

Internal Control – An Overview

April 2009



Russell W. Hinton
State Auditor

Department of Audits and Accounts
270 Washington Street, SW
Atlanta, GA 30334

TABLE OF CONTENTS

Introduction	3
Understanding Basic Principles behind the Establishment of Controls	4
Internal Control – An Overview	7
Internal Control – Integrated Framework (The COSO Report)	15
Control Self-Assessment – A Brief Introduction	20
Assessing Internal Controls	21
Assessment Survey	23
Control Evaluation Questionnaire	27

INTRODUCTION

Internal control includes five notable concepts:

- Internal control is a process integrated with all other processes within an agency.
- Internal control is established, maintained, and monitored by people at all levels within an agency.
- Internal control increases the possibility of an agency achieving its strategic goals and objectives.
- Internal control must be cost effective. The cost of implementing a control should not exceed the benefits derived from having the control in place.
- The system of internal control in an organization is the responsibility of all employees, from management who design, implement, and maintain controls to staff that execute various control activities.

UNDERSTANDING BASIC PRINCIPLES BEHIND THE ESTABLISHMENT OF CONTROLS

This section includes a discussion of:

- ✓ Management's role;
- ✓ Control as one of the four basic functions of management;
- ✓ Why we need internal controls; and,
- ✓ Risk.

Management's role

Management's role is to provide the leadership that the organization needs to achieve its goal 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.

Internal control is . . .

a technique used by managers to help an organization achieve its goal and objectives.

Management is responsible for establishing effective management controls. The lack of administrative continuity in government units because of continuing changes in elected legislative bodies and in administrative organizations increases the need for effective management controls.

The four basic functions of management

Planning, organizing, directing and controlling are the four basic functions of management. Internal control is the fourth function – controlling. Adequate internal controls allow managers to delegate responsibilities to subordinate staff and contractors with reasonable assurance that what they expect to happen, actually does. Managers must develop internal controls for each activity for which they are responsible. The internal controls exercised over individual activities, when taken collectively, become the internal controls of the program or administrative function of which they are a part.

Why do we need Internal Controls?

To Provide Accountability . . .

Public sector 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.

Public officials, legislators, and taxpayers are entitled to know whether government agencies are properly handling funds and complying with laws and regulations. They need to know whether government organizations, programs, and services are achieving the purposes for which they were authorized and funded. Officials and employees who manage programs must be accountable to the public.

. . . and To 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 coordinate 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. Department managers must develop, implement, monitor, and update an effective plan of internal controls. The exact plan developed will depend, in part, on management's estimation and judgment of the benefits and related costs of control procedures, as well as available resources.

Risk

What is Risk?

Risk is the probability of an event or action having an adverse affect on your organization. It is directly tied to your control objectives and is those events or actions that can prevent you from achieving these objectives. Generally, it is the risk that your:

- Operations are not operating effectively or efficiently;
- Assets (data, financial resources, inventory, property, or personnel) are not adequately safeguarded against loss;

Risk
Risk is the probability of an event or action having an adverse affect on your organization.

- Financial and operating reports are unreliable;
- Operations are not in compliance with laws, rules and regulations; and,
- Unit's mission or goals are not achieved.

What are the affects of uncontrolled risk?

Uncontrolled risk can severely handicap an organization and eventually can result in failure of the organization. The consequences are:

- Resources are acquired or used inefficiently or ineffectively resulting in shortages of funds or failure of a unit to meet goals;
- Loss of assets due to theft or unintentional errors;
- Unreliable (incorrect, untimely or incomplete) financial and operational reports, resulting in poor decision-making by management;
- Non-compliance with laws, rules, or regulations resulting in financial penalties or damage to the reputation of the unit; and,
- Customer dissatisfaction due to ineffective operations resulting in loss of customers or negative publicity.

What factors affect risk?

