State of Michigan

Office of Financial Management

Understanding Internal Controls

Self –Study

OVERVIEW.....1

BACKGROUND.....2

INTERNAL CONTROL DEFINED.....3

INTERNAL CONTROL COMPONENTS.....4

CONTROL ENVIRONMENT.....5

RISK ASSESSMENT.....5

CONTROL ACTIVITIES.....6

INFORMATION AND COMMUNICATION.....6

MONITORING.....7

HARD AND SOFT CONTROLS.....8

ROLES AND RESPONSIBILITIES.....10

RISK.....10

RISK ASSESSMENT PROCESS.....11

INTERNAL AUDIT AND RISK ASSESSMENT PROCESS.....13

BIENNIAL REPORTING REQUIREMENTS.....14

Overview

This self-study is useful to personnel desiring to increase their understanding of State of Michigan internal control evaluation practices. The purpose of *Understanding Internal Controls* is to assist employees in their stewardship role in achieving the State's objectives. It also serves to provide guidance for the existence of basic and consistent business controls throughout the State and to define responsibilities for managing them.

This guide is designed to satisfy basic objectives of most business systems as they relate to carrying out the work of the State and addresses five interrelated components of a business system:

- The organization's operating environment.
- Goals, objectives, and related risk assessment.
- Controls and related policies and procedures.
- Information systems and communication methods.
- Activities to monitor performance.

Understanding Internal Controls is based upon the internal control guidelines as recommended by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission (a federally sponsored group of business, government, and non-profit representatives responsible for development of an internal control assessment methodology). COSO was formed to support the Commission's recommendation to develop additional, integrated guidance on internal control. This organizational approach provides the State with a common, accepted, and recommended reference point to assess the quality of its internal control systems.

Objectives of *Understanding Internal Controls*:

I. Convey that management is responsible for ensuring that internal controls are established, properly documented, maintained, and adhered to in each office, agency, and Department.

II. Convey that all State employees are responsible for compliance with internal controls.

Background

In accordance with the Management and Budget Act, biennially, state departments report on evaluations of their system of internal controls. The Management and Budget Act states that each principal Department shall:

- Develop a system of reporting and general framework in performing evaluations on their respective accounting and administrative control systems.

- Establish and maintain an internal control system within the principal department.

- Provide a biennial report prepared by the principal department's internal auditor on the evaluation of the principal department's internal control system to the Governor, the Auditor General, the Senate and House Appropriations Committees, and the Director. The report shall include, but not be limited to, the following:

  - ✓ A description of any material inadequacy or weakness discovered in connection with the evaluation of the Department's internal control system as of October 1 of the preceding year, plans and a time schedule for correcting the internal accounting and administrative control system, described in detail.

  - ✓ A listing of each audit and investigation performed by internal audit pursuant to Sections 486(4) and 487.

The Act requires each principal department to maintain *documentation of its internal control system*. Meaningful documentation of the internal control system facilitates management's ability to document risks and controls, to effectively react to changes in the system, and substantiate conclusions about the effectiveness of the department's internal control system.

In December 1999, the State adopted a new framework to comply with provisions of the Management and Budget Act. The new framework encourages the use of the COSO model.

The DMB framework emphasizes that the system of internal control, in any organization, is intended to provide reasonable assurance regarding achievement of objectives related to effective and efficient operations, reliable financial reporting, and compliance with laws, rules, and regulations.

Internal Control Defined

Internal control is a process designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

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

I. ***People at every level of an organization affect internal control***. Internal control is, to some degree, everyone's responsibility. Within the State of Michigan the director or head of each principal department is the "owner" of the internal control system for the department. Other managers are responsible for internal control in their area of responsibility. The CFO and CIO have broad control responsibilities. Non-managerial personnel also play a role in the process of internal control.

