Internal Control Standards

A Guide for Managers

VERMONT

Department of Finance and Management

TABLE OF CONTENTS

Part I: Introduction

The four basic functions of management are usually described as planning, organizing, leading, and controlling. Internal control is what is meant when discussing the fourth function, controlling. Adequate internal controls allow managers to delegate responsibilities to staff and contractors with reasonable assurance that what they expect to happen, actually does. Internal control is an integral part of managing an organization. It comprises the plans, methods, and procedures used to meet missions, goals, and objectives and, in doing so, supports performance-based management systems. Internal control also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. In short, internal control, which is synonymous with management control, helps government managers achieve desired results through effective stewardship of public resources.

Purpose of Guide

Everyone experiences internal control in their daily business activities as well as in their personal lives. Yet it is a subject that is very often misunderstood, ignored or undervalued. Internal control helps bring order, direction and consistency to our lives and organizations. This publication is intended to explain how internal control plays an important part in the daily activities of every department[1] in Vermont state government.

Although an internal control system can vary widely among organizations, the standards for a good system are generally the same. The standards presented in this publication are applicable to all state government departments. These standards are not new ideas; many of the concepts are currently part of existing operations. We have prepared this publication to assist all state employees in managerial roles in fulfilling their responsibilities relating to internal controls. We do not suggest, however, that this publication is all-inclusive. Managers should view this guide as a framework for developing and evaluating their internal control systems, consistent with their department's operations and mission.

What Are Internal Controls?

Definition

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

[1] "Department" means any discrete agency, department, office, board or other administrative unit.

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

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

A less technical definition might state that:

Internal control is the integration of the activities, plans, attitudes, policies, and efforts of the people of a department working together to provide reasonable assurance that the department will achieve its mission.

Fundamental Concepts

These definitions denote certain fundamental concepts, that internal controls:

- affect every aspect of a department: all of its people, processes and infrastructure.
- are not stand-alone practices. They are woven into the day-to-day responsibilities of managers and their staff.
- incorporate the qualities of good management.
- are dependent upon people and will succeed or fail depending on the attention people give to it.
- must make sense within each department's unique operating environment and are effective when people work together.
- provide a level of assurance to a department, but does not guarantee success.
- help a department achieve its mission.
- should be cost effective.

Why Do We Need Internal Controls?

Encourage Sound Management Practices

Departments exist to achieve a mission and accomplish certain goals and objectives. The overall purpose of internal control is to help each department achieve its mission. An effective internal control system helps a department to:

- Promote orderly, economical, efficient and effective operations.
- Produce quality products and services consistent with the department's mission.
- Safeguard resources against loss due to waste, abuse, mismanagement, errors and fraud.
- Promote adherence to statutes, regulations, bulletins and procedures.
- Develop and maintain reliable financial and management data, and accurately report that data in a timely manner.

Accountability

Public sector managers are responsible for managing the resources entrusted to them to carry out government programs. A major factor in fulfilling this responsibility is ensuring that adequate controls exist. Public officials, legislators, and taxpayers are entitled to know whether government agencies are properly administering 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 intended. Officials and employees who manage programs must be accountable to the public. Frequently specified by statute, this concept of accountability is intrinsic to the governing process of our state.

Facilitate Preparation for Audits

Vermont state government is subject to annual audits by independent auditors (e.g. the single audit, federal auditors, the Office of the State Auditor) and, in some cases, internal audit units. These audits are conducted to ensure the following:

- Public funds are administered and expended in compliance with applicable statutes and regulations.
- Programs are achieving the purpose for which they were authorized and intended.

- Financial statements accurately represent the operating results and financial position of the State.
- Programs are managed economically; and
- Internal controls exist and provide a basis for planning the audit and planning the timing, nature, and extent of testing.

Auditors' reports will nearly always include an evaluation of the adequacy of the department's internal controls. When it appears warranted, auditors will make recommendations for improvements. Management is accountable for the adequacy of the internal control systems in their department. Weak or insufficient internal controls will result in audit findings and, more importantly, could lead to theft, shortages, operational inefficiency, or a breakdown in the internal control structure. Strong, effective, well-documented internal controls that have been made a part of the entity's operations allow audits to be performed more cost effectively.

Organizational Roles

An organization is a group of individuals working together to achieve a common purpose. Each person employed by an agency, department, office, board, or commission works for an organization that is a part of a larger organization, the State of Vermont. Every member of our state organization has a role in the system of internal control. Most importantly, internal control is people-dependent. It is developed by people; it guides people; it provides people with a means of accountability; and people carry it out. Individual roles in the system of internal control vary greatly throughout an organization. Very often, an individual's position in the organization determines the extent of that person's involvement in internal control.

