STATE UNIVERSITY OF NEW YORK
NEW PALTZ

OFFICE OF INTERNAL CONTROLS

CAMPUS INTERNAL CONTROLS HANDBOOK

http://www.newpaltz.edu/internalcontrols/

Campus Internal Control Handbook

Introduction

Everyone has experience with internal control, both in his or her daily business activities and 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 our organizations. So, how can a subject of such importance be so unappreciated? The answer may lie in the need to better define internal control and what it does. This document is intended to explain to New York State government employees how internal control plays an important part in their daily work activities.

An effective system of internal control can give managers the means to provide accountability for their programs, as well as the means to obtain reasonable assurance that the programs they direct meet established goals and objectives. However, all the people in an organization - not just managers - have a part in and a responsibility for internal control. Internal control impacts executive managers who establish an organization's strategic plan, as well as support staff who process the mail.

Definition of Internal Control

The following definition of internal control is the centerpiece for the remaining discussion in this document. Understanding the definition is critical to understanding the concepts, which follow.

Internal control or an internal control system is 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 objectives and mission.

This definition establishes that:

- Internal control impacts every aspect of an organization: all of its people, processes and physical structures;
- Internal control is a basic element that permeates an organization - not a feature that is added on;
- Internal control incorporates the qualities of good management;
- Internal control is dependent upon people and will succeed or fail depending on the attention people give to it;
- Internal control is effective when all of the people and the surrounding environment work together;
- Internal control provides a level of comfort to an organization; controls do not guarantee success; and
- Internal control helps an organization achieve its objectives and mission.

INTERNAL CONTROL SYSTEM COMPONENTS AND STANDARDS

CONTROL ENVIRONMENT

Control environment is the attitude toward internal control and control consciousness established and maintained by the management and the employees of an organization. It is a product of management's philosophy, style and supportive attitude, as well as the competence, ethical values, integrity, and morale of the organization's people. The organization structure and accountability relationships are key factors in the control environment.

COMMUNICATION

Communication is the exchange of useful information between and among people and organizations to support decisions and coordinate activities. Within an organization, information should be communicated to management and other employees who need it in a form and within a time frame that helps them to carry out their responsibilities. Communication also takes place with outside parties such as customers, suppliers and regulators.

ASSESSING AND MANAGING RISK

Risks are events that threaten the accomplishment of objectives. They ultimately impact an organization's ability to accomplish its mission. Risk assessment is the process of identifying, evaluating and determining how to manage these events. At every level within an organization there are both internal and external risks that could prevent the accomplishment of established objectives. Ideally, management should seek to prevent these risks. However, sometimes management cannot prevent the risk from occurring. In such cases, management should decide whether to accept the risk, reduce the risk to acceptable levels, or avoid the risk. To have reasonable assurance that the organization will achieve its objectives, management should ensure each risk is assessed and handled properly.

CONTROL ACTIVITIES

Control activities are tools - both manual and automated - that help prevent or reduce the risks that can impede accomplishment of the organization's objectives and mission. Management should establish control activities to effectively and efficiently accomplish the organization's objectives and mission.

MONITORING

Monitoring is the review of an organization's activities and transactions to assess the quality of performance over time and to determine whether controls are effective. Management should focus monitoring efforts on internal control and achievement of organization objectives. For monitoring to be most effective, all employees need to understand the organization's mission, objectives, and responsibilities and risk tolerance levels.

Four Purposes of Internal Control

As stated in the above definition, internal control is a means for achieving the organization's objectives and mission. That is its ultimate purpose. More specifically, as defined by the International Organization of Supreme Audit Institutions, there are four purposes of internal control:

1. To promote orderly, economical, efficient and effective operations and to produce quality products and services consistent with the organization's mission;
2. To safeguard resources against loss due to waste, abuse, mismanagement, errors and fraud;
3. To ensure adherence to laws, regulations, contracts and management directives; and
4. To develop and maintain reliable financial and management data, and to accurately present that data in timely report

If an organization addresses each of these four purposes in developing its internal control system, the organization will most likely achieve its objectives and mission. Failure to adequately address any one of these purposes may put the organization at risk. The question then is how does an organization ensure that it does address these four purposes? The answer lies in establishing a sound internal control system.

FIVE COMPONENTS OF INTERNAL CONTROL

1. CONTROL ENVIRONMENT

Control environment is the attitude toward internal control and control consciousness established and maintained by the management and the employees of an organization. It is a product of management's philosophy, style and supportive attitude, as well as the competence, ethical values, integrity, and morale of the organization's people. The organization structure and accountability relationships are key factors in the control environment.