Many factors affect the significance of a particular risk to operations or the probability that the risk will occur. We control risks by reducing these factors. Some of the more common factors are summarized below:

Common Factors Affecting Risk	
<u>FACTOR</u>	<u>EFFECT</u>
<i>Ethical Climate</i> maintained by management	Higher ethic = Lower risk
<i>Competence, Adequacy, and Integrity</i> of personnel	Over-worked or under-trained personnel = More errors and over-worked and unethical personnel = More irregularities
<i>Adequacy and Effectiveness</i> of the <i>System of Internal Control</i>	More effective/adequate system = Lower opportunity for errors/irregularities
<i>Degree of Computerization</i>	Higher automation = Lower risk of human error and more correction control
<i>Size, Complexity, Volatility, and Geographical Dispersion</i> of Operations	Larger, more complex, more volatile, more dispersed = Higher risks
<i>Degree of Regulation</i>	Higher regulation = More risk of noncompliance

INTERNAL CONTROL – AN OVERVIEW

This section includes a discussion of:

- ✓ Definition of internal control;
- ✓ Distinction between management and accounting controls;
- ✓ Limitations of internal controls;
- ✓ Biggest threats to the internal control structure;
- ✓ Four basic types of controls; and,
- ✓ Five specific control methods.

Definition of Internal Control

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:

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; and,
- Compliance with applicable laws and regulations.

This definition reflects certain fundamental concepts:

- Internal control is a process. It is a means to an end, not an end in itself.
- Internal control is effected by people. It is not just policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and board.
- Internal control is geared to the achievement of objectives in one or more separate, but overlapping, categories.

Because internal controls are a means to an end, they must help, rather than prevent or delay, an organization from reaching its objectives. The process of internal control also incorporates four basic principles. Before designing and implementing internal controls, the following basic principles should be considered:

- One* Internal controls must benefit, rather than hinder the organization.
- Two* Internal controls must make sense within each organization's unique operating environment.
- Three* Internal controls are not stand-alone practices. They are woven into the day-to-day responsibilities of managers and their staff.
- Four* Internal controls should be cost effective.

Consider internal controls as a continuous series of decisions affected by changing circumstances that will require periodic review and modification, rather than as a static system.

Distinction between management and accounting controls

Management control focuses on operations without necessarily a direct link to accounting records. Management controls, in the broadest sense, include the plan of organization, methods, and procedures adopted by management to ensure that its goals are met. Management controls include the processes for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance.

Of Concern in an Accounting Information System
Completeness - Are all transactions reflected in or captured by the accounting system?
Validity - Are only valid transactions recorded?
Authorization - Are all transactions properly authorized for inclusion in operations and in the accounting records?
Accuracy - Are reported numbers accurate representations of the economic transactions that have occurred?

While management controls are directed to overall operations, accounting controls are concerned with the integrity and accuracy of the accounting system and all financial reports being generated (see the desired attributes of an accounting information system in the box above).

Financial audits tend to emphasize accounting controls, while operational type audits tend to emphasize management controls that are more focused upon management's operating objectives. However, certain controls from each classification are likely to be relevant to any given audit activity.

Limitations of internal controls

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 ever installing an ideal system. Management will, correctly, choose to take certain risks because the cost of preventing such risks cannot be justified. Furthermore, 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 this perception may also affect staff's views on controls in general. If they consider internal controls as "red tape," this negative view could adversely affect their regard for and compliance with internal controls in general.

Despite limitations, the reasonable assurance that internal control does provide helps an organization to focus on reaching its objectives while minimizing risk.

Internal Auditing

Internal auditing is an important part of management control. When an assessment of management controls is called for, the work of the internal auditors can be used to help provide reasonable assurance that management controls are functioning properly and to prevent duplication of efforts.

Considering the wide variety of government programs, no single pattern for internal audit activities can be specified. Many government entities have these activities identified by other names such as inspection, appraisal, investigation, organization and methods, or management analysis. These activities assist management by reviewing selected functions.

Biggest threats to the internal control structure

Management Override

A well-designed control system, if set aside at management's discretion, can be equivalent to no controls in terms of risk. Circumstances may arise in which management override is justified. However, the control environment can be maintained if such an override is effectively monitored and limited to those settings in which the override is a practical necessity. You can minimize the risk of management override by establishing a documentation system for such overrides.

Access to Assets

The best way to safeguard assets is to control access to them. This control over access ranges from requiring identification badges in order to gain admittance to the premises to utilizing passwords to protect data files from unauthorized viewing or alteration.

Substance over Form

Controls may appear to be well designed and still lack substance. An example of form prevailing over substance are purchases exceeding a set dollar amount requiring necessary approvals, but the control is circumvented by breaking large orders into smaller purchases not requiring special approval. An additional example would be if competitive bids are required, but bids are only solicited from the same three suppliers every time, in spite of the availability of alternative suppliers, the purpose of the bidding procedure is defeated.

