


STATE OF DELAWARE

OFFICE OF

AUDITOR OF ACCOUNTS



INTERNAL CONTROL

GUIDE

The seal of the State of Delaware is centered in the background. It features two figures, a farmer on the left and a sailor on the right, flanking a central shield. Above the shield is a ship on a globe. A banner at the bottom of the seal reads "LIBERTY AND INDEPENDENCE".

MARCH 2000

A handwritten signature in black ink, reading "R. Thomas Wagner".

R. THOMAS WAGNER, JR., CGFM, CFE

AUDITOR OF ACCOUNTS

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION.....	1
PART I: INTERNAL CONTROL FRAMEWORK	
What Is Internal Control?.....	2
Why Have Internal Controls?.....	3
What Is Your Role?.....	3
PART II: FIVE COMPONENTS OF INTERNAL CONTROL	
Control Environment.....	5
Information and Communication	7
Risk Assessment.....	9
Control Activities	12
Monitoring.....	18
PART III: SUPPORTING ACTIVITIES	
Evaluation	22
Strategic Plans	24
Appendix A. References	26

INTRODUCTION

More than ever, taxpayers are demanding that government resources be used efficiently, economically and effectively. Government employees entrusted with public resources are responsible for safeguarding assets, complying with laws and regulations, and meeting goals and objectives. An adequate system of internal controls can assist government employees to carry out these responsibilities.

Internal control has been the focus of much attention, and several organizations have issued documents which present up-to-date thinking about internal control (see Appendix A). There are both similarities and differences among these documents. However, they are consistent in that they promote an expanded definition of internal control. Traditionally, internal control applied only to accounting activities. Today, internal control affects virtually every aspect of an organization's operations.

State agency managers and employees should view this information as a guide to assist them in managing their operations. This Guide is not intended to take the place of management's judgment or to dictate how management chooses to carry out its responsibilities. In addition to this Guide, my Office has developed a document that provides examples of control objectives, potential errors, and control activities to address the errors, for a number of operating cycles, e.g. revenue, disbursements, payroll, etc. Both the Guide and the supplemental document are available on the Office of Auditor of Accounts web page (www.state.de.us/auditor/) under the topic of Internal Controls.

For further explanation of any of the subjects discussed in this document, please refer to the referenced comprehensive literature on internal control listed in Appendix A.

PART I: INTERNAL CONTROL FRAMEWORK

In recent years, as governments have become more complex and as taxpayers have demanded more accountability, interest in internal control in government has increased. The public is now questioning the results and the performance of programs. Government managers not only need to account for funds spent on a program, but also to demonstrate the value of the program and its accomplishments. In order to succeed in both, government needs to manage its operations effectively. While there are numerous styles to manage effectively, they all have one common element - attention to internal control.

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, from executive management to support staff, have a responsibility for internal control. As organizations become more complex and introduce new processes, the need for internal control increases and the types of internal control activities become more sophisticated. For example, electronic commerce is currently in the forefront. While it presents new opportunities, it also poses new risks and challenges. Government organizations need to develop the means of controlling these risks. Although an internal control system can vary widely among organizations, the standards for a good system are generally the same. This Guide presents the minimum standards for a government organization.

Everyone has experience with internal control, often both in their daily business activities and in their personal lives. These standards are not new ideas; many of the concepts are currently part of existing government operations. This Guide should be used by State managers to evaluate their organization's internal control system. Any internal control elements not currently used by an agency should be added to its existing system.

What Is Internal Control?

In recent years, several professional organizations have published standards and guidelines on internal control and defined it in various ways. Those definitions are similar in recognizing that internal controls: are comprehensive, relate to achieving an organization's mission, and depend on people. Following is the definition of internal control we have derived from these professional documents. It is important to understand this definition in order to understand the subsequent concepts:

"Internal control is a process that integrates the plans, policies, attitudes, and activities of the people of an organization, working together to provide reasonable assurance that the organization will achieve its objectives regarding: reliability of financial reporting, compliance with applicable laws and regulations, and effectiveness and efficiency of operations."

