Division of Finance

SERVICES ELEVATED

State of Utah

Internal Control Guide

1/1/2013

Department of Administrative Services

DEPARTMENT OF ADMINISTRAVIVE SERVICES - DIVISION OF FINANCE

Internal Control Guide

2110 State Office Building, Capitol Hill Complex, 450 N. State St.
Salt lake City, UT 84114
http://finance.utah.gov

TABLE OF CONTENTS

TABLE OF CONTENTS - CHAPTER 2 (CONTINUED)

State of Utah

GARY R. HERBERT
Governor

GREG BELL
Lieutenant Governor

Department of Administrative Services

Kimberly K. Hood
Executive Director

Division of Finance

John C. Reidhead, CPA
Director

To: Legislative Leadership, Elected Officials, and Agency Heads
From: John C. Reidhead, Director of Finance
Date: 1/1/2013
Re: **Internal Control Guide**

I am pleased to issue this Internal Control Guide for use by all State agencies in the State of Utah. These principles reflect the concepts of broad-based objective setting, event identification, and risk response. This new guide is a bold step emphasizing the importance of internal control. This guide is based on the standards of the 1994 Committee of Sponsoring Organizations of the Treadway Commission (COSO) Report, as well as its framework for Enterprise Risk Management (ERM) that tie risk to strategic planning - which was released in 2004.

The Guide is designed to assist agencies in preparing internal controls and Internal Control Plans (ICPs), acknowledging that each agency has unique risks. Please remember that an effective ICP is a high level, agency-wide summarization of risks and controls for all of its business processes and is supported by lower level detail. Because internal control is a basic responsibility of all managers, we recommend that all agencies designate an Internal Control Officer to distribute this guide, along with any Internal Control Plan you might currently have, to all of your agency's managers. Agencies must update the ICP as often as changes occur in management, level of risk, program scope, etc., but at least annually.

The concepts of an "internal control plan" and an "internal control officer" and the related requirements in this Guide, including the Risk Assessment Internal Control Questionnaires (ICQ), are recommended for all State agencies; however, they are required of all agencies directed to have an internal audit function by the Internal Audit Act (see Utah Code 63I-5-201 (1) through (4) and 63I-4-401 (1) (f)). The Utah Internal Audit Act and other statutes require the following specific agencies to have an internal audit function: Administrative Office of the Courts, Administrative Services, Agriculture and Food, Alcoholic Beverage Control, Board of Education, Commerce, Community and Culture, Corrections, Environmental Quality, Health, Human Services, Natural Resources, Public Safety, Tax Commission, Transportation, and Workforces Services. These concepts are strongly encouraged, however, but not required of other agencies in the State of Utah. However, all agencies should complete the ICQs as applicable.

The benefits of this Internal Control Guide and the Internal Control Program include: (1) reduced risk of fraud and errors in financial reports; loss, misuse or waste of taxpayer dollars or other assets; noncompliance with State and federal laws and State policies and procedures, and embarrassment and repercussions that can come from related events. (2) a process to assist each agency in accomplishing their internal control objectives, (3) a process to assist the State's central management in assessing the condition of internal control systems in agencies, (4) a designated contact with each agency, who has a background in internal controls, (5) a designated contact with the State Division of Finance, who has a background in internal controls.

Introduction

Beginning with Watergate in the early 1970s, political and corporate corruption introduced the need for a method to monitor organizational activities. The Savings and Loan crisis soon followed these events. During the 1980s, numerous instances of inappropriate activities caused massive savings and loan association failures in the United States. By the end of the crisis, over 1,000 regularly audited savings and loan institutions failed, at a cost of $150 billion. Congress began investigating the crisis, culminating in the introduction of legislation intended to provide oversight to the audit profession. In response, the major audit associations united to sponsor the Treadway Commission. In 1987, the Treadway Commission issued its initial report, recommending that the organizations sponsoring the Commission work together to develop integrated guidance on internal control. The sponsoring groups accepted the recommendation, forming the Committee of Sponsoring Organizations (COSO). A Congressional majority determined that these actions by audit organizations meant that the legislation was unnecessary.

After COSO issued its report in 1992, various accounting organizations and the U.S. General Accounting Office (GAO) also began developing internal control guidance. By 2002, a wave of separate, but related, accounting scandals at companies like Enron and WorldCom became known to the public. This further evidence of inappropriate conduct renewed congressional interest in mandating requirements for stricter internal controls. These controls, based on COSO and on the guidance developed by accounting organizations, culminated in the passage of the Sarbanes-Oxley Act.

Internal control standards continue to evolve as audit organizations and government agencies use their experiences to refine and reshape the concept of acceptable internal control. Appendix 1 contains additional information on the regulations and guidance discussed above.

The concepts of an "internal control plan" and an "internal control officer" and the related requirements in this Guide, including the Risk Assessment Internal Control Questionnaire (ICQ) are required of all agencies directed to have an internal audit function by the Internal Audit Act (see Utah Code 63I-5-201 (1) through (4) and 63I-4-401 (1) (f)). The Utah Internal Audit Act in State statute requires the following specific agencies to have an internal audit function: Administrative Office of the Courts, Administrative Services, Agriculture and Food, Board of Education, Commerce, Community and Culture, Corrections, Environmental Quality, Health, Human Services, Natural Resources, Public Safety, Tax Commission, Transportation, and Workforces Services. These concepts are strongly encouraged, however, but not required of other agencies in the State of Utah. However, all agencies should complete the ICQs, including the Risk Assessment ICQ.

Chapter

1

Internal Control Program

Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an agency's management and board.

The State Division of Finance has prepared this Internal Control Guide and the Policy on Internal Control to help the agencies of the State (1) establish, maintain, and monitor sound internal controls and participate in the Internal Control Program.

Internal Control Objectives

Internal Control is a process effected by management designed to achieve three basic objectives:

- Efficiency and effectiveness of operations.
- Reliable financial reporting.
- Compliance with applicable laws and regulations.

Internal controls are what management puts in place to help ensure each of these objectives are reached. Management is responsible for internal controls – not external auditors.

State Policy on Internal Control

The State Division of Finance has issued a policy on Internal Control (FIACCT 20-00.00). The policy requires the following: (1) agencies must establish and maintain sound internal controls based on the five components of internal control, (2) agencies must establish and maintain proper segregation of duties, and (3) agencies must participate in the Internal Control Program. The policy is available on the Finance website (http://finance.utah.gov/index.html) by clicking on "Internal Control."

Purpose of the Program

The purpose of this program is to assist each agency with their responsibilities to maintain sound internal controls. It is our hope that the agencies and the agency heads will support this new program.

We realize this is an additional workload on agencies still coping with recent budget cuts. However, in light of recent events and some audit reports and legislative concerns, we feel the agencies need some assistance in performing risk assessments and maintaining sound internal controls.

Benefits of the Program

The benefits of the Program include the following:

- Reducing the risk of:
  - Fraud and errors in financial reports.
  - Loss, misuse or waste of taxpayer dollars or other assets.
  - Noncompliance with State and federal laws and State policies and procedures.
  - Embarrassment and repercussions that can come from related events.
- A process to assist each agency in accomplishing their internal control objectives/responsibilities.
- A process to assist the State's central management in assessing the condition of internal control systems in agencies.
- A designated contact with each agency, who has a background in internal controls.
- A designated contact with the State Division of Finance, who has a background in internal controls.

Authority to Establish the Program

The Division of Finance is authorized and required to do the following:

- Utah Code 63A-3-103.
  - "(b) provide for the accounting control of funds;"
  - "(e) prescribe other fiscal functions required … to transact all executive business for the state."
- Utah Code 63A-3-203
  - "(a) exercise accounting control over all state departments and agencies."
- Utah Code 63A-3-204.
  - "(b) maintain a financial control system according to generally accepted accounting principles."

We believe the State Division of Finance has the necessary authority to implement the new internal control policy and the new internal control program.

Internal Control Questionnaires (ICQ) & Field Audits

The Internal Control Questionnaire, commonly known as an ICQ, is a series of yes/no questions to assist in the identification of internal control weaknesses. The State Division of Finance has participated with the National Association of State Comptrollers in developing an internal control guide and a set of internal control questionnaires for use by states. The State Division of Finance has further modified and tailored the guide and several of the ICQs to conform to Utah systems and terminology. The ICQs and the schedule of when each

ICQ is to be completed and returned to the State Division of Finance are available on the Finance website (http://finance.utah.gov/index.html) by clicking on “Internal Control.”

Because of the comprehensive nature and length of the ICQs, questions are divided by topic into multiple sections. Since not all questions in each ICQ are applicable to all agencies, most agencies are able to skip one or more of the sections. Also, since not all ICQs are applicable to all agencies, most agencies are able to skip one of more of the ICQs. The State Division of Finance recommends that the internal control officer and the chief financial officer/director of finance work closely with senior management in responding to the ICQ questions. In larger agencies, several individuals will need to be involved.

Directions for Completing the ICQs

The specific directions for completing each ICQ are included on the ICQ form.

ACT Representative

Each agency has an agency coordinator team representative (ACT) who attends the monthly State Division of Finance ACT meetings. Ideally, the ACT is the agency’s Director of Finance or Comptroller. However, if someone else is assigned to attend ACT meetings, they should have a solid accounting and internal control background. Someone other than the ACT can be designated as the contact person in each agency, but they also would need to attend ACT meetings.

The ACT representative (or the internal control contact if delegated by the agency) for each agency will need to do the following: (1) attend the monthly ACT meetings, (2) complete the ICQs or distribute the ICQs to those who will complete them, (3) gather the completed ICQs back up after they are completed, (4) have the agency head/executive director review and acknowledge them, (5) send the completed and approved ICQs electronically back to the Division of Finance, and (6) send the completed and approved ICQs to the agency’s internal auditors, if the agency is required by the Internal Audit Act to have an internal audit function. Electronic submissions to the Division of Finance are strongly encouraged (Word, PDF, etc. attached to an email).

Chief Financial Officer

The Chief Financial Officer, Director of Finance, or Comptroller for each agency will need to do the following: (1) determine which and how many of each of the new ICQs are needed, (2) review and approve each ICQ after they are completed, (3) have the agency head/executive director review and acknowledge each of the completed ICQs, and (4) determine which optional ICQs will be completed.

Responding to ICQ Questions

Answer each question on the ICQ by checking or putting an “x” in the appropriate box (either Yes, No, or N/A). A “No” response identifies an internal control weakness or that the control is achieved with another compensating control. Please describe in the Comments field for each “No” answer:

- The plan to resolve the weakness, including the estimated date of completion, or
- The compensating control(s), and if not readily apparent, why they adequately compensate for the “No” response.

The “N/A” responses may need an explanation if the reason is not readily apparent.

Examples of Corrective Action Plans

Examples of "No" answer comments for ICQ questions for which agency management has prepared a corrective action plan for identified internal control weaknesses include the following:

Example #1 – Corrective Action Plan.

Question: "Are there procedures to prevent and detect splitting purchase orders to avoid obtaining and documenting higher levels of approval prior to the purchases?"

Answer: "No."

Comments: "The XYZ agency was unaware of this policy. All purchasing personnel are being trained on this State policy, and procedures are being implemented to ensure compliance. The estimated date of completion is March 10, 2012."

Example #2 – Corrective Action Plan.

Question: "If payments are received over the counter, are receipts controlled by cash register, pre-numbered receipts, or other means?"

Answer: "No."

Comments: "Though the University does not provide the student with a receipt when tuition is paid over the counter, a partially compensating control is that the student's check serves as their receipt. If the money is stolen or applied to the wrong student's account by the cashier, then the student will be billed again for the tuition and will come in and complain until the error is corrected. However, since it would be difficult to identify which cashier was responsible, we are changing our system to produce a pre-numbered receipt for all over-the-counter receipts. This change should be in place for the next semester beginning May 1, 2012."

Examples of Compensating Controls

Examples of "No" answer comments for ICQ questions for which agency management has identified one or more compensating controls for the internal control in question include the following:

Example #1 – Compensating Control.

Question: "Are responsibilities for preparing bank reconciliations segregated from cash receipt and disbursement responsibilities?"

Answer: "No."