The control environment has a pervasive influence on all the decisions and activities of an organization. A positive control environment is the foundation for all other standards of internal control, providing discipline and structure. The following information describes management's responsibilities for creating a good control environment, and the staff's responsibilities for helping to maintain it.

Ethical Values and Integrity

Key elements contributing to a good control environment are ethical values and integrity. Ethical values are the standards of behavior that form the framework for employee conduct. Management addresses the issue of ethical values when it encourages:

- Commitment to honesty and fairness;
- Recognition of and adherence to laws and policies;
- Respect for the organization;
- Leadership by example;
- Commitment to excellence;
- Respect for authority;
- Respect for employees' rights; and conformance to professional standards.

Ethical values, such as these, guide employees when they make decisions on the job. Management's failure to properly communicate such values could impair the organization's ability to accomplish its mission.

People in an organization 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 organization, it is everyone's responsibility to demonstrate the integrity that ensures adherence to those values.

Management encourages integrity by:

- Establishing and publishing a code of conduct;
- Complying with the organization's ethical values and code of conduct;
- Rewarding employee commitment to the organization's ethical values;
- Establishing methods for reporting ethical violations; and
- Consistently enforcing disciplinary practices for all ethical violations.

It is management's responsibility to ensure that processes and activities serve to strengthen integrity.

Competence

Competence is a characteristic of people who have the skill, knowledge and ability to perform a task. An organization should ensure that staff members possess the knowledge, skills and ability necessary to do their jobs.

Management's responsibility for ensuring the competency of its personnel should begin with establishing appropriate human resource policies and practices. Such policies and practices should reflect a commitment to:

- Establishing levels of knowledge and skill required for every position;
- Verifying the qualifications of job candidates;
- Hiring and promoting only those with the required knowledge and skills; and
- Establishing training programs that help employees increase their knowledge and skills.

Management should also ensure that staff has what they need - such as equipment, software and policy and procedure manuals – to perform their jobs. Staff should also have assurance that they will have access to the tools and the support they need to perform their tasks.

Morale

Morale is the attitude people have about their work, as exhibited by their confidence, their discipline and their willingness to perform tasks. Management should be aware of the importance of good morale in an effective control environment. People's attitude about their jobs, their work environment and their organization impacts how well they do their jobs. Management should monitor the level of staff morale to ensure employees are committed to helping the organization accomplish its mission. Management should also take actions to maintain high morale. Such actions should provide staff with a sense that:

- Their opinions and contributions are welcomed, valued and recognized;
- The organization is willing to help improve their level of competency;
- There is opportunity for continuous improvement;
- They have a stake in the mission, goals and objectives of the organization;
- The organization's appraisal and reward systems are fair; and
  the lines of communication are open.

Mission

The mission is the organization's reason for existing. It provides a sense of direction and purpose to all members of the organization, regardless of their position, and provides a guide when making critical decisions. During periods of change, it provides cohesion to the organization and helps keep it on its proper course. Without a clearly defined and communicated mission, an organization may drift aimlessly and accomplish little.

The mission of an organization should be a statement, approved by executive management and/or the governing board of the organization.

A well-defined mission should:

- Identify the customer(s) and customer needs;
- Provide direction and stability to the organization; and
- Motivate staff.

Management should tell employees about the organization's mission and explain how their jobs contribute to accomplishing the mission. The mission statement will be most effective if all employees perceive they have a personal stake in it.

As time passes, both internal and external changes can affect the organization's mission. Therefore, management should periodically review the mission and update it, as necessary, for adequacy and relevancy.

2. **COMMUNICATION AND INTERNAL CONTROL**

Management should ensure that good communication channels exist to carry information to people who need it throughout the organization. The organization's management and staff should be able to use these established channels to communicate relevant information to the right people in a timely way.

Management should have clear internal communication channels that:

- Inform employees of their duties and responsibilities;
- Report sensitive matters;
- Enable employees to provide suggestions for improvement;
- Provide the information necessary for all employees to carry out their responsibilities effectively; and
- Convey top management's message that internal control responsibilities are important and should be taken seriously.

People outside the organization, like customers, suppliers and regulators, also need reliable and timely information relevant to their specific needs. Therefore, management also needs to establish specific communication channels between the organization and these external parties.

However, communication is not an isolated internal control component. Communication issues affect every aspect of an organization's operations, and help support its system of internal control. Therefore, the extent to which a good communication network is established and used by both managers and employees can help management circulate guidance about internal control issues. The feedback from this communication network can help management evaluate how well the various components of the system of internal control are working, and which features need improvement.

