Internal Control Guide for Managers

Solano County

Table of Contents

CHAPTER I

Internal Control Overview

Internal Control Overview

Purpose of the Internal Control Guide

This guidance is designed primarily to help management with establishing and maintaining effective internal control over financial reporting and may be useful to management in more efficiently assessing internal control effectiveness.

Internal Control Guide for Managers serves as a reference tool to identify and assess basic weaknesses in operating controls, financial reporting, and legal compliance and to take action to strengthen controls where needed.

This guidance stresses the essential role of managers at all levels in developing and monitoring departmental internal controls. This addresses the five interrelated components of a business system:

- The organization's operating environment
- Its goals and objectives and related risk assessment
- Controls and related policies and procedures
- Its information systems and communication methods
- Its activities to monitor its performance

What is Management's Role and Responsibility?

Management is primarily responsible for implementing internal controls. Management's role is to provide the leadership that the organization needs to achieve its goals and objectives. Internal control is a technique used by managers to help an organization achieve these objectives. Internal controls are the structure, policies, and procedures used to ensure that management accomplishes its objectives and meets its responsibilities.

Each department head, manager, and employees participate in establishing, properly documenting, and maintaining internal controls in each department. All employees of the County are responsible for compliance with internal controls.

The State Administrative Manual of California states ***"The ultimate responsibility for good internal control rests with management."***

What are Internal Controls?

The current official definition of internal control was developed by the Committee of Sponsoring Organization (COSO) of the Treadway Commission. In its influential report, *Internal Control – Integrated Framework*, the Commission defines internal control as follows:

"Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations."

A less technical definition might state that:

Internal controls are tools that help management be effective and efficient while avoiding serious problems such as overspending, operational failures, and violations of law.

COSO defines internal control as having five components:

Control Environment – sets the tone for the organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control.

Risk Assessment – the identification and analysis of relevant risks to the achievement of objectives, forming a basis for how the risks should be managed.

Information and Communication – systems or processes that support the identification, capture, and exchange of information in a form and time frame that enable people carry out their responsibilities.

Control Activities – the policies and procedures that help ensure management directives are carried out.

Monitoring – processes used to assess the quality of internal control performance over time.

Each of the five components of internal control is important to achieving the objective of reliable financial reporting. Determining whether a company's internal control over financial reporting is effective involves a judgment. Internal control has five components that work together to prevent or detect and correct material misstatements of financial reports.

Why Do We Need Internal Controls?

Accountability

The State Manager's Accountability Act states:

> "*Because governments are susceptible to fraud, waste, and abuse, increased attention has been directed toward strengthening internal control to help restore confidence in government and improve its operations. In particular, the Financial Integrity and State Manager's Accountability Act was enacted to inhibit waste of resources and create savings.*"

Government Code (GC) 13400 through 13407 describes the Legislative findings, entity responsibilities, and entity reports on the adequacy of internal control. GC 13403 defines internal accounting and administrative controls and sets forth the elements of a satisfactory system of internal control. As stated in GC 13403, internal accounting and administrative controls are the methods through which state entity heads can give reasonable assurance that measures to safeguard assets, check the accuracy and reliability of accounting data, promote operational efficiency, and encourage adherence to prescribe managerial policies are being followed.

GC 13403 states the elements of a satisfactory system of internal accounting and administrative controls, shall include, but are not limited to:

- A plan of organization that provides segregation of duties appropriate for proper safeguarding of state assets.
- A plan that limits access to state assets to authorized personnel who require these assets in the performance of their assigned duties.
- A system of authorization and record keeping procedures adequate to provide effective accounting control over assets, liabilities, revenues and expenditures.
- An established system of practices to be followed in performance of duties and functions in each of the state agencies.
- Personnel of a quality commensurate with their responsibilities.
- An effective system of internal review.

Furthermore, the A-102 Common Rule and OMB Circular A-110 (2 CFR part 215) require that non-Federal entities receiving Federal awards establish and maintain internal control designed to reasonably ensure compliance with Federal laws, regulations, and program compliance requirements.

Encourage Sound Management Practices

Organizations exist to accomplish a goal. Managers are responsible for providing the leadership to reach this goal. That responsibility encompasses both identifying applicable laws and regulations and establishing internal control policies and procedures designed to provide reasonable assurance that the entity complies with those laws and regulations.