Comments: "The XYZ agency is a very small agency (20 employees) and proper segregation of duties is difficult. Our compensating control is that the accountant who performs both cash disbursement and bank reconciliation duties is closely supervised by their manager including reperforming the bank reconciliations on a surprise basis (approximately quarterly)."

Example #2 – Compensating Control.

Question: "Are the individuals responsible for the requisitioning/receiving and purchasing functions different from the individuals responsible for the invoice processing/accounts payable?"

Answer: "No."

Comments: "The compensating control for transactions processed through FINET is that FINET requires two individuals to process all payment transactions – one to enter and the other to approve."

Certification Statement

The last page of each ICQ is the Certification Statement. In this section, the ICQ preparer(s), the agency chief financial officer/director of finance, and the agency head must read and approve the statements, confirming that the information entered into the questionnaire is accurate.

Conclusion

Each of us plays a vital role in creating an environment that is accountable to the public while being responsive to the needs and direction of senior management. Internal controls are a critical element of this environment.

Field Audits

An internal control auditor will periodically visit each State agency to review certain internal control issues including ICQ questions and responses. Generally, the audit test work will be limited to inquiry and observation. However, the auditor may look at other issues of interest to the Division of State Finance. The auditor will write audit findings and include them in the quarterly Post-Audit Reports when internal control weaknesses or ICQ reporting inaccuracies are found.

Internal Control Manager Responsibilities

The role of the Internal Control Manager at the State Division of Finance includes the following:

- Answer agency questions about internal controls and ICQs but not make decisions for agencies.
- Review completed and approved ICQs.
- Follow up with agencies to ensure timely and complete ICQ submissions including corrective action plans for problems noted.
- Track agencies' progress and report to the DAS Director of Finance.
- Develop and update ICQs.
- Develop and update the Internal Control Guide.
- Develop new course on Internal Controls for State employees.
- Conduct field audits to help ensure agencies correctly completed the ICQs and implemented corrective action plans.
- Include noted internal control weaknesses, including ICQ reporting errors, in the quarterly post-audit reports to agencies.

Chapter

2

Internal Control Plan Framework

Internal Control Plan and Risk Assessment Cycle

An organization is a living entity which changes over time. As a result, the organization's mission statement, goals, objectives, performance measures, risks, and internal controls must be regularly evaluated and periodically revised. Thus, internal control is an ongoing process known as the Internal Control Cycle. After an organization analyzes its goals and objectives to determine its risks, management must analyze these risks and evaluate the policies and procedures in the identified high-risk areas. Part of the management process includes monitoring the progress made toward meeting goals and objectives. Monitoring also helps to ensure the effectiveness of the organization's internal controls and the effectiveness of the policies and procedures. Periodically, policies and procedures should be revised to mitigate risk and eliminate redundancy. They must also be communicated internally and externally, as necessary.

Everyone in an organization has responsibility for internal control.

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. The State of Utah has defined the internal control plan to be a high-level summary supported by lower level policy and procedures. Each agency's internal control plan will be unique; however, it should be based on the same framework – the organization's mission statement, goals and objectives, and components of internal control recommended by COSO. The plan should be reviewed and updated as conditions warrant, but at least annually.

Because the agency's policies and procedures provide the detail for the internal control plan, it is important that they be reviewed in conjunction with the plan. It is not uncommon for the detailed policies and procedures to be modified due to changes in personnel, audit or quality assurance recommendations, etc. As these modifications occur, the agency's documentation should be updated to reflect them.

Every agency head should designate an Internal Control Officer who is responsible for its internal control plan. It is recommended that the designated Internal Control Officer be a senior manager, equivalent in title or rank to an assistant or deputy to the agency head so they have sufficient authority to ensure the plan is updated and followed. It should be noted, however, that internal controls are the responsibility of every employee.

This chapter will discuss some concepts related to the Enterprise Risk Management (ERM) components of Internal Environment, Objective Setting, Event Identification, Risk Assessment, Risk Response, Control Activities, Information & Communication and Monitoring. It is important to realize that ERM is not a linear process but rather a multi-directional process in which almost any component can, and will, influence another component.

Tone at the Top

Management's attitude, actions, and values set the tone of an organization, influencing the control consciousness of its people. Internal controls are likely to function well if management believes that those controls are important and communicates that view to employees at all levels. If management views internal controls as unrelated to achieving its objectives, or even worse, as an obstacle, this attitude will also be communicated. Employees are aware of the practices followed by upper management including those that circumvent internal controls. Despite policies to the contrary, employees who note that their managers frequently override controls, will also view internal controls as "red tape" to be "cut through" to get the job done. Management can show a positive attitude toward internal control by such actions as complying with their own policies and procedures, discussing internal controls at management and staff meetings, and rewarding employees for following good internal control practices. Although it is important to establish and implement policies and procedures, it is equally important to follow them.

Management Philosophy & Operating Style

Management's philosophy and operating style affect the way the organization is managed. They determine, for example, whether the organization functions informally with verbal instructions or formally with written policies and procedures. They also define whether the organization is conservative or aggressive in its response to risks. In other words, they define the organization's "risk appetite" or the level of risk that is acceptable to the organization. To be successful, the organization's internal controls must be aligned with management's philosophy.

Ethics

An organization's culture evolves from the values of its members and the culture, in turn, exerts a strong influence on the actions, decisions, and behaviors of all employees.

Utah officials' and employees' conduct is also governed by the Utah Public Officers' and Employees' Ethics Act (see Utah Code 67-16-1 through 14).

Utah officials are also governed by the Utah Criminal Code relating to conflicts of interest (see Utah Code 76-8-109).

Accountability

Public sector managers are responsible for administering the resources entrusted to them to carry out government programs. A major factor in fulfilling this responsibility is ensuring that adequate internal 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. Frequently specified by law, this concept of accountability is intrinsic to the governing process of the State of Utah. Internal control is a technique used by managers to help an agency achieve these objectives. Internal control is the term we use for the structure, policies, and procedures used to ensure that the agency accomplishes its objectives and meets its responsibilities.

Mission Statement

A mission statement clearly identifies an organization's purpose and how it is accomplished. It should be a brief paragraph that is easily understood by the reader, including those outside the organization or field. The mission statement, therefore, should be free of jargon and/or shorthand.

An organization's mission statement may remain current for a number of years. However, it is a good idea to review it periodically – such as part of the annual internal control plan review – to fine-tune or update it. The mission statement should be consistent with, if not centered around, the key objectives (for the agency activities and programs) identified in federal and State law.

Goals / Long-Term Objectives

A goal is an end result the organization wants to attain. It should be a broad, long-range concept and not limited to what can be accomplished in a single fiscal year. When an organization sets its goals, it is determining its priorities.

Management sets agency goals and long-term objectives and priorities based upon identified legislative mandates established in statutes (enabling legislation) and priorities of the Governor.

Objectives

An objective is the action required to achieve the long-range goal. In contrast to a goal, an objective is narrowly focused and easily validated. It should, therefore, be an action that can be accomplished in an identified period of time, such as a fiscal year. A good objective is **SMART**:

Specific – What is the single result to be accomplished?

Measurable – How can it be measured? (Some objectives are more difficult to measure; however, they should have observable results.)

Attainable – Is it realistic given the resources currently available?

Results-focused – Does it make a difference if the objective is accomplished?

Timely – Is the timeline realistic?

Effectiveness & Efficiency

Effectiveness and efficiency are the most fundamental management responsibilities. Effectiveness is judged on the basis of results. We judge success by evaluating the effectiveness of an agency in meeting its goals and objectives. Management's role is to provide the leadership needed for an agency to realize that purpose. *Does this program accomplish what it is supposed to?* It is important that management remain focused on reaching intended objectives as well as day-to-day results.

Efficiency measures how well managers make use of available resources in achieving objectives. Because resources are always scarce, management is responsible for making the best use of the resources that are available. *Is resource use consistent with the agency mission?*

Performance Measures

Effectiveness and efficiency performance measures should be established for each goal/long-term objective based on the law.

Types of Performance Measures

Performance measures include the following four types:

- Effectiveness/Outcomes.

  Examples:
  - Percentage of all applications received that were processed during the period.
  - Percentage of people who initiated the reading program who achieved at least Level C on the final reading ability exam.

- Efficiency.

  Examples:
  - Total program costs during the year per application processed during the year.
  - Total program costs during the year per person who completed the reading program during the year.

- Inputs.

  Examples:
  - Total employees in the program.
  - Total dollars spent on the program during the year.
  - Total applications received during the period.
  - Total number of people entering the reading program during the year.

- Outputs.

  Examples:
  - Total applications processed during the period.
  - Total number of people completing the reading program during the year.
  - Total miles driven teaching reading classes.

Turning Inputs and Outputs into More Effective Performance Measures

Effectiveness and efficiency performance measures are superior to, and strongly recommended over, inputs and outputs when determining how effectively and/or efficiently the goals and objectives are being achieved. Inputs and outputs can usually be turned into effectiveness or efficiency performance measures by dividing them by some number which is often an input or output.

Examples:

- The output, "Applications Processed During the Fiscal Year" can be turned into an effectiveness performance measure by dividing it by the input "Applications Received During the Fiscal Year." The resulting effectiveness performance measure called, "Percentage of Applications Processed During the Fiscal Year" is more useful in assessing effectiveness.
- The input, "Miles Driven Teaching Classes" can be turned into an effectiveness performance measure by dividing it by the output, "Number of Enrolled Students Who Completed the Class Successfully." The resulting effectiveness performance measure called, "Miles Driven Per Student Who Completed the Class Successfully" is more useful in assessing effectiveness.
- The output, "Total Expenditures Related to Audits for the Fiscal Year" can be turned into an efficiency performance measure by dividing it by the "Number of Audits Performed During the Fiscal Year." The resulting efficiency performance measure called, "Total Cost Per Audit" is more useful in assessing efficiency.

Needed Elements of a Performance Measure

Each performance measure needs the following: (1) a definition, (2) a consistent and specific method of measurement, and (3) one or more internal controls to ensure its periodic measurement is complete and accurate since those measurements are used in management decision making. Each performance measure should be linked to an internal control.

Performance measures work well for repeated transactions or events and in situations where the agency has the ability to affect the achievement of the goals and objectives. For example, using the effectiveness performance measure "Percentage of Audit Recommendations Implemented" would be ineffective as a performance measures since auditors usually can't force the agencies to implement the recommendations. Also, using the output, "Number of Audit Recommendations Issued during the Fiscal Year" would be ineffective as a performance measure since the auditor could simply issue many lesser important recommendations usually not made just to appear to be achieving greater effectiveness.

Organizational Structure

The organizational structure provides the decision-making framework of an organization. This structure groups, divides, and coordinates the tasks required to achieve identified goals. To be effective, the structure must make the best use of available resources while maintaining adequate controls to ensure compliance with applicable requirements.

Competence

There are two types of competencies – position and personal. Position competencies are the skills needed to perform the required duty, regardless of the incumbent. Personal competencies are the skills, knowledge, expertise, and experience of the individual employee, regardless of whether they are tied to the employee's current position. Employees should have the skills to adequately perform their assigned duties.

Effective human resource policies strengthen an organization's internal controls. These policies should address hiring, training, performance evaluations, responsibilities, appropriate behavior and disciplinary actions. If employees understand that they are responsible and accountable, the control environment is strengthened.

An employee handbook can enhance an agency's control environment. It should include, but not be limited to, agency policies and procedures, control procedures, employee responsibilities, ethics, description of employee evaluations, job descriptions and possible disciplinary action to take when standards are violated.

Event Identification

Both internal and external events influence goals, objectives and strategies. They may be isolated or part of a chain reaction or rippling effect. Events with a potential negative impact are considered risks while those with a potential positive impact are opportunities. Some examples of events that affect organizations are:

- The organization's source of funding is being reduced or increased.
- Employees' productivity is increasing or dropping.
- Employees have different views of the organization's purpose.
- The level of commitment of the person at the top of the organization is high or low.