Conflicts of Interest

Employee conflicts of interest pose a threat to organizations. When an employee's loyalties are divided there is a distinct risk that the employee will choose a course of action detrimental to the organization's welfare.

Failure to Anticipate Certain Risks

Management may fail to anticipate certain risks, and thus fail to design and implement appropriate controls.

Collusion

Two or more employees may agree to circumvent internal controls.

Four Basic Types of Controls

Internal control systems may use four types of internal controls: preventative, detective, corrective, and compensating.

A concept that is important in relation to the types of controls is *Control Points* (see the definition in the box on the right).

Control point is . . .

a point in the process where an error or irregularity is likely to occur, creating a need for control.

Any operation is likely to have several key control points.

A variety of preventative, detective, corrective, and compensating controls may be employed at various points within a system to help ensure that the organization's internal control objectives are being met.

Preventative

Are designed to prevent the adverse action or risk from occurring. Preventative controls are before-the-fact controls that could trigger an obstacle that prevents the processing of a particular transaction.

Detective

Are designed to detect an error or adverse event after it occurs but within a reasonable time to permit correction and through awareness of the problem, helps prevent other errors from occurring.

Corrective

Correct the problems identified by detective controls. Many corrective controls rely on computer automation.

Compensating

Compensating controls can compensate for shortcomings elsewhere, so, at times, what appears to be a weakness in control is not really a problem due to the presence of compensating controls. Compensating controls represent a fail-safe approach to limiting risk exposure. This exposure must be analyzed in the context of what could happen, given particular system shortcomings.

Five Specific Control Methods

Organization Control . . .

Establishes the framework within which the entity conducts its various activities. These controls range from general to specific. There are five types of organizational controls.

Purpose, Authority, and Responsibility

Organizations establish overall guidance for their various departments and divisions with statements of purpose, authority, and responsibility. These statements outline the function to be performed, the authorized range of activities, and the specific responsibilities within the organization, including reporting responsibility.

Organizational Structure

Management organizes resources into various components. These divisions of responsibility establish a structure within which the overall mission of the organization may be accomplished. The most common method of setting forth organizational structure is through the organization chart.

Decision Authority

This outlines the key decisions for which the various organizational components are responsible.

Job Descriptions

Organizations typically outline in some detail the specific requirements of each job in the organization, including: specific responsibilities; reporting relationships; and job qualifications, including training and experience.

Segregation of Duties

A key element of the internal control structure is to ensure that incompatible functions are properly segregated so that one person is not in a position to both cause and conceal errors or irregularities.

Operational Controls . . .

Dictate the manner in which the organization performs its various activities and conducts its affairs. There are seven methods of operational control.

Planning

Effective planning is basic to the success of any enterprise and ranges from general to detailed. In all cases, organizations should document their plans, whether it is in the form of minutes of meetings where plans are formulated, or formally written and approved plans of operation.

Budgeting

Organizations formulate their plans into financial and activity budgets, usually on an annual basis. These budgets provide a detailed outline of anticipated financial and operational activity for the periods covered. Budgets provide effective control and allocation of an organization's resources.

Accounting and Information Systems

The accounting and information systems of an organization systematically tracks and documents summary reports of the organization's various activities. The reports generated by these systems provide management and others with important information related to their respective areas of responsibility. Without such information, decision-makers would be greatly limited in their knowledge of organizational performance.

Documentation

A fundamental practice of internal control is to document, usually in writing, the organization's various activities.

Authorization

Authorization or approval should be required before any business is conducted on behalf of the organization. Even when employees are given specific authority to make decisions, review procedures frequently are required to ensure abuses are avoided.

Policies and Procedures

Established policies and procedures provide the guidance that is necessary for most organizational activities. Policies and procedures help ensure consistent performance at a required level of quality. Without adequate policies and procedures, an organization is subject to performance that is inconsistent, unpredictable, and unreliable. The absence of appropriate policies and procedures, or noncompliance with such policies and procedures usually indicates a lack of adequate internal control.

Orderliness

The orderliness of records, work areas, storage areas, and processes is important to any operation.

Personnel Controls . . .

There are three controls that help ensure suitable performance by employees.

Recruiting and Selection of Suitable Personnel

Organizations generally establish qualification guidelines for personnel in different positions.

Orientation, Training, and Development

Typically, employees require an orientation and, usually, ongoing training and development in order to improve their abilities.

