COMPTROLLER of MARYLAND

Serving the People

Internal Control Manual
For Use by State Departments
And Independent Agencies

Volume I

Peter Franchot
Comptroller

General Accounting Division
March, 2008

STATE OF MARYLAND
INTERNAL CONTROL MANUAL FOR USE BY STATE DEPARTMENTS AND INDEPENDENT AGENCIES

TABLE OF CONTENTS

Volume II – Forms:

SECTION I

INTRODUCTION

I. Introduction

The ***Internal Control Manual for Use by State Departments and Independent Agencies*** was developed by the Comptroller's Office to provide the necessary guidance for the development, implementation and maintenance of a sound system of internal control. This manual has been revised to reflect the guidance in OMB Circular No. A-123, revised December 21, 2004, and for other changes in the State environment.

Internal Control affects every aspect of State government operations. It assures that the State functions efficiently and economically, satisfying the requirements of its constitution, laws, policies, rules, regulations, and contracts. Citizens, taxpayers, public officials, and others in state government are concerned about how well the State uses scarce and valuable resources. Investors in state bonds and organizations that rate the bonds are concerned about the financial well being of the State. Federal officials want to know that adequate controls exist to assure that grants are administered in compliance with federal laws, rules and regulations. State legislators want assurance that the programs they enact are being properly administered.

Management has a fundamental responsibility to develop and maintain effective internal control. The proper stewardship of State resources is an essential responsibility of agency managers and staff. Programs must operate and resources must be used consistent with agency missions, in compliance with laws and regulations, and with minimal potential for waste, fraud, and mismanagement.

Effective internal control provides assurance that significant weaknesses in the design or operation of internal control that could adversely affect the agency's ability to meet its objectives, would be prevented or detected in a timely manner.

The three objectives of internal control are to ensure the:

- **effectiveness and efficiency of operations,**
- **reliability of financial reporting, and**
- **compliance with applicable laws and regulations.**

Internal Control - The organization, policies, and procedures which are tools to help program and financial managers achieve results and safeguard the integrity of their programs. This Manual provides guidance on using the range of tools at the disposal of agency managers to achieve desired program results and implement accounting and administrative controls. Such controls are included in program, operational, and administrative areas as well as accounting and financial management.

The agency head must establish controls that reasonably ensure that:

"(i) obligations and costs are in compliance with applicable law; (ii) funds, property, and other assets are safeguarded against waste, loss, unauthorized use or misappropriation; and (iii) revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets."

In addition, the agency head must evaluate and report on the control and financial systems that protect the integrity of State programs.

Instead of considering internal control as an isolated management tool, agencies should integrate their efforts to meet the requirements of proper internal controls with other efforts to improve effectiveness and accountability. Thus, internal control should be an integral part of the entire cycle of planning, budgeting, management, accounting, and auditing. It should support the effectiveness and the integrity of every step of the process and provide continual feedback to management.

Managers must carefully consider the appropriate balance between controls and risk in their programs and operations. Too many controls can result in inefficient and ineffective government; agency managers must ensure an appropriate balance between the strength of controls and the relative risk associated with particular programs and operations. The benefit of controls should outweigh the cost. Agencies should consider both qualitative and quantitative factors when analyzing costs against benefits.

In Maryland, the Governor manages the operations of State departments and independent agencies. The Comptroller decides on the forms of keeping and stating accounts, and the Joint Budget and Audit Committee of the General Assembly receives evaluations and recommendations resulting from the Legislative Auditor's reviews of agencies' operations. These officials and others believe that a renewed and heightened emphasis on internal control will result in better management and delivery of services for the State.

This manual is organized into two volumes.

The first volume:

- discusses the general and specific standards of internal control,
- identifies management's responsibilities on matters of internal control,
- describes needed controls and testing for internal controls over financial reporting,
- provides specific, step-by-step guidance to departments for evaluating and improving controls, and
- describes the "Report on the Status of Internal Controls" which the head of each department or independent agency should prepare.

The second volume contains the forms to be used in this process.

If you would like the forms for this manual in an excel spreadsheet to modify for your department/agency, please request a copy by e-mail to gad@comp.state.md.us. Should you have any questions concerning the content of this manual, or need technical assistance, please contact the General Accounting Division in the Comptroller's Office at 410-260-7504, or send an e-mail.

A copy of this report may be found at: http://compnet.comp.state.md.us/General_Accounting_Division/State_Agencies/Forms_and_Manuals.

SECTION II

INTERNAL CONTROL STANDARDS

II. Internal Control Standards

Management accountability is the expectation that managers are responsible for the quality and timeliness of program performance, increasing productivity, controlling costs and mitigating adverse aspects of agency operations and assuring that programs are managed with integrity and in compliance with applicable law.

Internal control guarantees neither the success of agency programs, nor the absence of waste, fraud, and mismanagement, but is a means of managing the risk associated with the State's programs and operations. Managers should define the control environment (e.g., programs, operations, or financial reporting) and then perform risk assessments to identify the most significant areas within that environment in which to place or enhance internal control. The risk assessment is a critical step in the process to determine the extent of controls. Once significant areas of risk have been identified, control activities should be implemented. Continuous monitoring and testing should help to identify poorly designed or ineffective controls and should be reported upon periodically. Management is then responsible for redesigning or improving upon those controls. Management is also responsible for communicating the objectives of internal control and ensuring the organization is committed to sustaining an effective internal control environment.

Accordingly, State managers must take systematic and proactive measures to:

(i) develop and implement appropriate, cost-effective internal control for results-oriented management;

(ii) assess the adequacy of internal control in State programs and operations;

(iii) separately assess and document internal control over financial reporting;

(iv) identify needed improvements;

(v) take corresponding corrective action; and

(vi) report on internal control through management assurance statements.

Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

Management is responsible for developing and maintaining internal control activities that comply with the following standards to meet the above objectives:

- Control Environment,
- Risk Assessment,
- Control Activities,

- Information and Communications
- Monitoring

A. Control Environment

The control environment is the organizational structure and culture created by management and employees to sustain organizational support for effective internal control. When designing, evaluating or modifying the organizational structure, management must clearly demonstrate its commitment to competence in the workplace. Within the organizational structure, management must clearly define areas of authority and responsibility; appropriately delegate the authority and responsibility throughout the agency; establish a suitable hierarchy for reporting; support appropriate human capital policies for hiring, training, evaluating, counseling, advancing, compensating and disciplining personnel; and uphold the need for personnel to possess and maintain the proper knowledge and skills to perform their assigned duties as well as understand the importance of maintaining effective internal control within the organization.

The organizational culture is also crucial within this standard. The culture should be defined by management's leadership in setting values of integrity and ethical behavior although it is also affected by the relationship between the organization and central oversight agencies. Management's philosophy and operational style will set the tone within the organization. Management's commitment to establishing and maintaining effective internal control should cascade down and permeate the organization's control environment which will aid in the successful implementation of internal control systems.

The control environment in Maryland, like that of most other states, is complex. The State constitution and laws establish the framework for our control structure. Some controls are exercised by control departments and some controls are exercised by operating departments. Centralized control departments disseminate policies, procedures and detailed technical guidance to operating departments by issuing manuals. A representative list of manuals issued by the control departments is contained in Appendix D. Control departments also function as operating departments in carrying out their responsibilities. Therefore, good systems of internal control are the responsibility of each and every department, agency, or unit of State government.

In addition to developing controls to assure compliance with control agency manuals, State departments (and independent agencies) must also develop controls for situations unique to them. Each State department must ensure that its internal controls are consistent with its own mission and organizational structure, as well as with statewide controls.

B. Risk Assessment

Management should identify internal and external risks that may prevent the organization from meeting its objectives. When identifying risks, management should take into account relevant interactions within the organization as well as with outside organizations. Management should also consider previous findings; e.g., received from an auditor, from internal management reviews, or from noncompliance with laws and regulations, when identifying risks. Identified risks should then be analyzed for their potential effect or impact on the agency.

C. Control Activities

Control activities include policies, procedures and mechanisms in place to help ensure that agency objectives are met. Several examples include: proper segregation of duties (separate personnel with authority to authorize a transaction, process the transaction, and review the transaction); physical controls over assets (limited access to inventories or equipment); proper authorization; and appropriate documentation and access to that documentation.

Internal control also needs to be in place over information systems, i.e., general and application controls. General control applies to all information systems such as the mainframe, network, and end-user environments, and includes agency-wide security program planning, management, control over data center operations, system software acquisition and maintenance. Application control should be designed to ensure that transactions are properly authorized and processed accurately and that the data is valid and complete. Controls, such as edit checks, should be established at an application's interfaces to verify inputs and outputs. General and application control over information systems are interrelated, both are needed to ensure complete and accurate information processing. Due to the rapid changes in information technology, controls must also adjust to remain effective.

D. Information and Communications

Information should be communicated to relevant personnel at all levels within an organization. The information should be relevant, reliable and timely. It is also crucial that an agency communicate with outside organizations as well, whether providing information or receiving it. Examples include: receiving updated guidance from central oversight agencies; management communicating requirements to the operational staff; and operational staff communicating with the information systems staff to modify application software to extract data requested in the guidance.

E. Monitoring

Monitoring the effectiveness of internal control should occur in the normal course of business. In addition, periodic reviews, reconciliations or comparisons of data should be included as part of the regular assigned duties of personnel. Periodic assessments should be integrated as part of management's continuous monitoring of internal control, which should be ingrained in the agency's operations. If an effective, continuous monitoring program is in place, it can level the resources needed to maintain effective internal controls throughout the year.

Deficiencies found in internal control should be reported to the appropriate personnel and management responsible for that area. Deficiencies identified, whether through internal review or by an external audit, should be evaluated and corrected. A systematic process should be in place for addressing deficiencies.

F. Fraud

Fraud is caused by a number of factors. An individual's personality or circumstances, including financial stress, addiction, or dissatisfaction with work can cause the person to commit fraud. A more important factor is opportunity. Some people commit fraud simply because it becomes "irresistible". Therefore, opportunity not only permits fraud to occur, but promotes it. *The opportunity needed for fraud is created when management fails to meet its responsibility to establish and maintain a sound and comprehensive framework of internal controls.*

Because no system of internal controls is foolproof, management must have procedures in place to try to detect it. Remember that anyone can commit fraud. Many individuals get caught in fraud simply because they believe they are just "borrowing" funds temporarily. Also, tips come from all sources, especially hostile sources, and should not be dismissed. Use analytical reviews to identify potential problems. Look for situations where actual results differ from what might reasonably be expected in the circumstances. Carefully examine unusual transactions and supporting documentation.

SECTION III

EVALUATION AND IMPROVEMENT

III. Evaluation and Improvement

Executives and managers of the State's departments and independent agencies are responsible for maintaining an adequate internal control structure. Earlier sections established broad coverage of internal control as the framework for efficiency and economy in state government. An internal control structure concerns not only the financial and administrative activities of a department, but also the department's related programs and operational activities. To summarize, an internal control structure consists of the following:

- **Financial/Accounting Controls** - The controls on authorizing, processing, recording, and reporting transactions (which operate within the broader control environment of administrative controls). For example: Authorization and classification of expenditures under established guidelines. These guidelines should be clearly defined, documented, approved by appropriate authorities, and communicated. Contracts must be entered into the accounting system in a timely manner. Timely payments to contractors/vendors must be based on proper invoices approved by authorized persons and reconciled with ordering and receiving documents.