The strength of the system of internal control is dependent on people's attitude toward internal control and their attention to it. Executive management needs to set the organization's direction regarding internal control (i.e.: "tone at the top"). If executive management does not establish strong, clearly stated support for internal control, the organization as a whole will most likely not practice good internal control. Similarly, if control activities are not integrated with staff duties and responsibilities, the system of internal control will not be effective.

While everyone in an organization has responsibility for ensuring the system of internal control is effective, the greatest amount of responsibility rests with the managers of the organization. Internal controls are the structure, policies, and procedures used to ensure that management accomplishes its objectives and meets its responsibilities.

Limitations of Internal Control

Internal controls, no matter how well designed and operated, provide only reasonable assurance to management regarding the achievement of a department's objectives.

Certain limitations are inherent in all internal control systems. Despite these limitations, the reasonable assurance that internal control does provide enables a department to focus on reaching its objectives while minimizing undesirable events.

Costs versus Benefits

Prohibitive cost can prevent management from installing the ideal internal control system. Management will occasionally accept certain risks because the cost of preventing such risks cannot be justified. Furthermore, **more** control activities are not necessarily **better** in an effective internal control system. Not only can the cost of excessive or redundant controls exceed the benefits, but this may also affect staff's perceptions on controls. If they consider internal controls as obstructions to work processes or "red tape", this negative view could adversely affect their overall regard for internal controls.

Judgment

The effectiveness of an internal control system is limited by the realities of human frailty in making decisions. Decisions must often be made under the pressures of time constraints, based on limited information at hand, and relying on human judgment. Additionally, management may fail to anticipate certain risks, and thus fail to design and implement appropriate controls.

Breakdowns

Well-designed internal control systems can break down. Personnel may misunderstand instructions or they may make errors in judgment or they may commit errors due to carelessness, distraction, or fatigue.

Collusion

The collusive activities of two or more individuals can result in internal control failures. Individuals acting collectively to perpetrate and conceal an action from detection often can alter financial data or other management information in a manner that circumvents control activities and cannot be identified by the system of internal control.

Management Override

An internal control system can only be as effective as the people who are responsible for its functioning. Management has the capability to override the system. "Management override" means overruling or circumventing prescribed policies or procedures for illegitimate purposes – such as personal gain or an enhanced presentation of a department's financial condition or compliance status.

Management override should not be confused with “management intervention”, which represents management’s actions to depart from prescribed policies or procedures for legitimate purposes. Management intervention is necessary to deal with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately.

Part II: Five Standards of Internal Control

The ***COSO Report*** describes the internal control process as consisting of five interrelated components that are derived from and integrated with management processes. These components define the standards for internal control and provide the basis against which internal control is to be evaluated. These standards apply to all aspects of a department's operations: administrative, financial, and programmatic. These standards provide a general framework. Management is responsible for developing the detailed policies, procedures, and practices to fit their department's operations and mission.

Control Environment

> **Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management.**

The **control environment** sets the tone of the department and influences the effectiveness of internal controls within the department. The control environment is the foundation for all other components of internal control, providing discipline and structure and encompassing both technical competence and ethical commitment. If this foundation is not strong, if the control environment is not positive, the overall system of internal control will not be as effective as it should be. Many factors affect the control environment, including the following:

Ethical Values and Integrity

Ethical values and integrity are key factors contributing to a positive control environment. Ethical values are the standards of behavior that form the framework for employee conduct and guide employees when making decisions. People in a department have personal and professional integrity when they adhere to ethical values. While it is management's responsibility to establish and communicate the ethical values of the department, it is everyone's responsibility to demonstrate integrity. Management provides leadership in setting and maintaining the department's ethical tone ("tone at the top") by:

- Providing guidance for proper behavior through policy statements, codes of conduct and by behavioral example.

- Removing or reducing temptations for unethical behavior.

- Establishing methods for reporting ethical violations and consistently enforcing disciplinary practices when appropriate.

Management's Philosophy and Operating Style

This factor reflects management's basic beliefs regarding how the people and activities of a department should be managed. This factor determines the degree of risk the department is willing to take and management's philosophy towards performance-based management. Management's philosophy and style can be demonstrated in such areas as: acceptance of regulatory control imposed by others; management's attitude toward internal and external reporting; the use of aggressive or conservative accounting principles; the attitude of management toward information technology and accounting functions; and management's support for and responsiveness to internal and external audits and evaluations.

Commitment to Competence

Competence is a characteristic of people who possess and maintain the skill, knowledge and ability to perform their assigned duties. Management's commitment to competence includes hiring staff with the necessary skills and knowledge and ensuring that current staff receives adequate on-going training and supervision, as well as candid and constructive performance evaluations.

Structure

Structure refers to management's framework for planning, leading and controlling operations to achieve the department's objectives. The organizational structure should clearly define key areas of authority and responsibility and establish appropriate lines of reporting. An organizational chart can provide a clear picture of the functional sub-units of a department and the relationships among them. Management should provide policies and direct communications to ensure that employees are aware of their duties and responsibilities, understand how their individual actions interrelate and contribute to the department's objectives, and recognize how and for what they will be held accountable.