Supervision

Typically, employees require some degree of supervision. Supervisory responsibilities include specific job instructions, observation of the work process, and examination of the work product.

Periodic Review . . .

Three kinds of periodic review help organizations assess the progress and performance of their employees, operations, and programs.

Reviews of Individual Employees

Most organizations provide a performance review of individual employees at least annually.

Internal Review of Operations and Programs

Periodic reviews are conducted by the management of specific operations and program to determine the efficiency and effectiveness with which those activities are being conducted.

External Reviews

Any number of external parties may review the various operations of an organization.

Facilities and Equipment . . .

Organizations use a variety of physical facilities and equipment in their operations. Suitable facilities and equipment help build effective and efficient operations and help protect the organization's assets. Unsuitable facilities and equipment jeopardize both the operations and the assets.

INTERNAL CONTROL – INTEGRATED FRAMEWORK (THE COSO REPORT)

This section includes a discussion of:

- ✓ Introduction to COSO;
- ✓ Five Components of the COSO Report; and,
- ✓ Hard and Soft controls.

Introduction to COSO

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission published the Internal Control – Integrated Framework in 1992. The Treadway Commission was created by the joint sponsorship of the AICPA, the American Accounting Association, the Financial Executive Institute, the Institute of Internal Auditors, and the Institute of Management Accountants.

COSO is significant in at least three respects (see listing in box to the right).

COSO contains four

basic documents: an executive summary, framework, a discussion of reporting to external parties, and a volume on evaluation tools.

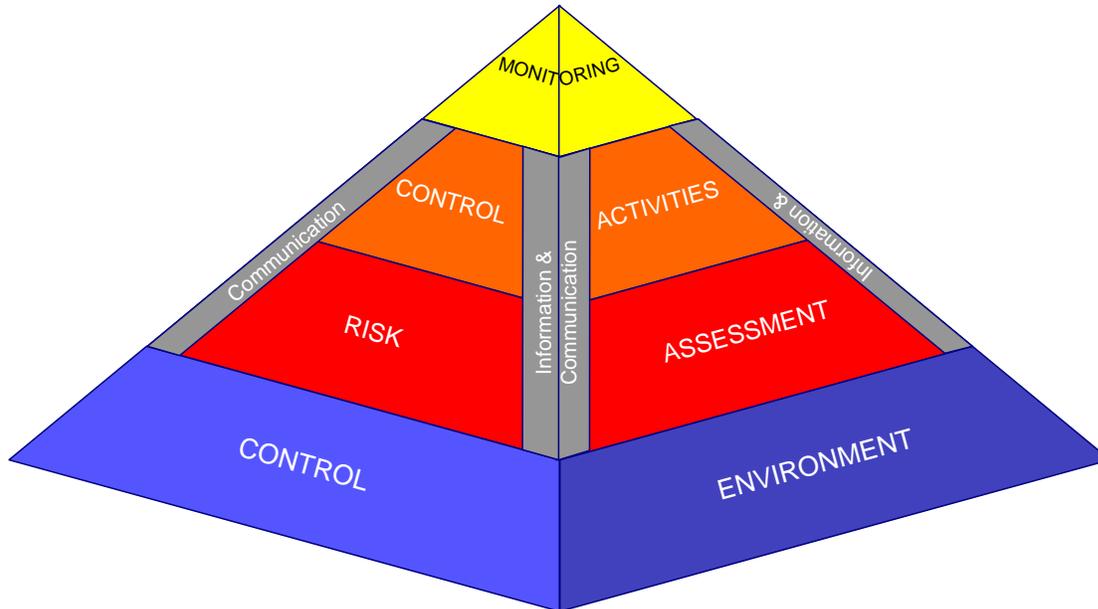
Significance of COSO	
	First consensus definition for internal control allowing all parties to use a standard definition for internal control.
	Defined internal control broadly rather than restricting it to financial or accounting terms only.
	Suggested guidelines for evaluating the effectiveness of an entity's system of internal control.

Five Components of the COSO Report

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, are graphically represented in the Exhibit on page 16 and in the subheads following.

EXHIBIT

Internal Control Components



"The *control environment* provides an atmosphere in which people conduct their activities and carry out their control responsibilities. It serves as the foundation for the other components. Within this environment, management *assesses risks* to the achievement of specified objectives. *Control activities* are implemented to help ensure that management directives to address the risks are carried out. Meanwhile, relevant *information* is captured and *communicated* throughout the organization. The entire process is *monitored* and modified as conditions warrant."