Internal controls coordinates a department's policies and procedures to safeguard its assets, check the accuracy and reliability of its data, promote operational efficiency, and encourage adherence to prescribed managerial policies. Managers must develop, implement, monitor, and update an effective plan of internal controls.

Facilitate Preparation for Audits

Each County department is subject to audits by independent auditors (as part of the Single Audit Act of 1984 with amendment in 1996), the Office of the State Controller and internal audits. These audits are conducted to ensure the following:

- Funds are administered and expended in compliance with applicable laws and regulations;
- Programs are achieving the purpose for which they were authorized and funded;
- Financial statements accurately represent the financial position of the County;
- Programs are managed economically and
- Internal controls exist and provide a basis for planning the audit and planning the timing, nature, and extent of testing.

Auditors' reports will nearly always include an opinion of the department's internal controls. When it appears warranted, auditors will make recommendations for improvements. Managers are accountable for the adequacy of the internal control systems in their departments. Weak or insufficient internal controls will result in audit findings and, more importantly, could lead to theft, shortages, operational inefficiency, or a breakdown in the control structure.

Limitations of Internal Control

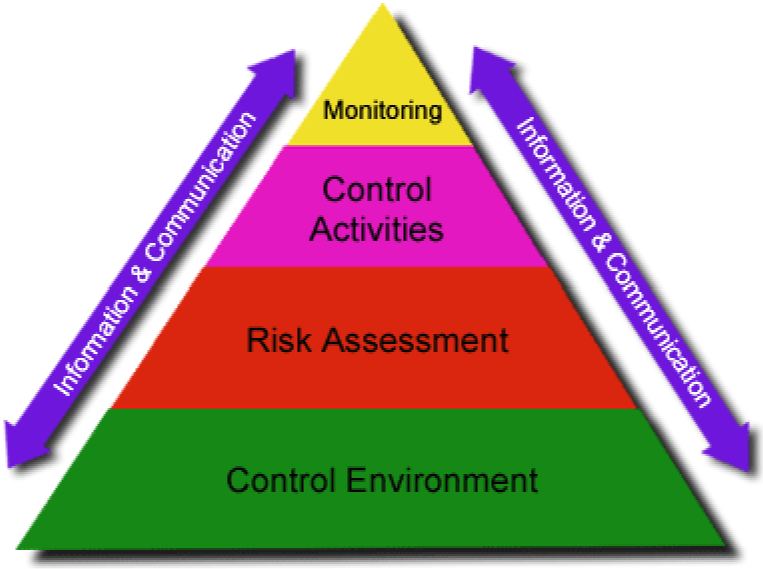
Internal controls, no matter how well designed and operated, can provide only *reasonable assurance* to management regarding the achievement of an entity's objectives, the reliability of reports, and compliance with laws and regulations. Certain limitations are inherent in all internal control systems.

Another limitation to internal controls is due to the reality that human judgment can be faulty; breakdowns can also occur because of human failures such as simple error or mistake. Management may fail to anticipate certain risks, and thus fail to design and implement appropriate controls. Two other limitations are that controls can be circumvented by collusion of two or more people and that management has the ability to override the system.

Despite these limitations, the reasonable assurance that internal control does provide, helps enable an organization to focus on reaching its objectives while minimizing unpleasant surprises. They promote efficiency, reduce the risk of asset loss, and help ensure the reliability of financial statements and compliance with laws and regulations.

CHAPTER 2

Five Components of Internal Control



Five Components of Internal Control

Overview

The *COSO Report* describes the internal control process as consisting of five interrelated components that are derived from and integrated with the management process. The components are interrelated, which means that each component affects and is affected by the other four. These five components, which are the necessary foundation for an effective internal control system, include:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

Control Environment

The control environment is the control consciousness of a department. It is the atmosphere in which people conduct their activities and carry out their control responsibilities. An effective control environment is an environment where competent people understand their responsibilities, the limits to their authority, and are knowledgeable, mindful, and committed to doing what is right and doing it the right way; they are committed to following an organization's policies and procedures and its ethical and behavioral standards. The control environment encompasses technical competence and ethical commitment; it is an intangible factor that is essential to effective internal control. The tone set at the top pervades all other activities in the department.