3. **RISK ASSESSMENT**

Management should evaluate each risk they identify in terms of its significance, likelihood and cause.

Significance is a measure of the magnitude of the effect on an organization if the unfavorable event were to occur. When determining the significance of each risk, management should consider the effect of the risk. The effect is the ultimate harm that may be done or the opportunity that may be lost. Managers should quantify this if possible, or at least state the effect in specific terms to help define the significance of the risk.

Likelihood is the probability that an unfavorable event would occur if there were no control activities (see the "Control Activities" section) to prevent or reduce the risk from occurring. Management should estimate the likelihood for each identified risk.

The cause of the risk is the reason why an unfavorable event may occur. Management should also determine the cause for each risk. This information is critical if management is to design control activities that will effectively limit the risk.

Managing Risk

Executive management should provide guidelines to managers throughout the organization to help them determine the level and the kinds of risk that are acceptable and not acceptable. Using these guidelines and the risk assessment information, managers should determine whether to accept the risk in a given situation, prevent or reduce the risk or avoid the risk entirely. For example, in deciding how to manage the risk that "unauthorized persons will gain access to computer files," managers should determine whether to:

- Accept the risk of unauthorized access;
- Establish control activities to prevent the risk or reduce it to an acceptable level; or
- Decide against carrying out the function when no risk is tolerable.

Accept the risk: Do not establish control activities

Management can accept the risk of unauthorized access because the consequences of such access are not that significant. For example, the files may contain data that is not sensitive, such as the roster of current employees. Management might also choose to accept the risk if the cost of associated control activities is greater than the cost of the unfavorable event (unauthorized access), should it occur.

Prevent or reduce the risk: Establish control activities

Management cannot accept the current level of risk of unauthorized access to files it must maintain. Such files may contain confidential or otherwise inherently risky data. Therefore, management establishes controls that work to prevent the risk of unauthorized access, or at least reduce the risk of such access to an acceptable level. However, the risk is prevented or reduced only as long as control activities function as intended and continue to be effective.

Avoid the risk: Do not carry out the function

Management cannot tolerate any risk of unauthorized access to the files or cannot control such access. For example, a file may contain extremely sensitive data, or access controls may not be feasible. In this case, management may decide that the impact of any unauthorized access to this file would be too destructive to bear, or that access is too difficult or too costly to control. Management decides not to carry out this function (i.e., decides not to maintain the data).

What is the cause of the risk?

Management should consider the reason the risk exists to help identify all the alternative 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 to 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 the prioritized list of risks to help decide how to distribute resources among the various control activities used to reduce the risks. The higher the priority, the greater the resources and control activities that should be used to reduce the risk.

4. **CONTROL ACTIVITIES**

Control activities are tools - both manual and automated - that help prevent or reduce the risks that can impede accomplishment of the organization's objectives and mission. Management should establish control activities to effectively and efficiently accomplish the organization's objectives and mission.

There are many control activities management can use to counter the risks that threaten an organization's success. Most of them can be grouped into four categories: directive, preventive, detective and corrective control activities.

Directive control activities are designed to guide an organization toward its desired outcome. Most directive control activities take the form of laws, regulations, guidelines, policies and written procedures.

Preventive control 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.

Detective control 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.

Corrective control activities are processes that keep the focus on undesirable conditions until they are corrected. They may also help in setting up procedures to prevent recurrence of the undesirable condition.

The documentation of an organization's system of internal control should include the organization's structure, policies, assessable units, control objectives and control activities. The various aspects of a system of internal control can be represented in narrative form, such as in policy and procedure manuals, and/or in the form of flowcharts or matrices.

DOCUMENTATION

Documentation involves preserving evidence to substantiate a decision, event, transaction or system. All documentation should be complete and accurate and be recorded promptly. It should contribute to achieving the organization's mission, help managers in controlling their operations, and assist in analyzing operations. Documentation without a clear purpose will hinder the efficiency and effectiveness of an organization.

There are three primary areas within an organization where documentation is very important: critical decisions and significant events, transactions and the system of internal control.

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 those contained in strategic plans, budgets and policies. By recording the information related to such events, management creates an organizational history that can serve as justification for subsequent actions and decisions. This type of documentation is also very valuable to use 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. For example, the documentation for the purchase of equipment would start with the authorized purchase request, and continue with the purchase order, the vendor invoice and the final payment documentation.

Management should ensure that this documentation is properly classified. Accurate classification makes it easy to promptly retrieve information when needed, and to prepare subsequent reports, schedules and financial statements.