- **Administrative Controls** - The broad controls on all activities carried out by officials to accomplish their objectives. Primarily, these activities concern planning, organization, productivity monitoring, improvement, and quality control activities. For example: The planning and budgeting activity should be synchronized with the management reporting system. Budget and management reports should be in the same format, at the same level of detail, and contain data classified in a manner consistent with the plans/budgets and should display planned and actual results. Departments should hire and train competent, qualified personnel. The plan or organization should provide for an appropriate segregation of functions. Determining need for contracts, seeking prospective contractors, negotiating contracts, and authorizing payments to contractors are activities which should be separated. Administrative controls can be divided into two groups: organizational and operational.

    - **Organizational Controls -** The controls on how management defines authority and assigns responsibility, delegates authority, establishes a hierarchy for reporting and supports human capital policies.

    - **Program and Operational Controls -** The controls on planning and accomplishing the department's missions and objectives - For example: Procedures exist to develop policies and procedures, results of department activities are regularly evaluated, and procedures exist for periodically evaluating the department's/organization's method of operation.

There are different ways to evaluate and report on internal controls. This manual provides an effective approach based on seven proven techniques applied in complex entities similar to the State of Maryland. The seven step process is summarized as follows:

1. **Organizing the Evaluation** - Assigning responsibilities for all participants to assure that each department completes the appropriate analyses and reports. It concerns: planning, directing, and controlling the evaluation process, tracking the status of the evaluation and corrective actions and developing other information necessary to manage the process.

2. **Segmenting the Department** - It is usually required because departments and institutions are too large to be included in a single control evaluation and because departments' programs are too diverse to be included in a single comprehensive review. It is recommended that each department be segmented into organizational or functional components, each identified as an "assessable entity".

3. **Conducting Risk Assessments** - Identifying the vulnerability of each assessable entity to waste, loss, unauthorized use, or misappropriation. First identify the factors that create an inherent risk in the entity; then, evaluate the controls in place and the environmental factors which influence the effectiveness of controls (such as competence of personnel) to determine if the system is adequate to minimize waste, loss, unauthorized use or misappropriation of resources.

4. **Developing Plans for Subsequent Action** - Base plans and schedules for subsequent actions on an evaluation of the results of the risk assessments and other considerations (management priorities, resource constraints, etc.) Examples of subsequent actions include updating policies on procedures, providing training, and conducting internal control reviews. Internal control reviews are conducted if an assessable entity manager is not certain how well the controls are functioning or if an assessable entity is deemed to be highly vulnerable.

5. **Conducting Internal Control Reviews** - For the selected assessable entities, conduct internal control reviews to ensure that the defined control objectives and techniques are functioning as intended. Special emphasis should be given to the controls over financial reporting. Then, recommendations to correct weaknesses in either the design or functioning of the internal control structure should be developed.

6. **Taking Corrective Action** - The reported recommendations resulting from the internal control reviews are analyzed, and corrective actions are scheduled if the anticipated cost of implementing the recommendation will not exceed the expected benefit.

7. **Preparing Reports** - Each department combines the results of each of its assessable entity reviews into a report on the status of internal controls. The report reflects the current status of each department's internal control structure. A copy of the report and all supporting documentation will be maintained in each department.

SECTION IV

ORGANIZING THE EVALUATION

IV. Organizing the Evaluation

The first step of the internal control evaluation is to organize the evaluation process. It is critical that a department, whether large or small, carefully organizes and assigns responsibilities to ensure that the evaluation, improvement and reporting on internal controls is effective. Key consideration should include, among other things, the following:

1. Assigning responsibilities

2. Internal reporting

3. Documentation

4. Personnel and supervision

5. Scheduling the evaluation process

Each participant in the evaluation process must be identified and responsibilities clearly assigned to prevent confusion and provide an orderly method for collecting and reporting information. Internal control reviews, and thus assignments, must take into consideration that there are two types of reviews, reviews for management controls and reviews of financial reporting controls. Responsibility for the individual internal control evaluations should be assigned to the lowest supervisory level. The suggested responsibilities of each participant are described as follows:

Department Heads - Are responsible for the overall review of information, evaluating the organizations under their authority and reporting on the status of the internal control structure of their department. Agency or department heads may create a senior management committee which may include the chief financial officer, senior procurement officer, chief information officer and managers of other functional offices to carry out their duties.

Specific responsibilities should include the following:

- Select an evaluation approach
- Assign responsibilities throughout the organization
- Appoint an internal control coordinator
- Maintain and demonstrate a positive attitude toward all participants concerning the necessity of an effective internal control environment
- Review internal control evaluation reports and discuss at progress meetings
- Report on the status of the department's internal controls
- Ensure that subsequent actions, including the correction of control weaknesses, are performed.

Internal Control Coordinator - Is responsible for providing assistance to the department head and the senior management committee by coordinating and managing the department's evaluations. Internal control coordinators also serve as contacts between the department and other individuals who are interested in the department's internal control structure. Specifically, the internal control coordinators:

- Determine that the department is segmented into manageable "assessable entities" to facilitate conducting the risk assessments
- Formalize a department-wide evaluation reporting and tracking system to make sure the risk assessments and internal control reviews are completed on a timely basis
- Review risk assessments and internal control review results and discuss at progress meetings
- Prepare the report for the department head's signature.

Assessable Entity Managers - Are responsible for ensuring that internal controls within the assessable (segmented) entity are adequate. This individual:

- Conducts the risk assessment for his or her segmented entity
- Schedules subsequent actions which may include internal control reviews or documenting policies and procedures
- Ensures that subsequent actions are performed
- Reports to the department's internal control coordinator on all internal control activities, including the results of assessments and reviews.

Department Internal Auditors - Internal auditors normally review internal control structures and report the results of their reviews to the highest levels of management in organizations. These reviews are usually undertaken on the auditor's own initiative, or at the request of the department head. They are either separate reviews of internal controls, or are reviews performed in conjunction with internal audits. Internal auditors are a valuable resource to the department and should provide technical guidance and oversight for all aspects of the evaluation process in each department. Specifically, the internal auditors:

- Provide technical assistance to assessable entity managers on conducting internal control evaluations
- Provide guidance to assessable entity managers on preparing internal control reports for submission to the internal control coordinator
- Provide advisory service to department heads and the internal control coordinators on preparing the internal control reports.

The internal control coordinator, as explained earlier, maintains the evaluation, data collection, and tracking system. This system should monitor the accomplishments of the various tasks that make up the evaluation and improvement process. The system should identify each assessable (segmented) entity and the responsible entity manager, track the conduct of risk assessments, track scheduling of subsequent actions and track the completion of subsequent actions.

The methods used, the personnel involved and their roles, the key factors considered and the conclusions reached must be documented to provide a permanent record. Written narratives and flow charts should be used when necessary to describe and illustrate various internal processes.

It is important that an adequate level of resources be committed to the process. It is likely that risk assessments and internal control reviews will be performed by persons from various parts of the department. These persons need to be competent on matters concerning internal control and the process described in this manual, so proper judgment can be made. Some specific considerations which should help are as follows:

- Hold an orientation meeting to explain the objectives of and procedures for conducting the assessments and reviews
- Assign personnel using a "team approach" so small groups of individuals can perform assessments/reviews jointly. This will provide some assurance that limitations of one individual can be offset by the strengths of another
- Provide adequate and active supervision of the entire process.

Assessments and reviews should be scheduled after carefully considering resource availability, statutory and other administrative requirements, cyclical operations, and other factors. It is essential; however, that work is completed in time to provide a basis for the report. Internal control reviews should be conducted periodically, and, in larger departments, throughout the year. This may be necessary because of the complexity of the department, the degree of compliance with established procedures may deteriorate over time, and changes in conditions may require changes in controls.

In summary, it is critical that department management commit the time and resources of its key personnel to planning and organization to ensure a good review.

SECTION V

SEGMENTING THE DEPARTMENT

V. Segmenting the Department

Most State departments are large, complex organizations with broad responsibilities over a variety of programs. As a result, it is often difficult to perform a risk assessment and an internal control review on the department as a whole. A senior assessment team should first be established. Depending on the size of the department/agency, this team may be the Senior Management Committee or may be a subset of the committee. This team should divide the department into "segmented" or "assessable" entities. With small, manageable entities, the risk assessment and internal control processes can be delegated to lower levels in the department where they can be better managed.

A department can be segmented according to the following two basic approaches or a combination thereof:

1. Transaction cycle approach and

2. Organizational structure approach.

For the first approach, appropriate functional transactional cycles must be identified. A transaction cycle is a stream of related events and processes which satisfy one overall functional need of the department.

This method will result in broad assessable entities (cycles) such as the revenue cycle, disbursement cycle, and budget cycle which cut across organizational lines. For example, the budget transaction cycle would include processes performed in the budget office as well as in the operating offices and accounting offices.

This method best clarifies the interaction of controls between different units. Controls in each unit will be evaluated and reviewed to see how they affect the department as a whole. The transaction cycle approach might be preferred for a small independent agency which is not as complex as a large department.

The drawbacks of this method include the need to cross over organizational lines of authority, often involving many managers, and the lack of organizational structure along cycle lines. These drawbacks can seriously impede an orderly and successful evaluation.

The organizational structure approach involves delegating internal control responsibilities to managers along formal organization lines. Factors to be considered in segmenting the department into assessable entities under this method are as follows:

- **Organization Chart -** Segmentation that closely follows the department's formal structure is usually efficient and effective when the organizational lines are clearly shown. When lines of authority and reporting responsibilities are interwoven, the organization chart becomes less useful as a tool for segmentation.

- **Physical Location** - A department's programs or administrative functions could operate in several locations. Since the control systems may vary among locations, it may be necessary to perform separate evaluations at each location. On the other hand, if a department's operations are confined to one location, it may be appropriate to have assessable entities that include more functions.

- **Autonomy** - The more independent a function, the more likely the function should be considered a separate assessable entity.

- **Materiality** - An important consideration in any organization is the commitment of personnel and dollars. The larger the program, the greater the likelihood that the function should be considered a separate assessable entity.

When segmenting the department, the support activities (cash receipts, cash disbursements, etc.) must be examined to determine whether they should be a separate assessable entity based on the degree of centralization and control. The greater the autonomy, the greater the risk and, therefore, the greater the need for accountability and emphasis of this function as a separate assessable entity. For example, in a large department, the support activity may be centralized at the "Office of the Secretary" organizational level. This activity should be studied to determine the extent of its control and responsibility to decide if it should be segregated from the administrative office as a separate assessable entity.

Persons responsible for support activities should answer applicable questions on the risk assessment forms. However, minor delegations of authority may require other entities to answer some of the questions.

For example, although there might be a centralized cash disbursement function, other units might be responsible for receiving and forwarding invoices or for petty cash funds and would answer the questions pertaining to these specific functions.