Risk Assessment

Internal control should provide for an assessment of the risks that an organization faces from both external and internal sources.

A precondition to risk assessment is the establishment of clear and consistent objectives at both the organization level and at the activity (program or function) level. Risk

assessment is the identification, analysis, and management of risks relevant to the achievement of the department's goals and objectives. Risks include internal and external events or circumstances that may occur and adversely affect operations. Once risks are identified, management should consider their impact (or significance), the likelihood of their occurrence, and how to manage them.

Risk Identification

Managers can start by analyzing the two circumstances most likely to threaten the achievement of objectives, **change** and **inherent risk**. The examples listed below are not all-inclusive, nor will every item apply to every department.

The risk to accomplishing objectives increases dramatically during a time of **change**. Because any change increases risk, managers must diligently monitor and assess all significant changes within their departments. Some examples of change that expose a department to increased risk are:

- Changes in personnel.
- Changes in the regulatory environment.
- New or revamped information systems and technology.
- Rapid growth or expansion of operations.
- Moving to a new location.
- New programs or services.
- Reorganizations within or between departments.

Activities with **inherent risk** have a greater potential for loss from fraud, waste, unauthorized use, or misappropriation due to the nature of the activity or asset. Cash, for example, has a much higher inherent risk for theft than a stapler does. Other examples of situations that may involve inherent risk:

- Complexity increases the danger that a program or activity will not operate properly or comply fully with applicable regulations.
- Third party beneficiaries are more likely to fraudulently attempt to obtain benefits when those benefits are similar to cash.
- Decentralization increases the likelihood that problems will occur.
  However, a problem in a centralized system may be more serious than a problem in a decentralized system because if a problem does exist, it could occur throughout the entire department.
- A prior record of control weaknesses will often indicate a higher level of risk because adverse situations tend to repeat themselves.

- Failure to remedy control weaknesses identified by auditors often result in the same weaknesses reoccurring in future years.

In further attempting to identify risks from both internal and external events, managers can ask the following questions:

- "What obstacles could stand in the way of achieving your objective?"
- "What can go wrong?"
- "What is the worst thing that has happened?"
- "What is the worst thing that could happen?"
- "What keeps you awake at night?"

Risk Analysis

After risks are identified, they need to be evaluated in terms of:

Likelihood - The probability that the unfavorable event would occur if there were no (or limited) internal controls to prevent or reduce the risk.

Impact (or Significance) - A measure of the magnitude of the effect to a department if the unfavorable event were to occur.

The specific risk analysis methodology used by departments can vary because of differences in missions and the difficulty in qualitatively and quantitatively assigning risk levels. (Refer to Appendix I.)

Risk Management

Executive management should provide guidelines to managers throughout the department to help them determine the level and the kinds of risk that are acceptable and not acceptable. Performing risk assessments assists managers in prioritizing the activities where controls are most needed. Managers use risk assessments to determine the relative potential for loss in programs and functions and to design the most cost-effective and productive internal controls. Using these guidelines and the risk assessment information, managers should determine whether to:

- **Accept the risk:** Do not establish control activities
- **Prevent or reduce the risk:** Establish control activities
- **Avoid the risk (*if possible*):** Do not carry out the function

The acknowledgement and acceptance of certain levels and kinds of risk is considered a department's **risk appetite**. When preventing risk or reducing it to an acceptable level, management should identify the most effective and efficient control activities available for managing the risk. Specifically, management should answer the following questions:

- ✓ **What is the cause of the risk?** Management should consider the reason the risk exists to help identify all the possible control activities that could prevent or reduce the risk.

- ✓ **What is the cost of control vs. the cost of the unfavorable event?** Management should compare the cost of the risk's effect with the cost of carrying out various control activities, and select the most cost-effective choice.

- ✓ **What is the priority of this risk?** Management should use a prioritized list of risks to help decide how to allocate resources among the various control activities used to reduce the risks. The higher the priority, the greater the resources allocated to the control activities intended to reduce the risk.

Management should maintain its analysis and interpretation as part of its documentation of the rationale that supports its risk management decisions. Management should review these decisions periodically to determine whether changes in conditions warrant a different approach to managing, preventing and reducing risk.

Control Activities

Internal control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the organization's control objectives.

Internal control activities are tools - policies, procedures, techniques, and mechanisms - that help identify, prevent or reduce the risks that can impede accomplishment of the department's objectives. They are essential for proper stewardship and accountability of government resources and for achieving effective and efficient program results.

Control activities occur at all levels and functions of the department. Management should establish control activities that are effective and efficient. When designing and implementing control activities, management should try to get the maximum benefit at the lowest possible cost. Here are a few simple rules to follow:

- The cost of the control activity should not exceed the cost that would be incurred by the department if the undesirable event occurred.