Seven principles relate to the control environment components:

1. **Integrity and Ethical Values** – Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting.
2. **Board of Directors** – The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control.
3. **Management's Philosophy and Operating Style** – Management's philosophy and operating style support achieving effective internal control over financial reporting.
4. **Organizational Structure** – The company's organizational structure supports effective internal control over financial reporting.

5. **Financial Reporting Competencies** – The company retains individuals competent in financial reporting and related oversight roles.
6. **Authority and Responsibility** – Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting.

<u>Control Environment Tips</u>

- Make sure that the following policies and procedures are available in your department (hard copy or internet access):
  - Administrative Procedures
  - Employee Handbook
  - Purchasing Manual
  - Personnel Memorandum
- Make sure that the department has a well-written departmental policies and procedures manual, which addresses its significant activities and unique issues. Employee responsibilities, limits of authority, performance standards, control procedures and reporting relationships should be clear.
- Make sure that employees are well acquainted with County and departmental policies and procedures that pertain to their job responsibilities.
- Discuss ethical issues with employees. If employees need additional guidance, issue departmental standards of conduct.
- Ask employees to disclose potential conflicts of interest.
- Make sure that job descriptions exist and correctly translate desired competence levels into requisite knowledge, skills, and experience; make sure that hiring practices result in hiring qualified individuals.
- Make sure that the department has an adequate training program for employees.
- Make sure that employee performance evaluations are performed at least annually. Good performances should be valued highly and recognized in a positive manner.
- Make sure that appropriate disciplinary action is taken when an employee does not comply with policies and procedures or behavioral standards.

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 the potential risks that could hinder or prevent an agency from achieving its objectives. In attempting to identify risk, managers need to ask the following questions:

- *What could go wrong?*

- *What assets do we need to protect?*
- *How could someone steal from the department?*
- *On what do we spend the most money?*
- *What activities are more complex?*
- *Where are we vulnerable?*

Over the course of a day, a week, a month. or a year, situations occur which could hinder or prevent a unit (or a department) from fulfilling its responsibilities and meeting its goals. Because of this possibility, successful managers continually identify and analyze potential risks to their organizations. Performing risk assessments assists managers in prioritizing the activities where controls are most needed. Managers use risk assessments to determine the relative potential loss in programs and functions and to design the most cost-effective and productive internal controls. When beginning a risk assessment, the manager can start by analyzing the two circumstances most likely to endanger unit objectives, **change and inherent risk.**

Review Changes

The risk to reaching objectives increases dramatically during a time of change (turnover in personnel, rapid growth, or establishment of new services, for example). Because any type of change increases risk, monitor and assess every significant, or likely to be significant, change. Some examples of circumstances that expose an agency to increased risk are the following:

- Changes in personnel
- New or revamped information systems
- Rapid growth
- New program or services

Identify Inherent Risk

The second type of potential problems is inherent risk. Examples include complex programs or activities, cash receipts, providing services through subrecipients (vendors), direct third party beneficiaries, and prior problems. Activities with inherent risk have a greater potential for loss from fraud, waste, unauthorized use, or misappropriation due to the nature of the activity or asset. Cash, for example, has a much higher inherent risk for theft than a stapler does. Other examples of situations that may involve inherent risk:

- *Complexity* increases the danger 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 (for example food stamps).

- *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 occur throughout the entire department.

- *A prior record of control weaknesses* will often indicate a higher level of risk because bad situations tend to repeat themselves.

- *Unresponsiveness to identified control weaknesses* by prior auditors often indicates that future weaknesses are likely to occur.

Evaluate identified risks

After identifying potential risks, analyze each risk to determine how best to manage it. Start with the following questions:

- How important is this risk?

- How likely is it that this risk will occur?

- How can we best manage this risk?

Internal control systems should provide reasonable assurance that assets are safeguarded, resources are properly used, and objectives are achieved. Absolute assurance may not be an achievable goal, because it may be prohibitively expensive and impede productivity. One would not expend a substantial amount of funds to protect a relatively inexpensive asset. For example, it is not prudent to spend $50 to safeguard a $25 carton of pens. Spending $50 to safeguard $5,000 in laptop computers, however, may be very sensible.

Control Activities

Once managers identify and assess risks, they need to evaluate and develop, if necessary, methods to minimize these risks. These methods are referred as **control activities**, the third component of internal control.