Examples of support activities that could be considered assessable entities at the department, agency, or institutional level are:

- **Strategic and Long-Range Planning** - This involves establishing and implementing broad, long-range goals and objectives. This process is important since it charts the general direction of the entity for the future.

- **Operational Planning** - This concerns setting objectives for the current budget cycle. The annual budget expresses the current year's objectives in financial terms.

- **Program Operations, Planning, and Management** - This includes maintaining performance standards and reports so that management may analyze performance (such as construction completion milestones, claims administered per employee, accounts processed for collection and transactions processing time).

- **Loans and Accounts Receivable Collection** - This support activity includes all procedures concerning collection of the organization's loans and accounts receivable.

- **Cash Receipts/Revenue/Sales** - This activity includes all actions associated with the receipt, depositing and safeguarding of cash, including imprest/working funds.

- **Cash Disbursements/Procurement** - This concerns all of the purchasing processes, accounting for the related liabilities and authorizations for payment.

- **Payroll** - This activity encompasses all duties and procedures related to time, attendance and payroll functions performed within the organization.

- **Property, Plant, and Equipment** - This includes all policies, procedures and operations concerning the acquisition, maintenance and disposition of the organization's fixed assets, including accounting.

- **Information Technology Systems** - This includes general and application controls on electronic data processing. Due to the widespread use of computers, the assessment process will require a significant commitment of resources to this area on a continuing basis.

- **Travel** - This process includes all policies related to travel by employees, including authorization, reporting, expenditure guidelines and cash advances.

The advantages of segmenting on an organizational basis include:

- An entity manager-in-charge is usually in place that has authority and responsibility for internal controls.
- There is a greater understanding of operations by personnel.
- It is easier to segment a department along lines of authority and responsibility that already exist.

A disadvantage of this method is that the flow of transactions may be disrupted. For example, information regularly flows between personnel, payroll, and accounting activities. Breaking these activities along organizational lines may cause inefficiencies later in the evaluation process.

Regardless of which approach to segmentation is used, all assessable entities should have the following characteristics:

- The entity facilitates management's efforts to reduce inherent risks caused by:

    - Material budget levels
    - Significant procurement/assistance responsibility

  - Significant complexity in the program's/system's services
  - Significant amounts of cash, negotiable instruments, or other assets
  - Significant decentralization of activities
  - Increasing/decreasing age and "life expectancy" (e.g. the entity is being phased out)
  - Special concerns outside the entity (entity being scrutinized by Attorney General)

- The entity has logical cycles for use, disposition or maintenance of the resources.

- The entity has specific control objectives relating to event cycles.

- In the entity, all managers directly accountable for its functions are included in the assessment process.

All important functions and activities must be included in the assessable entity. The exclusion of activities from an entity may result in improper management conclusions on the activities subject to the risk assessment and on the department's overall internal control structure.

The agency head's assessment of internal control can be performed using a variety of information sources. Management has primary responsibility for assessing and monitoring controls, and should use other sources as a supplement to, not a replacement for, its own judgment. Sources of information include:

- Management knowledge gained from the daily operation of agency programs and systems
- Management reviews conducted: (i) expressly for the purpose of assessing internal control, or (ii) for other purposes with an assessment of internal control as a byproduct of the review
- Reports, including legislative auditor's audits, inspections, reviews, investigations and outcome of hotline complaints or other products
- Program evaluations
- Audits of financial statements, including information revealed in preparing the financial statements; the auditor's reports on the financial statements, internal control, and compliance with laws and regulations; and any other materials prepared relating to the statements
- Reviews of financial systems which consider whether the requirements of the Comptroller's Office are being met
- Internal control assessments
- Federal agencies' audits
- Single Audit report findings for agencies receiving federal grants
- Reports and other information provided by the Legislative Auditor
- Other reviews or reports relating to agency operations; for example, for the Department of Health and Mental Hygiene, quality control reviews of the Medicaid programs.

Remember, the purpose of segmentation is to identify manageable entities of a department's activities to assure that:

1. All important inherent risks are identified
2. Meaningful evaluations are made to determine if the environment is conducive to effective internal control techniques
3. Knowledgeable individuals assess how well internal controls are meeting their stated objectives.

After each assessable entity has been identified, it should be assigned a control number and an entity manager. This and other information should be reported and documented in the department's evaluation tracking system

SECTION VI

REVIEW OF INTERNAL CONTROLS OVER FINANCIAL REPORTING

VI. Review of Internal Control over Financial Reporting

Introduction

This Section provides a methodology for agency management to assess, document, and report on the internal controls over financial reporting. This information and the procedures should be kept in mind and implemented as the steps of the risk assessments and action plans are performed. This document also encourages an integrated approach to assessing the internal controls over financial reporting considering the current legislative and regulatory environment in which State agencies operate.

The Sarbanes-Oxley Act of 2002 required that management of publicly-traded companies strengthen their processes for assessing and reporting on the internal controls over financial reporting. The passage of the Sarbanes-Oxley Act served as an impetus for the federal and state governments to reevaluate their current policies relating to internal control over financial reporting and management's related responsibilities. Accordingly, a separate section for financial reporting has been added to the internal control review process with a separate attestation on the internal controls over financial reporting provided in the Report on the Status of Internal Control.

This Section requires agencies to specifically document the process and methodology for applying the standards when assessing internal control over financial reporting. It also requires management to use a separate materiality level when assessing internal control over financial reporting. The agency head's report on the effectiveness of internal control over financial reporting required by this section is a subset of the assurance statement required on the overall internal control of the agency.

Scope

Effective internal control over financial reporting provides reasonable assurance that misstatements, losses, or noncompliance with applicable laws and regulations, material in relation to financial reports, would be prevented or detected.

Objectives of Internal Control over Financial Reporting

Internal control over financial reporting is a process to provide reasonable assurance regarding the reliability of financial reporting. Reliability of financial reporting means that management can reasonably make the following assertions:

- All reported transactions actually occurred during the reporting period, and all assets and liabilities exist as of the reporting date (existence and occurrence);
- All assets, liabilities, and transactions that should be reported have been included, and no unauthorized transactions or balances are included (completeness);
- All assets are legally owned by the agency, and all liabilities are legal obligations of the agency (rights and obligations);

- All assets and liabilities have been properly valued, and where applicable, all costs have been properly allocated (valuation);
- The financial report is presented in the proper form, and any required disclosures are present (presentation and disclosure);
- The transactions are in compliance with applicable laws and regulations (compliance);
- All assets have been safeguarded against fraud and abuse; and
- Documentation for internal control, transactions, and other significant events are readily available for examination.

Definition of Financial Reporting

Internal control over financial reporting should assure the safeguarding of assets from waste, loss, unauthorized use, or misappropriation as well as assure compliance with laws and regulations pertaining to financial reporting. Financial reporting includes annual closing statements of an agency as well as other significant internal or external financial reports. Other significant financial reports are defined as any financial reports that could have a material effect on a significant spending, budgetary, or other financial decision of the agency or that is used to determine compliance with laws and regulations on the part of the agency. An agency needs to determine the scope of financial reports that are significant, i.e., which reports are included in the assessment of internal control over financial reporting. In addition to the annual fiscal year end closing statements, significant reports might include: financial statements at the operating division or program level, budget submission reports, reports used to monitor specific activities such as specific revenues, receivables, or liabilities, or reports used to monitor compliance with laws and regulations.

Planning Materiality

Materiality for financial reporting is the risk of error or misstatement that could occur in a financial report that would impact management's or users' decisions or conclusions based on such report. The planning materiality for the assessment should be designed so as to ensure that items required to be reported will be detected. Therefore, the planning materiality should be at a lower threshold than the reporting materiality as defined below.

Materiality should be determined for each financial report included in the scope of the assessment. Materiality may differ from report to report. Materiality shall be considered when determining the extent of testing or work required to assess internal control over financial reporting as well as what deficiencies should be reported. Management must determine whether the internal controls over a financial report are sufficient to prevent or detect errors or misstatements that would be considered material for a specific financial report. Therefore, the extent of work performed and reporting threshold for control deficiencies must be determined on a report by report basis. Additionally, agencies should consider qualitative as well as quantitative measures to determine material items.

Definition of Deficiencies

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A design deficiency exists when a control necessary to meet the control objective is missing, or an existing control is not properly designed, so that even if the control operates as designed, the control objective is not always met. An operation deficiency exists when a properly designed control does not operate as designed, or when the person performing the control is not qualified or properly skilled to perform the control effectively.

A reportable condition is a control deficiency, or combination of various deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process or report external financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements, or other significant financial reports, that is more than inconsequential will not be prevented or detected.

A material weakness in internal control is a reportable condition, or combination of reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected. Material weaknesses in internal control over financial reporting shall be included in the internal control report, but separately identified.

Assessing Internal Control over Financial Reporting

A. Risk Assessment

The assessment should include obtaining sufficient knowledge of the agency's process on how management considers risks relevant to financial reporting objectives and decides about actions to address those risks. The assessment should determine how management identifies risks, estimates the significance of risks, assesses the existence of risks in the current environment, and relates them to financial reporting. The results of this assessment at the agency-wide level will drive the extent of testing and review performed at the segmented level, i.e., the process, transaction, or application level. Some significant circumstances or events that can affect risk include:

- Complexity or magnitude of programs, operations, transactions, etc.
- Accounting estimates
- Related party transactions
- Extent of manual processes or applications
- Decentralized versus centralized accounting and reporting functions
- Changes in operating environment
- New personnel or significant personnel changes
- New or revamped information systems
- Significant new or changed programs or operations

- New technology
- New or amended laws, regulations, or accounting standards.

B. Control Activities

Control activities are the policies and procedures that help ensure that management directives are carried out and that management's assertions in its financial reporting are valid. The assessment should include obtaining an understanding of the control activities applicable at the entity level such as:

- Policies and procedures
- Management objectives (clearly written and communicated throughout the agency)
- Planning and reporting systems
- Analytical review and analysis
- Segregation of duties
- Safeguarding of records
- Physical and access controls.

C. Information and Communication

The assessment should include obtaining an understanding of the information system(s) relevant to financial reporting. Such an understanding should include:

- The type and sufficiency of reports produced
- The manner in which information systems development is managed
- Disaster recovery
- Communication of employees control related duties and responsibilities
- How incoming external communication is handled.

D. Monitoring

The assessment should include obtaining an understanding of the major types of activities the agency uses to monitor internal control over financial reporting, including the source of the information related to those activities and how those activities are used to initiate corrective actions. Several examples include:

- Self assessments by management
- Evaluations by the Legislative Auditor or external auditor
- Direct testing.

Evaluating and Documenting Internal Control over Financial Reporting

A. This evaluation should include an evaluation of internal control at the process, transaction, or application level and should include the following steps.

1. Determine Significant Accounts or Groups of Accounts

For each financial report identified in the scope of the assessment, identify those accounts or groups of accounts that individually or collectively could have a material effect on the financial report. Agencies should consider qualitative as well as quantitative measures to determine material items.