- Management should build control activities into business processes and systems as the processes and systems are being designed. Adding control activities after the development of a process or system is generally more costly.

- The allocation of resources among control activities should be based on the significance and likelihood of the risk they are preventing or reducing.

Many different control activities can be used to counter the risks that threaten a department's success. Most control activities, however, can be grouped into two categories:

- **Prevention** activities are designed to deter the occurrence of an undesirable event. The development of these controls involves predicting potential problems before they occur and implementing ways to avoid them.

- **Detection** activities are designed to identify undesirable events that do occur, and alert management about what has happened. This enables management to take corrective action promptly.

Costs and benefits should be assessed before control activities are implemented. Management should also remember that an excessive use of controls could impede productivity. No one control activity provides all of the answers to risk management problems. In some situations, a combination of control activities should be used, and in others, one control activity could substitute for another. The following are descriptions of some of the more commonly used control activities. This is by no means an exhaustive listing of the alternatives available to management.

Documentation

Documentation involves preserving evidence to substantiate a decision, event, transaction or system. All documentation should be complete, accurate and recorded timely. Documentation should have a clear purpose and be in a usable format that will add to the efficiency and effectiveness of the department. Examples of areas where documentation is important include:

Critical decisions and significant events usually involve executive management. These decisions and events usually result in the use, commitment, exchange or transfer of resources, such as in strategic plans, budgets and executive policies. By recording the information related to such events, management creates an organizational history that can serve as justification for subsequent actions and decisions and will be of value during self-evaluations and audits.

Documentation of **transactions** should enable managers to trace each transaction from its inception through its completion. This means the entire life cycle of the transaction should be recorded, including: (1) its initiation and authorization; (2) its progress through all stages of processing; and (3) its final classification in summary records.

Documentation of **policies and procedures** is critical to the daily operations of a department. These documents set forth the fundamental framework and the underlying methods and processes all employees rely on to do their jobs. They provide specific direction to and help form the basis for decisions made every day by employees. Without this framework of understanding by employees, conflict can occur, poor decisions can be made and serious harm can be done to the department's reputation. Further, the efficiency and effectiveness of operations can be adversely affected.

Approval and Authorization

Approval and authorization is the confirmation or sanction of employee decisions, events or transactions based on a review. Management should determine which items require approval based on the level of risk to the department without such approval. Management should clearly document its approval requirements and ensure that employees obtain approvals in all situations where management has decided they are necessary.

Authorization is the power management grants employees to carry out certain duties, based on approval received from supervisors. Authorization is a control activity designed to ensure events or transactions are initiated and executed by those designated by management. Management should ensure that the conditions and terms of authorizations are clearly documented and communicated, and that significant transactions are approved and executed only by persons acting within the scope of their authority.

Verification / Reconciliation

Verification (or reconciliation) is the determination of the completeness, accuracy, authenticity and/or validity of transactions, events or information. It is a control activity that enables management to ensure activities are being performed in accordance with directives. Management should determine what needs to be verified, based on the risk to the department if there were no verification. Management should clearly communicate and document these decisions to those responsible for conducting the verifications. The list below offers some examples of verification and reconciliation.

- Reviewing vendor invoices for accuracy by comparing to purchase orders and contracts.
- Comparing cash receipts transactions to a cash receipts log and tracing to bank deposit records.
- Reviewing and verifying a participant's eligibility for State program services.
- Reconciling a department's cash records to bank statements.

Separation of Duties

Separation of duties is the division or segregation of key duties and responsibilities among different people to reduce the opportunities for any individual to be in a position to commit and conceal errors (intentional or unintentional), or perpetrate fraud in the normal course of their duties. The fundamental premise of segregated duties is that different personnel should perform the functions of initiation, authorization, record keeping, and custody. No one individual should control or perform all key aspects of a transaction or event. These are called incompatible duties when performed by the same individual. The list below offers some examples of incompatible duties:

- Individuals responsible for data entry of payment vouchers should not be responsible for approving these documents.
- Individuals responsible for acknowledging the receipt of goods or services should not also be responsible for purchasing or payment activities.
- Managers should review and approve payroll expenses and time sheets before data entry, but should not be involved in preparing payroll transactions.
- Individuals performing physical inventory counts should not be involved in maintaining inventory records nor authorize withdrawals of items maintained in inventory.
- Individuals receiving cash into the office should not be involved in authorizing and recording bank deposits in the accounting records.
- Individuals receiving revenue or making deposits should not be involved in reconciling the bank accounts.

In cases where duties cannot be effectively separated, management can substitute increased review or supervision as an alternative control activity that can help prevent or reduce the risks. In an environment with a very limited number of employees, management needs to be involved in documenting, reviewing, and approving transactions, reports, and reconciliations.