This definition establishes that internal control:

- impacts all aspects of an organization - all of its people, and processes;
- is a basic element that permeates an organization - not a feature that is added on;
- depends on people and will be effective when everyone works together;
- does not guarantee, but provides reasonable assurance of success; and
- helps an organization achieve its objectives and mission.

Five elements have been identified as essential for achieving the objectives and mission of an organization on a long-term basis. These components are: Control Environment, Information and Communication, Risk Assessment, Control Activities, and Monitoring. They will be discussed in detail in subsequent sections of this Guide.

Why Have Internal Controls?

The ultimate purpose of internal control is as a means for achieving the organization's objectives and mission. The International Organization of Supreme Audit Institutions has identified the following specific purposes of internal control:

- to promote orderly, economical, efficient and effective operations;
- to produce quality products and services consistent with the organization's mission;
- to safeguard resources against loss due to waste, abuse, mismanagement, errors and fraud;
- to ensure compliance with laws, regulations, contracts and management directives; and
- to develop and maintain timely and reliable financial and management data.

An organization will most likely achieve its objectives and mission if it addresses each of these purposes in developing its internal control system. An organization may be at risk if any of these purposes is not addressed.

What Is Your Role?

Since every activity in an organization should be directed toward achieving its mission, all members of the organization have a role in the system of internal control.

Internal control depends on people. It is developed by people; it guides people; it provides people with a means of accountability; and people carry it out. Individuals' roles in internal control systems vary greatly throughout an organization. Obviously, the role of the agency head varies significantly from that of front-line staff.

The strength of an internal control system depends on people's attitude toward internal control and their attention to it. In this regard, executive management needs to set "the tone at the top". If executive management does not establish strong support for internal control, it is not likely that the organization, as a whole, will perform good internal control practices. Also, the system of internal control will not be effective if those responsible for control activities are not attentive to their duties. Furthermore, people can also deliberately defeat the internal control system. For example, a manager can override a control activity because of time constraints, or two or more employees can act together in collusion to circumvent control and "beat the system". To avoid these kinds of situations, the organization needs to continually monitor employee activity.

To some extent, everyone in an organization is responsible for ensuring the internal control system is effective. However, the organization's managers have the most responsibility. The agency head, as the lead manager, has the ultimate responsibility because he or she has been entrusted with achieving the organization's mission. To the extent that the agency head authorizes other individuals to manage the activities of the organization, those managers then become responsible for the portion of the internal control system that they administer.

Many employees believe internal control is the responsibility of the auditors who periodically review their activities. This may occur because they hear about internal control only during or after an audit. It is true that auditors routinely review an organization's internal control system and cite weaknesses in that system. However, it is the organization's management, not the auditors, who are responsible for establishing the system, and for preventing breakdowns in the system. To some extent, managers impact the integrity of the internal control system. Managers establish policies and plans, make decisions and create the work atmosphere which influence the internal control system. Therefore, managers are often held accountable for failures of the system.

In some cases, an agency may find it beneficial to assign the responsibility for coordinating the internal control activities of the agency to one individual. Typically, this individual's responsibilities would include providing assistance to establish a system of internal control, provide all employees with management policies and guidelines, implement internal control training, and establish a process for reviewing internal controls. However, the responsibility of all managers to oversee internal control in their operations is not diminished by the existence of such a position.

PART II: FIVE COMPONENTS OF INTERNAL CONTROL

As previously noted, five elements have been identified as essential for achieving the objectives and mission of an organization on a long-term basis. These components are: Control Environment, Information and Communication, Risk Assessment, Control Activities, and Monitoring. Details on each of these elements follow. For the most part, the discussion on these elements is based on the report Internal Control - Integrated Framework, issued September 1992, by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

CONTROL ENVIRONMENT

The COSO report states that the control environment sets the tone of an organization, influencing the control consciousness of its employees. It is the foundation of the other elements of internal control. Control environment factors include the integrity, ethical values and competence of the organization's people; management's philosophy and operating style; the way management assigns responsibility and authority, and organizes and develops its people. Following is additional information on both management's responsibilities for developing a good control environment and staff's responsibilities for helping to maintain it.