Risk Assessment

A risk assessment is a formal process to identify and analyze factors that may affect the achievement of a goal. In general, risk factors may include the control environment, size of the organization, complexity, change, and results of previous reviews/audits. It is important to remember that not all risks are equal. Some risks are more likely to occur while others will have a greater impact. For example, risks to safety or security of individuals, data or personal information could have significant consequences. Once identified, the assessment regarding the probability and significance of each risk is critical. The risk assessment design should be understandable, consider relevant risk factors and, to the extent possible, be objective.

Risk Response

Risk responses fall into four basic categories: (1) accept the risk and monitor it, (2) avoid the risk by eliminating it, (3) reduce the risk by instituting controls, or (4) share the risk by partnering or entering into a strategic alliance with another agency or external entity.

Determining a risk response is an important decision. Because risk events by definition are uncertain, deciding whether to accept or avoid risk-related activity can have significant consequences for an organization. By choosing to reduce risk, an organization is committing to implement control activities which generally consume resources.

Internal Control

Internal Control is a process effected by management designed to achieve three basic objectives:

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

Internal controls are what management puts in place to help ensure these objectives are reached. Management is responsible for internal control – not external auditors.

We divide controls into two main types – preventive and detective. A sound internal control plan will combine both preventive and detective controls to mitigate key risks. Preventive controls, as the term implies, work to prevent problems. However, since they may be time consuming and expensive, management should ensure that the benefits outweigh the cost. Examples of preventive controls include authorization lists, computer edits, segregation of duties, and prior supervisory approval.

Detective controls do not prevent fraud or errors. They will identify that a problem has occurred. On the other hand, detective controls are more efficient in that they do not slow business processes. They are less effective because they can only identify an incident after the fact, not stop it from happening. The existence of detective controls, however, can also serve to prevent irregularities. An individual tempted to use agency funds inappropriately may be deterred by the knowledge that the bank account is regularly reconciled. Examples of detective controls include reconciliations, exception reports, and supervisory review.

Policies and Procedures

Controls are most frequently comprised of policies and procedures. After identifying and assessing risks, managers need to evaluate (and develop, when necessary) methods to minimize these risks. A policy establishes what should be done and serves as the basis for the procedures. Procedures describe specifically how the policy is to be implemented. It is important that an organization establish policies and procedures so that staff knows what is to be done and compliance can be properly evaluated.

Security

Agency Head Signature Authorization

An agency head is responsible for all activities conducted by the agency. Because in most agencies the agency head cannot personally review and certify all business transactions, the agency head is responsible for setting up the agency's business operations with a series of checks and balances (internal controls) to balance risks and efficiencies. Agency heads must directly authorize individuals within their chain of command to be their designee for approval of fiscal documents or other legal obligations on their behalf. There can be no sub-delegation by designees.

Security of Records

Agency management must ensure the security of records and sensitive information provided or available. The security of records and data in hard copy or electronic format involves system security, data security and physical security. Threats to security may come from within, as well as from the outside of an agency so consideration for each is needed.

System Security

Agency management must determine each individual's Human Resources, Payroll, and FINET security access by both business area and security level. Management can limit access to one or more specific business areas, such as Accounts Receivable, Payroll, or Fixed Assets. Within each business area, management must also select the appropriate security levels.

Data Security

Data security is the means of protecting data, whether in hard media (paper, microfilm) or in computer and communications systems, against unauthorized disclosure, transfer, modifications or destruction whether accidental or intentional. Therefore, data security helps to ensure privacy. It also helps in protecting confidential data concerning clients, consumers and employees.

Data security consists of procedures that prevent unauthorized access to computer resources. Appropriate security procedures should not significantly hinder a person from performing their work. Security procedures should, however, protect data from unintentional acts, as well as intentional ones. Examples of data security include:

- Define carefully the level of system access an employee is given.
- Select appropriate password safeguards.
- A hard to guess password.
- Periodic password changes.
- Alphanumeric characters per password.
- Password kept confidential.
- Screen-saver passwords.
- Assign each user a unique user ID.
- Limit user access to system software.
- Control access to specific applications and data files.
- Limit access to what is required to perform a person's job function and to allow for appropriate segregation of duties.
- Review security logs.
- Limit concurrent logins.
- Activate intruder detection and prevention mechanisms.
- Implement adequate virus protection procedures.

Access to enterprise systems (large-scale applications/software packages) should be reviewed perhaps quarterly, as well as when significant turnover occurs in sensitive positions or in realignment of duties.

Physical Security

Physical security is the protection of personnel, clients, records, and assets. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism. Security engineering involves three elements of physical security: (1) obstacles to frustrate trivial attackers and delay serious ones, such as locks and swipe card access; (2) detection devices such as alarms, security lighting, and security guards to make it likely that attacks will be noticed; and (3) security response to repel, catch or frustrate attackers when an attack is detected.

Segregation of Duties

Segregation of duties is a primary principle in any internal control plan in order to provide adequate checks and balances. The basic goal of segregation of duties is that no one person should have excessive control over one or more transactions or critical processes. It also defines authority and responsibility over activity and use of the State's resources.

Discussion

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

- Managing both the operation of and record keeping for the same activity.
- Managing custodial activities and record keeping for the same assets.
- Authorizing transactions and managing the custody or disposal of the related assets or records.
- Operating and programming computer system.

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

- (Entry) Recording transactions: This duty refers to the accounting or record keeping function, which in most organizations, is accomplished by entering data into a computer system.
- (Approval) Authorization to approve payment: This duty belongs to persons with authority and responsibility to have others initiate and enter transactions.
- (Custody of assets) Custody of assets involved in the transactions: This duty refers to the actual physical possession or effective physical control/safekeeping of property. Property can take the form of cash, checks, or other assets (including the receiving of assets purchased function).
- (Reconciliation) Periodic reviews and reconciliation of existing assets to recorded amounts: This duty refers to making comparisons at regular intervals and taking action to resolve differences.

The advantage derived from proper segregation of duties is twofold:

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

Ideally, the following activities should be segregated:

- Individuals responsible for data entry of purchasing and payment transactions should not be responsible for approving these documents.
- A department should not delegate expenditure transaction approval to data entry personnel or to the immediate supervisor of data entry staff when they also have the ability to enter transactions. Individuals approving expenditure transactions should not supervise data entry staff. In FINET, a

compensating control for this weakness is that no one can both enter and approve the same transaction.

- Delegated expenditure authority must be in writing and approved by the appointing authority.
- Individuals responsible for acknowledging the receipt of goods or services should not be responsible for purchasing or accounts payable activities.
- Individuals who prepare/record payments should not approve the payments.
- Individuals who prepare/record payments should not perform budget compliance and review.
- Individuals responsible for cash receipts functions should be separate from those responsible for cash disbursements.

Internal controls are designed to prevent and/or detect errors. However, internal controls are also designed to prevent and/or detect fraud – except in the case of fraud by collusion. Generally, internal controls strong enough to prevent and/or detect fraud by collusion are not cost effective. The questions in this ICQ were designed with these points in mind."

Smaller Organizations

Maintaining segregation of duties is especially challenging for units with very small numbers of employees. However, this situation is rare in State agencies since they usually have several employees. Also, since senior administrators are involved in the day-to-day operations of the organization, these managers may have more opportunities to override the controls or misstate financial statements.

Managers of such agencies must consider this principle when designing and defining job duties; they must implement control procedures to assure segregation of duties exists. In an environment with limited numbers of personnel, management should develop alternate management procedures. The list below offers some examples of alternate procedures:

- Being more involved in day-to-day operations/activities.
- Increasing supervision of the employee, unit, bureau or office.
- Periodically reperforming some employees' duties (such as bank reconciliations).
- Involving other employees with unrelated job responsibilities in limited ways (such as (1) periodically verifying that all receipts are pre-numbered and a copy of all receipts is retained – even voided receipts or (2) periodically verifying that the daily mail receipts log agrees to the validated deposit slip).
- Monitoring and analyzing data from reports of financial activity.

Management is responsible for sound internal controls including proper segregation of duties. Though more difficult for smaller organizations, it is just as important. An attitude of "we can only do what we can do" or "we will do the best we can with the resources we have" is just not acceptable. As the list above shows, increased supervision can fully compensate for what would otherwise be an inadequate segregation of duties.

Costs Versus Benefits of Internal Control

The expected benefits from increasing the likelihood of achieving agency objectives and/or decreasing expected losses or errors must exceed the personnel and other costs of the internal control. In other words, the cost of a control should not exceed the benefit to be derived from it. As agencies assess existing internal controls or establish new internal controls (including segregation of duties), they should always consider the cost versus benefit of the internal control.

Internal control can provide reasonable, not absolute, assurance that the objectives of an agency will be met. The concept of reasonable assurance implies a high degree of assurance, constrained by the costs and benefits of establishing incremental control procedures.

A control that prevents a loss is usually superior to a control that detects a loss after it has occurred. Early detection is essential if prevention fails. When a failure occurs, corrective action reduces future losses.

Management's attitude toward internal control is the most critical element. If management shows little concern, others will not be as likely to be diligent.

Compliance with laws, regulations, and policies and procedures is critical. Those organizations issuing the laws, regulations, and policies and procedures have or should have already determined that compliance is cost beneficial. The State Division of Finance does not give approval or waivers, except where specifically mentioned in Finance Policies, to not follow Finance policies.

Information

Management requires data to make effective decisions. Data alone is not enough, however; data provided must be the right information, in an understandable format, which is timely enough to be useful. Information systems produce reports, containing operational, financial, and compliance-related information that makes it possible to run and control an agency. This information should reveal the organization's progress toward meeting goals and objectives. Management also needs information that allows it to evaluate the efficiency of operations and to ensure that the organization follows applicable laws and regulations.

Questions to consider include the following:

- Does management regularly collect and review information that alerts it to both internal and external risks?
- Does the agency get information that tells management whether it is achieving its objectives?

Communication

Communication is the exchange of useful information between and among people and organizations to support decisions and coordinate activities. Information should be communicated to management and other employees who need it in a form, and within a timeframe, that helps them to carry out their responsibilities.

Management should establish communication channels that:

- Provide timely information;
- Can be tailored to individual needs;
- Inform employees of their duties and responsibilities;
- Enable the reporting of sensitive matters;
- Enable employees to provide suggestions for improvement;
- Provide the information necessary for all employees to carry out their responsibilities;
- Convey top management's message that internal control responsibilities are important and should be taken seriously; and
- Convey and enable communication with external parties.

Communication is multi-faceted – verbal, non-verbal and written. It is important to remember that effective verbal communication is two way, requiring that management welcome, and listen to, suggestions and feedback. Staff must be comfortable enough to share their awareness of problems with managers who can act on this information. Non-verbal messages, through gestures and facial expressions, are a major influence on creating a climate conducive to effective communication. Verbal communication should be in support of, not in place of, written documentation of policies and procedures. All written documentation, whether it is official policy/procedure, memo, or e-mail, must be distributed to anyone who requires the information in order to perform his or her responsibilities.

Communication is also multi-dimensional – from the top down, bottom up and across the organization. Effective communication informs all levels of the organization and must be ongoing. Communication systems can be formal or informal. Formal communication systems, from sophisticated computer technologies to staff meetings, provide input and feedback relative to an organization's activities, including the achievement of goals and objectives. Informal conversations with employees, contractors, vendors and regulators often provide some of the most critical information needed to identify risks and opportunities.

External communication can take a variety of forms, including annual reports, web sites, press releases, newsletters, and informational brochures. Other methods of communication include focus groups, presentations at conferences, and oral updates. Regardless of the methods used, maintaining open lines of communication with outside parties will enhance an agency's internal control. For example:

- Vendors, service providers, and consultants can provide significant input on the quality and design of agency products and services.
- Auditors, advocacy groups, and other outside reviewers can alert management to minor problems before they become major difficulties.
- Suppliers and contractors who are made aware of the agency's ethical standards can help deter or detect inappropriate purchasing or bidding practices.
- Complaints or inquiries can point out control problems, or the agency's ability to supply accurate information to the media or concerned citizens.

Monitoring

Monitoring is the review of an organization's activities and transactions to assess the quality of performance over time and to determine whether internal controls are effective. Management should focus monitoring efforts on achievement of the organization's mission, goals and objectives. For example, management must consider whether internal controls are operating as intended and if they are appropriately modified when conditions change. 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 an internal control plan is prepared, updated, and carried out and if all ERM components are present and functioning as designed.