Safeguarding of Assets

Safeguarding of assets involves restricting access to resources and information to help reduce the risk of unauthorized use or loss. Management should protect the department's equipment, information, documents and other resources that could be wrongfully used, damaged or stolen. Management can protect these resources by limiting access to authorized individuals only. Access can be limited by various means such as locks, passwords, electronic firewalls and encryption. Management should decide which resources should be safeguarded and to what extent. Management should make this decision based on the vulnerability of the items being secured and the likelihood of loss.

The list below offers some examples of the safeguarding of assets.

- Securing mobile items within locked facilities.
- Reviewing insurance coverage limits for reasonableness and adequacy.
- Performing periodic physical inventories of assets for verification of values, location, and appropriate utilization.

Supervision

Supervision is the ongoing oversight, management and guidance of an activity by designated employees to help ensure the results of the activity achieve the established objectives. Those with the responsibility for supervision should:

- Assign tasks and establish written procedures for completing assignments.
- Systematically review each staff member's work.
- Approve work at critical points to ensure quality and accuracy.
- Provide guidance and training when necessary.
- Provide documentation of supervision and review (for example, initialing examined work).

Reporting

Effective and accurate reporting is a means of conveying information. It serves as a control when it provides information on issues such as timely achievement of goals, financial position and employee concerns. Reporting also helps to promote accountability for actions and decisions. The list below offers some examples of effective and accurate reporting.

- Project status reports to alert management to potential cost or time overruns.
- Reports to monitor employee leave balances, position vacancies and staff turnover to determine effectiveness of workplace and employment practices.
- The State’s Comprehensive Annual Financial Report (CAFR) issued for the public’s review of Vermont’s financial performance and position.

Communication & Information

Information should be recorded and communicated to management and others within the organization who need it and in a form and within a time frame that enables them to carry out their internal control activities and other responsibilities.

For a department to run and control its operations, it must have relevant, valid, reliable, and timely communications relating to internal and external events. Managers must be able to obtain reliable information to determine their risks and communicate policies and other information to those who need it.

Information

Managers need operational and financial data to determine whether they are meeting their department's strategic and annual performance plans and if they are meeting their goals of accountability for effective and efficient use of resources. Operating information is also needed to determine whether the department is achieving its compliance requirements under various statutes and regulations. Financial information is needed for both external and internal uses. It is required to develop financial statements for periodic external reporting, and, on a day-to-day basis, to make operating decisions, monitor performance, and allocate resources. Pertinent information should be identified, captured, and distributed in a form and time frame that permits people to perform their duties efficiently. Moreover, effective management of information technology is critical to achieving useful, reliable, and accurate recording and communication of information.

Communication

Effective communications should occur in a broad sense with information flowing down, across, and up the department. In addition to internal communications, management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders (e.g. recipients, vendors, other organizations and departments) that may have a significant impact on the department achieving its goals.

Management should establish communication channels that:

- Provide timely information.
- Inform employees of their duties and responsibilities.
- Enable the reporting of sensitive matters including fraudulent or unethical behaviors.

- Enable employees to provide suggestions for improvement.
- Provide the information necessary for all employees to carry out their responsibilities effectively.
- 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 not an isolated internal control component. It affects every aspect of a department's operations and helps support its system of internal control. The feedback from this communication network can help management evaluate how well the various components of the system of internal control are working.

Monitoring

Monitoring is the review of the organization's activities and transactions to assess the quality of performance over time and to determine whether controls are effective.

Monitoring is a basic management duty included in routine financial and program activities like ongoing supervision, reconciliations, comparisons, performance evaluations, and status reports. Internal control systems should generally be designed to ensure that ongoing monitoring occurs in the course of normal operations. Proper monitoring ensures that controls continue to be adequate and function properly.

Focus Areas

The monitoring performed by a department should focus on the following major areas:

- **Control Activities** - Control activities are established to prevent or reduce the risk of problems occurring. If these activities fail, the department becomes exposed to risk. Therefore, management should establish procedures which monitor the effectiveness of control activities and the use of control overrides. Effective monitoring gives management the opportunity to identify and correct any control activity deficiencies or problems and to minimize the impact of unfavorable events.
- **Mission -** Monitoring activities should include the development and review of operational data that would allow management to determine whether the department is achieving its mission. This can be achieved by periodic comparison of operational data to the department's strategic plan.

- **Control Environment -** Executive management should monitor the control environment to ensure that managers at all levels are maintaining established ethical standards of behavior and that staff morale is at an appropriate level. Managers should also ensure that the staff is competent, that adequate training is provided and that management styles and philosophies foster accomplishment of the department's mission.

- **Communication** - Managers should periodically verify that employees are receiving and sharing information appropriately, and that this information is timely, sufficient and appropriate for the users. Management should ensure that there are open lines of communication, which encourages reporting of both positive and negative results.