Ethical Values and Integrity

Essential elements of 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 excellence, commitment to honesty and fairness; leadership by example; recognition of and adherence to laws and policies; respect for authority; respect for employees' rights; and adherence to professional standards. Ethical values, such as these, guide employees when they make decisions on the job.

Management encourages integrity by: publishing a code of conduct; complying with the organization's code of conduct and ethical values; rewarding employee commitment to its ethical values; establishing a method for reporting ethical violations; and consistently disciplining for all violations of ethical values. It is management's responsibility to ensure that processes and activities serve to strengthen integrity.

Competence

An organization's management should ensure that its staff possesses the knowledge and skills to do their jobs. To do this, management must establish appropriate human resource policies and practices including: establishing the competence levels of jobs and translating those competence levels into the requisite knowledge and skill requirements; establishing training programs that help employees increase their knowledge and skills; and hiring and promoting only those with the required knowledge and skills.

Management should also ensure that staff have the other resources they need, e.g. equipment, computer hardware and software and policy and procedure manuals - to perform their jobs. Staff also need to have assurance that they can access the tools and support they need to perform their jobs.

Management Operating Style and Philosophy

Management's operating style and philosophy reflect management's beliefs on how to manage the people and activities of an organization. There are many styles and philosophies. Management should practice the most effective style and philosophy for the organization, making sure that they reflect the ethical values of the organization, and positively affect staff morale. Once an appropriate style and philosophy are established, management should implement them by communicating them to staff and by practicing them. Management needs to periodically re-evaluate whether the style and philosophy are effective and whether they are practiced.

Internal control can be affected by the level of risk management is willing to accept and the extent of economic or regulatory control imposed by external organizations. Other elements affecting the entity's philosophy and style include attitudes regarding the use of aggressive or conservative practices for reporting (both financial and program information). In addition, management's attitude toward reliability derived from data processing and accounting functions can significantly affect internal control.

As part of its philosophy and style, management should demonstrate a supportive attitude in order to encourage the achievement of the organization's mission. A supportive attitude fosters the atmosphere needed for a sound internal control system. This atmosphere can be created if top management demonstrates: minimal use of control overrides; an openness to internal reviews of controls and independent external audits and assessments of controls; prompt responsiveness to issues raised by audits and assessments; and ongoing training for employees to ensure they understand the internal control system and their role.

Management also needs to be aware of the importance of good morale in an effective control environment. Employees' attitudes about their jobs and their organization impact how well they do their jobs. Management needs to take actions to maintain high morale, and thereby ensure employees are committed to achieving the organization's objectives. Management needs to provide staff with a sense that: their opinions and contributions are welcomed, valued and recognized; the organization is willing to help them improve; continuous improvement is desired; they have an important stake in the organization; and the organization's appraisal and reward systems are fair.

Organizational Structure

Structure is the framework in which the organization's plans are carried out. It should define the functional subunits of an organization and the relationships between them. Typically, an organization's structure is presented in the form of a chart. An organization chart should provide a clear picture of authority and functional relationships. The chart should be used to help

employees understand the organization as a whole, and where they fit in. The organization chart should be updated as the organization changes.

In order to accomplish its mission, management must delegate the following throughout the organization: authority, responsibility for operating activities, reporting relationships, and authorization activities. Each employee needs to know how his or her actions impact others and how they contribute to achieving objectives. As the delegation of authority and responsibility is increasingly distributed throughout the organization, management needs procedures to monitor results. Individuals should be held accountable for their decisions and actions.

Delegating authority and responsibility implicitly requires management to provide supervision and to monitor results. Supervision helps ensure that employees know their duties and responsibilities and how they are accountable.

INFORMATION AND COMMUNICATION

Communication is the exchange of relevant information among people and organizations to coordinate activities and to provide a supporting basis for decisions. Communication occurs within an organization, and with parties external to that organization, e.g. customers, suppliers, and oversight organizations.