II. ***Effective internal control helps an organization achieve its operating, financial reporting, and compliance objectives***. Effective internal control is a built-in part of the management process (i.e., planning, organizing, directing, and controlling). Internal control keeps an organization on course towards its objectives achieving its mission, and minimizing surprises along the way. Internal control promotes effectiveness and efficiency of operations, reduces risk of asset loss, helps ensure compliance with laws and regulations, and ensures the reliability of financial reporting (i.e., all transactions are recorded and all recorded transactions are valid, properly valued, timely, properly classified, and correctly summarized and posted).

III. ***Internal control can provide reasonable assurance – not absolute assurance – regarding achievement of an organization's objectives.*** Effective internal control helps an organization achieve its objectives; it does not ensure success. There are several reasons why internal control cannot provide absolute assurance that objectives will be achieved: cost/benefit realities, collusion among employees, or external events beyond organizational control.

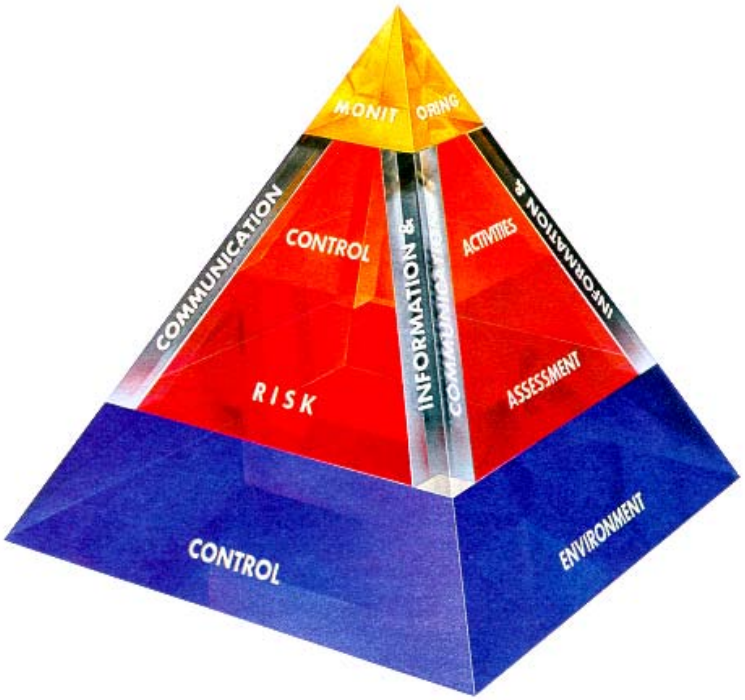
Components of Internal Control

Internal control consists of five interrelated components:

- Control environment.
- Risk assessment.
- Control activities.
- Information and communication.
- Monitoring.

All five components must be present to conclude that internal control is effective.

<u>From the COSO Report</u>



Control Environment

The control environment is the control consciousness of an organization; it is the atmosphere in which people conduct their activities and carry out their control responsibilities.

An effective control environment is an environment where competent people understand their responsibilities, the limits to their authority, and are knowledgeable, mindful, and committed to doing what is right. They are committed to following an organization's policies and procedures and its ethical and behavioral standards. The control environment encompasses technical competence and ethical commitment; it is an intangible factor essential to effective internal control.

Management is responsible for "setting the tone" for their organization. Management should foster a control environment that encourages:

- Highest levels of integrity and personal and professional standards.
- Leadership philosophy and operating style that promote internal control throughout the organization.
- Assignment of authority and responsibility.

Effective human resource policies and procedures enhance an organization's control environment. These policies and procedures address hiring, orientation, training, evaluations, counseling, promotions, compensation, and disciplinary actions. In the event that an employee does not comply with an organization's policies and procedures or behavioral standards, an organization must take appropriate disciplinary action to maintain an effective control environment. The control environment is greatly influenced by the extent to which individuals recognize that they will be held accountable.

Risk Assessment

Risk assessment is the identification, analysis, and management of risks relevant to an organization's business process or activities.

The fundamental theme of internal control is to identify risks to the achievement of an organization's objectives and to manage those risks. Thus, setting goals and objectives is a precondition to internal controls.

Departments must be aware of and deal with the risks they face. They must set objectives, integrated with financial and other activities, so that the organization is operating in a coordinated manner, and establish mechanisms to identify, analyze and manage related risks.