- **Risks and Opportunities** - Managers should also monitor the department's internal and external environment to identify any changes in risks or the development of opportunities for improvement. If changes are identified, managers should take appropriate action to address these new conditions. Management should recognize that delays in responding to risks could result in damage to the department or a missed opportunity may result in lost revenue or unattained cost savings.

Internal Evaluations

Controls need to be monitored for effectiveness ("Are they are operating as intended?") and to ensure they have not become obsolete. Separate evaluations of control activities can also be useful by focusing directly on the controls' effectiveness at a specific time. The scope and frequency of separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures. Separate evaluations may take the form of self-assessments or the direct testing of internal controls. Deficiencies found during ongoing monitoring or through separate evaluations or testing should be communicated to those responsible for the function and to at least one higher level of management. Serious matters should be reported to top management.

Audit Resolution

Monitoring of internal control should include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. Managers are to (1) promptly evaluate findings from audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate the department's operations, (2) determine proper actions in response to findings and recommendations from audits and reviews, and (3) complete, within established timeframes, all actions that correct or otherwise resolve the matters brought to management's attention. The resolution process begins when audit or other review results are reported to management, and is completed only after action has been taken that corrects identified deficiencies, produces improvements, or demonstrates the findings and recommendations do not warrant management action.

Glossary

Accountability: The recognition and acceptance that one is answerable for whatever happens within a particular area of activity of assigned responsibility regardless of the cause.

Component: One of five standards of internal control. The internal control components are the control environment, risk assessment, control activities, communication and information, and monitoring.

Communication and Information: The fourth component of internal control; an organization must have relevant, reliable, and timely communications relating to internal and external events.

Control Activities: The third component of internal controls; the structure, policies, and procedures, which an organization establishes so that identified risks do not prevent the organization from reaching its objectives.

Control Environment: The first component of internal controls; it sets the tone of the organization influencing the effectiveness of internal controls and is the foundation for all other components of internal control, providing discipline and structure and encompassing both technical competence and ethical commitment.

Control Objectives: The objectives of an internal control system: (1) reliable financial reporting, (2) effective and efficient operations, and (3) compliance with applicable laws and regulations.

COSO: The Committee of Sponsoring Organizations of the Treadway Commission. It consists of the following organizations: the American Institute of Certified Public Accountants, the American Accounting Association, the Institute of Internal Auditors, the Institute of Management Accountants, and the Financial Executives Institute.

Detective Control: A control designed to discover an unintended event or result (contrast with *Preventative Control)*.

Effectiveness: The degree to which an organization or program is successful at meeting goals, objectives, and statutory mandates.

Efficiency: The degree to which an organization or program is successful at meeting goals and objectives with the least use of resources.

Goal: An elaboration of the mission statement, developed with greater specificity of how an organization will carry out its mission. The goal may be of a programmatic, policy, or fiscal nature, and is expressed in a manner that allows a future assessment to be made of whether the goal was or is being achieved.

Inherent Limitations: Those limitations of all internal control systems. The limitations relate to the limits 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, the possibility of management overrides, and collusion.

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

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

A less technical definition might define Internal Control as…

> The integration of the activities, plans, attitudes, policies, and efforts of the people of an organization working together to provide reasonable assurance that the organization will achieve its mission.

Internal Control System: A synonym for ***Internal Control***

Management Intervention: Management's actions to override prescribed policies or procedures for legitimate purposes; management intervention is usually necessary to deal with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately by the system. (Contrast this term with *Management Override.*)

Management Override: Management's overruling of prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's financial condition or compliance status. (Contrast this term with *Management Intervention.*)

Mission: The fundamental purpose for which an organization exists. A *mission statement* establishes the basis for the goals of the organization by describing in broad terms what the organization intends to accomplish.

Monitoring: The fifth component of internal control, it ensures that controls are adequate and function properly.

Objective: A sub-goal identified in specific, well-defined, and measurable terms that contributes to the achievement of an organization's goal.

Organization: An entity of any size, established for a particular purpose. An organization may be, for example, an agency, a department, an office, a commission or a board.

Policy: Management's directive of what is required to effect control. A policy serves as the basis for the implementation of management directives.

Preventative Control: A control designed to avoid an unintended event or result. (Contrast with *Detective Control.*)

Procedure: An action that implements a policy.

Process: A series of activities that are linked to perform a specific objective.

Reasonable Assurance: The concept that internal control, no matter how well designed and operated, cannot guarantee an organization's objectives will be met. This is because of inherent limitations in all internal control systems.

Reliable: A high degree of certainty and predictability for a desired outcome.

Risk: Anything that endangers the achievement of an objective.

Risk Appetite: The amount of risk exposure or potential impact from an event that a department is willing to accept or retain.

Risk Assessment: The second internal control component; the process used to identify, analyze, and manage the potential risks that could hinder or prevent an organization from achieving its objectives.