Information can be transmitted verbally and in writing. Verbal communication may be sufficient for most day-to-day activities, however, important information should be in writing. This provides a permanent record and enables all members of the organization to review the information. Within an organization, information should flow in all directions to ensure that everyone in the organization is kept informed and that the actions of different organization subunits are communicated and coordinated.

Good communication is necessary for an organization to maintain an effective internal control system, and therefore, to achieve its mission and objectives. A communication system consists of the records and procedures established to identify, retain and exchange useful information. Information is useful when it is provided timely, and in a format - sufficiently detailed and appropriate to the user - to enable them to carry out their responsibilities.

- Information is timely when it is available when the user needs it. Based on the specific situation, timeliness can be achieved if the data is current or is provided at a time when it is most beneficial.
- Sufficiently detailed information provides enough detail to help the user achieve his or her responsibilities and objectives. However, information should not be so detailed that it becomes unmanageable. Information must be tailored to the user's needs; different levels of employees require different types of information to do their jobs. For example, managers may rely on broad or summary information to monitor performance. However, front-line employees may need detailed information to carry out their responsibilities.

Communication and Internal Control

Management is responsible for establishing communication channels that provide information to all members of the organization. Management and staff should use these communication channels to provide relevant information to those who need it. These internal communication channels should: convey top management's message that internal control responsibilities are important; inform employees of their duties and responsibilities; report sensitive matters; enable employees to provide suggestions; and provide the information employees need to effectively carry out their responsibilities.

Parties external to the organization may also need reliable and timely information relevant to their specific needs. Therefore, the organization's management also needs to establish specific communication channels for these external parties.

Communication affects every aspect of an organization's operations and can help support its internal control system. A good communication network can be used to help management circulate guidance about internal control issues. Furthermore, feedback from this network can help management determine how well the internal control system is working, and where improvement is needed. Following is a description how communication impacts the other internal control components.

Control Environment

Good communication channels enable management to tell employees about the organization's plans, objectives, policies and procedures. Management can also tell employees about their jobs, including their job descriptions, the purpose of their work and the importance of how their work efforts contribute to achieving the organization's mission and objectives.

Communication channels should be used to distribute the organization's ethical values, codes of conduct and standards of discipline. Management also needs to establish processes for employees to report sensitive breaches of internal controls, such as unethical behavior, without retribution. To maintain effective communication, management must also be receptive to negative feedback, such as employee complaints and unfavorable customer feedback.

Risk Assessment

Good communication channels help managers identify new risks or changes in existing risks. Managers can communicate these new risk-related issues and proposed actions to address these issues to management and/or those who carry out risk management activities.

Control Activities

A good communication network enables management to explain control activities and responsibilities to those members of the organization who must carry them out and those who are affected by them. A good network will also alert management when a control activity needs improvement.

Monitoring

The monitoring component involves significant communication. Operations staff need to communicate the details of their work activities to supervisors. Supervisors need to communicate the results of their monitoring in two directions - to operating staff to correct errors and/or reinforce appropriate work activities, and to the next level of management to report operating results, including objectives achieved or problems identified. Management needs to respond to supervisors and staff about any changes to plans or objectives as a result of monitoring activities.

RISK ASSESSMENT

Risks threaten the accomplishment of an organization's mission and objectives. Risk assessment involves identifying, evaluating and determining how to manage risks. Risks can be external or internal. Risks exist at every level within an organization. Management should seek to prevent risks, however, it may not be possible to prevent risks from occurring. When that happens, management needs to decide whether to take steps to reduce the risk to an acceptable level, avoid the risk, or accept the risk. By ensuring that each risk is assessed and properly addressed, management will have reasonable assurance that the organization will achieve its mission and objectives.

How Does An Organization Prepare For Assessing Risks?

To properly assess risk, management needs to not only identify all its organizational and operational objectives, but its control objectives as well. Generally, control objectives are derived from the previously stated purposes of internal control. These control objectives are stated in a format that reflects responsibilities of the organization's units. Following are examples of control objectives in this format:

Purpose: "To promote orderly, economical, efficient and effective operations.≡ A control objective that addresses this purpose, but is stated in terms specific to a unit within the organization might be: Obtain five written price quotes for all purchases exceeding \$10,000.