Control Activities

Control activities are actions, supported by policies and procedures that, when carried out properly and in a timely manner, manage or reduce risks. Control policies and procedures must be established and executed. This will help ensure that actions identified by management, as necessary to address risks (related to achievement of Department objectives) are effectively carried out.

In the same way that managers are primarily responsible for identifying the financial and compliance risks for their operations, they also have responsibility for designing, implementing, and monitoring an internal control system. Control activities include approvals, authorizations, verifications, reconciliations, reviews of performance, security of assets, segregation of duties, and controls over information systems.

Controls can be preventive or detective. Preventive controls attempt to deter or prevent undesirable events from occurring. They are proactive controls that help to prevent a loss, i.e., separation of duties, proper authorization, adequate documentation, and physical control over assets. Detective controls attempt to detect undesirable acts. They provide evidence that a loss has occurred, but do not prevent a loss from occurring, i.e, reviews, variance analyses, reconciliations, physical inventories, and audits.

Both types of controls are essential for an effective internal control system. From a quality standpoint, preventive controls are essential because they are proactive and emphasize quality. Detective controls play a critical role in providing evidence that preventive controls are functioning and preventing losses.

Information and Communication

Information and communication are essential to effecting control; information about an organization's plans, control environment, risks, control activities, and performance must be communicated up, down, and across an organization. Reliable and relevant information from both internal and external sources must be identified, captured, processed, and communicated to the people who need it—in a form and timeframe that is useful. Information systems produce reports containing operational, financial, and compliance-related information that makes it possible to run and control an organization.

Information and communication systems can be formal or informal. Formal information and communication systems – which range from sophisticated computer technology to simple staff meetings – should provide input and feedback data relative to operations, financial reporting, and compliance objectives; such systems are vital to an organization's success. Informal conversations with customers, suppliers, regulators, and employees often provide some of the most critical information needed to identify risks and opportunities.

Monitoring

Monitoring is the assessment of internal control performance over time; it is accomplished by ongoing activities and by separate evaluations of internal control such as self-assessments, peer reviews, and internal audits. The purpose of monitoring is to determine whether internal control is adequately designed, properly executed, and effective. Internal control is properly executed if all five internal control components (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring) are functioning as designed. Internal control is effective if management and interested stakeholders have reasonable assurance that:

- The extent to which operations objectives are being achieved is understood.
- Published financial statements are prepared reliably.
- Applicable laws and regulations are complied with.

While internal control is a process, its effectiveness is an assessment of the condition of the process at some point in time.

Just as control activities help to ensure that actions to manage risks are carried out, monitoring helps to ensure that control activities and planned actions to effect internal control are carried out properly, in a timely manner, and that the end result is effective control. Ongoing monitoring includes various management and supervisory activities that evaluate and improve the design, execution, and effectiveness of internal control. Self-assessments and internal audits are periodic evaluations of internal control components resulting in a formal report on internal control. Department employees perform self-assessments; internal auditors who provide an independent appraisal of internal control perform internal audits.

Hard and Soft Controls

The COSO report, *Internal Control – Integrated Framework* has established and defined an overall framework and philosophy that organizations can use to manage risks and achieve objectives. This document clearly indicates that the key to organizational effectiveness goes beyond the tangible, measurable controls that have been the traditional purview of internal auditors. This document emphasizes the importance of "soft" or "behavioral" controls, like trust and effective leadership that are difficult to evaluate.

Soft controls focus on ethics, integrity, competency, and relationship building (internally and externally). Soft controls deal with how management knows that employees are adhering to the entity's policy on ethics.

Hard controls deal more with the tangibles–Existence of policies and procedures, proper document/payment approval, segregation of duties, etc. Hard controls are controls over systems, processes, and/or procedures, that when applied correctly demonstrate that a specific organization policy or procedure is being adhered to. Examples follow:

- Requiring employees to acknowledge by signature that they have read the entity's code of conduct.
- Requiring employees to provide evidence of receiving training in specific areas.
- Documented approval by a specified responsible party.
- Double signatures by responsible parties for disbursement checks above specific dollar amount.
- Requiring matching of documents, before paying a vendor invoice.