The documentation of an organization's system of internal control should include the organization's structure, policies, assessable units, control objectives and control activities. The various aspects of a system of internal control can be represented in narrative form, such as in policy and procedure manuals, and/or in the form of flowcharts or matrices.

Approval and Authorization

Approval is the confirmation or sanction of employee decisions, events or transactions based on a review. For example, a manager reviews a purchase request, as required, to determine whether the item is needed. Upon determining the item is needed, the manager signs the request indicating approval of the purchase. Management should determine which items require approval based on the level of risk to which the organization would be exposed without such approval. Management should clearly indicate 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 approved by management. Management should ensure that the conditions and terms of authorizations are clearly stated and communicated, and that significant events and transactions are approved and executed only by persons acting within the scope of their authority. For example, a manager may be authorized by his/her superiors to approve purchase requests, but only those up to a specified dollar amount.

Verification

Verification 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 done in accordance with directives. Management should determine what needs to be verified, based on the risk to the organization if there were no verification. Management should clearly communicate these decisions to those responsible for conducting the verifications.

Examples of circumstances that may require verification are: during the hiring process, verification of a candidate's qualifications to minimize the risk of hiring someone who is not capable of doing the job, or who does not meet the required standards; and in purchasing equipment, verifying that there is a need for the purchase, that a fair price has been obtained and that funds are available to pay for the purchase.

Supervision

Supervision is the management or guidance of an activity to help ensure the results of the activity achieve established objectives. Those with the responsibility for supervision should: monitor, review and approve, as appropriate, the work of those performing the activity to ensure the work is accurate and that it flows as intended; (Refer to the "Monitoring" section for details about the monitoring aspects of supervision). Provide the necessary guidance and training to help minimize errors and waste and to ensure that employees understand and follow management directives; and clearly communicate the duties and responsibilities assigned to those performing the activities.

An example of supervision is when a supervisor reviews a purchase request of an employee to determine whether it represents a valid need and whether it is completed accurately. The supervisor signs the order to signify his/her review and approval. However, if there are any errors, or if the supervisor determines there is no need for the purchase, the supervisor would return the order to the employee and explain how to complete the request properly or why the purchase is not needed.

Separation of Duties

Separation of duties is the division of key tasks and responsibilities among the various employees and subunits of an organization. No one individual should control all the key aspects of a transaction or event. By separating key tasks and responsibilities - such as receiving, recording, depositing, securing and reconciling assets - management can reduce the risk of error, waste, or wrongful acts occurring or going undetected. The purchasing cycle is a key area where the separation of duties can minimize the risk of inappropriate, unauthorized or fraudulent activities. Specifically, the various activities related to a purchase (initiation, authorization, approval, ordering, receipt, payment and record keeping) should be done by different employees or subunits of an organization. However, in cases where tasks cannot be effectively separated, management can substitute increased supervision as an alternative control activity that can help prevent or reduce these risks.

Safeguarding Assets

To safeguard assets is to restrict access to resources and information to help reduce the risk of unauthorized use or loss. Management should adequately protect the organization's assets, files, documents and other resources that could be wrongfully used, damaged or stolen. Management can protect these resources by limiting access to authorized individuals. Access can be limited by various means, such as locks, passwords and guards. Management should decide which resources should be subject to safeguarding and to what extent.

Management should make this decision based on the vulnerability of the items being secured and the perceived risk of loss, and reassess this decision periodically. For example, management could safeguard newly purchased computers by storing them in a locked room of the receiving department until they are requisitioned.

Reporting

Reporting is a means of conveying information. It serves as a control when it prevents or reduces the risk that an unfavorable event will occur. Reporting assists in monitoring (See "Monitoring" section) when it provides information on such issues such as timeliness, achievement of goals, budget status and employee concerns. Reporting also helps to promote accountability for actions and decisions (See the discussion of Structure in the "Control Environment" section). An example of a report that serves as a control activity would be one that compares purchasing activities to the approved budget, along with explanations of significant variances.

Control Activities for Computer Systems (for the non-systems manager)

The concept of directive, preventive, detective and corrective controls, as well as the control activities described above, applies to both manual and computerized processes. However, several additional control activities are unique to a computer environment. They exist to address the characteristics that distinguish computerized processes from manual processes. These controls apply to all computerized information systems - mainframe, minicomputer, and end-user environments. Computer control activities are typically categorized as either general or application controls.

General controls are those that relate to all activities in the computer environment, including access security over both hardware and electronic files. They often include controls over the development, modification and maintenance of computer programs and the use of, and changes to, data maintained on computer files.