Control activities are performed at various levels of a company to reduce risks in achievement of financial reporting objectives. These are actions supported by policies and procedures that help assure management directives to address risk are carried out properly and timely.

Controls can be either preventive or detective. The intent of these controls is different. Preventive controls attempt to deter or prevent undesirable events from occurring. They are proactive controls that help to prevent a loss. Examples of preventive controls are separation of duties, proper authorization, adequate documentation, and physical control over assets.

Detective controls, on the other hand, attempt to detect undesirable acts. They provide evidence that a loss has occurred but do not prevent a loss from occurring. Examples of detective controls are reviews, analyses, variance analyses, reconciliations, physical inventories and audits.

Both types of controls are essential to an effective internal control system. From a quality standpoint, preventive controls are essential because they are proactive and emphasize quality. However, detective controls play a critical role, providing evidence that the preventive controls are functioning and preventing losses.

Control activities include approvals, authorizations, verifications, reconciliations, reviews of performance, security of assets, segregation of duties, and controls over information systems and are further explained as follows:

Approvals, Authorizations, and Verifications (Preventive)

Management authorizes employees to perform certain activities and to execute certain transactions within limited parameters. In addition, management specifies those activities or transactions that need supervisory approval before they are performed or executed by employees. A supervisor's approval (manual or electronic) implies that he or she has verified and validated that the activity or transaction conforms to established policies and procedures.

An important control activity is authorization/approval. Authorization is the delegation of authority; it may be general or specific. Giving a department permission to expend funds from an approved budget is an example of general authorization. Specific authorization relates to individual transactions; it requires the signature or electronic approval of a transaction by a person with approval authority. Approval of a transaction means that the approver has reviewed the supporting documentation and is satisfied that the transaction is appropriate, accurate and complies with applicable laws, regulations, policies and procedures. Approvers should review supporting documentation, question unusual items, and make sure that necessary information is present to justify the transaction – before they sign it. Signing blank forms should not be done. To ensure proper segregation of duties, the person initiating a transaction should not be the person who approves the transaction.

Reconciliations (Detective)

An employee relates to different sets of data to one another, identifies and investigates differences, and takes corrective action, when necessary.

Reconciliation is a comparison of different sets of data to one another, identifying and investigating differences, and taking corrective action, when necessary. To ensure proper segregation of duties, the person who approves transactions or handles cash receipts should not be the person who performs the reconciliation.

A critical element of the reconciliation process is to resolve differences. It does not do any good to note differences and do nothing about it. Differences should be identified, investigated, and explained – corrective action must be taken. Reconciliations should be documented and approved by management.

Reviews of Performance (Detective)

Management compares information about current performance to budgets, forecasts, prior periods, or other benchmarks to measure the extent to which goals and objectives are being achieved and to identify unexpected results or unusual conditions that require follow-up.

Management review of reports, statements, reconciliations, and other information is an important control activity. Management should review such information for propriety, consistency, and reasonableness. Reviews of performance provide a basis for detecting problems. Management should compare:

- Budget to actual comparison
- Current to prior period comparison
- Performance indicators
- Follow-up on unexpected results or unusual items

Security of Assets (Preventive and Detective)

Access to equipment, inventories, securities, cash and other assets is restricted; assets are periodically counted and compared to amounts shown on control records.

Liquid assets, assets with alternative uses, dangerous assets, vital documents, critical systems, and confidential information must be safeguarded against unauthorized acquisition, use or disposition. Typically, access controls are the best way to safeguard these assets. Examples of access controls are as follows: locked door, key pad systems, card key system, badge system, locked filing cabinet, terminal lock, computer password, menu protection, automatic call-back for remote access, smart card and data encryption. Missing items should be investigated, resolved timely, and analyzed for possible control deficiencies; perpetual records should be adjusted to physical counts if missing items are not located.

Segregation of Duties (Preventive)

Duties are segregated among different people to reduce the risk of error or inappropriate action. Normally, responsibilities for authorizing transactions, recording transactions (accounting), and handling the related asset (custody) are divided.

