, the accounting manual may also provide important documentation that is relevant for entity-wide controls, such as those related to the annual financial closing process.

B. Surveys and Inquiries

Employee Surveys

Reviewing the written code of conduct and personnel policies, by themselves, will most likely not be sufficient to determine whether entity-level controls are operating effectively. One way to gather additional information is to develop and conduct an employee survey.

To ensure the most reliable and most valid results, many of the same concepts applicable to statistical sampling methods should be employed.

- The more respondents, the more reliable the results.
- Survey employees in several divisions or locations. In other words, stratify the sample. Try to obtain results from different levels of employees, ranging from executive management down to clerical staff.
- Each employee within the population being sampled should have an equal chance of being selected.
- The internal control team should consider whether it is appropriate to exclude a group from the survey just because they are not directly involved in the financial reporting process. Operational and administrative personnel may provide valuable insights.

Employees will need time to complete the survey and the internal control team will need time to follow up and compile the results. The internal control team should keep this in mind when developing its work schedule.

All responses should be returned directly to the internal control team. To score the survey, assign a numerical value to each of the five possible answers: Strongly Agree = 5; Agree = 4; Neither Agree or Disagree = 3; Disagree = 2; Strongly Disagree = 1. The results can then be broken down into the following categories.

- **Awareness:** Low scores in this area could mean ineffective communications. The agency should consider (1) increasing the frequency of communication concerning agency policies and procedures, (2) revising existing policies for greater clarity and (3) requiring signed acknowledgements from employees that policies have been read and understood.
- **Attitudes:** Low scores for this category may indicate negative attitudes that require (1) changes in management behavior and/or (2) interactive communications between management and employees in which frank and open discussion is encouraged.
- **Actions:** Low scores may indicate that a "disconnect" exists between what management says and what management does. Either written policies should be revised or the behavior of managers should change. If the latter condition is true,

agencies should consider additional training for managers and informal coaching or mentoring of managers. In some cases, the allocation of additional resources may be required to relieve overburdened managers.

Management Inquiries

In addition to employee surveys, the internal control team should develop a questionnaire to interview key financial managers regarding entity-level controls. Depending on the answers to the questions, it may be necessary to develop follow-up questions. The goal of this exercise is to determine if entity-level controls can be relied on to support the effective operation of day-to-day controls at the activity-level.

The interview process should provide sufficient information to form an opinion on the reliability of entity-level controls:

- **Limited awareness:** Managers demonstrate only a limited awareness of the importance of internal controls, including the perception that internal controls are separate from the agency's main operations and someone else's responsibility. Control policies and procedures are ad hoc, generally undocumented, and highly dependent on the skills, competence and ethical values of individuals, rather than the agency, as an integrated whole. There is a lack of formal communication and training.
- **Knowledgeable:** Managers understand that internal controls are an integral part of the agency's business and maintaining an effective system is one of their primary responsibilities. Substantial resources are devoted to developing formal documentation of policies and procedures. The effectiveness of the system of internal control depends more on the agency's internal organization taken as a whole than on the capabilities of individuals.
- **Proactive:** Managers are committed to a process of continuous improvement of internal controls. The agency uses automated tools and sophisticated techniques to monitor controls on a real-time basis and makes changes as needed.

C. General Computer Controls

Computer controls consist of both general and application-specific controls. General controls apply to many if not all application systems and help ensure their continued, proper operation; while application controls ensure the proper processing of various types of transactions and include both computerized steps within the application software and manual follow-up procedures.

Before beginning a detailed assessment of computer general controls, the internal control team or IT specialist should seek answers to the following questions:

- Have there been any significant changes to the agency's IT systems (changes in hardware, software, processes or personnel)? What risks do the changes create? If there have been no significant changes, what previously identified risks remain?

- How many different computing platforms or environments exist within the agency? Do the various systems interface with each other? How is the data exchanged and how is the exchange controlled?
- What might impair the reliability of the agency's IT systems or otherwise negatively affect the ability to capture, process and store data?

ACTIVITY-LEVEL TESTS

Transaction processing begins with the capture of raw transactional data and ends with posting to the general ledger. Along the way, the raw data is converted into accounting information. It may be combined with other data, added, multiplied, subtracted and divided, or otherwise manipulated to create new information. Throughout this process, controls are needed to ensure that the information retains its integrity.