Source: "Internal Control - Integrated Framework," September 1992, Committee of Sponsoring Organizations of the Treadway Commission, p.13

Control Environment . . .

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors. Many factors determine the control environment, including the following:

- Management's attitude, actions, and values set the tone of the 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. If management views internal controls as unrelated to achieving its objectives, or as an obstacle, this attitude will also be communicated.

- Commitment to competence includes a commitment to hire, train, and retain qualified staff. It encompasses both technical competence and ethical commitment. Management's commitment to competence includes both hiring staff with the necessary skills and knowledge and ensuring that current staff receives adequate on-going training and supervision.
- Advisory board participation - The involvement of an entity's advisory board, if one exists, in a review of internal controls and audit activities can be a positive influence on the agency's control environment.

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 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, we need to ask: What could go wrong?

Risk assessment is . . .
the process used to identify, analyze, and manage the potential risks that could hinder or prevent an agency from achieving its objectives.

Over the course of a day, a week, a month, or a year, situations occur which could hinder or prevent a unit from fulfilling its responsibilities and meeting its goals. Because of this possibility, successful organizations continually identify and analyze potential risks. Performing risk assessments assists managers in prioritizing the activities where controls are most needed. Organizations use risk assessments to determine the relative potential for loss in programs and functions and to design the most cost-effective and productive internal controls. Two circumstances can be analyzed when beginning a risk assessment, 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). Some examples of circumstances that increase risk are the following:

- Changes in personnel;
- New or revamped information systems;
- New programs or services;
- Increased delegation of spending authority;

- Reorganizations within or between state agencies; and,
- Moving to a new location.

Inherent risk – 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. Examples of activities with high inherent risk are:

- Complex programs or activities – 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;
- Decentralization – increases the likelihood that problems will occur;
- A prior record of control weaknesses – will often indicate a higher level of risk as bad situations tend to repeat themselves;
- Unresponsive to identified control weaknesses – by prior auditors often indicates that future weaknesses are likely to occur; and,
- Cash receipts – cash is easily transferable.

After identifying potential risks, analyze each risk to determine how best to manage it. Factors in analyzing each risk are: the importance of the risk, the likeliness that the risk will occur, and what is the best way to manage the risk.

Control Activities . . .

Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, segregation of duties, job descriptions, and organizational charts.

Information and Communication . . .

Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information

about external events, activities and conditions necessary to informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across, and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, State Legislature, oversight agencies, and federal grantors.

Monitoring . . .

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

Hard and Soft controls

“Hard” and “Soft” controls are a useful, though not precisely definable terms. Hard and soft controls are best explained with common characteristics and examples.

Common Characteristics of "Hard" and "Soft" Controls	
<u>HARD CONTROLS</u>	<u>SOFT CONTROLS</u>
TEND TO BE:	
Formal Objective Quantitatively Measurable	Informal Subjective Intangible
EXAMPLES INCLUDE:	
Policies & Procedures Organizational Structure System of Authorization Reconciliations Input/Output Review Inspections	Competence Integrity & Ethical Values Shared Values Strong Leadership High Expectations Openness
FOLLOWING IS A LIST OF HARD AND SOFT CONTROLS APPLICABLE TO THE USE OF PURCHASING CARDS:	
Policies & Procedures Picture Identification Audit Function/Reconciliation Spending Limitations	Integrity & Ethical Values Education on the use of the Cards Communicating the Expectations for Use Understanding Benefits and Limitations Communication of the Audit Function

CONTROL SELF-ASSESSMENT (CSA) – A BRIEF INTRODUCTION

This section includes a discussion of:

- ✓ Introduction; and,
- ✓ Significant Components.

Introduction

The CSA process forms the nucleus for a comprehensive internal control evaluation process. CSA generally consists of a series of workshops conducted throughout the organization.

The workshops are attended by eight to 15 employees and are conducted by facilitators from internal audit. Workshops are structured to accomplish three primary goals: 1) define and discuss the function’s goals, 2) discuss the methods (controls) used by the group to achieve those goals, and 3) work together to assess the effectiveness of their controls. The data collected is categorized according to the COSO or another business model and added to the database of information collected throughout the organization from similar workshops. At some point, the database is analyzed and an assessment is developed regarding the overall condition of the internal control system throughout the organization. In addition, the results of the individual workshops provide information enabling the appropriate organization to focus on specific, defined problems. This may result in a traditional internal audit of a particular function, or some other action focused on specific problems.