With COSO's emphasis on employee and managerial behavior, soft controls and soft controls testing, take on a greater significance for internal and external auditors. Examples follow:

- **Knowledge and competence performance standards** used for hiring and promotion.
- Performance standards distributed to employees outlining **appropriate ethical behavior.**
- Employees and managers periodically tested to determine **awareness** of environmental risks and related procedures.
- Education and training **competencies** established for all employees and managers.
- Feedback solicited from personnel to determine if they are adapting to **changing operating conditions.**
- **Feedback** solicited from customers, suppliers, and others to determine if employees and managers are adhering to policies and procedures.

Roles and Responsibilities

All state employees are responsible for managing internal controls. Each office, agency, or department director or head is specifically responsible for ensuring that internal controls are established, properly documented, and maintained in each organization. **Director or head of principal department** is the "owner" of the internal control system for that Department. **Managers** are responsible for internal control in their area of responsibility. The CFO and CIO have broad control responsibilities.

Internal Auditors play an important role in evaluating the effectiveness of control systems and thereby contribute to their ongoing effectiveness. They are primarily responsible for assisting management in their oversight and operating responsibilities through independent audits and consultations designed to evaluate and promote internal control systems.

Risk

Risk is defined as the probability that an event or action may adversely affect the organization.

Effects of risk may involve:

- An erroneous decision.
- Erroneous record keeping, inappropriate accounting, fraudulent financial reporting, financial loss and exposure.
- Failure to safeguard assets appropriately.
- Failure to adhere to organizational policies and procedures.
- Failure to comply with relevant laws, rules, and regulations
- Failure to accomplish objectives and goals.
- Customer dissatisfaction, negative publicity, damage to reputation.
- Acquiring and utilizing resources uneconomically and inefficiently.

Risk factors are criteria used to identify the relative significance of, and likelihood that conditions and/or events could adversely affect the organization.

Risk factors include:

- Ethical climate.
- Pressure on management to meet objectives.
- Competence, adequacy, and integrity of personnel.
- Asset size, liquidity, transaction volume.
- Financial and economic conditions.
- Competitive conditions.
- Complexity or volatility of activities.
- Impact of customers, suppliers, and government regulations.
- Degree of computerized information systems.

- Geographical dispersion of operations.
- Adequacy and effectiveness of the internal control system.
- Management judgments and accounting estimates.
- Acceptance of audit findings and corrective action taken.
- Date and results of previous audits.

Types of Risks

I. Inherent Risk

The risk found in the environment and in human activities that is part of existence.

II. Control Risk

The tendency of the internal control system to lose effectiveness over time, and to expose or fail to prevent exposure of the auditable activity.

III. Detection Risk

The probability that an incorrect conclusion will be drawn from results of audit activities. The process itself does not detect weaknesses within internal controls.

Risk Assessment Process

In 1992, COSO outlined five essential components of an internal control system. One component is Risk Assessment, defined as a process to identify, analyze, prioritize, and manage risks. Management is responsible for ensuring that overall risks within their organization are properly assessed and managed.

I. Determine Goals and Objectives

At the highest levels, goals and objectives should be presented in a strategic plan that includes a mission statement and broadly defined strategic initiatives. At the Department level, goals and objectives should support the organization's strategic plan. Goals and objectives are classified in the following categories:

- ***Operations objectives*** pertain to achievement of the basic mission(s) of a Department and the effectiveness and efficiency of its operations, including performance standards and safeguarding resources against loss.

- ***Financial reporting objectives*** pertain to preparation of reliable financial reports, including the prevention of fraudulent public financial reporting.

- ***Compliance objectives*** pertain to adherence to applicable laws and regulations.

Clear goals and objectives are fundamental to the success of a department. Specifically, a department or work unit should have a mission statement; written goals and objectives for the department as a whole; and written goals and objectives for each significant activity in the department. Goals and objectives should be expressed in terms that allow meaningful performance measurements.