Within the information-processing stream, errors can be introduced at various points.

- The point in the system where events or transactions are initially identified, authorized and captured.
- The point where updating and maintenance is performed for databases, master files, or other electronic storage systems.
- The processing points in the stream where information is manipulated (matched to or combined with other data; used as part of a calculation) or processed, such as posted to the general ledger, subsidiary ledger, or other accounting records.

The goal of the internal control team is to identify these points in the information processing stream and to test and evaluate the effectiveness of the related control measures. Several different types of tests may be used, including individual or group inquiries, direct observation methods, and re-performance of control procedures and reconciliations.

A. Using Focus Groups

Conducting an internal control evaluation provides the opportunity to bring people together in the agency, who may not interact on a regular basis. Hopefully, through participation in a focus group, agency personnel will gain a better understanding of their responsibilities and how these fit into the big picture.

To conduct a group discussion, the following suggestions are offered:

- First, review the policies/procedures and other written documentation for the transaction cycle or processing stream under evaluation to determine who does what. To the extent possible, include individuals who have experience with every process, control, document, or electronic file described in the documentation. However, too large a group can make it difficult to have a meaningful discussion.

- A generic flowchart of the processing stream should be prepared in advance on a large piece of paper that allows for revisions. Post the flowchart on the wall and walk the participants through the process.
- The internal control team should develop a set of questions to facilitate the discussion. The group should reach a decision on what “should happen” and then identify those instances in which exceptions exist. “Stickies” can be used to modify the flowchart so it reflects what really happens.
- Establish boundaries. The internal control team should make certain that focus groups understand they are concerned only with the information that flows into the financial statements. In addition, the discussion should be limited to what the agency or business unit does internally, not on how outside parties prepare information that the agency or business unit uses.
- Set an expectation that differences of opinion are acceptable.
- Try to quantify the information gained, whenever possible: “*How often do you encounter . . . ?*” “*About what percentage of transactions . . . ?*”
- At some level, try to reach agreement on the issues.

B. Observation

The IC Team may be able to *observe* the application of some control procedures, such as computer edit checks. Another procedure that is easily observed is physical inventory accounts. If the physical count is performed only occasionally, it may be possible to observe the control each time it is performed.

C. Re-performing Control Procedures

In some cases, the internal control team may decide to test the effectiveness of control procedures by selecting a random sample of transactions and *re-performing* the procedures.

For example, the process for paying vendor invoices might require:

- Physically matching a receiving document with the invoice
- Determining whether bids and a formal purchase order/contract was necessary.
- Determining that the invoice was properly approved for payment, as evidenced by an authorized signature.
- Determining whether a price agreement was in affect.

To test the effectiveness of the controls over payment processing, a team member might examine the underlying documentation to determine that:

- The invoice was physically matched to a receiving document.

- Bids were obtained and attached; a copy of the signed purchase order is attached or the underlying contract number is noted, if applicable.
- The receiving copy of the PO or other receiving document is signed/initialed and dated.
- Approval signature is noted on invoice.

To determine that the control was performed properly, the team member would ensure that:

- The purchase order and/or bids (if any), receiving document and invoice are for the same transaction.
- Where a price agreement applies, the appropriate vendor was used.
- Signers approving payment of the invoice have the appropriate authority.

Before the internal control team begins its test of transactions, the team should clearly define what is considered a control procedure error. To conclude that a control has been properly performed, both of the following statements should be true:

- There is evidence that the control procedure was performed, and
- The re-performance of the procedure indicates it was performed properly.

D. Reconciliations

Reconciliations are a common control procedure, such as bank reconciliations or the reconciliation of a subsidiary ledger balance to the general ledger account balance. The internal control team can test the effectiveness of reconciliation procedures through observation and re-performance:

- Review the documentation to determine that the reconciliation was performed on a timely basis throughout the year.
- Re-perform the reconciliation to confirm that all reconciling items were identified.
- Investigate the resolution of significant reconciling items.