Application controls relate to specific tasks performed by the computer system. Their purpose is to provide reasonable assurance that data entered into the system is properly recorded, processed and reported.

General and application control over computer systems is interrelated. If the general control is inadequate, the application control is unlikely to function properly and could be overridden. The application control assumes that the general control will function properly and provide immediate feedback on errors, mismatches, incorrect format of data, and inappropriate data access (by unauthorized persons). Therefore, general control supports the functioning of application control, and both are needed to ensure complete and accurate information processing.

The field of computer information processing is one of rapid technological change. Changes in technology will change the specific control activities that may be employed and how they are implemented, but the basic requirements of control will not have changed. As more powerful computers place more responsibility for data processing in the hands of the end users, the necessary controls (for example, routines within computer programs that validate data or persons/vendors and the procedures performed by users to ensure accurate processing by the computer) should be identified and implemented.

This information, and the discussion of Backup and Disaster Recovery, Input Controls and Output Controls that follows, is not meant to be a complete explanation of all computer-related control activities. Rather, it is intended to give non-systems managers who use computers in their operations and overview of basic computer-related control activities.

Systems managers should seek further guidance on information technology (IT) security and control measures from sources such as Control Objectives for Information and Related Technology (CobiT) and Systems Auditability and Control (SAC). These resources have been developed to provide generally applicable and accepted standards for good practices for IT controls that provide a reference framework for management, users and auditors.

Backup and Disaster Recovery

All computer systems should have adequate backup and disaster recovery procedures to prevent or reduce the risks related to system failure, power loss or other potential threats to the system or data. Managers should ensure that there are specific reconstruction and recovery plans for important systems and for the data used in their operations. These plans should include procedures for:

- Duplicating or regenerating important programs and data files;
- Arranging for storage of backup copies of files at a secure off-site location; and
- Resuming processing on another system or at another location.

An example of a common backup technique is the "grandfather-father-son" method, which involves the creation of three generations of master files over a three-day period. These master files are retained during this period along with the transaction files. If the current (son) file is destroyed or damaged, the information can be reconstructed using the father and the current transaction files. If both the father and the son files are destroyed or damaged, the grandfather along with the previous and current transaction files can be used to reconstruct the data.

Input Controls

Input controls help ensure that the data ready for processing has been authorized and converted into a machine-readable format. In addition, these controls enable the user to determine whether any data has been lost, suppressed, added, duplicated or otherwise
improperly altered. Examples of input controls are:

- Edit checks programmed into software such as: error listings, record counts, sequence checks, validity checks and hash totals;
- Key verification, which entails re-keying the input and comparing the results; redundancy checks, which require sending additional data to serve as checks on other transmitted data;
- Echo checks which verify transmitted data by sending data back to the user's terminal; and
- Completeness checks, which verify whether all necessary information has been sent.

Output Controls

Output controls ensure that system generated information is accurate and that only authorized users receive this information. Examples of output controls are:

- The daily proof account activity listings, which show changes, made to the master file. Managers should review activity listings to ensure that only accurate, authorized changes have been made;
- Error listings indicating data that could not be processed by the system. Managers should ensure that this data is reviewed, corrected and resubmitted for processing;
- Distribution registers that list the people authorized to receive reports and other information from the system. Management should periodically review the register to ensure its accuracy;
- End-of-job markers which should appear on the last page of system generated reports. The presence of these markers helps users of a report to verify that they have received the entire report; and
- A quality assurance review of output by system users. This process can help those who input the data to verify that the output is complete and reasonable.

5. **MONITORING**

Monitoring is the review of an organization's activities and transactions to assess the quality of performance over time and to determine whether controls are effective. Management should focus monitoring efforts on internal control and achievement of organization objectives. For monitoring to be most effective, all employees need to understand the organization's mission, objectives, and responsibilities and risk tolerance levels.

Monitoring Responsibilities and Duties

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 staff persons; supervisors, mid-level managers and executive managers will not have the same focus.

Staff

The primary focus of staff should be on monitoring their own work to ensure it is being done properly. They should correct the errors they identify before work is referred to higher levels for review. Management should educate staff regarding control activities and encourage them to be alert to and report any irregularities. Because of their involvement with the details of the organization's daily operations, staff has the best vantage point for detecting any problems with existing control activities. Management should also remind staff to note changes in their immediate internal and external environments, to identify any risks and to report opportunities for improvement.

Supervisors

Supervision is a key element of monitoring. Supervisors should monitor all activities and transactions in their unit. Their monitoring focus should be on ensuring that:

- Control activities are functioning properly;
- The unit is accomplishing its goals;
- The unit's control environment is appropriate;
- Communication is open and sufficient; and
- Risks and opportunities are identified and properly addressed.