The fundamental premise of segregated duties is that an individual or small group of individual 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. The list below offers some examples of incompatible duties:

- Managing operations of an activity and record keeping for the same activity
- Custody of assets and recording receipt of those assets
- Authorization of transactions and custody or disposal of the related assets or records

Different personnel should perform the different functions of data entry, authorization, custody, and report review. If this control activity is properly planned, implemented, and adhered to, departments can safeguard state funds against a single individual's "irregularity".

A department internal control plan should ensure that all of the following activities, at a minimum, are properly segregated:

Personnel & Payroll Activities

- Individuals responsible for hiring, terminating and approving promotions should not prepare payroll or personnel transactions or input data.
- Managers should review and approve payroll deductions and time sheets before data entry, but should not be involved in preparing payroll transactions.
- Individuals involved in payroll data entry should not have payroll approval authority.

Other Expenditure Activities

- Individuals responsible for data entry of encumbrances and payment vouchers should not be responsible for preparing or approving these documents.
- A department should not delegate expenditure transaction approval to the immediate supervisor of data entry staff or to data entry personnel. Individuals responsible for acknowledging the receipt of goods or services should not also be responsible for purchasing or payment activities.

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 recirds.

Check Writing Activities

- Persons preparing checks should not be signing the checks.
- Persons signing the checks should not be reconciling the checking account.

Revenue Activities

- Individuals receiving cash into the office should not be involved in authorizing bank deposits.
- Individuals receiving revenue or making deposits should not be involved in reconciling the bank accounts.

Controls over Information Systems (Preventive and Detective)

Controls aver information systems are grouped into two broad categories – general controls and application controls. General controls commonly include controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance. Application controls such as computer matching and edit checks are programmed steps within application software; they are designed to help ensure the completeness and accuracy of transaction processing, authorization, and validity. General controls are needed to support the functioning of application controls; both are needed to ensure complete and accurate information processing.

Four principles relate to control activities:

1. Integration with Risk Assessment – Actions are taken to address risk to the achievement of financial reporting objectives.
2. Selection and Development of Control Activities – Control activities are selected and developed considering their cost and potential effectiveness in mitigating risks to the achievement of financial reporting objectives.
3. Policies and Procedures – Policies related to reliable financial reporting are established and communicated throughout the company with corresponding procedures resulting in management directives being carried out.
4. Information Technology – Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting objectives.

Information and Communication

Information systems identify, capture, process, and distribute information supporting achievement of financial reporting objectives.

Four principles relate to the information and communication component:

1. Financial Reporting Information – Pertinent information is identified, captured, used at all levels of the company, and distributed in a form and timeframe that supports the achievement of financial reporting objectives.
2. Internal Control Information – Information needed to facilitate the functioning of other control components is identified, captured, used, and distributed in a form and timeframe that enables personnel to carry out their internal control responsibilities.

3. Internal Communication – Communication enable and support understanding and execution of internal control objectives, processes, and individual responsibilities at all levels of the organization.

4. External Communication – Matters affecting the achievement of financial reporting objectives are communicated with outside parties.

Information and communication are essential to effecting control; information about an organization's plans, control environment, risks, control activities, and performance must be communicated up, down, and across an organization. Reliable and relevant information from both internal and external sources must be identified, captured, processed, and communicated to the people who need it – in a form and timeframe that is useful. Information systems produce reports, containing operational, financial and compliance-related information that makes it possible to run and control an organization.

Information and communication systems can be formal or informal. Formal information and communication systems – which range from sophisticated computer technology to simple staff meetings – should provide input and feedback data relative to operations, financial reporting and compliance objectives; such systems are vital to an organization's success.

Information: Although a department or unit manager may have developed excellent policies and procedures, if these are not communicated to the staff that performs these duties, they may as well not exist. Well-designed internal controls outline the specific authority and responsibility of individual employees. They can also serve as a reference for employees seeking guidance on handling unusual situations.

Communication: An internal control plan should provide for information to be communicated both within the organization (up as well as down) and externally to those outside, for example, vendors, recipients, and other departments. Management should distribute copies of the department's internal control plan to all staff whose jobs are affected in any way by the information in the plan. Sending information electronically allows management to immediately distribute new procedures and other information to a large staff. Departments should conduct in-house training sessions upon releasing new or extensively revised internal control plans to explain the meaning of the plan and the importance of internal controls. This training should also be part of the orientation of new employees.

Monitoring

Internal control systems are monitored to assess the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two.