Purpose: "To produce quality products and services . . ." A control objective that addresses this purpose might be: Ensure that eligibility for services are properly determined.

Purpose: "To safeguard assets against loss . . ." A control objective that addresses this purpose might be: Ensure access to sensitive equipment is properly controlled.

Purpose: "To ensure compliance with law, regulations . . ." A control objective that addresses this purpose might be: Ensure that receipts are deposited daily.

Purpose: "To develop and maintain timely and reliable financial and management data." A control objective that addresses this purpose might be: Ensure that computer applications process financial and management data accurately and completely.

After identifying all of the objectives, managers need to determine all risks (both external and internal) associated with each objective. External risks include natural disasters, changes in laws, etc.; internal risks include fraud, human error, computer system malfunctions, etc.

What Is Included In The Risk Assessment Process?

There are two primary elements in evaluating risks: (1) the significance of the risk and (2) the likelihood that the risk will occur. All risks identified through the process discussed above need to be evaluated.

Significance represents the magnitude of the impact (extent of harm done or lost opportunity) on the organization if the unfavorable event were to occur. The organization should attempt to quantify the significance, and if not possible, specifically indicate what the effect(s) will be.

Likelihood is the degree that an unfavorable event may occur if there are no controls (see the "Control Activities" section) to prevent or reduce the risk from occurring. The likelihood for each identified risk needs to be estimated.

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.

Once management has identified the significance and likelihood for all risks, it needs to prioritize the risks. Generally, risks should be ranked from those risks having the greatest potential impact and the highest likelihood to occur to those with a low impact and the least likelihood to occur. Management should use the information obtained from this process to help determine: how to manage risk; how to prevent or reduce risk; and the frequency of evaluations.

How Does An Organization Manage Risk?

Top management should provide direction to help managers determine whether risks are acceptable or not. Based on this direction, managers can determine what actions are to be taken with respect to each identified risk - reduce the risk, avoid the risk or accept the risk. Examples of scenarios of how decisions may be reached for the following risk: "unauthorized persons will gain access to equipment and/or supplies":

Reduce the Risk:

This is accomplished by establishing controls. In this case, the manager decided that because of the sensitivity of equipment and supplies - cost, transportability, desirability, etc. - the risk of unauthorized access to the equipment was not acceptable. In such a case, the manager would establish controls, such as physical security, inventory records, etc., to reduce the risk. The risk will be reduced as long as the controls continue to work.

Avoid the Risk:

In this case, the manager has determined unauthorized access is not acceptable, but sufficient controls cannot be put in place to preclude unauthorized access. For example, the organization may use a highly toxic substance in its processes. In this case, the manager may decide that: (1) it would be too costly to establish controls to prevent unauthorized access, and (2) the potential impact of unauthorized access to a supply of this toxic substance- widespread disease and/or death, is not acceptable. The manager may decide not to store the substance on site, but to make arrangements for prompt delivery on an as needed basis.

Accept the Risk:

In this case, controls are not established. The manager may determine that equipment and supplies are not sensitive, and the cost associated with establishing controls over the items in inventory exceeds the cost of the impact should unauthorized access occur.

What Is The Process For Reducing Risk?

When an organization determines that the proper course is to reduce risk, it needs to identify the most efficient and effective control activities to address the risk. Following are three questions that management needs to answer to assist in identifying the most appropriate control activities:

What is the cause of this risk?

Management needs to know why the risk exists in order to identify all possible control activities that could prevent or reduce the risk.

What is the cost of control vs. the cost of the risk's impact?

Management should compare the cost of carrying out various control activities with the cost of the risk's impact. Based on that comparison, management should select the most cost-effective choice.

What is the priority of this risk?

Management should allocate resources among control activities based on its list of prioritized risks. The higher the priority of the risk, the greater the level of resources and control activities that should be applied to reduce the risk.