Middle Management

Middle management's monitoring responsibilities should cover the review of how well controls are functioning in multiple units within an organization, and how well the supervisors are performing monitoring in their respective units. These managers' focus should be similar to that of supervisors, but extended to cover all the units for which they are responsible.

Executive Management

Executive management's monitoring responsibilities should be similar to those of middle management, except that the executive manager's focus is on major divisions of the organization. Because of this broader focus, executive managers should place even more emphasis on monitoring the organization's achievement of its goals. Executive managers should also monitor for the existence of risks and opportunities in either the internal or external environment that might indicate the need for a change in the organization's plans.

MAJOR AREAS FOR MONITORING

Control Activities

Control activities are established to prevent or reduce the risk of an unfavorable event from occurring. If these activities fail, the organization becomes exposed to risk. Control activities can fail when controls are overridden, or when there is collusion for fraudulent purposes. Therefore, management should establish procedures to monitor the functioning of control activities and the use of control overrides. Management should also be alert to signs of collusion. Effective monitoring gives management the opportunity to correct any control activity problems - and to control the risk - before an unfavorable event occurs.

Mission

Monitoring activities should include the development and review of operational data that would allow management to determine whether the organization is achieving its mission. By regularly monitoring, management can determine if the organization is accomplishing its mission.

Control Environment

Management should monitor the control environment to ensure that managers at all levels maintain ethical standards of behavior and promote good staff morale. Managers should also ensure that staff are competent, that training is sufficient and that their management styles and philosophies foster accomplishment of the organization's mission.

Communication

Managers should regularly ensure that the people they are responsible for are receiving and sharing information appropriately, and that this information is timely, sufficient and appropriate to the user(s).

Risks and Opportunities

Managers should also monitor the organization's internal and external environment to identify any changes in risks and new opportunities. If changes are identified, managers should take appropriate action to address these new or changed risks and opportunities. Management should recognize that delays in responding to risks could result in damage to the organization; a missed opportunity may result in a loss of new revenue or savings, or may eventually become a risk for the organization.

Monitoring Results

Management should ensure that there are open lines of communication for both staff and management to use. Open communication fosters reporting of both positive and negative results to the appropriate level of management without the fear of reprisal. Management should ensure that it takes the proper actions to address these results. For example, management may decide to: establish new goals and objectives to take advantage of newly identified opportunities; counsel and retrain staff to correct procedural errors; or adjust control activities to minimize a change in risk.

SUPPORTING ACTIVITIES

There are two additional items that support a good internal control system - evaluation and strategic plans. While these are not standards for a good internal control system, they do provide management with additional tools to help ensure that the mission of the organization will be achieved.

Evaluation

Evaluation is the process management uses to assess whether an organization's operations are effective in achieving its mission. The purposes of evaluation are to provide management with a reasonable assurance that:

- The organization will likely achieve its mission, plans, goals and objectives;
- The elements of the organization's system of internal control are functioning effectively; and
- They can identify both risks to the organization and opportunities for improvement.

Evaluation vs. Monitoring

It is important to note the distinction between evaluation and monitoring. Monitoring involves performing daily or routine procedures - like supervision, transaction review and problem resolution - that help to ensure operations are in compliance with the organization's system of internal control. Evaluation, on the other hand, involves doing periodic assessments of the organization's performance over time. Management's purpose in doing an evaluation is to get an answer to the question: "Are we doing things the way we should to accomplish our mission?"

The Basis for Evaluation

Evaluation is accomplished through self-assessments and independent assessments. Self- assessment is the process whereby an organization evaluates itself. Independent assessments are evaluations done by people who are not directly involved in the organization's operations. Self-assessment should be the primary basis for evaluation. It is a self-helping process that gives management an opportunity to improve the organization. Regular self-assessments help management detect problems early, and minimize the costs that may be incurred if problems continued until detected through independent assessments. Self-assessments should be regularly scheduled efforts, conducted throughout the organization. Management should determine the frequency of self-assessments based on the results of the organization's risk assessment.

Internal auditors, who should be independent of operations to ensure their assessments are objective, can do independent assessments. External auditors and consultants who are outside of the organization can also perform independent assessments.
Management may find it useful to coordinate the efforts of the organization's internal audit unit, external auditors and/or consultants to obtain more objective, in-depth and targeted analyses of their operations. Independent assessments can also serve as a control activity to help ensure that management is performing self-assessments, and performing them effectively. Audits should not be a substitute for routine self-assessments, but should serve to supplement them. Management should perform self-assessments of the system of internal control, the accomplishment of the organization's mission, the organization's responses to risks and opportunities and the ways in which it communicates - and acts on - the results of self-assessments.