Significant Components

The CSA has several significant components as follows:

CONTROL SELF-ASSESSMENT SIGNIFICANT COMPONENTS			
<u>Drivers</u>	<u>Risk Assessment Committee</u>	<u>Control Self-Assessment Workshops</u>	<u>Activities & Reports</u>
The drivers for the process are business requirements such as the performance expectations communicated by management to employees, the ideal business model depicting the way the organization wants to operate and defining employee roles within the organization, significant emerging issues which affect the business objectives, compliance requirement placed on the organization from various sources, etc. These drivers help form the ideal model against which the controls are evaluated.	The function of the committee is to evaluate the results of the assessment process and to assure that appropriate actions are taken to address control problems.	The CSA workshops themselves provide the data to be used by the Risk Assessment Committee and other managers to identify control problems and address them.	A variety of activities may result from CSA workshops including traditional internal audits, quality assurance audits, management conferences wherein a management team meets to discuss and solve specific control problems, and process improvements. In addition, reports can be prepared for individual groups, and for the organization as a whole. The feedback from each of these activities and reports is also used by the Risk Assessment Committee to address control weaknesses.

A COSO or five-step approach to evaluating internal controls

Analyze the control environment . . .

Review the control environment including attitudes and actions. If a specific procedure requires constant exceptions, it is better to change or eliminate the procedure than establishing an attitude of “rules are made to be broken.”

Organizations 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. They assist their staff by furnishing tools such as job descriptions and policy and procedure manuals that clearly communicate responsibilities and duties.

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. The structure should be documented through organizational charts that are made available to all staff.

Assess Risk . . .

The risk assessment process contains two major steps: (1) identify and prioritize activities that are most likely to have problems, and then (2) analyze those specific activities to determine their components.

Determine potential problems

Examples of circumstances with potential for problems includes programs that have undergone recent change in staff or structure, functions that receive complaints or have had problems in the past, and complex activities.

A moderate loss that is likely to occur presents as much danger as a more serious loss that is less likely to occur.

You can rank identified risks by asking: Where do we face the greatest possible harm? And which types of losses are most likely to occur?

Identify and analyze control cycles

A control cycle is a group of actions used to initiate and perform related activities. A single function usually contains several control cycles. Control cycles provide the focal point for evaluating internal controls. For example, in a social service program the process to determine eligibility could be a control cycle. After listing the control cycles, you can use the following process to document them:

- interview the personnel involved in the cycle and observe the activity;

- prepare either a narrative explanation or a flow chart;
- review the completed documentation with the persons providing the information; and,
- use the documentation to track one or two transactions through the process.

After documenting the control cycle, use the following steps to analyze the cycle:

- Review your flow chart to determine:
 1. Who is performing each step;
 2. What is involved in the step; and,
 3. Any resulting documentation.
- Review the information available in policy and procedure manuals. Use written materials such as organizational charts, job descriptions, reviews, checklists, departmental records, and reports to determine if the control cycle is operating as intended.
- Supplement written sources through conversations and observations.

Assess control activities

Evaluate the control cycle to determine if the system, as defined, sufficiently safeguards the department's resources, assures the accuracy of its information, and promotes effectiveness and efficiency.

Communicate Information

Are the internal control systems communicated throughout the organization?

Monitoring

Are the internal control systems monitored? At minimum, internal controls should be evaluated on an annual basis. Internal and external changes, personnel turnover, new programs, administrative activities, and priorities should be considered. Testing controls helps determine whether the controls continue to be adequate and are still functioning as intended. Program monitors, internal auditors, and other reviewers can be a resource in monitoring internal controls.

Assessment Survey

Please indicate the response that best describes your reaction to each statement.

SA = strongly agree A=agree D=disagree SD=strongly disagree NO=no opinion

Section 1: Agency Culture

The agency culture sets the tone of the organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control.