Certain activities are significant to all Departments: budgeting, purchasing goods and services, hiring, evaluating employees, accounting for vacation/sick leave, and safeguarding property and equipment. Thus, Departments should have appropriate goals and objectives, policies and procedures, and internal controls over these areas.

II. Identify Risks after Determining Goals

Who is responsible? To properly manage their operations, managers should determine a level of operations, and financial and compliance risks they are willing to assume. Risk assessment is management's responsibility and enables management to act proactively in reducing unwanted surprises. Failure to consciously manage risks can result in a lack of confidence that operational, financial, and compliance goals will be achieved.

A risk assessment can be used to:

- Determine which area within a business process should be reviewed.
- Design tests to verify the adequacy of identified controls.
- Support a cyclical approach to auditing.

Risk Identification. A risk is anything that could jeopardize the achievement of an objective. For each of the department's objectives, risks should be identified. Asking the following questions helps to identify risks:

- What could go wrong?
- How could we fail?
- What must go right for us to succeed?
- Where are we vulnerable?
- What assets do we need to protect?
- Do we have liquid assets or other assets?
- How could someone steal from the Department?
- How could someone disrupt our operations?
- How do we know whether we are achieving our objectives?
- On what information do we most rely?
- On what do we spend the most money?
- What activities are most complex?
- What activities are regulated?
- What is our greatest legal exposure?

Risk identification must be comprehensive at the department level and at the activity or process level (for operations, financial reporting, and compliance objectives). Both external and internal risk factors need to be considered.

III. Risk Analysis

After risks have been identified, an analysis should be performed to prioritize risks:

- Assess the likelihood (or frequency) of the risk occurring.
- Estimate potential impact if the risk were to occur; consider quantitative and qualitative costs.
- Determine how the risk should be managed; determine what corrective actions are necessary.

Prioritizing helps Departments focus attention on managing significant risks (i.e., risks with reasonable likelihood of occurrence with large potential impact).

Internal Audit and Risk Assessment Process

The internal auditor's role is to ensure that the Department has sufficient and continuous internal audit coverage over those areas judged to have a high risk profile or that otherwise require internal audit attention based on management or legislative requirements.

The internal audit risk assessment process serves as an aid to management and internal auditors in evaluating and planning internal audit activities. Information produced by the risk assessment process provides a basis for interpreting whether sufficient internal audit coverage has been established, based upon risk, and whether internal audit activities and resources are directed toward areas of greatest risk.

Objectives of the internal audit risk assessment process:

- Focus limited internal audit resources on areas of greatest exposure.
- Evaluate sufficiency of internal audit plans and resources.
- Support management's responsibilities for establishing sufficient internal audit coverage.
- Conform with legislative guidelines and professional standards.

Risk assessment can be used to determine which areas within a business process should be reviewed to design tests to verify the adequacy of identified controls and to support a cyclical approach to auditing. However, this process should never replace professional judgment or specific priorities established in the determination of internal audit activities.

Reporting – Biennial Reporting Requirements

The Management and Budget Act requires the head of each principal state department to issue a report (to the Governor, the Office of the Auditor General, Senate and House Appropriation Committees, and the DMB Director) summarizing results of its evaluation of the Department's internal control structure. The report is due May 1 (each odd number year) based on an evaluation of the system as of October 1 (of previous year). This report must be accompanied by a second report, prepared by the department's internal auditor, describing the adequacy of the evaluation process. (The reporting process is further detailed in the *Administrative Guide*, procedure 1270.01.)

A department's evaluation (regardless of the evaluation tools used and internal reports maintained) must provide the basis for departmental leadership to conclude whether the internal control structure has been designed to prevent or detect potential risks and whether controls are working as prescribed. Internal controls must provide a reasonable assurance that measures are being used to:

- Develop reliable financial reports.
- Promote effective and efficient operations, including safeguarding of State assets.
- Encourage compliance with applicable laws, rules, and regulations (including prescribed managerial policies).

This information must be documented and reported on an ongoing basis or during the biennial assessment process.