Assessing the System of Internal Control

Management should begin the self-assessment process by first identifying assessable units within the organization. The managers of assessable units should have the responsibility for determining the effectiveness of the system of internal control within their respective units. In doing this self-assessment, managers should get answers to questions, such as those that follow, about the integrity of each aspect of internal control.

Organization

- Do the unit's objectives provide it with a clear direction?
- Do people in the unit understand the objectives, and how achievement of the objectives helps to accomplish the organization's mission?

Control Environment

- Does the control environment help to foster achievement of the unit's objectives?

Assessing and Managing Risk

- Does this unit have a means of effectively identifying and managing risk?

Control Activities

- Has unit management established the controls needed to minimize risk?
- Are these controls functioning as designed?
- Are these controls both effective and efficient in accomplishing their purpose?

Communication

- Does the unit receive the timely, accurate and useful information needed to achieve its objectives?

- Are communication lines sufficient to meet our needs, both as senders and receivers of information in the organization?

Monitoring

- Is monitoring within the unit effective in ensuring that daily operations are in compliance with the system of internal control?
- Is the unit effectively monitoring the accomplishment of objectives, the control environment and the communication process?
- Does monitoring adequately identify changes in the internal or external environment that affect risk and opportunities?

By examining the answers to these and related questions, management will be able to determine the effectiveness of the organization's system of internal control, and identify and correct any weaknesses within the system. Management should ensure that the system of internal control is effective before assessing accomplishment of the mission.

Assessing Accomplishment of the Mission

Management should assess accomplishment of the mission at all levels of the organization on a regular basis. At production or operational levels, management should compare the actual accomplishments of the specific subunits to their operational plans and objectives. Management should compare the actual accomplishments of the major organizational divisions to the strategic plans and organizational objectives. Management should do these assessments following the evaluation of the system of internal control. If the system is working effectively, management will have reasonable assurance of the accuracy of the information it is using to determine the organization's accomplishments. Any deficiencies identified, as the result of the assessment, along with their cause and remedy, should be followed-up and resolved.

Assessing Risk and Opportunities

Management should also conduct assessments to determine how effectively the organization identifies and responds to new risks and opportunities. These assessments should help management determine whether:

- The monitoring and evaluation processes identify new risks that might threaten the organization and new opportunities that might enable the organization to improve and grow;
- New risks and opportunities are being communicated to those responsible for making responsive changes; and
- Those responsible for taking action make appropriate changes and responses in a timely manner.

To complete the process that allows an organization to improve and grow, executive management should also conduct an organizational overview assessment. This assessment should view the organization as a whole and should help executive management:

- Determine whether newly identified opportunities should result in changes in the organization's direction, including its mission, strategic plans and/or its organizational objectives; and
- Challenge the assumptions used to develop the mission, strategic plans and organizational objectives.

Information from these assessments will help management evaluate whether the organization is effectively protecting itself from external and internal threats, whether it can continue to improve and grow and whether it is accomplishing what it should be accomplishing.

Assessment Documentation

Management should ensure that it performs all aspects of its self-assessment according to plans that clearly define: responsibilities; evaluation methodologies, including the sources and types of information needed for accurate assessments; reporting requirements; and the method for ensuring any deficiencies identified are promptly corrected.

Communicating and Using Evaluation Results

For an evaluation to serve its purpose, management should communicate all assessment results, both good and bad. Positive results should be communicated to all who performed or were responsible for the activities being evaluated. Management should do this both to reinforce good business practices and to foster good morale. When results indicate a need for improvement, management should give the information to those who are responsible for making the necessary changes that will lead to improvement.

For the evaluation process to be effective, management should have processes in place that ensure appropriate and prompt actions are taken to address any deficiencies identified through self-assessment and independent assessment. In addition, management should include a review of such actions in a subsequent evaluation process to determine whether they have produced the desired outcomes.

Finally, when the results of these assessments indicate that there should be major changes within the organization, management should have processes in place to ensure these results are considered when changing or establishing new plans and organizational objectives. This will help ensure the improvement and growth of the entire organization.

Strategic Plans

Strategic plans are the courses of action that will enable an organization to achieve its mission, objectives and goals. Planning should begin at the top levels of management with a strategic plan that focuses on the long-range direction of the organization. The strategic planning process should include establishing the organization's broad organizational objectives (see "Objectives" below) and developing the strategies that should be followed to achieve them. Based on the direction provided by the organization's strategic plan, management should develop a strategic plan for each major organizational division with a long-range focus specific to that division. The divisional strategic plans guide managers in developing shorter-range operational plans for each of the major functions performed within their respective divisions.