2. Identify and Evaluate the Major Classes of Transactions

For each significant account or group of accounts, identify the major classes of transactions that materially affect those accounts. In identifying transactions, specifically consider whether a class of transactions is routine, non-routine, or represents an accounting estimate. This type of classification can help the senior assessment team identify the inherent risk and the controls necessary to adequately mitigate such risks. The assessment should include obtaining an understanding of the specific processes and document flow involved in each class of transactions. Thoroughly understanding the processes and document flow will help in understanding where errors could occur and what control objectives and techniques may prevent or detect those errors.

3. Understand the Financial Reporting Process

Obtain an understanding of the process and workflow that links the accounting system to the financial report(s). Oftentimes, financial information is not directly transferable from the accounting system to the financial report, but requires intervening calculations, summarizations, etc. This represents another point where errors can be introduced into the financial report, and it is important to understand where such errors could occur and what control objectives and control techniques can prevent or detect these errors.

4. Understand the Controls Designed to Achieve Management's Assertions

Prepare a control evaluation(s) for each significant account or group of accounts that aligns specific controls with management's assertions for each account or group of accounts. An individual assessment of the potential effectiveness of the design of the controls for each account or group of accounts should be made considering the risk of error and the controls that are designed and in place to prevent or detect such errors. Assessing the effectiveness of the design of a control is concerned with whether the control is suitably designed to prevent or detect a material error related to an account or group of accounts. Procedures to obtain such evidential matter ordinarily include inquiries of appropriate agency personnel; inspection of documents, reports, or electronic files; and observation of the application of specific controls. This is sometimes referred to as a "walk through", and helps the senior assessment team ensure its understanding of the controls. An assessment of the control design should identify controls as effective, moderately effective, or not effective.

5. Controls Not Adequately Designed

If a control over a significant account or group of accounts is missing, or its design is determined to be not effective considering the associated risk of error, the senior assessment team does not need to test this control for the purpose of concluding on control effectiveness. This instance should be noted in the report of deficiencies with suggestions for improvement. However, management may, nevertheless, seek to further test affected transactions to determine if there was any actual loss, fraud, error, improper payment or noncompliance resulting from those ineffective controls.

6. Test Controls and Assess Compliance to Support Management's Assertions

For those controls whose design is deemed effective or moderately effective, the senior assessment team should test them to determine the extent to which the controls were applied, the consistency of their application, and who applied them. Tests of controls ordinarily include procedures such as inquiries of appropriate agency personnel; inspection of documents, reports, or electronic files, indicating performance of the control; observation of the application of specific controls; and re-performance of the application of the control by the senior assessment team. If testing indicates that a significant control is not operating as designed, it should be reported as a deficiency.

B. Overall Assessment of the Design and Operation of Internal Control over Financial Reporting

The final step in the assessment is an overall conclusion as to the design and operation of the internal controls over financial reporting based on the assessments at the entity level and the process, transaction, or application level. The overall assessment should conclude whether the internal controls over financial reporting are operating effectively or whether material weaknesses exist in the design or operation. A sample statement of assurance can be found in Exhibit I.

C. Reliance on Other Work to Accomplish Assessment

The assessment of internal control over financial reporting should be coordinated with other activities to avoid duplication of efforts with similar activities. Reviews performed by management, or at management's direction, may be used to help accomplish this assessment.

D. Documenting Internal Control over Financial Reporting

The senior assessment team should document its understanding of the agency's internal control over financial reporting. The form and extent of documentation depends in part on the nature and complexity of the agency's controls. The more extensive and complex the controls, the more extensive the documentation. Documentation may be electronic, hard copy format or both and should be readily available for examination. Documentation could include organizational charts, flow charts, questionnaires, decision tables or memoranda. Documentation may already exist as part of normal agency policy or procedure; however, the senior assessment team should separately identify, verify and maintain the documentation it uses in making its assessment. The documentation prepared by internal or external auditors may also be used, but again, the senior assessment team must take responsibility and verify and maintain that documentation. Documentation should also include appropriate representations from officials and personnel responsible for monitoring, improving and assessing internal controls. After an initial assessment, subsequent assessments may focus on updating existing documentation. All documentation and records shall be properly managed and maintained; therefore, agencies will need to establish, or review, existing retention policies for documentation (paper and electronic media).

SECTION VII

RISK ASSESSMENTS AND ACTION PLANS

VII. Risk Assessments and Action Plans

After all assessable entities have been identified; a manager is assigned to review each assessable entity. The entity manager should be responsible for, and understand, the day to day activities of the entity. The entity manager must:

- Identify the major risks associated with each entity, and then
- Assess the controls in place to mitigate the identified risks

There are two purposes for completing the risk assessment. One is to identify those entities within the department that have the greatest potential for errors and should be earmarked for detailed internal control reviews. The other is to point out specific areas of weakness in internal control which can be readily corrected.

Entities may be selected for internal control reviews based on a variety of factors ascertained during the assessment process, including:

- A weak general control environment
- Areas of high inherent risk with weak internal controls
- An inability to complete the evaluation knowledgeably.

After considering such factors as management priorities, resource constraints, etc., the manager should schedule appropriate internal control reviews and related actions.

Generally, entities having a high risk assessment rating should be identified for immediate internal control reviews unless the internal auditor, the Legislative Auditor, or others have made a suitable comprehensive review within the last two years. Such determinations should be documented in writing and retained in the assessment working papers. The regularly scheduled audit by the Legislative Auditor or the State's independent auditor would not be considered sufficiently comprehensive to substitute for an internal control review. If a suitable comprehensive review has not been performed, then the entity should be scheduled for review as indicated.

How often should a risk assessment be performed? This will vary depending on the susceptibility of each organization to waste, loss, or mismanagement. However, an assessment should be conducted at least biennially, and, in larger and complex departments, continually throughout the year. Factors such as significant changes in organizational structure, personnel, automated systems, or financial resources of an assessable entity may affect the frequency of the assessments.

Plans and schedules should be prepared in advance of the assessing year to make sure that all assessable entities are scheduled and studied in a timely manner. The department coordinator should plan in coordination with the department heads and assessable entity managers.

A risk assessment consists of the following steps:

1. Analysis of the general control environment
2. Analysis of inherent risk
3. An evaluation of safeguards
4. Assessment of evaluation results and development of subsequent action plans.

Step 1 - Analysis of the General Control Environment

Internal controls operate within the framework of the general control environment. The general control environment includes all aspects of the workplace which influence the effective functioning of the internal control techniques (procedures). The entity manager must determine if acceptable general controls exist and identify needed corrective actions. For example, program eligibility requirements which are not sufficiently detailed, documented, and checked to ensure that the program beneficiaries are qualified to receive benefits, seriously impede effective internal control. The following factors should be evaluated in assessing the general control environment:

- **Management Attitude** - Management commitment to establishing and maintaining a strong system of internal control must be communicated to all employees through actions and words.

- **Organizational Structure** - Identify the organizational entities and their reporting relationships.

- **Personnel** - The competence and integrity of the organization's personnel.

- **Delegation and Communication of Authority and Responsibility** - Appropriate delegation or limitation of authority.

- **Policies and Procedures** - Do adequate policies and procedures exist so that employees know what to do in various situations?

- **Budgeting and Reporting Practices** - Have goals been defined and met?

- **Organizational Checks and Balances** - Establishing a satisfactory level of financial and other supervisory controls, and where appropriate, the creation of professional internal audit programs.

- **Information Systems** - When utilized, information systems can greatly enhance an overall internal control system. Having these systems requires that special control features be built into the systems.

Sources of information to assist the assessing manager in evaluating the general control environment include:

- Organization charts
- Planning and budget documents
- Job descriptions
- Inventory of statutory responsibilities and authorities
- Policies and procedures manuals
- Reports
- Audits, management reviews, program evaluations, etc.
- Internal control policies and procedures.

Suggested questions for the Analysis of the General Control Environment, Form IC-1, are provided in Volume II. The questionnaire approach shows the detailed criteria which should be used in evaluating the control environment in each assessable entity of the department. For each of the elements in the control environment, a determination is made as to whether sufficient controls exist or corrective action is required.

Step 2 - Analysis of Inherent Risk - The second step in the risk assessment process is to analyze the inherent potential for waste, loss, unauthorized use or misappropriation. This step is critical and must be properly performed before the other steps in the assessment process can be undertaken. This analysis will identify areas where the internal control systems need to be strong and should be regularly and closely evaluated and monitored. High inherent risk is not necessarily a reflection of management performance or lack of control; rather, high inherent risk points to areas needing attention. This step will produce an inventory of inherent risks unique to the assessable entity.

When assessing inherent risks, it is suggested that the questionnaire shown as Form IC-2 in Volume II be used. This questionnaire presents specific factors each entity manager must consider in assessing assigned areas of responsibility. Broad areas which are covered in detail in the questionnaire are:

- **Purpose, Objectives, and Characteristics** - What are the purpose and characteristics of the assessable entity that makes the entity susceptible to waste, loss, unauthorized use or misappropriation? If not already available, information about the purpose, objectives, and characteristics may be obtained by reviewing background material such as the relevant enabling legislation and legislative history, regulations, planning documents, and other statements concerning missions, goals and objectives, operating procedures and policies and budget information. Factors that contribute to fraud, waste and abuse include:

    - Broad or vague legislative authority or regulations
    - Cumbersome legislative or regulatory requirements
    - Broad, vague, or nonexistent missions, goals or objectives
    - High degree of complexity
    - Third party beneficiaries such as contractors or grantees
    - Handling of classified or valuable information

- Activities involving the handling of cash, maintenance of accounts/taxes receivable or custody of property, equipment or supplies easily converted to personal use
- Activities operating under severe time or personnel constraints
- Activities which affect outside parties involving approval of applications, granting of authority, certifications, issuance of licenses or permits, inspections or enforcements.

- **Budget Level** - Programs or activities involving large amounts of money are more susceptible to waste, loss, unauthorized use or misappropriation than programs or activities involving small amounts. The level of funding, including personnel time allocated to the assessable entity, should be determined by reviewing the department's budget and supporting data. In situations where the budget data does not show the amount of money involved, estimates should be made. For example, a separate budget often does not exist for a function such as property management. In order to measure the full financial significance of this function, the value of the property controlled must be determined to assess risk.

- **Procurement/Assistance** - Assessable entities often procure large amounts of goods and services, including technical and financial assistance. The risks to the department may be greater in cases where a third (outside) party is performing work for, or on behalf of, the government because of the lack of direct control.

- **Age and Life Expectancy** - The age and life expectancy of the assessable unit should be considered. Entities which are new or are undergoing substantial modification or reorganization, or are phasing out, are more susceptible to waste, loss, unauthorized use, or misappropriation than stable programs because:

    - New or changing entities may lack written policies or procedures, adequate resources, experienced personnel, or devices to measure performance.

    - Entities that are phasing out may lack adequate resources, may involve closeout activities for which controls have not been developed, or may involve large amounts of money or other resources which must be accounted for. Personnel turnover and lack of motivation are other phase-out problems.

- **Degree of Centralization** - The degree of centralization can affect the entities' susceptibility to unauthorized use or misappropriation of resources. Highly centralized functions tend to have less risk than decentralized functions.