Separation of Duties: An internal control activity to detect errors and prevent wrongful acts; it requires that different personnel perform the functions of initiation, authorization, record keeping, and custody.

Valid: Produces or relates to the intended results or goal.

Internal Control Reference Sources

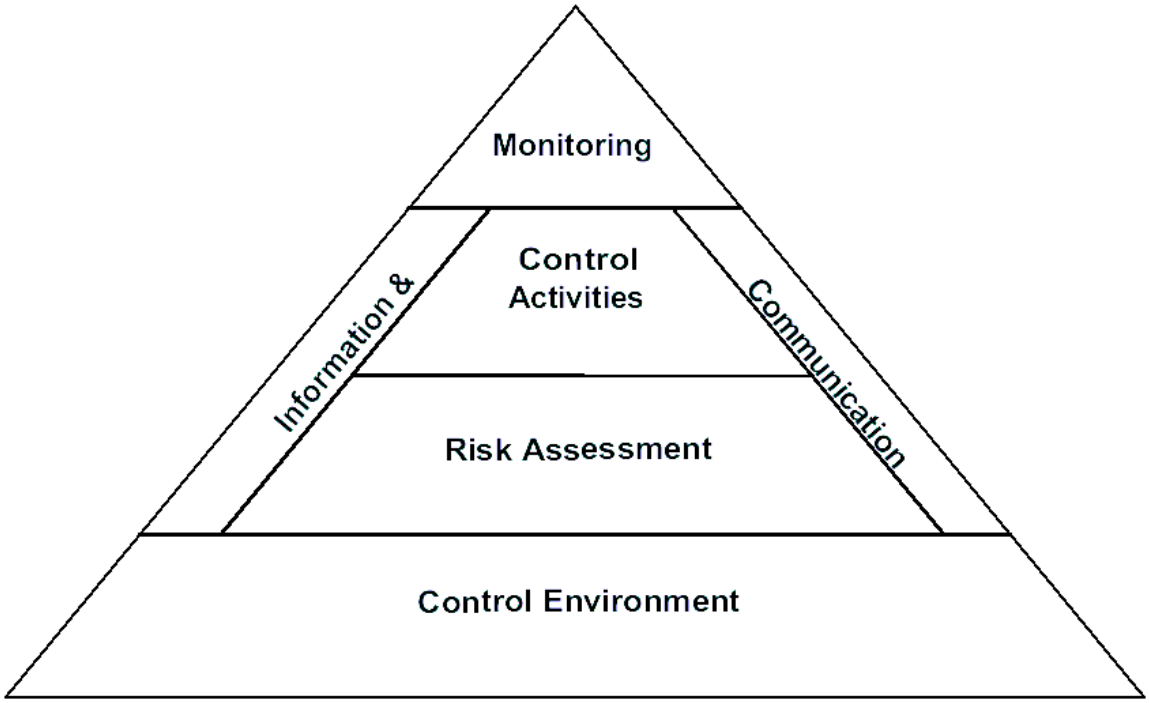
Committee of Sponsoring Organizations of the Treadway Commission (COSO)
http://www.coso.org/
Internal Control – Integrated Framework

Massachusetts Office of the Comptroller
http://www.mass.gov/comptroller/guidance-for-agencies/internal-controls.html
Internal Control Guide

New York State Internal Control Association
http://www.nysica.com/

New York State Office of the State Comptroller
http://www.osc.state.ny.us/agencies/ictf/
Standards for Internal Control in New York State Government

U.S. Government Accountability Office
http://www.gao.gov/
Standards for Internal Control in the Federal Government (The Green Book)



Components of Internal Control

This pyramid presents the five components of internal control, demonstrating that each of the components can and does influence the others.

Appendix I

To assist departments in evaluating risk (Risk Assessment), below are examples of "likelihood" and "impact" scales that a department might use to measure each risk that it identifies:

Likelihood - Simple Scale

1	Low	Very unlikely (practically impossible) to remotely possible
5	Moderate	Somewhat possible to quite possible
10	High	Very likely to virtually certain

Impact - Simple Scale

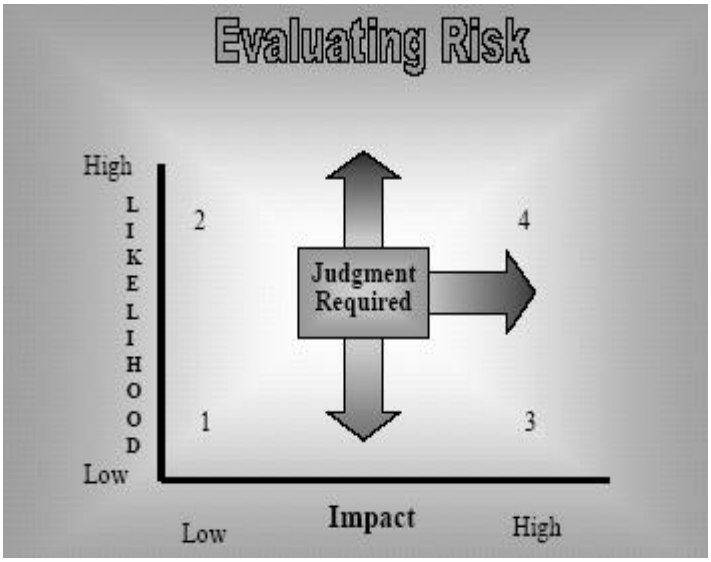
1	Low	Very small (inconsequential) to small (insignificant)
5	Moderate	Important (material) to serious (very material)
10	High	Pervasive (extremely material) to extraordinary (may threaten department's existence)