In considering the extent to which the continued effectiveness of internal control is monitored, both ongoing monitoring activities and separate evaluations of the internal control structure should be considered. Ongoing monitoring occurs during normal operations and includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performance of their duties. It includes ensuring that managers and supervisors know their responsibilities for internal control and the need to make control monitoring part of their regular operating processes. Separate evaluations are a way to take a fresh look at internal control by focusing directly on the control's effectiveness at a specific time. These evaluations may take the form of self assessments as well as a review of control design and direct testing, and may include the use of checklists.

For monitoring to be most effective, all employees need to understand the organization's mission, goals, objectives, risk levels and their own responsibilities. Everyone within an organization has some responsibility for monitoring. The position a person holds in the organization helps to determine the focus and extent of these responsibilities. Therefore, the monitoring performed by managers, supervisors and staff will not have the same focus. For example:

- Executive management should focus their monitoring activities on the major divisions within the organization. With this broad focus, they emphasize the organization's mission and goals.
- Managers assess how well internal controls function in multiple units within the organization.
- Supervisors monitor all activities within their respective units to ensure staff are performing their assigned responsibilities, internal control activities are functioning properly, and the unit is accomplishing its goals and objectives.
- Staffs monitor their own work to ensure it is being done properly. They should be trained by supervisors and management regarding internal controls and be encouraged to report any irregularities.
- Access to systems and sensitive data should be reviewed quarterly to ensure employees have needed access, but not more than what is needed to complete their responsibilities.

Authorization

Authorization is the power that management grants employees to carry out certain duties. It is a control activity designed to ensure that activities are authorized and executed only by persons acting within the scope of their authority. It is management that authorizes employees to perform certain activities and/or to execute certain transactions within limited parameters. Management should ensure that the conditions and terms of authorization are clearly documented and communicated.

Periodic Comparison/Reconciliation

The purpose of periodic comparison/reconciliation is to verify that the processing or recording of transactions is valid, properly authorized and recorded on a timely basis. Integral parts of the reconciliation process include identifying and investigating discrepancies from established standards, and taking corrective action when necessary.

Continuous Supervision

Qualified and continuous supervision must be provided to ensure that internal control objectives are achieved. Supervision is the ongoing oversight, management and guidance of an activity by designated employees to help ensure that the results of the activity achieve the established objectives. The duties of the supervisor in carrying out this responsibility should include:

- Clearly communicating the duties, responsibilities and accountability assigned to each staff member.
- Systematically reviewing each employee's work to the extent necessary.
- Approving work at critical points to ensure that work flows as intended.

Recording Transactions

Agencies must manage transactions and other significant events by their prompt recording, clear documentation and proper classification.

Access to Resources

Management is required to protect the organization's equipment, information, documents, and other resources that could be wrongfully used, damaged, or stolen. The agency head is responsible for maintaining accountability for the custody and use of resources and shall assign qualified employees for that purpose. Management can protect resources by limiting access to authorized individuals. Access may be limited by various means such as locks, passwords, electronic firewalls, and encryption. Also, management must occasionally inventory the physical resources and the records to reduce the risk of unauthorized use or loss of resources and protect against wasteful and wrongful acts.

Documentation

Documentation involves preserving evidence to substantiate a decision, event, transaction, or system. All documentation should be complete, accurate, and recorded timely. It should have a clear purpose and be in a usable format that will add to the efficiency and effectiveness of the organization.

The agency's internal controls, for example, should be clearly documented and readily available for examination. This documentation provides guidance for implementing controls and, along with agency policies and procedures, sets forth the fundamental framework and the underlying methods and processes that all employees rely on to do their jobs. It provides specific direction to staff, helps form the basis for daily decisions, and can serve as a basis for training new personnel. Further, it is a necessary reference tool when management and auditors need to research the history of transactions and perform internal control risk assessment and testing.

Chapter

3

Evaluating the Internal Control Plan

Internal control is effected by people. It is not merely policy manuals and forms, but people at every level of the organization.

The management of each state agency is responsible for establishing and maintaining an effective internal control structure. To fulfill this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs for internal control policies and procedures. The objectives of an internal control structure are to assist management in meeting objectives by providing reasonable assurance that assets are safeguarded against loss from unauthorized use or disposition. The internal control structure also ensures that financial transactions are executed in accordance with management's authorization and are recorded properly to permit the preparation of financial statements in accordance with generally accepted accounting principles (GAAP).

A well-designed internal control structure will reduce improper activity. The responsibility of designing and implementing internal controls is a continuous process. As conditions change, control procedures may become outdated and inadequate. Management must anticipate that certain procedures will become obsolete and modify the internal control structure in response to these changes. The questions below can assist the agency in evaluating internal controls regularly and in being responsive to changes in the internal control environment.

Evaluation Points

Consider the following questions as you evaluate your internal control plan:

1. Does the agency have a written internal control plan? If so, when was it last updated?

2. Is the internal control plan a high-level summarization, on an agency-wide basis, of the agency's risks and of the controls used by the agency to mitigate those risks?

3. Is the internal control plan supported by low-level detail such as agency policies and procedures?

4. Was the agency head and senior management instrumental in developing the plan?

5. Does the plan include the ERM components of:
    a. Internal Environment
    b. Objective Setting

c. Event Identification

d. Risk Assessment

e. Risk Response

f. Control Activities

g. Information and Communication

h. Monitoring

The eight ERM components above are recommended but not required by State agencies.

6. Does the internal control plan include an agency-wide risk assessment? Or, does the risk assessment include only financial or fiscal areas? Are any business areas missing from the risk assessment?

7. Do risks appear to match the stated mission, goals, and/or objectives?

8. Does the risk assessment identify the most significant areas that could keep the agency from attaining its mission, goals and objectives?

9. Are the stated risks cross-referenced to internal controls?

10. Do the policies, procedures and organizational structure (control activities) actively attempt to control the risks that were identified in the risk assessment?

11. Does the internal control plan include information explaining how and when management monitors the goals, objectives and activities contained in the plan?

12. Are performance measures (a) established to measure the effectiveness and efficiency being achieved for each goal/long-term objective and (b) cross-referenced to internal controls in place to help ensure complete and accurate measurement?

13. Does the internal control plan describe the method that should be used by staff to report internal control issues such as unresolved reconciling items, policy violations, and unachieved performance measures?

14. Does the internal control plan indicate to whom in the agency the internal control plan is distributed?

15. Has the agency trained new managers and other employees in internal controls within the past year? Have managers and other employees attended the internal control training provided by the State Division of Finance?

16. Has the agency established unit(s) whose primary responsibility is internal audit, quality assurance, internal control or quality control? If yes, how many staff are assigned? What do they review? To whom do they report? Does the Internal Audit Director report to the agency head or the agency head's deputy in accordance with standards issued by the U.S. General Accounting Office (Yellow Book) and the Institute of Internal Auditors?

Chapter

4

Internal Control Plan Workbook

Internal control is a process. It is a means to an end, not an end in itself.

All operating agencies in Utah state government are required to develop and maintain agency internal controls. Also, agencies required to have an internal audit function must also prioritize and summarize their internal controls into an agency internal control plan based on a risk assessment. Responsibility for the agency internal control plan resides with the agency's Internal Control Officer (ICO). The role of the ICO is to be an official, equivalent in title or rank to an assistant or deputy to the agency head, whose responsibility is to ensure that the agency has written documentation of its internal accounting and administrative control system on file. The internal control official will, annually, or more often as conditions warrant, evaluate the effectiveness of the agency's internal control system and establish and implement changes necessary to ensure the continued integrity of the system.

The State Division of Finance defines an agency-wide risk assessment as the identification and analysis of the risks that could prevent the agency from attaining its goals and objectives. The identification and analysis form the basis for determining the risk management strategy. A precondition to risk assessment is the establishment of the organization's mission statement, long-term goals, objectives, and performance measures. A risk assessment is an integral part of an internal control plan. Internal controls must be established to ensure that each objective is periodically measured and is consistently complete and accurate.

An internal control plan as a high level agency-wide summarization of the agency's risks (as the result of a risk assessment) and the controls designed to mitigate those risks. This high level summary must be supported by lower level detail, i.e. agency policies and procedures. This summary would usually be from ten to fifty pages in length depending on the size and complexity of the agency. Large and/or complex agencies will find it useful to replicate this plan for major programs, divisions, or other subdivisions. At a minimum, each agency should prepare an agency level internal control plan.

Agencies will find it helpful to use the following workbook during their annual Internal Control Plan review or to further refine major programs, bureaus, or other agency subdivisions.

Getting Started

Little or No Previous Experience

An agency without previous experience in developing an internal control plan might use the following steps to prepare the ten to fifty page internal control plan:

1. Review the agency's mission, goals, and objectives.

   If the agency has no clear mission statement or list of goals, the agency head and other senior management need to analyze the legislation that establishes the agency and describes the reasons for the agency's existence and develop measurable long-term goals and objectives.

2. Review the agency's control environment.

   This review should include senior management's attitudes and actions.

3. Identify and analyze the potential risks to the agency.

   Identify specific risks to meeting long-term goals and objectives. Determine which objectives are most important and most vulnerable.

4. Assess risk.

   A risk assessment is an integral part of an internal control plan and is the identification and analysis of the risks that could prevent the agency from attaining its long-term goals and objectives. A precondition to risk assessment is the establishment of the agency's mission, goals, and objectives. 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.

5. Cross reference existing policies and procedures.

   Determine whether the existing policies and procedures are sufficient to control the identified risks. These policies and procedures would not normally be included in the internal control plan, but should be referenced. Appropriate controls may include both external and internal control remembering that the work of external auditors may not be considered as internal controls.

6. Summarize the risks.

   The final internal control plan should be a summary. The risks should be related to the agency's goals and objectives. The controls identified to mitigate those risks should be referenced to agency or state policies and procedures and operation manuals that serve to control the risks.

In many cases, because of good controls, the agency does not even think of these areas as "risks" because they see no likelihood of failure. Actually, the "risk" may have been identified a long time ago – and the controls that were put in place work well. Think of this in terms of the top five or ten issues that are at a level high enough that a problem in any of the areas might actually keep the agency head awake at night.

Different Approaches

Agencies can approach the identification and documentation of agency-wide risks in a variety of ways:

1. One approach is to provide each division director with a copy of the Internal Control Guide who in turn provides it to their managers. The managers at each level of the organization hold brainstorming sessions to identify risks at their level. The agency internal control officer or the chief financial officer then reviews the risks identified by each division considering the overall mission of the agency and develops the agency-wide risk assessment.
2. In some states, agencies have contracted out the function of developing the initial internal control plan, including the risk assessment, to a consulting firm.
3. Some agencies in some states have implemented this process by having all agencies start over and begin a new strategic planning process to better define its mission and goals. Then, management has assessed the risks associated with the clearly defined mission and goals.
4. In one state, the agency asked each bureau manager to prepare a report identifying long-term goals, short-term objectives, important risks, and the associated internal controls. After reviewing these reports, senior management identified six critical responsibilities that would result in serious problems for the agency if the related internal controls failed.

Broad Examples of Risks

Some broad examples of risks are as follows:

A College:

1. Failure to gain and maintain accreditation.
2. Failure to attract sufficient, qualified students.
3. Lack of security for students, personnel and campus.
4. Poor community relations.
5. Loss of eligibility for student financial aid.

A human services agency:

1. Failure to reach target population.
2. Failure to be effective in program outcomes (measured by performance measures).
3. Loss of funding.
4. Substantial failure by a subrecipient to provide services.
5. Failure to treat recipients with respect and dignity.

A transportation agency:

1. Insufficient infrastructure to carry current and expected traffic.
2. Poor design of infrastructure leading to congestion or to safety hazards.
3. Significant failure of infrastructure, such as a bridge failure.
4. Failure to attract sufficient users.
5. Failure of projects to meet environmental standards.

A revenue collecting agency:

1. Failure to provide security and privacy over private information.

2. Inadequate communication of complex laws and regulations and required forms.
3. Poor controls over accounts receivable/revenue cycle systems.
4. Incorrect interagency and interstate intercept of off-set payments.
5. Poorly defined customer refund cash disbursement systems.