E. Application Controls

After completing the applications control checklist, the internal control team or IT specialist may decide to test the processing controls related to individual application systems. One method is to prepare a file of test transactions and run them through the system to determine that all pre-defined errors are identified. The internal control team should also review suspense account entries occurring throughout the year to ensure they were properly resolved.

When reviewing IT controls over financial applications, it is important that the internal control team/IT specialist understand the business risks and then identify the *key* process controls and

the relevant automated procedures. In some situations, the internal control team/IT specialist may find a “user” control procedure that management relies on to promptly and effectively detect the failure of a key automated procedure. Although the internal control team/IT specialist should examine evidence that the automated control is operating appropriately, the focus of the team/specialist in this situation would be testing the reliability of the detective control.

F. Summary

The amount of testing to be performed is a matter of judgment. It will depend on the internal control team’s assessment of the agency’s overall control environment; the significance of the business cycle, process or activity to the agency’s mission; and the results of the team’s initial testing – all the while bearing in mind that the ultimate goal is to draw a conclusion about the effectiveness of internal control *as a whole*, not individual controls standing alone.

Finally, it should be reiterated that internal control can provide management with only reasonable assurance that the agency’s goals and objectives will be achieved. *Within the context of this Guidebook, the effectiveness of internal controls should be evaluated on the basis of the financial statements and whether any errors that internal controls fail to detect or prevent might be material.*

CHAPTER SEVEN: THE BOTTOM LINE

The internal control team's next step is to evaluate its findings and prepare a report for senior management. The report should highlight the positive aspects of the agency's system of internal control, as well as describe the control deficiencies. Recommended corrective actions and division/business unit responses should also be included. The report should be addressed to the agency's director and signed by both the agency's chief fiscal officer and the internal control officer. Copies of the report should be distributed to the agency's internal audit unit and governing board.

A. Judging the Severity of Internal Control Deficiencies

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

A *significant deficiency* is a control deficiency or a combination of control deficiencies that adversely affects an agency's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is *more than a remote likelihood* that a misstatement of the [State of Name] Comprehensive Annual Financial Report (CAFR) that is *more than inconsequential* will not be prevented or detected.

A *material weakness* is a significant deficiency or a combination of significant deficiencies that results in *more than a remote likelihood that material misstatements* in the information provided by an agency for preparation and inclusion in the [State of Name] CAFR will be not be prevented or detected.⁸

In determining whether an internal control deficiency is more than inconsequential and should be reported, the internal control team should perform a risk assessment that takes into account the following criteria.⁹

- **Likelihood of Misstatement**

Many factors affect the likelihood that a deficiency, or a combination of deficiencies, could result in a misstatement of an account balance or disclosure. Some of the factors the team should consider include, but are not limited to, the following:

- The nature of the financial statement accounts, disclosures, and assertions involved. For example, suspense accounts and related party transactions involve greater risk.

⁸ The factors for determining the severity of a control deficiency are based on the criteria set forth in *Statement on Auditing Standards (SAS) No. 112, Communicating Internal Control Related Matters Identified in an Audit*, May 2006 and similar criteria presented by Mr. Michael Ramos in his book entitled *How to Comply with Sarbanes-Oxley Section 404 – Assessing the Effectiveness of Internal Control*, John Wiley & Sons, Inc., Hoboken, NJ, 2004.

- The susceptibility of the related assets or liabilities to loss or fraud.
 - The subjectivity and complexity of the amount involved, and the extent of judgment needed to determine that amount.
 - Whether the control in question is automated and whether it can be expected to perform consistently over time.
 - The interaction or relationship of the control with other controls. For example, what is the relative importance of the control and is the *overall* control objective achieved by interaction with other control activities and mitigating factors?
 - The cause and frequency of any known or detected exceptions related to the operating effectiveness of a control. For example, if a deficiency is deemed to be an operating deficiency (rather than a deficiency in the design of a control feature), what is the operating failure rate, i.e., repeated failures versus isolated occurrences?
 - The interaction of the control deficiency with other control deficiencies.
 - The possible future consequences of the deficiency.
- **Magnitude of Misstatement**

If the likelihood is high that an internal control deficiency could result in a financial statement misstatement, the next step is to assess the magnitude of the potential misstatement. The following factors should be considered:

 - The financial statement amounts or total of transactions affected by the deficiency and the financial statement assertions involved.
 - Whether the deficiency relates to an entity-level or activity-level control. Weaknesses in entity-level controls that seem relatively insignificant, by themselves, could result in material financial statement misstatements because they affect many accounts and classes of transactions.
 - The volume of activity in the account balance or class of transactions exposed to the deficiency that has occurred in the current period, or that is expected in future periods.