Two principles relate to the monitoring component:

1. Ongoing and Separate Evaluation – Ongoing and/or separate evaluations enable management to determine whether the other components of internal control over financial reporting continue to function over time.

2. Reporting Deficiencies – Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to management and the board as appropriate.

The purpose of monitoring is to determine whether internal control is adequately designed, properly executed and effective. Internal control is adequately designed and properly executed if all five internal control components are present and functioning as designed.

Life is a change; internal controls are no exception. Satisfactory internal controls can become obsolete through changes in external circumstances. Therefore, after risks are identified, policies, and procedures put into place, and information on control activities communicated to staff, managers must then implement the fifth component of internal control, monitoring. Managers must continually monitor the effectiveness of their controls. Monitoring assesses the quality of internal controls over time. Like the other four components, monitoring is a basic management duty included in management activities like performance evaluations, ongoing supervision, and status reports. Proper monitoring ensures that controls continue to be adequate and continue to function properly.

Even the best internal control plan will be unsuccessful if it is not followed. Monitoring allows the manager to identify whether controls are being followed before problems occur. For example, a unit's internal control plan may identify cross-trained staff to perform certain duties if the assigned individual is not available. However, the manager who does not monitor this arrangement by asking staff to occasionally perform the back-up duties may discover, too late, that the individual was cross-trained so long ago that substantial changes have occurred and he or she has no idea what to do.

Managers must also monitor previously identified problems to ensure that they are promptly corrected. In the same way, managers must review weaknesses identified by audits to determine whether related internal controls need revision.

Chapter 3

Evaluating Internal Controls &

Preparing an Internal Control Plan

Evaluating Internal Control & Preparing an Internal Control Plan

Evaluating current internal controls is the first step toward preparing an internal control plan. An internal control evaluation is a detailed examination of a unit's functions undertaken to determine whether adequate internal controls exist and function as intended and to make necessary improvements.

Five-Step Approach to Evaluating Internal Controls

We have developed a five-step approach to evaluating internal controls to correspond with the five components of internal control. Managers should do this for each unit that reports to them. *Before beginning the five steps, review the department's goals and objectives.* Next, identify specific risks to meeting these objectives. Determine which objectives are most important and most vulnerable. Prioritize your efforts by first evaluating activities with an unfavorable control environment and a high degree of inherent risk. Then start to apply the five steps listed below for each of the most important objectives.

Step 1: Analyze the Control Environment

Attitude: Review the department's control environment including your and any subordinate managers' attitudes and actions. If a specific procedure requires constant exceptions, you are better off changing or eliminating the procedure than establishing an attitude of "rules are made to be broken".

Whether they realize it or not, managers set an example by their behavior. If managers make exceptions to their own procedures whenever they find themselves inconvenienced, staff and contractors will feel they too can also make exceptions whenever they want.

Supervision: Departments with the best control environment attempt to hire qualified individuals while making an effort to retain skilled employees. Their managers train new and current staff to excel at their jobs and to use appropriate internal controls in all areas. They assist their staff by furnishing tools such as job descriptions and policy and procedure manuals that clearly communicate responsibilities and duties. They provide sufficient but not excessive supervision, reviewing to the extent necessary. While they allow as much autonomy as possible to competent, experienced staff, they continue to approve work at critical points to ensure that work flows as intended.

Structure: Managers should develop an organizational structure that clearly defines supervisory responsibilities and chains of command. The structure should also take into account the need to segregate certain duties. Document this structure through organizational charts made available to all staff.

Step 2: Assess Risk

Because evaluating internal controls can be a lengthy process, and because every risk to an organization's objectives is not equally significant, managers must prioritize their efforts before analyzing specific actions. The risk assessment process contains two major steps: (1) identify and prioritize activities that are most likely to have problems, then (2) analyze those specific activities to determine their components.

Identify potential problems: Begin by reviewing both the unit's goals and objectives and the organization's control environment. Next, determine potential problems. Examples of circumstances with potential for problems includes programs that have undergone recent changes in staff or structure, functions that receive complaints or have had problems in the past, and complex activities.

Rank the identified risks by asking the following questions: “Where do we face the greatest possible harm?” and, “Which types of losses are most likely to occur?” Use this evaluation to prioritize your efforts.