A direct service providing agency:

1. Failure to implement programs in a meaningful way.
2. Ineligible recipients receiving benefits.
3. Eligible recipients receive incorrect cash disbursement.
4. Lack of adequate database systems to develop statistics and reports.
5. Failure to meet federal required accuracy standards.

A highly computer dependent agency:

1. Security breach by hackers.
2. Inability to hire an adequate number of the qualified staff required.
3. Failure to meet major milestones for large, expensive, multi-year, build and design contracts.
4. Loss of adequate, affordable and reliable electricity supply.
5. Breach of physical site security.

An agency that issues licenses (professional or motor vehicle):

1. Failure to secure issuance of licenses and registration plates.
2. Inadequate revenue collections and cash systems.
3. Failure to provide quality customer service.
4. Failure to revoke licenses when warranted.
5. Failure to determine when licenses should be revoked.

Identify Change and Inherent Risks

Risk increases during times of change. Consider risks such as changes in personnel, new or revamped systems, rapid growth, new programs, new services, reorganizations, and moving to a new location. Also consider inherent risks such as complex programs, complex activities, providing services through subrecipients, prior problems still not corrected, and decentralization.

Additional Steps

Develop and document the internal control activities that each agency uses to minimize the risks identified in the risk assessment. "Control activities" is the term used to describe the lower-level detail supporting the higher level summary that comprises the internal control plan or the structure and policies and procedures that an agency establishes so that identified risks do not prevent the agency from reaching its goals and objectives.

Test the internal controls established to minimize the risks. Testing methods might include reviewing policies and procedures, reviewing agency strategic planning documents, focus groups, employee surveys, internal control questionnaires, selecting random samples of transactions and re-performing the procedures, preparing flowcharts of systems, employee interviews, examine documentation, and re-perform reconciliations.

Questions You Must Ask

The questions below can be used as a starting point for internal control discussions and as concepts to consider while preparing or evaluating agency internal controls.

Management
Does management emphasize by both word and action the importance of integrity and ethical values?
Does management place a high degree of importance on the work of external audits and other evaluations? Is management responsive to the results of the information?
Does top management set an example by following its own controls?

Objectives
How frequently are the mission statement, goals, objectives, and performance measures reviewed?
Are each of the objectives based on federal and State laws and specific enough to clearly apply to this particular agency?
Does each objective have at least one documented effectiveness/ (outcome) performance measure and at least one efficiency performance measure?
Does each of the performance measures include a documented definition, a consistent calculation method, and internal controls to help ensure completeness and accuracy?
Are the objectives clearly communicated to all employees?
Are the resources needed to meet the objectives available? If not, does management have plans to acquire resources?
Do program objectives flow from and link to the agency-wide goals and objectives?
Are all levels of staff included in establishing and achieving objectives relevant to their specific area of authority?

Risks
What potential circumstances could result in a failure to carry out the agency's mission, goals, or objectives?
How frequently are these potential problems evaluated against changes in the mission or goals?
Do mechanisms exist to identify risks from external factors?
Are the controls appropriate to the risks? For example, are they too cumbersome or inadequate?

Policy and Procedure
Are documented policies and procedures in place for each major business and administrative area?
Are the current policies and procedures effective in reducing both the most harmful and the most likely risks?
How often are they reviewed?
How are policies and procedures, as well as any changes, communicated to staff?
How are policies and procedures tested? How often?
How often, and under what circumstances, do policies and procedures change?
How often is on-line access to agency and statewide systems reviewed by senior management?

Your Workbook (Linking internal controls to risks and performance measures)

What is your mission statement?

Mission Statement

What are the goals (long-term objectives) that support your mission statement?
Are the goals based on federal and State laws?

1. Goal #1
2. Goal #2
3. Goal #3

What are the shorter term objectives (if needed) that support each of your long range goals? Short-term objectives could also be those for divisions while the goals could be more agency-wide.

1. Goal #1
    a. Objective #1 for Goal #1
    b. Objective #2 for Goal #1
2. Goal #2
3. Goal #3

What are the risks associated with each goal (and objective)?

1. Goal #1
    a. Objective #1 for Goal #1
        1) Risk #1 for Objective #1 for Goal #1
        2) Risk #2 for Objective #1 for Goal #1
    b. Objective #2 for Goal #1
        1) Risk #1 for Objective #2 for Goal #1
        2) Risk #2 for Objective #2 for Goal #1
2. Goal #2
    a. Risk #1 for Goal #2

   b. Risk #2 for Goal #2

3. Goal #3

   a. Risk #1 for Goal #3

   b. Risk #2 for Goal #3

What are the internal controls to mitigate the risks?

1. Goal #1

   a. Objective #1 for Goal #1

      1) Risk #1 for Objective #1 for Goal #1

         a) Internal Control #1 for Risk #1 of Objective #1 for Goal #1

         b) Internal Control #2 for Risk #1 of Objective #1 for Goal #1

      2) Risk #2 for Objective #1 for Goal #1

         a) Internal Control #1 for Risk #2 of Objective #1 for Goal #1

         b) Internal Control #2 for Risk #2 of Objective #1 for Goal #1

   b. Objective #2 for Goal #1

      1) Risk #1 for Objective #2 for Goal #1

         a) Internal Control #1 for Risk #1 of Objective #2 for Goal #1

         b) Internal Control #2 for Risk #1 of Objective #2 for Goal #1

      2) Risk #2 for Objective #2 for Goal #1

         a) Internal Control #1 for Risk #2 of Objective #2 for Goal #1

         b) Internal Control #2 for Risk #2 of Objective #2 for Goal #1

2. Goal #2

   a. Risk #1 for Goal #2

      1) Internal Control #1 for Risk #1 of Goal #2

      2) Internal Control #2 for Risk #1 of Goal #2

   b. Risk #2 for Goal #2

        1) Internal Control #1 for Risk #2 of Goal #2

        2) Internal Control #2 for Risk #2 of Goal #2

3. Goal #3

    a. Risk #1 for Goal #3

        1) Internal Control #1 for Risk #1 of Goal #3

        2) Internal Control #2 for Risk #1 of Goal #3

    b. Risk #2 for Goal #3

        1) Internal Control #1 for Risk #2 of Goal #3

        2) Internal Control #2 for Risk #2 of Goal #3

What are the effectiveness and efficiency performance measures for each goal and objective to measure performance over time?

What are the internal controls for each performance measure to help ensure completeness and accuracy in measurement?

1. Goal #1

    a. Objective #1 for Goal #1

        1) Effectiveness Performance Measure for Objective #1 for Goal #1

            a) Completeness Internal Control for Effectiveness PM for Objective #1 for Goal #1

            b) Accuracy Internal Control for Effectiveness PM for Objective #1 for Goal #1

        2) Efficiency Performance Measure for Objective #1 for Goal #1

            a) Completeness Internal Control for Efficiency PM for Objective #1 for Goal #1

            b) Accuracy Internal Control for Efficiency PM for Objective #1 for Goal #1

    b. Objective #2 for Goal #1

        1) Effectiveness Performance Measure for Objective #2 for Goal #1

        a) Completeness Internal Control for Effectiveness PM for Objective #2 for Goal #1

        b) Accuracy Internal Control for Effectiveness PM for Objective #2 for Goal #1

    2) Efficiency Performance Measure for Objective #2 for Goal #1

        a) Completeness Internal Control for Efficiency PM for Objective #2 for Goal #1
        b) Accuracy Internal Control for Efficiency PM for Objective #2 for Goal #1

2. Goal #2

    a. Effectiveness Performance Measure for Goal #2

        1) Completeness Internal Control for Effectiveness PM for Goal #2

        2) Accuracy Internal Control for Effectiveness PM for Goal #2

    b. Efficiency Performance Measure for Goal #2

        1) Completeness Internal Control for Efficiency PM for Goal #2

        2) Accuracy Internal Control for Efficiency PM for Goal #2

3. Goal #3

    a. Effectiveness Performance Measure for Goal #3

        1) Completeness Internal Control for Effectiveness PM for Goal #3

        2) Accuracy Internal Control for Effectiveness PM for Goal #3

    b. Efficiency Performance Measure for Goal #3

        1) Completeness Internal Control for Efficiency PM for Goal #3

        2) Accuracy Internal Control for Efficiency PM for Goal #3

APPENDIX 1

Regulations and Guidance

The State Division of Finance establishes minimum standards for internal control systems at State agencies for administrative and financial operations. Each agency is required to designate a high-ranking official, in addition to his or her regular duties, the responsibility of maintaining the written documentation of the internal control structure and evaluate the effectiveness of the structure annually, or more often as conditions warrant, to ensure the continued integrity of the structure. This official also has the responsibility to take timely corrective action on audit results and implement the audit recommendations.

COSO

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) was created in 1987 to identify factors associated with fraudulent financial reporting and to make recommendations to reduce fraud. COSO then retained Coopers & Lybrand, a major CPA firm, to study the issues and author a report regarding an integrated framework of internal control which was issued in 1992 and re-published with minor amendments in 1994, and was entitled *Internal Control - Integrated Framework*. This report presented a common definition of internal control and provided a framework against which internal control systems can be assessed and improved.

As stated on its web site, "COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance." COSO is jointly sponsored by the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Internal Auditors, and the Institute of Management Accountants.

Internal Control – Integrated Framework

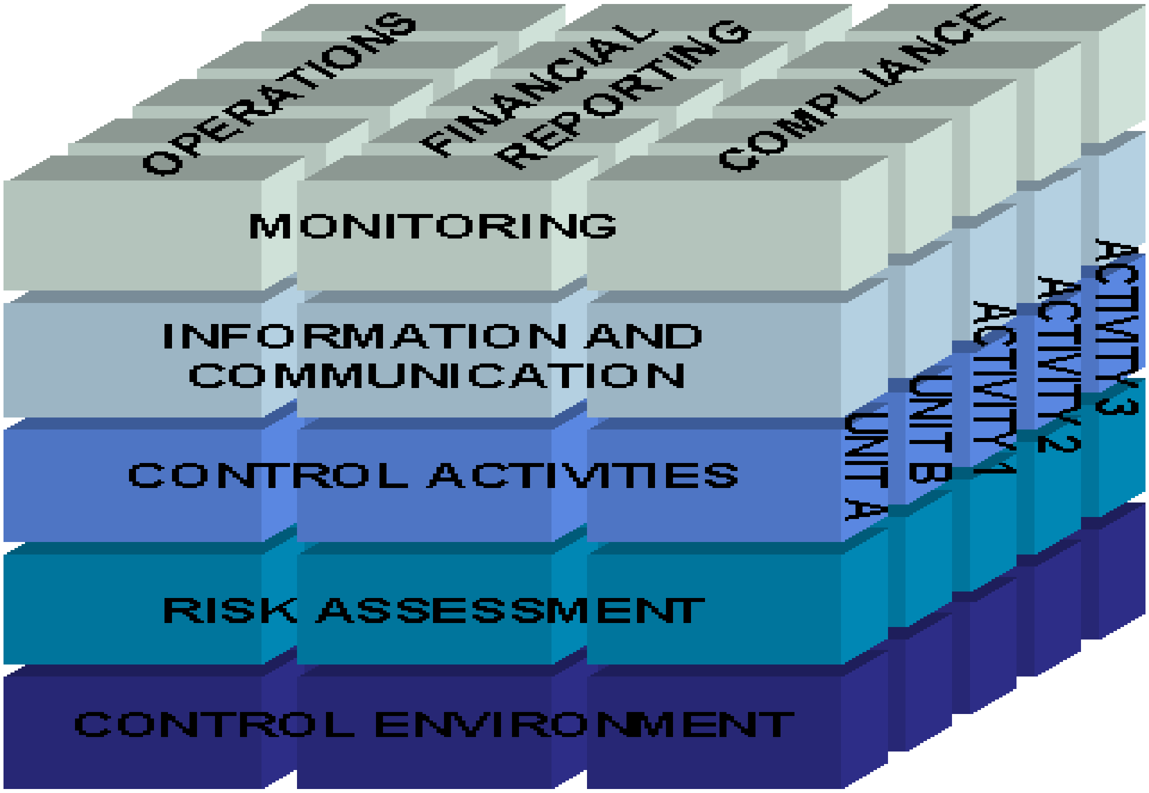
COSO defines internal control as "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations, reliability of financial reporting, compliance with applicable laws and regulations."