To help evaluate the risk's potential impact, departments can consider the following list:

Impact Rating (Highest to Lowest)

- Threat to health and safety
- Long-term disruption to statewide operations
- Significant loss of revenue or assets, public distrust
- Significant disruption to operations
- Large loss of revenue or assets
- Minor disruption to operations
- Procedural Issues (objectives met but could be more effective or efficient)
- Small loss of revenue or assets
- Minor errors/mistakes
- No impact

The following chart graphically depicts a reasonable approach to evaluating risks, with quadrant 1 representing the lowest priority and quadrant 4 representing the highest priority risk. Management should use judgment to establish priorities for risks based on their impact and their likelihood of occurrence. Risks should be ranked in a logical manner, from the most significant (high impact) and most likely to occur (high likelihood) - as indicated in quadrant 4 - to the least significant (low impact) and least likely to occur (low likelihood), as indicated in quadrant 1 of the graph.



Appendix II

To assist in understanding how the five standards of internal control are applied to your workplace, presented below are some representative examples specific to the State of Vermont. These processes and procedures, which many state managers and employees are familiar with, are followed by the associated internal control standard(s).

- User Identification and password to log into your department's computer network.
  [Control Activity – Safeguarding Assets]

- *VISION System Operator Access Request* form.
  [Control Activity – Approval/Authorization and Safeguarding Assets]

- Accounts payable vouchers (1) entered into VISION by the originating department, (2) check warrants generated by Finance & Management, and (3) checks issued by the State Treasurer's Office (3).
  [Control Activity – Separation of Duties] (Note: Appropriate separation of duties and approvals must also exist within each department in this example.)

- Employee Newsletters such as DHR's *HR Connect* or F&M's *Internal Control News*.
  [Communication & Information]

- Performing professional and educational reference checks prior to hiring a new employee.
  [Control Environment – Commitment to Competence]

- Consumer and staff satisfaction surveys by the Agency of Human Services.
  [Monitoring – Mission (consumer) and Control Environment (staff)]

- State of Vermont (DHR) Personnel Policy and Procedures (e.g. #5.6 "Employee Conduct").
  [Control Environment – Ethical Values and Integrity]

- Dept of Health's Pandemic Influenza Response Plan.
  [Risk Identification and Risk Assessment]

- Department Organization Charts.
  [Control Environment – Structure]

- Employees prepare & certify time sheets, supervisors review & approve, and the Dept. of Human Resources process the paychecks.
  [Control Activity – Separation of Duties]

- Use of a safe or locking cabinet etc. to secure cash receipts or petty cash.
  [Control Activity – Safeguarding Assets]

- Dept. of Public Safety's Radiological Emergency Response Program for the VT Yankee nuclear power station.
  [Risk Assessment]

- Reconciling federal funds drawn/received to funds expended per VISION to "SEFA" (Schedule of Expenditures of Federal Awards) reports.
  [Control Activity – Reconciliation]

- Departmental staff meetings, retreats, strategic planning sessions, etc.
  [Control Environment and Communication & Information]

- Use of checklists (or similar) to identify and manage the status of critical activities such as monthly and annual financial closings.
  [Risk Assessment and Control Activity - Supervision]

- Dept. of Finance and Management's Self-Assessment of Internal Control Questionnaire.
  [Monitoring – Internal Evaluations]

- Annual employee performance evaluations.
  [Control Environment – Commitment to Competence]

- Periodic unannounced inventory audits by Dept. of Liquor Control coordinators at retail liquor agencies.
  [Monitoring - Control Activities – Separation of Duties]

- VISION budget-checking prohibits departments from expending funds in excess of appropriated and authorized amounts.
  [Control Activity – Authorization]

- Reconciling a petty cash checking account to the monthly bank statement
  [Control Activity – Reconciliation]

- Dept. of Motor Vehicles requiring customers to provide specific documentation (e.g. proof of identify, automobile insurance card) prior to issuing an operator's license.
  [Control Activity – Verification]

- Agency of Agriculture, Food and Markets spot-checking store scales and measuring devices to ensure accuracy for consumers.
  [Monitoring - Control Activities – Verification]