Identify and Analyze Control Cycles: It is easy to become overwhelmed by the volume and complexity of controls within even a single program or administrative function. To simplify this task, we suggest grouping activities of the program or function into control cycles. A control cycle is a group of actions used to initiate and perform related activities. A single program or administrative function usually contains several control cycles. Control cycles provide the focal point for evaluating internal controls.

After listing the control cycles, use the following process to document them:

- First, interview the personnel involved in the cycle and observe the activity.
- Second, prepare either a narrative explanation or a flow chart. The documentation should contain sufficient detail to permit an analysis of the internal controls.
- Third, review the completed documentation with the persons providing the information.
- Fourth, use the documentation to track one or two transactions through the process.

Performing all four of the above actions will assure that the documentation and your understanding of the cycle are accurate and complete. After documenting the control cycle, use the following steps to analyze it:

- Prepare a written narrative or flow chart explaining how the cycle is supposed to be handled by describing each activity or transaction within the cycle. In the narrative, describe:
    - Who is performing each step?
    - What is involved in the step?
    - Any resulting documentation, for example, reports.
- Review the information available in policy and procedure manuals. Use written materials such as organizational charts, job descriptions, reviews, checklists, department records, and reports.
- Supplement written sources through conversations and observations.
- Finally “walk through” the process to be sure you understand every item.

Step 3: Implement Management Control Activities

Evaluate the control cycle to decide whether the system, as defined, sufficiently safeguards the department’s resources, assures the accuracy of its information, and promotes effectiveness and efficiency. We do this as follows:

- Define objectives and risks for each control cycle. Objectives express the reasons we use policies and procedures to control specific identified risks. We establish objectives because control activities (policies and procedures) minimize the likelihood that an identified risk will occur.

- Examine the documentation of the cycle to determine whether sufficient policies and procedures already exist for the control objectives to be met and remember to identify any outside policies and procedures that can off-set potential risk.

- If appropriate policies and procedures do not exist, develop them and communicate to all staff. If the procedures do exist, determine whether they are being followed.

- Identify any controls that are excessive or unnecessary and modify or eliminate them. Appropriate controls include external as well as internal controls. Excessive control is inefficient. Identify outside policies or procedures that can offset potential risks.

Step 4: Communicate Information

Prepare and distribute the results of the evaluation and any related changes. Changes in internal controls must be discussed with affected managers and staff along with the department's internal control officer. In evaluating possible alternatives, consider the costs and expected benefits of implementing control objectives in a cost-effective manner.

Step 5: Monitoring

At a minimum, evaluate your internal controls on an annual basis. When reviewing, consider internal and external changes, personnel turnover, new programs, administrative activities, and priorities. Schedule monitoring on a regular basis or it is likely to be by-passed by the emergencies of day to day work. Testing controls at least annually allows you to determine whether the controls continue to be adequate and are still functioning as intended.

The final step in an internal control evaluation is testing the controls to determine whether they function as intended. Program monitors, auditors, and other reviewers can be a resource in monitoring internal controls.

Prepare an Internal Control Plan

An internal control plan is a description of how an agency expects to meet its various goals and objectives by using policies and procedures to minimize risk. In preparing the plan, refer to the five components. Use the information acquired throughout the evaluation to prepare an internal control plan. Internal control plans can take many different forms, depending on the organizational structure and business practices of the organization. In general, however, the internal control plan would:

- discuss the goals and objectives of the department/division

- briefly state the integrity and ethical values expected to all staff and especially the ethical values top management expects of itself (control environment)

- describe the risks to meeting goals and objectives and

- explain how the structure, policies, and procedures of the organization act to control the risk (control activities)

In a small department, the plan might include all the department's policies and procedures. In a large department, the plan might incorporate the various policy and procedure documents by reference. As a constituent part of the department's plan, however, these policies and procedures would also need to be reviewed and updated at least annually. Finally, the internal control plan would also include a section describing to whom the plan is distributed and another section describing how the plan is to be monitored.

Sources:

Gauthier, Stephen J. *Evaluating Internal Controls: A Local Government Manager's Guide.* Chicago, Illinois: Government Finance Officers Association, 1996.

Committee of Sponsoring Organizations of the Treadway Commission. *Internal Control – Integrated Framework*. New Jersey: Committee of Sponsoring Organizations of the Treadway Commission, July, 1994.