In other words, internal controls are tools that help managers be effective and efficient while avoiding serious problems such as overspending, operational failures, and violations of law.

Internal control has been further defined as consisting of five interrelated components:

1. The **control environment** sets the tone of the organization and influences the effectiveness of internal controls.
2. A **risk assessment** is the process used to identify, analyze, and manage the potential risks that could hinder or prevent the achievement of goals and objectives.

3. The **control activities** established to minimize the identified risks include structure, policies, and procedures.
4. **Information and communication** is the means by which risks, policies, and procedures are shared with members of the organization.
5. By **monitoring** the effectiveness of internal controls, an organization ensures that their controls reflect the current environment.



Because internal controls are a means to an end, they must help, rather than prevent or delay, an organization in reaching its objectives. Before designing and implementing internal controls, managers should consider the following four basic principles:

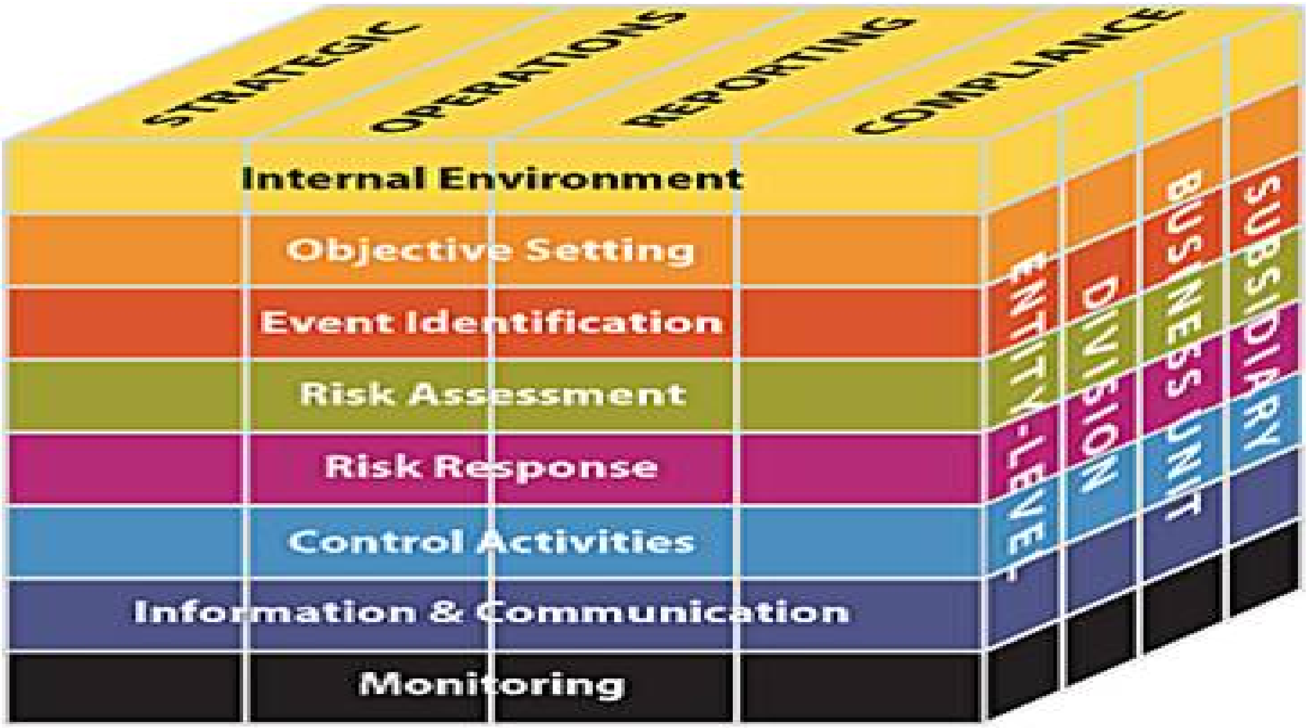
- Internal controls must benefit, rather than hinder, the organization.
- Internal controls must make sense within each organization's unique operating environment.
- Internal controls are not stand-alone practices. They are woven into the day-to-day responsibilities of managers and their staff.
- Internal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

Enterprise Risk Management – Integrated Framework

In September 2004, COSO issued its framework for enterprise-wide risk management, *Enterprise Risk Management – Integrated Framework* also known as COSO II. Enterprise Risk Management (ERM) is a broader framework that incorporates key concepts set out in COSO's earlier *Internal Control – Integrated Framework*. ERM augments the original framework because they are based on the same conceptual foundation. ERM is defined as "…a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage the risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." The ERM framework requires an entity to take a portfolio view of risk from two perspectives: business unit level and entity level. It expands and elaborates on the risk assessment and internal environment components of the Internal Control – Integrated Framework. For example, it breaks out internal environment into two components (internal environment and objective setting) and risk assessment into three components (event identification, risk assessment and risk response).

The eight interrelated components of ERM:

1. The **internal environment** is the tone of an organization which, among other things, determines an organization's "risk culture" and provides the basis for its internal controls.
2. **Objective setting** is a critical process that supports an organization's mission.
3. **Event identification** identifies internal and external events that impact an organization achieving its objectives. Events that may have a negative impact represent risks while those that may have a positive impact represent opportunities.
4. The **risk assessment** allows an organization to understand the extent to which potential events may impact objectives. Risks should be assessed from both the likelihood of happening and the impact if it happens.
5. The **risk response** evaluates options to an identified risk and determines the course of action. Options available are (a) accept the risk and monitor it, (b) avoid the risk by eliminating it, (c) reduce the risk by implementing controls, and (e) share the risk with another entity.
6. An organization's **control activities** include policies and procedures, directives, etc. They occur throughout the organization at all levels and functions.
7. **Information and communication** is the identification and dissemination of pertinent information in a form and timeframe that enables people to carry out their responsibilities. Communication occurs in all directions – flowing down, across and up the organization.
8. **Monitoring** the effectiveness of components includes ongoing activities and/or separate evaluations and making modifications as necessary.



Yellow Book

The Comptroller General of the United States issues *Government Auditing Standards* (known as the Yellow Book, January 2007 Revision), through the U.S. Government Accountability Office (GAO). These standards, also referred to as generally accepted government auditing standards (GAGAS), explain the rules that auditors must follow during audits of governmental entities, programs, activities, and functions. Audit organizations must also use *Government Auditing Standards* during reviews of governmental assistance that is administered by contractors and nonprofit organizations, when required by statute or other mandates, or when auditors hold themselves out as following government auditing standards. The Yellow Book establishes requirements for auditors' professional qualifications, the quality of audit effort, and the characteristics of professional and meaningful audit reports. It includes requirements and guidance for the following types of reviews: financial audits, attestation engagements, and performance audits.

The revised "Yellow Book" issued by David M. Walker, Comptroller General of the United States and head of the U.S. Government Accountability Office, emphasizes the critical role of the government audits in achieving credibility and accountability in government, with an increased focus on the ethical principles underlying the work of those who audit government programs and activities.

Sarbanes-Oxley (SOX)

The Sarbanes-Oxley Act of 2002, also known as the Public Company Accounting Reform and Investor Protection Act of 2002 is a federal law passed in response to several major corporate and accounting scandals (Enron, Tyco, and WorldCom). The law is comprehensive and strengthens standards for all U.S. public company boards, management, and public accounting firms. It instituted drastic changes for the accounting profession, especially in the area of auditor independence.

Auditing has become more of a regulated industry since SOX was passed. Organizations have greater financial reporting and control responsibilities and auditors are expected to hold their clients to a higher standard of accountability for financial reporting and compliance controls as well as financial reporting transparency. SOX requires management to establish and maintain adequate internal controls and procedures for financial reporting. It also emphasizes that management is responsible for internal controls.

The Director of the U.S. Government Accountability Office (GAO) states that "where appropriate, auditor opinions on internal control are critical for monitoring an organization's internal control and accountability." While most provisions of SOX apply only to public companies and their auditors, many oversight agencies have pushed to use SOX to increase the accountability of public sector groups, mostly non-profit organizations. Recently, there has been an effort to use the reforms included in SOX to increase the accountability and mitigate the risks of state and local governments.

OMB Circular A-123

In December 2004, the Office of Management and Budget (OMB) reissued Circular number A-123 to define the management responsibilities for internal financial controls in federal agencies. This Circular provides guidance to federal managers on improving the accountability and effectiveness of federal programs and operations by establishing, assessing, correcting, and reporting on management controls. Circular A-123 is a re-examination of the existing internal control requirements for federal agencies and was initiated in light of the new internal control requirements for publicly-traded companies contained in the Sarbanes-Oxley Act of 2002. Under A-123, agencies and individual federal managers are required to take systematic and proactive measures to:

1. Develop and implement appropriate, cost-effective management controls for results-oriented management,
2. Assess the adequacy of management controls in federal programs and operations,
3. Identify needed improvements,
4. Take corresponding corrective action, and
5. Report annually on management controls.

OMB Circular A-133

In June 1996, the Office of Management and Budget (OMB) issued a revised Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations, to provide administrative guidance for implementing the single audit requirements. A single audit is an organization-wide audit that includes both the agency's financial statements as well as its federal awards. Effective January 2004, A-133 audit guidelines require entities that expend $500,000 or more a year in federal awards to have a single or program-specific audit conducted. Under A-133, those governments or organizations that expend $500,000 or more in federal awards during the fiscal year must do the following:

1. Maintain internal control for federal programs,
2. Comply with the laws, regulations, and the provisions of contracts or grant agreements,
3. Prepare appropriate financial statements, including the schedule of expenditures of federal awards,
4. Ensure that the required single audits are properly performed and submitted when due, and
5. Follow up and take corrective actions on audit findings.

SAS No. 112

In May 2006, the AICPA issued Statement on Auditing Standards (SAS) No. 112, Communicating Internal Control Related Matters Identified in an Audit. It is effective for audits of financial statements for periods ending on or after December 15, 2006. SAS No. 112 has two unconditional requirements: (1) the auditor must evaluate identified control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses; and (2) the auditor must communicate, in writing, significant deficiencies and material weaknesses to management and those charged with governance. It is likely that more audit findings will be reportable because SAS No. 112 clarifies the significance of a control deficiency is dependent on the potential for misstatement, not whether the misstatement actually occurred.

Audit Committees

Within the public sector, an audit committee is an extension of the governing body. Committees are formed to fulfill the governing body's responsibilities, not expand them. Officials are able to increase their oversight of specific issues by assigning various matters to committees.

In this light, the audit committee is an integral element of public accountability and governance. It plays a key role for the governing body in carrying out its legal and fiduciary responsibilities, especially with respect to the integrity of the government's financial information, system of internal control, and legal and ethical conduct of management and employees.

The roles of the audit committee may vary from agency to agency depending on the complexity and size, as well as the requirement of the governing body. However, the one common responsibility for all audit committees, among all their potential roles, is risk management oversight.

Every organization faces a variety of potential risks, such as:

- Loss of key staff
- Loss of funding or reduction of revenue sources
- Regulatory non-compliance
- Conflicts of interest
- Fraudulent activities resulting from weaknesses in internal controls

> An audit committee has three fundamental goals. First, it must satisfy itself that management is maintaining a comprehensive framework of internal control. Second, the audit committee must ensure that management's financial reporting practices are assessed objectively. Third, the committee needs to determine to its own satisfaction that the financial statements are properly audited and that any problems disclosed in the course of the audit are satisfactorily resolved.
>
> \- *Audit Committees* by Stephen J. Gauther

From the definitions found in the Internal Audit Act, we learn the following regarding audit committees in the executive branch:

- For state agencies, the Governor is the "appointing authority." (see 63i-102(3)(a))

- For state agencies, if the agency even has an audit committee, the audit committee members are to be appointed by the Governor. (see 63i-5-102(4))

- The Governor's appointments either come from the agency's governing board or commission [for example, the State Tax Commission if governed by a commission, however, most state agencies like Health have no governing board or commission] or from individuals who have no administrative responsibilities in the agency. (see 63i-5-102(4))

- Some agencies have no governing board or commission who can remove the executive director. For such agencies, the audit committee members, if there is an audit committee at all, should be appointed by the Governor from individuals outside department management.