Since they are key to risk management decisions, management should maintain documentation of its analyses and interpretation of the risk assessment information. Also, management needs to

periodically review these decisions to determine whether they are still appropriate, or whether alternatives are needed. This is particularly important when an organization is undergoing change. In such a case, management needs to monitor how each change affects risk. As part of this process, management should keep people informed of proposed changes, and solicit input on how those changes might impact risks. Finally, managers should monitor the environment for factors that could impact risks affecting their respective unit.

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.

Management should also closely monitor and evaluate control activities to ensure they are functioning properly and that things, such as managerial overrides, collusion or careless judgments, are not compromising their effectiveness. (Refer to the "Monitoring" and "Evaluation" sections for further details on how this should be done.)

When designing and implementing control activities, management should try to get the maximum benefit from the control activities it establishes 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 organization 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 distribution of resources among the control activities should be based on the significance and likelihood of the risk it is preventing or reducing. (Refer to the "Risk Assessment" section for more details.)

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.

There is no one control activity that 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. However, 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 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 activities, 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 superiors. 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 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 which 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 concepts of directive, preventive, detective and corrective controls, as well as the control activities described above, apply 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 controls over computer systems are interrelated. If general controls are inadequate, application controls are unlikely to function properly and could be overridden. Application controls assume that general controls will function properly and provide immediate feedback on errors, mismatches, incorrect format of data, and inappropriate data access (by unauthorized persons). Therefore, general controls support the functioning of application controls, 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 an 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 a framework of generally applicable and accepted standards for good practices for IT controls 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 that 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 that 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, which 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.
- 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.

The above examples are representative of output controls; some agencies may use different terminology to describe these controls.

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, 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 members, 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 staffs 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.

PART III: SUPPORTING ACTIVITIES

There are two additional elements that support a good internal control system - evaluation and strategic plans. They provide management with tools to help ensure that the mission and objectives of the organization will be achieved.

EVALUATION

The purposes of evaluation are to provide management with a reasonable assurance that the organization will likely achieve its mission, plans, goals and objectives; and the organization's system of internal control is functioning effectively. Evaluations can also identify both risks to the organization and opportunities for improvement.

How Is Evaluation Different Than Monitoring?

Monitoring involves performing routine or daily procedures, e.g. supervision and transaction review, to help ensure activities comply with the organization's internal control system. On the other hand, evaluation is a periodic assessment of an organization's performance over time.

What Is An Evaluation About?

The purpose of an evaluation is to answer the question: "Are we doing things the way we should to accomplish our mission and objectives?" An evaluation can be accomplished through a self-assessment or an independent assessment. A self-assessment is the process where an organization evaluates itself. Independent assessments are evaluations performed by individuals who are not directly involved in the organization's operations.

Self-assessment should play the primary role in evaluation. Regularly scheduled self-assessments help management detect and correct problems early. This will minimize the costs that might be incurred if problems were allowed to continue until independent assessments are performed. Self-assessments should be conducted throughout the organization; the frequency of self-assessments should be based on the results of the organization's risk assessment.

Independent assessments can be performed by an organization's internal auditors, provided they are independent of the activity being evaluated. Independent assessments can also be performed by external auditors and consultants who are not part of the organization. Independent assessments should not be a substitute for routine self-assessments, but should supplement them. Management should perform the following self-assessments:

- Assessing the Internal Control System

The process is initiated by management first identifying assessable activities within the organization - the concept of assessable activities is discussed later in this section. The managers of assessable activities should be responsible for determining the effectiveness of the internal control system within their respective units. In performing this

self-assessment, managers should obtain answers to questions about the integrity of each aspect of internal control. The reference materials cited in this document, particularly the COSO report, provide examples of questions that the managers should ask.

The objective of this self-assessment is to provide management with the ability to determine the effectiveness of the internal control system, and identify and correct any weaknesses within the system. Management should ensure that the internal control system is effective before proceeding to the next self-assessment - is the mission being accomplished?