- **Special Concerns Outside the Department** - Special interest in an activity may indicate that it is highly susceptible to waste, loss, unauthorized use or misappropriation and should be treated as such. Special attention focused on the department/entity is a source of pressure that might create risk. The following should be considered in evaluating the inherent risk:

  - Special interest exhibited by the Governor, the Legislature, or the Department head
  - Deadlines set by legislation
  - Media attention
  - Litigation

- **Prior Reviews** - Review prior audit reports submitted by the department internal auditor, the State Legislative Auditor, the State's external auditor, and other internal and external reports for any indications that the entity has been subject to losses due to waste, loss, unauthorized use, or misappropriation. Consider the amounts of actual/estimated losses, if any, and the period covered by the prior review. Also, consider management's responsiveness to recommendations made in the aforementioned reports/reviews. This includes actions taken to correct deficiencies. A lack of management responsiveness suggests a higher degree of risk.

Step 3 - Evaluation of Safeguards

An in-depth review of the existing controls is not appropriate at this stage. However, the entity manager should decide, based on knowledge of the functions, and not assumptions, if internal controls exist and if they are adequate.

Two questionnaires are included in Volume II for the Evaluation of Safeguards. These forms (Forms IC-3.1 and IC-3.2) have been designed for evaluating the controls in place. The questions in Form IC-3.1 address, in some detail, the department's program operations and administrative functions. Form IC-3.2 addresses information technology (IT) operations, and will be completed by entities which use significant amounts of IT in their operations. These forms are detailed because of varying functions of the State's departments and agencies. They should be tailored to each entity's specific environment and activities. Chapter VI. Review of Internal Control over Financial Reporting, should be read before completing this form as a guide to the controls that should be in place.

Questions on these forms are phrased so that a "yes" answer indicates a generally satisfactory position. A "no" answer indicates a weakness which must be addressed. The weakness should be considered for corrective action unless compensating controls can be identified which in effect nullify (cancel) the "no" answer.

The comments column on the forms should be used to briefly describe the known compensating controls. References to supporting documentation, e.g., detailed descriptions of compensating controls, procedures manuals, and/or organization charts, if needed, should also be included in the comments column.

The assessable unit manager must exercise good judgment at this point in the risk assessment, especially in determining which weaknesses ("no" answers) are to be scheduled for further consideration. All weaknesses identified by a "no" answer must be considered unless compensating controls exist. The manager must carefully decide if a compensating control cancels a "no" answer.

Step 4 - Assessing Evaluation Results and Developing Subsequent Action Plans

Agency managers are responsible for taking timely and effective action to correct deficiencies. Correcting deficiencies is an integral part of management accountability and must be considered a priority by the agency.

The extent to which corrective actions are tracked by the agency should be commensurate with the severity of the deficiency. Corrective action plans should be developed for all internal control weaknesses and progress against plans should be periodically assessed and reported to agency management. Management should track progress to ensure timely and effective results.

In Step 4, the assessable entity manager inventories all the risks and weaknesses identified in Steps 1 to 3 needing further consideration and collects information to help the department coordinator and department head develop a plan for subsequent action for the department's entities. Form IC-4, shown in Volume II, is designed for collecting the information necessary to develop an appropriate action plan. The information for completing this form will be gathered from the weaknesses identified in Forms IC-1, IC-3.1, and IC-3.2.

Form IC-2 helps management identify entities which are inherently at risk, i.e., an entity that collects large amounts of cash is more at risk than an entity that does not collect any cash. Form IC-2 must also be considered while completing Form IC-4. This method allows managers to compare the relative weaknesses and associated risks of assessable entities within the departments.

Specifically, Form IC-4 should be completed for each assessable entity to provide the following:

- Assessable entity and weakness identification code. These codes will be used to identify the specific weakness in the department tracking system.

- Brief description of the risk or weakness. This information is obtained from Forms IC-1, IC-2, IC-3.1, and IC-3.2. Make an entry on Form IC-4 for each "no" answer for which there is not a valid compensating control. Generally, "no" answers on Form IC-2 are only indications of high risk areas and do not indicate a need for corrective action.

- An estimate of the dollar value associated with the risk, a brief summary statement that describes what can go wrong and the basis for the dollar valuation estimate. For example: the entity's expenditure budget might be associated with weaknesses in the procurement or disbursement section; revenues could be associated with an overall weakness in handling of cash collections; value of property and equipment might be associated with weaknesses in the fixed assets section.

- A brief narrative of potential subsequent actions should include the implementation cost estimate. Specific examples of subsequent actions which may be taken are as follows:

    - Develop new policies and/or procedures
    - Provide additional training
    - Functionally realign responsibilities to improve the segregation of duties
    - Perform a management review
    - Schedule detailed internal control review
    - Eliminate duplicate or unnecessary controls.

- Give any reasons why subsequent action should not be taken. For example: cost to implement corrective action exceeds the value of the relative risk; legal mandate requires that the controls be in place even though costs exceed perceived benefits.

- If subsequent action is required, the entity manager should designate the person responsible and indicate tentative beginning and ending dates for the action.

A copy of the competed Form IC-4 for each entity should be furnished to the department coordinator for review with the department head. After the department head has reviewed and approved the plans, the data on Form IC-4 should be recorded in the department tracking and reporting system. As discussed earlier in this manual, a tracking and reporting system can monitor control weaknesses until all appropriate actions are taken. It will also aid the preparation of the *Report on the Status of Internal Control*.

The remainder of this section summarizes guidance in selecting appropriate subsequent actions. In determining subsequent actions, the manager should remember the primary purpose of the evaluation process is to strengthen the internal control structure in a cost efficient manner.

One type of subsequent action is to schedule a detailed internal control review. This is recommended when:

- The risk assessment cannot be completed accurately because the procedures are not known.

- The assessment shows weaknesses that cannot be easily corrected and/or the corrective action would be costly and, therefore, should be studied in more detail.

- The responses to the Inherent Risk, or the General Control Environment questionnaire, show areas of high risk that, in management's judgment, require more analysis than was done with the "Evaluation of Safeguards".

- Management perceives a need for one.

If it is determined that a detailed internal control review is required, it can be performed by an internal auditor, external auditors, or by the manager, assisted by technical staff.

In certain situations, it may not be desirable or cost efficient to conduct an internal control review. If weaknesses identified during the assessment can be corrected immediately, an internal control review may be unnecessary. In other situations, weaknesses may be addressed by means other than a detailed internal review. For example, a corrective action may be the implementation of a basic control, e.g., all disbursements must be approved by the program manager before being forwarded to the Comptroller's Office for payment. Examples of other subsequent actions which can also help correct the noted weaknesses or reduce the effects of inherent risk and were mentioned earlier are repeated here as a reminder:

- Develop new policies and/or procedures
- Provide additional training
- Functionally realign responsibilities to further segregate duties
- Perform a management review
- Eliminate duplicate or unnecessary controls.

Identification of Deficiencies - Agency managers and employees should identify deficiencies in internal control from the sources of information described above and the results of their assessment process. Agency employees and managers shall report control deficiencies to the next supervisory level which will allow the chain of command structure to determine the relative importance of each deficiency.

A control deficiency or combination of control deficiencies that in management's judgment represents significant deficiencies in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives is a reportable condition (internally tracked and monitored within the agency). A reportable condition that the agency head determines to be significant enough to be reported outside the agency shall be considered a material weakness and included in the report. As it relates to financial reporting, agencies should also consider qualitative as well as quantitative measures to determine material items. This designation requires a judgment by agency managers as to the relative risk and significance of reportable conditions. Definitions of reportable conditions and material weaknesses for management's assessment of internal control over financial reporting are provided in Section VI, *Review of Internal Control over Financial Reporting*.

Correcting Material Weaknesses in Internal Control - Each agency shall establish systems to assure the prompt and proper resolution and implementation of corrective action on identified material weaknesses. These systems shall provide for a complete record of action taken on the material weaknesses identified.

SECTION VIII

DETAILED REVIEWS AND CORRECTIVE ACTION

VIII. Detailed Reviews and Corrective Action

Before proceeding further, it is important to distinguish between a risk assessment and a detailed internal control review. A risk assessment is a review of the "susceptibility" of a program or activity to the occurrence of waste, loss, unauthorized use or misappropriation. The tools used to make this assessment are structured to identify: 1) weaknesses that make the program or activity "susceptible" to waste, loss, unauthorized use or misappropriation; and 2) actions which can reduce or eliminate those weaknesses. A detailed review would be required if the results of the risk assessments showed a vulnerability to loss that could not be corrected without further in-depth study.

An internal control review is a "detailed examination" of a "system" of internal control to determine whether: 1) adequate control "measures" exist; and 2) they are implemented either in a cost effective manner or in response to statutory mandates to "prevent" or "detect" the occurrence of potential risks. Procedures within transaction cycles or event cycles are targeted in detail control reviews. Some of the same steps are included in both types of reviews.

Maryland's internal control review has six recommended steps:

1. Identifying event cycles
2. Analyzing the general control environment
3. Documenting each event cycle
4. Evaluating the internal controls within each event cycle
5. Testing the internal controls
6. Assessing the results of the internal control review and developing corrective action plans.

The remainder of this section discusses these steps and suggested sub-steps in detail. Sample forms for use in conducting a detailed internal control review are shown in Volume II.

Identifying Event Cycles - The first step in conducting an internal control review is to identify "event cycles" within the assessable entity. Event cycles isolate the various processing systems of the entity in logical work-flow patterns for conducting effective reviews.

Event cycles are defined as a series of processes which initiate and achieve an end product, create the necessary documentation and gather and report related data. In other words, an event cycle is a stream of related events and processes which satisfy one overall functional need of the entity.

Each event cycle is structured with defined beginning and ending points. For example, the disbursement cycle in the General Accounting Division of the State Comptroller's Office begins with the receipt of the disbursement transmittal forms from a state department and ends with the delivery of a warrant drawn on the State Treasury for the preparation of a check. Another example might be a student loan event cycle which could begin with the receipt of an application and conclude with the disbursement of the loan.

It is important to note that event cycles typically are framed in totality within an assessable entity. Therefore, in a large organization, the ending point for the event cycle in one entity might be the starting point for the event cycle in another assessable entity.

All event cycles in an assessable entity selected for review should be identified. Also, all functions and activities performed within the assessable entity should be included in one of the event cycles identified.

On the other hand, management in some cases may determine that certain activities are performed uniformly within many assessable entities and, therefore, these activities should be considered for internal control review as a totality in another assessable entity. An example might be time and attendance processing which should be an activity performed throughout the organization in accordance with standard policies and uniform procedures. Where such standards and uniformity exist, management may decide to perform the detail internal control review on the whole activity once and not repeat the review or portion of it with each assessable entity.

Identifying event cycles in an assessable entity is accomplished by the following sub-steps:

(a) Gathering background information
(b) Conducting interviews
(c) Completing a general narrative and/or flowchart of the assessable entity
(d) Preparing a list of event cycles
(e) Selecting event cycles for detail internal control reviews.