Internal Audit

As defined by the Institute of Internal Auditors, "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes."

Management is responsible for establishing and maintaining an adequate system of internal controls. An internal audit office is charged by management with "… assessing the effectiveness of the design and execution of the system of internal controls and risk management processes."

Internal auditors continuously evaluate risk exposures in relation to:

- Effectiveness and efficiency of operations.
- Reliability and integrity of financial and operational information.
- Safeguarding of assets.
- Compliance with laws, regulations, policies and procedures, and contracts.
- Accomplishment of established operational goals and objectives.

Internal auditors are responsible for making recommendations for improvement in internal controls to top management and, if applicable, a governing board of directors. To maintain independence, and to perform in an objective capacity, internal auditors should not engage in any operational or programmatic responsibilities. Also, the Internal Audit Director should report to the agency head or the agency head's deputy in accordance with standards issued by the U.S. General Accounting Office (Yellow Book) and the Institute of Internal Auditors.

Work performed by internal auditors may be relied upon by management as internal controls; however, the work performed by external auditors may not be relied upon as internal controls.

APPENDIX 2

Glossary

Accounting Controls - Methods and procedures which an organization's management institutes to (1) safeguard assets, (2) authorize transactions, (3) monitor financial activities, and (4) ensure the accuracy and validity of accounting records.

Administrative Controls - Methods through which management supports the accomplishment of its objectives (e.g., planning, organizing, monitoring productivity, improving operations, and ensuring quality control). These controls are necessary to ensure that:

- All resources, including personnel, are properly obtained, maintained, and used;
- Decisions regarding the expenditure of funds are made based on reliable information; and,
- Budgets are properly developed and monitored to ensure consistency between planned and actual expenditures.

Agency - An organization or entity of any size, established for a particular purpose. A State governmental agency may be, for example, an agency, a department, a division, or a bureau or work unit. In higher education, an agency may be a college, a department, or an administrative unit.

Application Controls - Programmed procedures in application software and related manual procedures, designed to help ensure completeness and accuracy of information processing. Examples include computerized edit checks of input data, numerical sequence checks, and manual procedures to follow up on items listed in exception reports. These controls vary based upon the business purpose and specific application to which they apply. Application controls may also help ensure the privacy and security of data transmitted between applications.

Audit Committee - A group formed by the governing body to oversee audit operations and circumstances. The Committee selects and appraises the performance of the external auditors. The Committee may be composed of outside directors. Besides evaluating external audit reports, the Committee may evaluate internal audit reports as well. Management representations are also reviewed. The Committee may also get involved with public disclosure of the government’s activities. The Audit Committee may also, under some circumstances, intervene in the resolution of deficiencies uncovered during an audit.

Cash - A current asset account which includes currency, coins, checking accounts, and undeposited checks received from customers.

Change Fund - An amount of cash held by a department or office and used to give change to customers when they are paying for goods or services.

Compliance - Conforming with laws, rules, and regulations applicable to an agency.

Computer Controls - Controls performed by computer; i.e., controls programmed into computer software (contrast with Manual Controls). Controls over computer processing of information, consisting of general controls and application controls (both programmed and manual).

Control – A policy or procedure, inherent in an agency's organizational structure, hierarchy of authority, or system of work flows, designed to help an agency accomplish its objectives. The effects of such policies and procedures. The act of implementing such policies and procedures.

Control Account – A control account is a summary account in the general ledger. The details that support the balance in the summary account are contained in a subsidiary ledger—a ledger outside of the general ledger. The purpose of the control account is to keep the general ledger free of details, yet have the correct balance for the financial statements.

Control Activities – An element of the COSO internal control framework. Actions, supported by policies and procedures, established and implemented to reduce risk and provide reasonable assurance that specific agency objectives are met. Control activities occur throughout an agency at all levels, and in all functions. They include (1) authorization, (2) review and approval, (3) verification, (4) reconciliation, (5) physical security over assets, (6) segregation of duties, (7) education, training, and coaching, and (8) performance planning and evaluation.

Control Categories – Controls can be categorized as to purpose and when they occur in the transaction cycle.

- *Preventive control*, deters the occurrence of undesired events.
- *Detective control*, reveals the occurrence of undesired events
- *Corrective control*, remedies the effects of undesired events.

Control Environment – An element of the COSO internal control framework. The agency's "corporate culture," showing how much the agency's leaders value ethical behavior and internal control. It is the control consciousness of an organization and the atmosphere in which people in that organization conduct their activities and fulfill their responsibilities. Factors include:

- Values stated and promoted for integrity and ethical behavior
- Management philosophy and operating style
- Direct and active involvement of the agency management team
- Commitment to competence
- Organization structure
- Assignment of authority and responsibility
- Human Resource policies and practices
- Internal control philosophy
- Risk Management philosophy
- Oversight by control agencies

- Oversight by the agency's governing board or commission (where applicable)

Control Framework - A control framework is a set of fundamental controls that must be in place to mitigate organizational risk and reduce the likelihood of loss. The most familiar and used of the control frameworks are those promulgated by COSO and ISACA. COSO's original and now nearly universal internal control frame consisted of five *Components*, q.v., while its newer, expanded version contains eight.

Control Objectives - Goals or targets to be achieved for each internal control. Objectives should be tailored to fit the specific operations in each agency. The objectives of internal control include the determinations that:

- Transactions are:
  - Valid
  - Accurate
  - Complete
  - Properly authorized
  - Properly valued
  - Properly classified
  - Properly dated and attributed to the correct period
  - Properly posted
  - Properly summarized
  - Recorded at the proper time
- Physical safeguards are adequate
- Proper security is in place
- Error handling is timely and appropriate
- Segregation of duties is maintained
- Programs are managed in accordance with sound business practices

Corrective Control - Controls designed correct previously detected errors or irregularities. The identification of such errors or irregularities and the understanding of how they occurred can at time be used by management in the design of preventive and detective controls.

COSO - The Committee of Sponsoring Organizations of the Treadway Commission, created in 1985. COSO developed the internal control framework that, in one form or another, virtually all organizations currently use.

COSO Component – An element of either the original COSO or updated COSO-ERM internal control frameworks. Also referred to as an internal control component. The original COSO model contains five components: (1) Control Environment; (2) Risk Assessment; (3) Control Activities; (4) Information & Communication; and, (5) Monitoring. The updated COSO-ERM is expanded to include eight components: (1) Internal Environment; (2) Objective Setting; (3) Event Identification; (4) Risk Assessment; (5) Risk Response; (6) Control Activities; (7) Information and Communication; and, (8) Monitoring. Both frameworks are commonly used to identify, evaluate and categorize control weaknesses in organizations.

COSO-ERM – COSO-Environment Risk Management. An updated and expanded version of the original COSO Internal Control Framework. Refer to *COSO Component* for more a more details.

COSO Internal Control Framework – A set of guidelines, developed by COSO, to be used by organizations in establishing and maintaining internal controls. See *COSO Component*

Criteria – In general sense, the standards against which a management control system can be measured in determining effectiveness. The internal control components, taken in the context of inherent limitations of internal control, represent criteria for internal control effectiveness for each of the three control categories. When used in the context of auditing, criteria, one of the elements of an auditor's finding, are what the operation was supposed to accomplish or the conditions that should have existed.

Debarment – The action taken by a government agency to restrict or prohibit future business with an organization or individual.

Deficiency - A perceived, potential, or real internal control shortcoming; or an opportunity to strengthen the management control system, to provide a greater likelihood the agency's objectives are achieved.

Design – (1) Intent. As used in the definition of internal control, management control systems are designed to provide reasonable assurance as to achievement of objectives--when the intent is realized, the system can be deemed effective. (2) Plan. The way a system is supposed to work, contrasted with how it actually works.

Detective Control - A control designed to discover an unintended event or result. Detective controls, as distinct from preventive controls, provide evidence that an error or irregularity has occurred but do not prevent the error or irregularity from occurring.

EDP – Electronic Data Processing. The software and hardware comprising an IT system or the procedures and practices relating to the IT system.

Effective Control - The state or condition of internal control within an agency's management control system in which management (as well as any other governing body) has reasonable assurance of the following:

- Management understands the extent to which the agency's operational objectives are being achieved.
- Organizational resources are being used responsibly.
- Compliance with applicable laws and regulations is enforced.

Effective Management Control System - A synonym for *Effective Control.*

Enterprise Risk Management (ERM) - A process, effected by an agency's directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the agency, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of agency objectives.

Entity - An organization or agency of any size, established for a particular purpose. A governmental entity may be, for example, a state, an agency, a division, a department, or a work unit. In higher education, an entity may be a college, a department, or an administrative unit.

Entity-level Evaluation - An evaluation of an entity, based at least in part on conclusions drawn from *activity-level evaluations*.

Ethical Values - Moral criteria enabling a decision maker to determine an appropriate course of behavior. These values should be based on what is "right," and may go beyond what is "legal."

Event Cycle - Processes used to initiate and perform related activities to create the necessary documentation and to gather and report related data (e.g., accounts payable cycle).

Event Identification – A COSO Component. Internal and external events affecting achievement of an agency's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.

Financial Reporting - Used with "objectives" or "controls"—having to do with reliability of published financial statements.

Fraud – An intentional deception that drains value from the organization. All organizations are subject to fraud risks. Large frauds have led to the downfall of entire organizations, massive investment losses, significant legal costs, incarceration of key individuals, and erosion of confidence in capital markets.

GAAP - "Generally Accepted Accounting Principles" promulgated by the Governmental Accounting Standards Board (GASB) and other standards-setting entities.

General Controls (Information Technology) - Policies and procedures to help ensure the continued, proper operation of computer information systems. General controls include controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance. General controls support the functioning of programmed application controls. Other terms sometimes used to describe general controls are general computer controls and information technology controls.

General Controls (Organization) – Practices that broadly support the general control environment of an agency. These include such commonly prescribed safeguards as:

- Segregation of duties.
- Use of pre-numbered checks, invoices, vouchers, etc.
- Appropriately securing cash and check stocks.
- Limiting the number of authorized signers of checks, purchase orders, etc.
- Limiting access to cash, checks, sensitive or confidential information.
- Requiring payment from invoices rather than statements.

- Timely third-party review of transactions.
- Timely reconciliation of accounts.
- Requiring multiple signatures on checks, purchase orders, etc.

General Control Environment - Various factors that can influence the effectiveness of internal controls over program and administrative functions such as an excessive use of a petty cash fund due to heavy travel requirements, which may result in bypassing internal controls. This includes the integrity, ethical values, and competence of an agency's employees, management's philosophy and operating style, organization structure, delegation of authority and responsibility, and written policies and procedures.

Governance – To control, direct, or strongly influence actions or conduct. To exercise power and authority in controlling.

Imprest – A fund, account or cache of money of a fixed amount. Expenditures from an imprest fund will be periodically replenished to maintain the fund's fixed balance.

Imprest Funds – See *Petty Cash*

Information and Communication – An element of the COSO internal control framework. Communicating relevant information in a timeframe to enable people to carry out their responsibilities is an important component of internal control. Effective communication flows in all directions of an agency. An effective information and communication process ensures that all personnel receive a clear message from the head of the agency that internal control must be taken seriously. Information and communication includes an organization's policies and procedures as well as its records of actual events.

Information Technology – A term that encompasses computer systems, their hardware and software components, and the processes that support them. IT concerns itself with automating processes, compiling and distributing information, connecting users, and developing productivity tools.

Inherent Limitations - Limitations applicable to all internal controls within a management control system. The limitations of human judgment; resource constraints and the need to consider the cost of controls in relation to expected benefits; the reality that breakdowns can occur; and the possibilities of management override and of collusion.

Inherent Risk - Degree to which things or activities are exposed to the potential for financial loss, inappropriate disclosure or other erroneous conditions or the risk that one or more factors will prevent an objective from being accomplished, if the agency does not implement risk mitigation measures. For example, activities conducted within severe time constraints have greater inherent risk than those that are not subject to time constraints and cash is more susceptible to misappropriation than large, tangible assets.