		SA	A	D	SD	NO
1.	The organization has a clear statement of ethical values that is understood at all levels of the organization.					
2.	A formal code of conduct has been adopted and adequately communicated to employees and board members, including policies on conflicts of interest.					
3.	Senior management demonstrates high ethical and work standards.					
4.	Senior management strives to comply with laws/regulations and agency policy.					
5.	Senior management monitors adherence to policies, principles of integrity and ethical values.					
6.	Senior management takes appropriate action for known departures from laws/regulations and approved policies.					
7.	My supervisor complies with laws/regulations and agency policy.					
8.	The performance measures in my work area are realistic and obtainable.					
9.	Employees in my work area have the knowledge, skill and training to perform their job adequately.					
10.	We learn from our mistakes.					
11.	Personnel turnover has not impacted the ability to effectively perform our functions.					
12.	Priority is given to ensuring that key operating positions are adequately staffed.					
13.	Mandatory vacations are required and job duties rotated appropriately.					
14.	Employees are treated fairly and justly.					
15.	Employees in my work area do not have to take unnecessary safety risks to perform their job.					
16.	Procedures are in place to appropriately limit the authority and responsibility of key personnel.					

Section 2: Goals, Obstacles and Risks

Organizations identify and analyze potential obstacles to the achievement of goals and risks of material misstatement in order to determine how to manage these obstacles and risks.

		SA	A	D	SD	NO
17.	Effective risk assessment mechanisms are in place that involve appropriate levels of management.					
18.	Appropriate risk consideration is given to internal and external factors.					
19.	Risk analysis includes estimating the likelihood of the risk occurring and the potential impact.					
20.	Procedures are in place to ensure that reassessment of risks are performed appropriately as changes occurs.					
21.	Incentives, pressures, attitudes, rationalization and opportunity are considerations in management's fraud risk assessment.					
22.	Job descriptions clearly define duties and responsibilities and are adequately communicated to employees.					
23.	For the coming year I am accountable for obtaining defined, measurable objectives.					
24.	I have sufficient resources, tools and time to accomplish my objectives.					
25.	In my area, we identify barriers and obstacles and resolve issues that could impact achievement of objectives.					
26.	In my area, the processes supporting new equipment, technology, and other significant changes are adequately managed.					
27.	The vision and mission of the agency are clearly understood.					
28.	The objectives of my work area are clearly communicated and understood.					
29.	The objectives of my work area are consistent with the mission of the agency.					
30.	People understand their role in achieving work area objectives.					
31.	My work area has been successful in achieving its objectives on a consistent basis.					
32.	Management is aware of and understands the obstacles and problems encountered by employees in fulfilling their responsibilities.					
33.	Performance targets and expectations are clearly defined and communicated.					
34.	Critical decisions are made by the people with the necessary expertise, knowledge and authority.					
35.	Performance is monitored against relevant targets and indicators.					

Section 3: Policies and Procedures*Policies, procedures and other safeguards help ensure that objectives are accomplished.*

		SA	A	D	SD	NO
36.	The policies and procedures in my work area allow me to do my job effectively.					
37.	Employees who steal from the agency (physical property, time, etc.) will be discovered.					
38.	Employees who steal from the agency and are discovered will be subject to appropriate consequences.					
39.	Policies and procedures are updated in a timely manner to reflect changes in practices.					

Section 4: Information and Communication*Pertinent information must be identified, captured and communicated in a form and time frame that enables people to carry out their responsibilities.*

		SA	A	D	SD	NO
40.	Are information systems providing management with timely reports on performance relative to established objectives.					
41.	The interaction between senior management and my work area enables us to perform our jobs effectively.					
42.	The communication across agency boundaries enables us to perform our job effectively.					
43.	The communication across my work area boundaries enables people to perform their jobs effectively.					
44.	I have sufficient information to do my job.					
45.	Senior management is informed and aware of my work group's actual performance.					

Section 5: Evaluation and Feedback

Through evaluation and feedback processes, an organization assesses, tracks and monitors its performance.

		SA	A	D	SD	NO
46.	Information reported to senior management reflects the actual results of operations of my work group.					
47.	I have enough information to monitor contractor performance.					
48.	Contracts are awarded in a prompt, fair and reasonable manner.					
49.	Contracts clearly define deliverables, terms and clauses.					
50.	I have enough information to monitor public satisfaction or dissatisfaction (either internal or external).					
51.	External and/or internal feedback (public, contractors, and other work areas) and complaints are followed-up on in a timely and effective manner.					
52.	The quality of output in my workgroup is measurable.					
53.	Employees in my work group know what actions to take when they find mistakes or gaps in performance.					
54.	Management takes corrective action to address deficiencies identified by internal or external reviews/audits.					
55.	Sufficient documentation for reports issued by the organization is maintained.					
56.	Reports are reviewed for accuracy and approved before release.					