Gathering Background Information

The person assigned to perform the internal control review must become familiar with the day-to-day activities of the assessable entity if they aren't already. Background information gathered in the risk assessment may be helpful to the person conducting the detailed internal control review. Such background information may include:

- Department goals/objectives
- Budgets/plans
- Risk assessments
- Organizational charts/functional statements
- Process flowcharts/narratives
- Policies and procedures manuals
- Program evaluations and other reviews
- Financial statements

The reviewer should also study reports issued by the department's internal auditor, the Legislative Auditor, or the state's external auditor. The reports usually provide clues in identifying areas needing management attention.

Conducting Interviews

The reviewer should interview assessable entity personnel to make sure that he or she has identified and understands all activities and functions accurately.

Completing a General Narrative and/or Flowchart of the Assessable Entity

The responsible reviewer should document the entity with a general systems narrative and flowchart. This process ensures that the reviewer has considered all the significant processes and workflows within the entity. The systems narrative and flowchart should be of a high level or summary nature. Entity operating personnel should review the document to make sure it is accurate and complete.

Preparing a Listing of Event Cycles

After identifying and listing all functions, the reviewer should determine if each function merits its own event cycle or if it combines with other functions to form an event cycle. Event cycles should not be defined in such detail as to create unnecessary burdens on the entity in the form of numerous, costly, and duplicative reviews. For example, receiving student tuition payments could be combined with depositing payments.

Selecting Event Cycles for Detail Internal Control Reviews

After all event cycles are identified, the reviewer should list them on Form IC-5 (Volume II) and determine which event cycles are to be reviewed. Explain/justify this determination in the comment section on the form. The results of the analysis of the general control environment (Form IC-1) and the risk assessment (Form IC-2) should help make this determination.

Documenting Each Event Cycle

To document each event cycle for a thorough understanding of how it operates, the reviewer should 1) interview the person(s) involved in the cycle, 2) review existing documentation, 3) observe the activity, and 4) prepare either a narrative explanation or a flowchart accompanied by appropriate narrative information in sufficient detail to permit an in-depth analysis of the existence and adequacy of internal controls. The documentation should identify for each cycle such things as the procedures, the personnel performing the procedures, the forms and records developed and maintained, and the number or dollar value of events processed, and any error rate.

The reviewer should verify the accuracy of the flowchart and narrative by conducting interviews and walkthroughs. Walkthroughs consist of tracing transactions or events from start to finish, noting specifically how the transaction or event is processed.

Proper documentation allows the reader to visualize an individual event moving through the cycle from start to finish, identifying all key control points and processes. Flowcharting and working paper documentation guidelines are provided in Appendix B.

Evaluating the Internal Controls Within Each Event Cycle

The reviewer must study the flowcharts, narratives, and other documentation to determine if the current techniques, as documented, meet the control objectives. There are three sub-steps in this process:

(a) Identify control objectives
(b) Identify control techniques
(c) Match objectives and techniques and make a preliminary assessment of controls.

Identify Control Objectives

Control objectives are desired goals or conditions for a specific event cycle. By achieving control objectives, the potential for waste, loss, unauthorized use, or misappropriation is minimized. Appendix A lists sample control objectives which can be used for typical assessable entities. Once identified, the control objectives should be summarized and listed on Form IC-6 which is included in Volume II.

For control objectives to be effective, compliance must be measurable and observable. To measure compliance, the reviewer must identify and evaluate control techniques.

Identify Control Techniques

The reviewer must identify existing control techniques from detailed event cycle narratives and flowcharts prepared in *Documenting Each Event Cycle.* A control technique is defined as "a procedure, process, or document that is being relied on to efficiently and effectively accomplish a control objective and thus help safeguard an activity from error". The most common control techniques and specific illustrations of them are included in the following table.

Common Techniques	Illustrations
Documentation: • Operation/financial plans • Organizational charts/job descriptions • Quality control procedures • Control agency manuals	• Written procedures for completing time and attendance forms
Records - Recording of Transactions: • Periodic progress reports • Use of computerized/manual inventory systems • Use of logs/checklists • Cash receipts/register tapes	• Weekly/daily reconciliation of cash journal
Authorization - Execution of Transactions: • Clearly written chain of command • Periodic inspection of critical forms to ensure proper completion/authorized signature • Required approval of changes in existing systems, procedures, and personnel assignments	• An authorized signature is required for receipts of all contracted services or supplies
Structure - Separation of duties: • Separate personnel assigned to key duties such as: authorizing, processing, recording, and reviewing • Investigations are conducted by impartial individuals • Periodic reviews/audits routinely conducted by impartial individuals • Appointment of alternate personnel to fill in for absent personnel	• Personnel receiving goods/services are different from the personnel purchasing them
Supervision: • Performance standards/evaluations • Provisions for training • Scheduled and unscheduled review of work • Automated reconciliation and checking of work • Periodic verification that standard operating procedure is followed	• Supervisors provide on-the-job training until employees meet specified performance criteria
Security - Access to resources: • Controlled custody and pre-numbering of critical forms (e.g., blank checks, purchase order, signature plates, etc.) • Physical barriers (e.g., locked doors, fences, safes, etc.) • Access restrictions (e.g. magnetic key devices "Do Not Enter" signs, employee badges, sign-in logs, etc.) • Detection and prevention devices (e.g., fire alarms, electronic sensing, security guards, etc.) • Off-site backup storage for critical automated/manual files	• People entering buildings must have an authorized badge or pass

Additional examples of specific techniques together with related control objectives and risks of failure of the controls techniques are shown in Appendix A.

Match Objectives and Techniques and Make a Preliminary Assessment of Controls

Using the form "List of Internal Control Objectives and Techniques," Form IC-6 (Volume II), the reviewer must make a preliminary assessment of the validity of control techniques and note the result in the comment section of the form. This helps the reviewer to identify:

1. Internal control techniques which are strengths and must be tested under the next step, *Testing the Internal Controls*.

2. Control objectives for which control techniques are not adequate and for which system corrections must be made.

3. Control techniques that are unnecessary or excessive and can be eliminated.

Testing the Internal Controls - All control techniques (other than those determined to be inadequate and/or unnecessary) should be tested to verify that they are functioning as intended. The internal control techniques to be tested should be listed on Form IC-7, Tests of Internal Controls, (Volume II). Testing may be done by selecting a sample of transactions or events, reviewing the documentation supporting those transactions, making other observations and inquiries, and determining whether the specific techniques are satisfactorily employed.

A sample includes a representative number of transactions or events. The sample size will vary depending on the nature and significance of the technique being tested, the characteristics of the individual transactions, and the degree of assurance required. Sampling is used because verifying the entire population is unnecessary and impractical. The number of transactions to be tested should be the minimum necessary to provide the reviewer reasonable assurances that control techniques are functioning as intended (perhaps 20 transactions randomly selected are adequate). Test documentation must support the reviewer's conclusions. This documentation typically includes pertinent information such as personnel interviewed, observations performed, documents tested, dates, transaction types, amounts, and any other distinguishing data.

After the documentation is completed, each event cycle control objective is evaluated to determine whether the existing control techniques provide reasonable assurance that the objective is achieved in an efficient and effective manner and/or that legally mandated control objectives are being achieved. Collect and summarize results on Form IC-7. First, evaluate the control technique as either functioning or not functioning and then, if it is functioning, assess the adequacy of the technique in meeting the objective. The reviewer should note:

- Test results which indicate that the technique is not being performed
- Test results which indicate that the technique is either not necessary (over control) or not meeting the stated objectives (weakness).

The reviewer then makes corrective action recommendations for further consideration.

Making a Final Assessment of the Results of the Internal Control Review and Developing Corrective Action Plans - In this step, the reviewer inventories all weaknesses identified on Forms IC-4, IC-6 and IC-7, which need further consideration and collects information to assist the department coordinator and department head in planning subsequent action. Form IC-8, Assessment of Results on Internal Control Review, in Volume II helps the reviewer collect information necessary to develop an appropriate action plan. This form should be completed for each assessable entity:

- To provide assessable entity and weakness identification codes. These codes will be used to identify the specific weakness and related information in the department tracking system.

- To identify the event cycle, control objective, control technique and recommendation for each weakness noted in the detail internal control review. This information is obtained from Forms IC-4, IC-6 and IC-7. Enter each weakness from these forms which action is recommended onto Form IC-8.

- To estimate the monetary cost of the risk created by the weakness and estimate the cost to implement the recommended action. Refer to Form IC-4. If the weakness or required action listed on IC-4 has changed as a result of the detail internal control review, or if the estimates are outdated, new estimates will be required.

- To justify why corrective action should not be taken. For example: cost to implement exceeds value of risk related to weakness; legal mandate required controls be in place even though the controls are excessive.

- To designate the persons responsible for carrying out any needed corrective action and to indicate tentative beginning and ending dates for the action.

A copy of the completed Form IC-8 for each entity should be furnished to the department coordinator for review with the department head. After the department head has reviewed and approved the plan, the data on this form should be recorded in the department tracking and reporting system. As mentioned earlier, a tracking and reporting system can effectively monitor control weaknesses until all appropriate actions are taken. It can also aid preparation of the "Report on the Status of Internal Control" described in Section IX.

Uniform Documentation Guidelines

Each State department should prescribe guidelines for uniform documentation appropriate for that department. This may be done in concert with the department internal auditors where they exist or the State Legislative Auditor. Appendix B contains recommended documentation guidelines.

SECTION IX

PREPARING THE REPORT ON THE STATUS OF INTERNAL CONTROL

IX. Preparing Report on the Status of Internal Control

This Section provides guidance to departments for preparing the "Report on the Status of Internal Control" to be signed by the Internal Control Coordinator of each State department or independent agency and submitted to the senior executive, or whomever requested the review to be performed. The senior executive is the officer who is directly accountable to the Governor. The report will summarize the results of the risk assessments, evaluation of safeguards and, if required, the results of the detailed internal control reviews described earlier in this manual.

In Section IV, the Internal Control Coordinator was given responsibility for preparing the report. If the department has established a tracking and reporting system as suggested earlier in this manual, the coordinator can use that system to prepare the report. The forms in Volume II, "Assessment of Evaluation Results," Form IC-4, and "Assessment of the Results of Internal Control Reviews", Form IC-8, should be reviewed. The Internal Control Coordinator will use these forms and the updated status of subsequent action plans to prepare the report.

The Report must contain both management's Assurance Statement on Internal Control and management's Assurance Statement on Internal Control over Financial Reporting.

These statements are management's assessment of the effectiveness of the agency's internal control as of March 31, or any date of the agency's choosing, of that fiscal year (see Exhibit 1). These assurance statements are required to include the following:

- A statement of management's responsibility for establishing and maintaining adequate internal control for the agency.
- An assessment of the effectiveness of the agency's internal control as of March 31, for example, including an explicit conclusion as to whether the internal controls over financial reporting are effective.
- If a material weakness is discovered by March 31, but corrected by June 30, a statement identifying the material weakness, the corrective action taken, and that it has been resolved by June 30.
- If a material weakness is discovered after March 31, but prior to June 30, the statement identifying the material weaknesses should be updated to include the subsequently identified material weakness.