Objectives

Objectives are the organization's desired outcomes. They are a product of the planning process and are necessary for coordinating efforts within an organization. Without clearly defined objectives, employees could be working in conflicting directions.

Objectives can be organizational or operational. Management derives organizational objectives from the mission and often develops them during the strategic planning process. They are long-range, broad statements, which define the desired outcomes of the organization as a whole. Good organizational objectives can serve as starting points for more specific and detailed objectives within the subunits (i.e., divisions, departments, bureaus and assessable units) of the organization. They also serve as standards for evaluating overall organizational performance.

Management derives operational objectives from the broad organizational objectives. Operational objectives are shorter-range, more specific and define the desired outcomes of each of the organization's subunits. They should be structured in a hierarchy so that each subunit's accomplishment of its operational objectives helps the next higher level achieve its operational objectives, all of which helps management meet its organizational objectives.

All objectives should be in writing. Management should provide employees with written organizational and operational objectives along with the mission statement. Management should ensure that employees understand the objectives and how their work helps to achieve them.

Finally, just as changes in the environment can affect the adequacy and relevancy of the mission statement, these same factors also affect an organization's objectives. For an organization to function effectively and grow, it should periodically reassess its organizational and operational objectives.

Goals

Goals are objectives translated into specific, measurable targets. They are quantifiable and provide a means for assessing the accomplishment of objectives.

Management should translate all objectives into attainable goals. Progress toward these goals can measure accomplishment of an objective. However, sometimes it is difficult to translate an objective into a quantifiable goal. In such instances, management should identify some appropriate indirect measure. For example, a reduction in calls to a tax department's customer help line may indicate that new instructions make it easier for taxpayers to complete forms.

Operational Plans

Managers at all levels should be able to use operational plans to determine the priority and timing of objectives, to resolve conflicts between objectives, to establish the organization's policies and procedures, and to help set budgets, schedules and resource assignments. Planning should be based on the most objective and accurate information available. All planning processes should identify the most efficient alternatives available for accomplishing the objectives.

The plans should be provided to and understood by everyone who must follow him or her. Management should also establish a process that identifies how and when plans should be changed to reflect both changing conditions and the availability of more accurate information. Plans should be flexible enough to allow for such changes.

Assessable Units

To perform an orderly, systematic evaluation of an organization's system of internal control, management should segment the organization into "assessable units." Assessable units are not usually the functional subunits found on an organization chart (e.g., a bureau), but are segments of them. For example, a bureau may have five or more assessable units in it, each of which performs a distinct function.

An assessable unit has certain primary characteristics. It has an ongoing, identifiable purpose that results in the creation of a service or product (used either internally or externally) and/or that fulfills a law, regulation or other mandate. An assessable unit should be large enough to allow managers to evaluate a significant portion of the activity being examined, but not so large that managers cannot perform a meaningful evaluation without extensive time and effort.

Management should maintain a listing of the assessable units along with the purpose and objectives of each assessable unit, and use it when planning any review of the system of internal control.

Summary

Internal controls are already part of our daily operations. The controls developed and exercised by managers and their staffs are the substance of the internal control program. SUNY New Paltz's Internal Control Program helps to ensure that the controls are properly documented and that they are functioning as intended.

The goal is not to make each person an expert in internal controls, but to increase our awareness and understanding of internal controls. In fact, the single most important success factor of the Internal Control Program is a high level of individual awareness and understanding. Internal controls are everyone's responsibility; therefore, it is critical that each person is able to identify the internal controls that exist in their unit. We are all responsible to know what internal controls exist and how to evaluate their effectiveness.

A successful Internal Control Program will help to streamline our processes and improve the level and quality of our services. The result of SUNY New Paltz's Internal Control Program will be a better, more enjoyable work place and a quality institution of higher education.

For more information on internal controls or the status of SUNY New Paltz's internal control program, please contact SUNY New Paltz's Department of Internal Controls.

Contacts:

Julie Majak
Asst Vice President & Internal Control Officer
Office of Vice President - Administration
Haggerty Administration Building – HAB 905B
Phone: (845) 257-3295
E-mail: majakj@newpaltz.edu

Peter Fairbrother
Internal Control Coordinator
Office of Internal Controls
Haggerty Administration Building – HAB 302
Phone: (845) 257-6960
E-mail: fairbrop@newpaltz.edu