When evaluating the significance of a potential misstatement, the focus should be on the *potential* for misstatement, not on whether a misstatement has actually occurred.

Strong Indicators of a Significant Weakness

SAS No. 112 suggests that deficiencies in the following areas should be regarded, at a minimum, as significant deficiencies in internal control over financial reporting:

- Controls over the selection and application of accounting policies.
- Antifraud programs and controls.

- Controls over non-routine and non-systematic transactions.
- Controls over the year-end financial reporting process, including controls over procedures used to (1) enter transaction totals into the general ledger; (2) initiate, authorize, record, and process journal entries into the general ledger; and (3) record recurring and non-recurring adjustments to the financial statements.

Strong Indicators of a Material Weakness

Identification of fraud of any magnitude on the part of senior management should be considered a significant, if not, material weakness. In addition, significant deficiencies that have been communicated to management by the financial statement auditors or the agency's internal auditors that remain uncorrected after a reasonable period of time should be regarded as a strong indicator that a material weakness exists.

B. Reporting Guidelines

Once the team has evaluated its findings, the next step is to review them with division and business unit managers to reach consensus on the appropriate corrective actions. At the conclusion of this process, the team should be ready to prepare its final report. The report should include:

- A statement describing management's responsibility for establishing and maintaining internal control over financial reporting;
- A statement of the framework or criteria used to evaluate the effectiveness of internal control over financial reporting;
- A statement about the inherent limitations of internal control systems;
- The internal control team's assessment of the overall effectiveness of internal control over financial reporting, including disclosure of any significant or material control deficiencies identified by the team; and
- A summary of the steps each division or business unit plans to take to correct any reported deficiencies and the estimated dates of completion. Corrective actions that management plans to address through a budgetary request should also be noted.

Lastly, the report should address control weaknesses identified in prior reports, commenting on (1) whether the weaknesses have been corrected and (2) whether the new policies and/or procedures have been in place for a sufficient period of time to determine they are operating effectively.

REFERENCES

American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards (SAS) No. 112: *Communicating Internal Control Related Matters Identified in an Audit*, May 2006, <http://www.aicpa.org/download/members/div/auditstd/AU-00325.PDF>

COBIT, IT Governance Institute (ITGI), Rolling Meadows, Illinois, USA, <http://www.isaca.org>

Committee of Sponsoring Organizations of the Treadway Commission (COSO), <http://www.coso.org>

Enterprise Risk Management—Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission (COSO), American Institute of Certified Public Accountants, USA, 2004

Internal Control—Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission (COSO), American Institute of Certified Public Accountants, USA, 1992

Internal Control Guide, Vols. 1 and 2, Commonwealth of Massachusetts, Office of the Comptroller, <http://www.mass.gov/osc/Homeview/CONTROL/CONTENTS.HTM>

ISO IEC 17799, *Code of Practice for Information Security Management*, International Organization for Standardization (ISO), Switzerland, 2000, <http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html>

IT Control Objectives for Sarbanes-Oxley, Information Systems Audit and Control Association (ISACA) and IT Governance Institute (ITGI), Rolling Meadows, IL, 2004, <http://www.isaca.org>

Ramos, Michael, *How to Comply with Sarbanes-Oxley Section 404 – Assessing the Effectiveness of Internal Control*, John Wiley & Sons, Inc., Hoboken, NJ, 2004

State of [Name], [State Accounting Manual], [Policy XXXX – Title], [Link]

Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 5: *An Audit of Internal Control over Financial Reporting That is Integrated with an Audit of Financial Statements*, June 12, 2007, http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_5.pdf

The Standard of Good Practice for Information Security, Information Security Forum (ISF), 2004, <http://www.isfsecuritystandard.com>