In its assurance statement on the internal controls, management is required to state a direct conclusion about whether the agency's internal controls are effective. The statement must take one of the following forms:

- Unqualified statement of assurance (no material weaknesses reported);
- Qualified statement of assurance, considering the exceptions explicitly noted (one or more material weaknesses reported); or
- Statement of no assurance (no processes in place or pervasive material weaknesses).

Management is precluded from concluding that the agency's internal control, or internal control over financial reporting, is effective if there are one or more material weaknesses that remain uncorrected. Management must make the final determination with regard to what constitutes a material weakness.

The remaining pages in this section present a sample "Report on the Status of Internal Control" (Exhibit I).

Exhibit I

State of Maryland

Sample Report on the Status of Internal Control

The Honorable
(Governor)
State House
Annapolis, MD 21401

Dear Governor: (or Secretary; Chief Executive, etc.),

An evaluation of the internal controls of (name of department) in effect as of March 31, 2xxx, was performed in accordance with the "*Internal Control Manual for Use by State Departments and Independent Agencies*".

The objectives of the system of internal controls of (name of department) are to provide reasonable assurance that:

- Resource use is consistent with laws, regulations, and policies;
- Resources are safeguarded against waste, loss, and misuse;
- Reliable financial and statistical data are obtained, maintained and fairly disclosed in reports for decision making and other use of the data and statistics, and
- Federal laws and supporting administrative regulations are complied with.

The concept of reasonable assurance recognizes that the cost of internal control should not exceed the value of the benefits and that benefits may reduce the risks of failing to achieve the stated objectives. Estimates and judgments are required to assess the expected benefits and related costs of control procedures. Furthermore, errors or irregularities may occur and not be detected because of inherent limitations in internal controls, including those limitations resulting from resource constraints, legislative restrictions and other factors. Finally, projection of any evaluation to future periods is subject to the risk that procedures may be inadequate because of changes in conditions or that the degree of compliance with the procedures may deteriorate.

The results of the evaluation indicate that the internal controls of (name of department or independent agency) in effect as of March 31, 2xxx, or other date, comply with the objectives to provide the reasonable assurance described in the preceding paragraph. (If this is not the case, delete this sentence and add the last paragraph instead.)

In addition, based on the results of the evaluation, the (name of department or independent agency) can separately provide reasonable assurance that internal control over financial reporting as of March 31, 2xxx, or other date, was operating effectively and no material weaknesses were found in the design or operation of the internal control over financial reporting. (If this is not the case, delete this sentence and add the next paragraph instead.)

The evaluation did disclose certain weaknesses. Attachment A to this statement identifies internal control weaknesses of the (name of department or independent agency), the plans and related schedules for correcting the weaknesses, and the status of actions taken to correct weaknesses identified in prior years' reports.

(Signature of department head, Chief executive of department, or Internal Control Coordinator)

Exhibit I

Attachment A

State of Maryland

Attachment "A" to the Report on the Status of Internal Control

Department:________________________________

Assessable Entity:___________________________

Weakness:

Corrective Action:

Schedule of dates for implementation of Corrective Action:

Comments on Current Status of Implementation (Actual Progress Compared to Schedule):

APPENDIX A

SAMPLE INTERNAL CONTROL OBJECTIVES AND TECHNIQUES

Sample Internal Control Objectives and Techniques

Receipts

Control Objectives	Control Techniques	Risks of Failure
1. To receive correct amounts of money in accordance with laws, regulations and management policy.	1a. Clear statement of rates or other criteria.	1a. Receipts accepted at unauthorized amounts, unacceptable to management.
	1b. Approved price lists to communicate prices and terms.	1b. Overpayment or underpayment of amounts due.
	1c. Written credit and collection policy.	1c. Receipts which violate laws and regulations.
2. To record and deposit all receipts accurately.	2a. Bank reconciliations prepared at regular intervals.	2a. Receipts not recorded or deposited.
	2b. Prenumbered receipt slips.	2b. Receipts deposited but not recorded.
	2c. Cash receipts reconciled to deposits by someone not involved in recording receipts.	2c. Receipts recorded but not deposited. 2d. Receipts recorded incorrectly.
	2d. Lockbox used for mail receipts.	
	2e. Daily reconciliation of cash register tape totals to deposit slips.	
	2f. Segregation of duties for handling and listing cash receipts.	
	2g. Perform audits.	
3. To allocate all receipts to the correct period and fund or account.	3a. Bank reconciliations prepared at regular intervals.	3a. Receipts credited in wrong period.
	3b. Supervisory review of processing and reports.	3b. Receipts credited to wrong fund or account.
	3c. Independent investigation and follow-up of overdue receivable balances.	3c. Receipts recorded incorrectly. 3d. Inaccurate inputs to general ledger accounts.
	3d. Individual independent of the billing and receiving functions investigates complaints.	3e. Transactions incorrectly classified in reports.
	3e. Segregation of duties for handling and recording receipts.	3f. Weakened budgetary control over operations.
	3f. Perform audits.	

	3g. Documented processing, cutoff and period-end procedures.	
4. To substantiate and evaluate recorded balances of receipts and accounts receivable, and related transaction activity.	4a. Reconciling recorded receipts with bank statements. 4b. Reconciling general ledger balances with subsidiary ledger balances. 4c. Periodic physical counts of cash and cash items. 4d. Policy statements, procedures manuals, and organization charts. 4e. Verify reports. 4f. Perform audits.	4a. Inaccurate or incomplete reports. 4b. Critical decisions based on erroneous data. 4c. Omission of journal entries. 4d. Incorrect coding. 4e. Improper cutoffs.
5. To permit access to cash and cash items received only according to management's criteria.	5a. External storage (Bank). 5b. Insurance and fidelity bonds. 5c. Restrict access to work areas. 5d. Lock doors, cabinets and safes. 5e. Timely deposits. 5f. Minimum cash balances maintained by cashiers. 5g. Policy statements, procedures manuals and organization charts. 5h. Outside services to move cash (armored car).	5a. Stolen, lost or temporarily diverted cash. 5b. Adverse publicity.
6. To permit access to receipts and receivable records, forms, processing areas only according to management's criteria.	6a. Prenumbering forms. 6b. Policy statements, procedures manuals and organization charts. 6c. Segregating responsibilities and restricting access. 6d. Safe, locks and off-site backup of records storage. 6e. Performing audits.	6a. Lost or destroyed records. 6b. Records misused or altered by unauthorized personnel. 6c. Adverse publicity. 6d. Computer programs altered by unauthorized persons.
Grants Management		
1. to authorize grant eligibility requirements according to laws, regulations and management policy.	1a. Management and general counsel approve the written detail requirements used in the evaluation process. 1b. Management authorized specific personnel who can approve grant	1a. Unauthorized grants are made. 1b. Program objectives are not met. 1c. Eligible grant recipients are denied grants.

	applications.	
2. To establish and maintain grant application processing procedures according to laws, regulations and management policy.	2a. Processing procedures are defined and communicated in approved procedures manuals. 2b. Management approves all changes to program procedures. 2c. Perform periodic procedures audits.	2a. Unauthorized grants are made. 2b. Program objectives are not met. 2c. Eligible grant recipients are denied grants. 2d. Grant expenditures exceed budget.
3. To use economical and efficient procedures to review, process and report grants and related transactions.	3a. Program results are assessed and costs compared to benefits. 3b. Costs are compared to costs of similar programs. 3c. Design forms to expedite processing. 3d. Eliminate unnecessary clerical steps. 3e. Perform management audits. 3f. Trained personnel.	3a. Program does not accomplish all objectives. 3b. Grant system costs are excessive. 3c. Funds needed for grants must be used to pay administrative costs.
4. To approve only those grant requests that meet the eligibility requirements.	4a. Compare grant requests in detail to eligibility requirements. 4b. Management reviews and approves large or unusual requests. 4c. Make reports to management of grants approved and disapproved. 4d. Persons not responsible for initial review process appeals. 4e. Perform periodic audits. 4f. Trained personnel.	4a. Program objectives are not met. 4b. Improper grant awards are made. 4c. Adverse publicity.
5. To accurately and properly report grants issued.	5a. Defined reporting procedures. 5b. Proper working relationship between operating and financial systems. 5c. Trained personnel. 5d. Management review of program cost reports.	5a. Unreported expenditures. 5b. Unspent funds. 5c. Spending exceeds budget.
6. To summarize and classify grants and costs of processing each period according to management's policy.	6a. Proper working relationship between operating and financial systems. 6b. Defined accounting requirements. 6c. Trained personnel. 6d. Supervisor and management review reports. 6e. Perform periodic audits.	6a. Unreported expenditures. 6b. Unspent funds. 6c. Spending exceeds budget. 6d. Misclassification of data. 6e. Critical decisions based on erroneous data. 6f. Inaccurate entry into general ledger accounts.

7. To review and evaluate recorded grant data.	7a. Management reviews reports. 7b. Program manager reviews reports. 7c. Perform periodic audits.	7a. Unreported expenditures. 7b. Unspent funds. 7c. Spending exceeds budget. 7d. Misclassification of data.
8. To permit access to grant and cost accounting records, forms, processing areas and procedures according to management policy.	8a. Control access to files and processing areas. 8b. Identify personnel allowed access to specific records forms.	8a. Records misused by unauthorized personnel. 8b. Records altered by unauthorized personnel. 8c. Records destroyed or lost; making it impossible to prepare reliable reports.
9. To periodically substantiate and evaluate grantee records.	9a. Independent audits of grantee records. 9b. Comparing grantee reports to grant forms. 9c. Grant manager reviews reports. 9d. Comparing prior and current period grantee reports. 9e. Certification of reports by grantee. 9f. Take prompt and appropriate grant close-out actions.	9a. Grantee not maintaining appropriate records. 9b. Grantee not complying with grant requirements. 9c. Payment to grantee for nonallowable costs. 9d. Program objectives are not met.

APPENDIX B

HOW TO PREPARE FLOWCHARTS AND WORKING PAPERS

Flowcharts

A. **Be Brief** - Flowcharts should be simple and uncluttered to keep the visual map clear and useful. Begin each step with a verb if possible. Avoid complete sentences in the flowchart. Include necessary explanations and in-depth information in a supplemental narrative. The flowchart should, however, contain sufficient detail to identify and evaluate internal controls.

B. **Show Steps in Sequence** - Flowcharts present steps in the sequence in which they occur. Show the flow of steps and documents vertically from top to bottom and from left to right. Use arrows to point out the order of steps. Identify beginning points clearly.

C. **Show All Documents** - When making a flowchart, show every copy of any documents produced. Each copy of a document should be numbered or otherwise identified. The flowchart must also show every document entered into the system.

D. **Show Work Flow Among Units** - A flowchart is advantageous because it presents relationships between steps and between different operating personnel or units. Flowcharts should include documentation flowing between personnel or work units.

E. **Identify Workers by Job Title** - Most flowcharts should identify the person performing each operation by job title rather than by name. The job title provides the reviewer with a clear indication of the level and type of personnel responsible for performing each step. Job titles also help the reviewer identify areas of inconsistent duties (and possible internal control weaknesses). Finally, a flowchart giving job titles and not names does not require revision when there is a personnel change.