Integrity – When applied to persons, the quality or state of being of sound moral principle; uprightness, honesty, and sincerity; the desire to do the "right" thing; and to profess and live up to a set of values and expectations. When applied to things, such as systems, the quality of being complete, sound or unimpaired.

Internal Control – The policies, guidance, instructions, regulations, procedures and other methods designed to provide reasonable assurance regarding achievement of objectives and to mitigate risks in the following categories:

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

Internal Control Policies and Procedures – The entity's policies and procedures provide the detail for the internal control plan. It is important that they be reviewed in conjunction with the plan. It is not uncommon for the detailed policies and procedures to be modified due to changes in personnel, audit or quality assurance recommendations, etc. As these modifications occur, the entity's documentation should be updated to reflect them.

Internal Control Components – See *COSO Component.*

Internal Control Concepts - Fundamental concepts of internal control are:

- Internal control is a process – a means to an end, not an end to itself.
- Internal control is affected by people. It is not merely policy manuals and forms, but people at every level of the organization.
- Internal controls are expected to provide only reasonable assurance, not absolute assurance, to an agency's management.
- Internal control focuses on the achievement of objectives in one or more separate but overlapping categories.

Internal Control Review - Examination of an agency or operating system to determine whether adequate internal control procedures exist and are effectively implemented to prevent or detect the occurrence of potential risks in a cost-effective manner.

Internal Control System - A synonym for *Internal Control.* Comprises the internal control plan and all methods and procedures adopted by an agency to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies. Internal control systems include both internal accounting and administrative controls. These two elements of internal control often overlap; however, it is not the intent of this policy to specifically address internal administrative controls.

- Internal accounting controls encompass the internal control plan and all procedures and records that are designed to provide reasonable assurance that:
    - Obligations and costs are in compliance with applicable laws, regulations and policies;
    - Funds, property and other assets are safeguarded against waste, loss, unauthorized use or misappropriation; and
    - All asset, liability, equity, revenue, expenditure/expense and budgetary transactions are

properly authorized, recorded, and accounted for to permit the preparation of accurate accounts and reliable financial and statistical reports and to maintain accountability over assets.

- Administrative controls encompass all operational controls within an agency. Their purpose is to insure that agency objectives are met economically, efficiently and effectively, to assure adherence to applicable laws, regulations and policies; and that reliable information is maintained for evaluating managerial and organizational performance to promote operational efficiency.

Internal Control Plan (ICP) – An internal control plan is a description of how an entity expects to meet its various goals and objectives by using policies and procedures to minimize risk. The plan should be reviewed and updated as conditions warrant, but at least annually. An effective ICP is a high level, entity-wide summarization of risks and controls for all of its business processes and is supported by lower level detail.

Internal Environment – A COSO Component. Encompasses the tone of an agency (often referred to as the "tone at the top"), and sets the basis for how risk is viewed and addressed by an agency's staff, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

ISACA – Information Systems Audit and Control Association. An organization that focuses on IT governance and control. Its internal control framework is known as COBIT.

IT – See *Information Technology*.

Management – The collective body of those who manage or direct an enterprise.

Management Control System - A set of policies, procedures, and management philosophies, designed to assist management in achieving the strategic objectives of its particular agency. When a management control system satisfies specific criteria in achieving strategic objectives, it can be deemed effective.

Management Controls - Controls performed by one or more managers at any level in an agency.

Management Intervention – See *Management Override*.

Management Override - Management's overruling of prescribed policies, procedures or controls. Management override may occur for legitimate or illegitimate purposes. When undertaken for legitimate purposes, it is sometimes referred to as management intervention. Legitimate purposes include dealing with non-recurring or non-standard transactions that might otherwise be incorrectly handled. Illegitimate purposes include both those actions that attempt to achieve illicit personal gain at the expense of the organization and those that misrepresent an agency's financial condition or compliance.

Management Oversight - More than any other individual, the agency head sets the "tone at the top" that affects integrity and ethics and other factors of a positive control environment. In a large agency, the agency head fulfills this duty by providing leadership and direction to senior managers and reviewing the way they are controlling the business. Senior managers, in turn, assign responsibility for establishment of more specific internal control policies and procedures to personnel responsible for the unit's functions. In a smaller agency, the influence of the agency head, often acting as a manager, is usually more direct. In any event, in a cascade of responsibility, a manager is effectively the head of his or her sphere of responsibility. Of particular significance are financial officers and their staffs, whose control activities flow in all directions of the operating and other units of an agency.

Management Process - The series of actions taken by management to run an agency. A management control system is a part of and integrated with the management process.

Manual Controls - Controls performed manually, rather than by computer (contrast with *Computer Controls).*

Master File - A file containing relatively permanent information about the agency or activity to which it pertains. Data elements such as names, addresses, phone numbers, tax rates and the like are generally contained in a master file. Data relating to individual transactions, such as invoice numbers, check amounts, etc., by contrast, are not contained in a master file.

Merchant Fees - Fees associated with a purchase by credit card.

Monitoring – An element of the COSO internal control framework. Monitoring is the assessment of internal control performance over time; it is accomplished by both ongoing monitoring activities and periodic evaluations (i.e., self-assessments, peer reviews, internal audits, etc.)

Objective – Something an organization is legitimately trying to accomplish or attain.

Objective Category - One of four groupings of objectives an agency strives to achieve. The categories are: Strategic – high-level goals aligned with and supporting its mission; Operations - effective and efficient use of resources; Reporting - reliability of reporting; and Compliance – compliance with applicable laws and regulations. The categories overlap, so any one particular objective might fall into more than one category.

Objective Setting – A COSO Component. Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the agency's mission and are consistent with its risk appetite.

OMB Circulars - Instructions or information issued by the Office of Management and Budget (OMB) to federal agencies. They are expected to have a continuing effect of two years or more. A complete list of current OMB Circulars can be found on the White House website at
http://www.whitehouse.gov/omb/circulars/.

Operations - Used with *objectives* or *controls*—having to do with the effectiveness and efficiency of an agency's programs or activities.

PCI - The payment card industry (PCI) denotes the debit, credit, prepaid, e-purse, ATM, and point-of-sale (POS) cards and associated businesses. The term is sometimes more specifically used to refer to the Payment Card Industry Security Standards Council, an independent council originally formed by

American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International on Sept. 7, 2006, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard.

Petty Cash - A current asset account that represents an amount of cash for making small disbursements such as postage due and reimbursements for small amounts of supplies. See *Imprest Funds.*

Policy - Management's directive as to what should be done to effect control. A policy serves as the basis for procedures for its implementation.

Pooled Cash - Consists of funds deposited by the individual agencies with the pooled cash accounts of the State Treasurer. Because it is immediately available to the funds, it is considered a form of cash equivalent.

Preventive Control - A control designed to avoid an unintended event or result (contrast with *Detective Control*). Preventive controls proactively attempt to prevent loss. Preventive controls include control activities such as segregation of duties and proper authorization of transactions.

Procedure - An action to implement a policy.

Process - A series of logically related tasks, involving people, machines, and methods; used to change materials, resources, or data (input) into a specified product or service (output).

Program Controls - Controls surrounding the planning and accomplishing of the agency's programmatic goals and objectives. These represent a further level of detail of administrative controls. Examples of program controls are:

- Routine evaluations of the agency's goals, objectives and activities and the extent to which overall objectives are met, and
- Evaluation of how the agency operates to meet their objectives.

Program Objectives - Specific goals, intended changes and desired outcomes of an agency's program activities that can be evaluated and measured.

Public Work - A public work is a construction or engineering project carried out by the government on behalf of the public. Public works include both infrastructure assets (such as airports, canals, dams, dikes, pipelines, railroads, roads, tunnels, and artificial harbors) and non-infrastructure assets (such as mines, schools, hospitals, water purification and sewage treatment centers).

Public Use – In a broad and non-legalistic context, the fairly unrestricted access to a facility by the populace. In a narrow, legalistic context, the right of the public to access or benefit from property condemned by the government through the exercise of eminent domain.

Published Financial Statements - Financial statements, interim and condensed financial statements, and selected data derived from such statements (such as monthly budgetary status reports), reported publicly.

Reasonable Assurance - The concept that internal control, no matter how well designed and operated, cannot guarantee an agency's objectives will be met--because *inherent limitations* exist in all management control systems. Reasonable assurance represents a judgment, based upon an evaluation of available information, that an organization's systems of internal control are operating effectively.

Recipient (Prime Recipient) – Prime recipients, also known as "recipients," are non-federal entities that receive the proceeds of federal awards directly from the Federal Government.

Reconciliation - An accounting process used to compare two sets of records to ensure the figures are in agreement and are accurate. Reconciliation is the key process used to determine whether the money leaving an account matches the amount spent, ensuring that the two values are balanced at the end of the recording period.

Reliability of Reporting - Used in the context of published financial statements, reliability is defined as the preparation of financial statements fairly presented in conformity with generally accepted (or other relevant and appropriate) accounting principles and regulatory requirements for external purpose, within the context of materiality. Supporting fair presentation are the five basic financial statement assertions, as follows:

- Existence or occurrence.
- Completeness.
- Rights and obligations.
- Valuation or allocation.
- Presentation and disclosure.

When applied to interim or condensed financial statements or to select data derived from such statements, both the *factors representing fair presentation* and the *assertions* apply only to the extent they are relevant to the presentation.

Reportable Conditions - An internal control deficiency related to financial reporting—a significant deficiency in the design or operation of the management control system. The deficiency could adversely affect the agency's ability to record, process, summarize, and report financial data consistent with the management's *assertions* in the financial statements.

Residual Risk - The risk that remains after management responds to inherent risk. Once risk responses have been developed, management then considers residual risk.

Response to Risk – See *Risk Response.*

A complete response to a given risk may include more than one alternative.

Risk – Anything that could jeopardize the achievement of an objective.

Risk Assessment – An element of the COSO internal control framework. Risk assessment is the identification and analysis of risks associated with the achievement of operations, financial reporting, and compliance goals and objectives. Risk assessment involves analyzing potential events and determining their likelihood of occurrence and their impact on achieving agency objectives. Risk assessment forms a basis for determining an agency's responses to risk.

A risk assessment is a process to identify and analyze factors that may affect the achievement of a goal. In general, risk factors may include the control environment, size of the entity, complexity, change, and results of previous reviews/audits. It is important to remember that not all risks are equal. Some risks are more likely to occur while others will have a greater impact. For example, risks to safety or security of individuals, data or personal information could have significant consequences.

Risk Identification - A risk is a factor that could prevent an individual, group, or agency from accomplishing an objective as intended or planned. Risk identification encompasses the activities to recognize, discover and categorize the risks pertinent to an organization. It is an element of an organization's risk assessment.

Risk Response – A COSO Component. The set of alternatives used to manage, reduce or tolerate a risk and its potential impact:

- Avoid risk – exit the activities that cause the risk.
- Reduce risk – mitigate the likelihood or negative impact of risk.
- Share risk – assign a portion of risk's impact to another, e.g., through insurance.
- Accept risk – take no action to affect the impact or likelihood of risk.

Segregation of Duties – The concept and practice of having more than one person required to complete a task.

Sight Drafts - A draft or bill that is payable on demand or upon presentation. Also called demand draft. Money is payable at sight, or when the completed documents are presented, or within a specified period called days of grace.

Strategic – Used with objectives; having to do with high-level goals that are aligned with and support the agency's mission (or vision).

Sub-recipient – Sub-recipients are non-federal entities that are awarded funding through a legal instrument from a Prime Recipient.

Subsidiary ledgers – A group of similar accounts, such as accounts receivable or accounts payable, whose combined balance equals the total for that group of accounts in the general ledger. Subsidiary ledgers contain the details that support the *Control Account* in the general ledger.

Warrants - Warrants are, in effect, checks issued by government entities. Warrants are issued for payroll to individuals and for accounts payable to vendors. Legally, a warrant is a promise to pay when there are sufficient funds in the government's treasury to do so, while a check is a demand draft.

Work Process - A synonym for *Process.*