Section 6: Information Systems

Data maintained and processed through computerized system should be protected.

		SA	A	D	SD	NO
57.	Integrity of data maintained in information systems is appropriately protected.					
58.	Policies and procedures are adequate to address potential loss of information maintained in information systems including disaster recovery/business continuity, back up process, etc.					
59.	System risk assessments are performed on a regular basis or whenever conditions change.					
60.	Security awareness policies are adequately communicated to all employees.					
61.	Access authorizations are appropriate based on employee's job duties.					
62.	Passwords are required to be changed periodically.					

Control Evaluation Questionnaire

I. Control Environment

A. Integrity and Ethical Values

1. How have we adopted and communicated to employees a formal code of conduct?
2. How do we know that our codes are comprehensive and fit our current organization and operating environment?
3. How do we know that all of our employees and administrators really understand the codes and standards and the consequences of noncompliance?
4. What other statements or activities have we used to convey the importance of integrity and ethical values (e.g., agency value statements, human resource policies)?

B. Tone at the Top

1. What have we done to communicate top management's commitment to sound internal controls and expectations regarding employee internal control responsibilities?
2. What processes are in place for management to monitor adherence to policies, principles of integrity and ethical values?
3. What have we done to effectively encourage employees to proactively communicate control breakdowns or overrides and potential violations?
4. How well have our managers and supervisors delivered the tone at the top via deeds and words? (Can you think of any recent positive or negative examples?)
5. What actions have been taken for potential or actual violations? (Were actions timely, consistent and appropriate?)

C. Competence

1. How does the organization ensure that all employees are aware of their responsibilities?
2. What process is used to monitor the knowledge and skill level needed to adequately perform each job?
3. What specific training programs (internal and external) are used for your work area to ensure that employees receive the knowledge and skills necessary to perform their jobs?
4. How does management ensure that key positions are adequately staffed?

D. Human Resources

1. Are backgrounds and references of applicants applying for financial, IT and other key positions verified? If so, by whom?
2. Is job performance periodically evaluated and reviewed with employees?
3. How do you ensure that all employees are appraised at least annually?
4. Describe the established policies that define responsibilities and criteria for hiring, training, promoting and compensating employees.

II. Risk Assessment

A. Activity Level Objectives

1. How do written mission statements/strategic plans/objective apply specifically to your duties?
2. Explain how mission statements and objectives are communicated to employees.
3. Describe the process used to ensure that all levels of management are involved in setting objectives.

4. Describe the process used to ensure that objectives exist for each major area of the organization.

B. Risks

1. Describe the process used to identify major external risks in your organization such as changes in technology, revenue, environmental regulations and political conditions.
2. Describe the process used to identify major internal risks in your organization such as retention of key personnel and availability of funds for new and continuing projects.
3. Describe any activities you believe may have been implemented to address operational risks, but do not seem to add value to the process.

C. Managing Change

1. Describe the methods in place to anticipate, identify and react to the following:
 - a. Changes in operational environment.
 - b. New or redesigned information systems.
 - c. New technology.
 - d. New equipment.
 - e. Changes in revenue.

III. Control Activities

A. Effectiveness of Policies and Procedures

1. List the primary policy and procedures manuals used by your agency and indicate who is responsible for issuing them and keeping them current.

2. If your work area is responsible for maintaining any manuals, describe the process used to periodically evaluate the policies/procedures for appropriateness and accuracy.

IV. Information and Communication

- A. Explain how employees receive information (from both external and internal sources) that is timely, in sufficient detail and communicated to the proper level to carry out responsibilities effectively and efficiently?
- B. What method is used in your work area to encourage employees to make suggestions on ways to improve operations?
- C. Is communication between various work areas of the organization adequate to enable employees to effectively perform their responsibilities?
- D. What method(s) are used to ensure timely and appropriate follow-up by management on communication received directly from contractors, suppliers, public and/or external parties?

V. Monitoring

- A. What procedures are in place to ensure that the organization's internal control environment is functioning as designed?
- B. If deficiencies are identified, at what levels are they reported?
- C. Provide examples of any self-assessment activities used (operational review checklist, management visits, etc.).