- Assessing Whether the Mission Is Being Accomplished

Management needs to regularly assess whether the mission is being accomplished at all levels of the organization. At the operating level, management should compare the actual results of the specific sections, units and subunits to their operational plans and objectives. For larger organizational units, such as divisions, management should compare the actual results with the strategic plans and organizational objectives. If the internal control system is working effectively, management will have reasonable assurance that it is using accurate information to determine the organization's accomplishments. If deficiencies are identified through these self-assessments, their cause and remedy should also be determined. Such deficiencies should be followed-up and resolved.

- Assessing Risk and Opportunities

Management also needs to assess how effectively the organization identifies and responds to new risks and opportunities. As part of these assessments, management should 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; the 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 this process, top management should also perform an overall assessment of the organization. This overall assessment is intended to help top management: determine whether newly identified opportunities should result in changes in the organization's direction, including its mission, strategic plans and/or its objectives; and question the assumptions used to develop the mission, strategic plans and objectives.

How Are Self-Assessments Documented?

Management should establish a formal plan for performing self-assessments and ensure that it performs all aspects of its plan. Such a plan should define: responsibilities; evaluation methodologies to be used, the sources and types of information needed for accurate assessments; reporting requirements, and the method for ensuring any deficiencies identified are promptly

corrected. Generally, the results of self-assessments should be formalized into a written document.

How Are Evaluation Results Communicated and Used?

The results of all assessments, whether good or bad, need to be communicated. Positive results should be communicated both to reinforce good practices and to foster good morale. When results show a need for improvement, management should give the information to those who are responsible for making the necessary changes that will lead to improvement. Management should develop a standard process for communicating the results of assessments - both self-assessments and independent assessments.

Management should also have a process to ensure that deficiencies identified in assessments are promptly and appropriately addressed. As part of this process, management should follow-up on any corrective actions to determine whether they have produced the desired results.

Where assessments indicate major organizational changes are needed, management needs to ensure such results are considered when changing or establishing new plans and organizational objectives.

What Is An Assessable Activity?

To facilitate an evaluation of an organization's system of internal control, management should segment the organization into "assessable activities". Assessable activities are not usually the functional subunits found on an organization chart (e.g., division, section, and unit), but are segments of them. For example, a section may have more than one assessable activity, each of which represents a distinct function.

An assessable activity has certain primary characteristics. It has an ongoing purpose that results in the creation of a service or product (internal or external) and/or that fulfills a stated requirement, e.g. a law or regulation. An assessable activity should be large enough to allow managers to evaluate a significant portion of the activity being examined, but not so large that extensive time and effort must be expended on the evaluation.

STRATEGIC PLANS

Strategic plans are the courses of action that will enable an organization to achieve its mission, objectives and goals. Generally, 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 mission and broad organizational key objectives and developing the strategies that should be followed to achieve the mission and key objectives. Based on the direction provided by the organization's strategic plan, strategic plans should be developed for each major organizational division with a long-range focus specific to that division. Division managers should use the division strategic plans as a guide to developing short-range operational plans for each of the division's major functions. As part of the strategic

planning process, the organization needs to develop performance measures that provide meaningful information concerning whether objectives are being achieved and how programs are working.

The State of Delaware's Office of the Budget has developed Strategic Planning Guidelines which set forth the process that Delaware State agencies should follow to develop their strategic plans. These Guidelines include information concerning the attributes and development of performance measures. We refer you to these Guidelines for details on the strategic planning process for Delaware State agencies.

Appendix A

REFERENCES

Internal Control - Integrated Framework issued in September 1992 by the Committee of Sponsoring Organizations of the Treadway Commission (commonly referred to as COSO)

Guidance on Control issued in November 1995 by the Canadian Institute of Chartered Accountants (commonly referred to as COCO)

Guidelines for Internal Control Standards issued in June 1992 by the International Organization of Supreme Audit Institutions

Report by the Committee on Financial Aspects of Corporate Governance issued in December 1993 (commonly referred to as the Cadbury Report)

Governance, Control and Audit for Information and Related Technology issued in April 1998 by the Information Systems and Control Association (commonly referred to as the COBIT Report)

Strategic Planning Guidelines, issued December 1997, by the Delaware Office of the Budget