F. **Highlight Existing Internal Controls** - While evaluating the system, highlight existing internal controls directly on the flowchart.

G. **Include Supplemental Narrative When Necessary** - Use a supplemental narrative to expand upon or explain the graphic information shown on the flowchart. Often including explanatory comments in a separate narrative will help keep the flowchart uncluttered.

The narrative should include relevant time frames, estimates (e.g., number of things processed, dollar amount processed, error rate), and cross-references to supporting documentation.

H. **Use Flowchart Symbols** - Use flowchart symbols to represent both steps and documentation. Symbols show the exact point where each step occurs.

APPENDIX B

Working Paper Documentation Guidelines

Working papers provide a permanent written record of the work performed. Detail internal control review working papers may include the following documentation of work performed:

- An index
- Reason for selecting assessable entities for review
- Reason for selecting event cycle for review
- Detail plans for conducting a detail internal control review
- Event cycle background information (as appropriate)
- Interview notes
- Flowcharts
- Overview narrative descriptions
- Samples of pertinent event cycle forms
- Test plan documentation
- Test schedules
- Conclusions and recommendations
- Memos to files
- Draft reports
- Explanations for any changes to the draft
- Final Report

APPENDIX B

Because the scope and approach of each detail internal control review may be somewhat different, it is impractical to suggest a single working paper design. However, the following points will be useful in providing consistency and establishing a trail of work accomplished.

1. Each working paper is identified, dated, indexed, and initialed by the preparer.

2. Working papers indicate the purpose and scope of work performed.

3. The working papers identify the sources of data such as an interview, observation, or records.

4. Summarize results and conclusions in the report. The summary must be cross-referenced to the applicable supporting working papers.

5. Working papers carry data forward from detail supporting schedules to the report.

6. A legend is provided for any tick marks or symbols used.

7. Working papers are indexed to facilitate an orderly review and to evaluate cross-referencing between pages. The system used should be kept as simple as possible to allow for easy revisions and expansion.

8. Working papers should be reviewed by the ICR Manager.

Appendix C

Internal Control Guidance – Excerpt from the *Accounting Procedures Manual*

State agencies are responsible for establishing an effective system of internal control. Internal control is the overall plan of organization and all the coordinate methods used to safeguard assets; ensure the reliability of accounting data; promote efficient operations and ensure compliance with established governmental policies, laws, regulations and contracts. To accomplish these objectives, certain basic standards must be present in any effective system of internal control. The general standards concern reasonable assurance of achieving control objectives, supportive attitude, competent personnel, and control objectives and techniques. Specific standards which are central to the standard of control objectives and techniques involve documentation, recording of transactions and events, execution of transactions and events, separation of duties, adequacy of supervision, access to and accountability for resources, and efficient and effective use of resources.

The specific internal control procedures needed by an agency will vary with each situation encountered. In determining which controls should be in place, estimates and judgments are required to assess the expected benefits and related costs or risks of implementing or not implementing control procedures. For example, it is recognized that certain agencies may not have sufficient personnel to fully or adequately segregate duties. Under these circumstances, it is the responsibility of management to exercise prudent judgment to ensure that the best internal control procedures are in place.

Basic internal control procedures include, but are not limited to, the following:

5.1 Cash

- Centralization of the cash receipts collection function to the maximum extent possible.
- Immediate recording of cash receipts for accounting control purposes (e.g., utilization of mail receipts listings, cash registers, pre-numbered receipt forms).
- Restrictive endorsement of checks "for deposit only" immediately upon receipt.
- Provision of separate cash drawers (or similar control devices) for each employee responsible for collections to affix individual responsibility and accountability for collections until deposited.
- Segregation of the cash receipts handling duties from the cash receipts and accounts receivable record keeping, billing and reconciliation functions.
- Reconciliation of cash receipts recorded on cash register tapes, pre-numbered receipt forms and/or mail listings with the cash receipts ledger and amounts deposited (e.g., per validated deposit tickets, R*STARS records) by an employee independent of the cash receipts functions.

- Independent verification of the continuity of cash register tapes by comparing the ending transaction number from one tape to the beginning transaction number of the next tape.
- Accounting for the numerical sequence of pre-numbered receipt forms as to issued, voided and on hand.
- Supervisory review and approval of voided transactions and adjustments to cash receipts and accounts receivable records.
- Existence of adequate facilities to store and safeguard cash receipts until deposit.
- Prompt and intact deposit of cash receipts.
- Monitoring of advances for proper use and prompt reimbursement.
- Substantiation of the use of petty cash with vouchers that are signed and dated.
- Surprise cash counts performed by someone other than the Petty Cash Fund custodian.

5.2 Accounts Receivable

- Maintenance of adequate records to account for billings and related collections, as follows:
    - Billings should be pre-numbered and accounted for.
    - Cash receipts totals should be periodically compared with corresponding totals of credits to accounts receivable.
    - Detail accounts receivable records and a control account should be maintained; the aggregate balance of the detail records should be periodically reconciled to the control account balance.
- Written and implemented credit and collection procedures.
- Accounts that are aged, reviewed, and sent to the Central Collection Unit in a timely manner.

5.3 Revenues – Taxes, Licenses, Fees

- A method to establish that taxpayers have reported payments due.
- Review of remittances, tax returns, forms, etc., for mathematical accuracy.

- Initial control of returns, i.e., pre-numbering control totals or control log.

- Reconciliation of total of cash and checks with total of returns, license applications, forms, etc.

5.4 Payroll

- Use of positive recording for attendance records which are compared to the exception time report submitted to the Central Payroll Bureau.

- Segregation of duties for:

  - Preparation of exception time report.
  - Approval and submission of exception time report to Central Payroll Bureau.
  - Receipt of checks.

- Procedures to ensure compliance with DBM's Personnel regulations.

- Procedures to ensure proper use of special payments payroll.

5.5 Procurement

- Segregation of duties for functions of:

  - requisitioning and receiving,
  - purchasing,
  - approval, and
  - accounting.

- Procedures which ensure compliance with the ***Procurement Manual*** issued by the Department of General Services.

5.6 Accounts Payable/Cash Disbursements

- Prompt processing of invoices.

- Checking of invoices (ADPICS should be used)

  - against purchase orders and receiving reports for terms, prices and quantities.
  - for proper Federal Identification Number.
  - to verify it is an original and not a duplicate payment.

- Verifications made to assure that:

  - recurring payments are not missed or duplicated.
  - proper object/sub-object codes are charged.
  - proper vendor number is used and address is current.
  - payment is made through vendor number table.
  - all transmittals with supporting documentation are reviewed and approved by authorized personnel.

- Periodic review of undeliverable and canceled checks by someone independent of the transmittal process.
- A listing maintained of all outstanding travel advances and compared to appropriate expense reports when received.
- Designation of an employee to act as an agency travel coordinator to monitor compliance with the Standard Travel Regulations.
- Adequate approval process and review of "Expedited" payments in R*STARS.

5.7 Inventory

- Maintenance of perpetual inventory records when required under the guidelines promulgated by the Department of General Services.
- Performance of physical inventories with comparison of counts to recorded amounts and needed write-offs approved by the department head or designee.
- Segregation of duties for store keeping, record keeping and inventory taking.
- Preparation of a receiving document and verification with actual goods received.
- Assignment of accountable officers for custodial responsibility of equipment.
- Timely identification and reporting of excess equipment for transfer or disposal.
- Identification by etching or labeling of all items.

5.8 Financial Reporting

- Segregation of duties for:
  - responsibility of approval of journal entries and financial reports from responsibility for their preparation.
  - maintenance of general ledger and custody of the assets.
- Monthly reconciliation of separate agency-based systems' interfaces to R*STARS.

- Journal entries clearly referenced to indicate their source, and reviewed and approved by a responsible official.

- Procedures to ensure that all required forms and reports are submitted within the prescribed time frame.

5.9 Grant Administration

- Assignment of a specific individual for overseeing compliance with major terms of grants received.

- Formalized written procedures to assist personnel in adhering to Federal grant guidelines.

- Monitoring of sub-grantees or subcontractors to provide reasonable assurance of their compliance with grant requirements.

- Adequate support for all billings and financial status reports sent to the Federal government.

5.10 Information Technology Systems

- Security controls to protect hardware and software.

- Segregation of duties for programming, computer operation and manual control.

- Standard documented procedures.

- Batch controls to assure:

    - batches balance
    - rejected entries/corrections are identified and properly reentered
    - manually prepared totals verified against computer posted totals.

- Verification of accuracy of inputted critical data.

- Programmed validity checks for data.

- Consultation of auditors in systems design development.

In addition, it is the State agency's responsibility to ensure that the security accesses requested for employees to FMIS applications are appropriate and consistent with the duties and responsibilities of the employees for whom accesses are requested. When making requests, the following factors should be considered:

- Proper segregation of duties and responsibilities so that no one person performs two or more of these functions:

    - Authorizes transactions
    - Records transactions
    - Custody of assets related records
    - Approval of transactions
    - Reconciliation of assets with recorded amounts.

- Proper review procedures are in place to prevent, detect or correct errors and irregularities. Reviews should be made for validity, completeness, authorization, accuracy and proper classification.

- Proper authorization of transaction (approval paths) should specifically delineate the lines of authority from the highest to the lowest level position.

- Details of the ADPICS internal control and security requirements are enumerated in the FMIS ***Internal Control and Security Policy and Procedures Manual.***

User Class Guidelines

The following guidelines, which are also included in the FMIS security manual, should be considered by the agencies when establishing the aforementioned internal controls and assigning the R*Stars user class combinations.

Agencies will decide, based on the complexities of their accounting operations, how to set up and assign R*STARS user classes. If the agency has sufficient personnel, segregation of duties can be accomplished at a detailed level. For example, groups of individuals may be given user classes for grants, user class 05; accounts receivable, user class 06; cash receipts, user class 07; and journal entries, user class 08. Each of these groups can have a supervisor who has "level 1 approval" for agency action codes, i.e., - includes user classes 15, 16, 17, and 18, respectively, and, if needed, "level 2 approval" i.e., user classes 25, 26, 27 and 28 respectively for each function. User class 11 or 21, assigned depending on the number of approval paths or agency action codes established, will give the accounting manager the ability to approve all transactions.

If the accounting operations have limited personnel and an accountant inputs all accounting entries, then master user class 01 may be given to the accountant. However, in all cases, these transactions should be reviewed and approved before final release and posting. Accordingly, there should be a supervisor or manager with master user classes 11 and/or 21 to approve transactions.

Individuals, i.e., agency vendor coordinators, with update access to the 52 screen, the vendor profile, should not be able to change a disbursement in ADPICS or R*STARS and approve the transaction, (i.e., user classes 01, 08, 11, 18, 21, 28, 80, with the 89 user class and user class 99, with accounting transaction indicator > 0).

Agencies must carefully segregate the disbursement transaction data entry and the ability to change the transactions in R*STARS from the final approval of these transactions and subsequent transmission to the General Accounting Division (GAD). If the person with user class 89, is the person assigned the final detailed review, whether or not they have release ability on the 32 screen, then this person with user class 89, should not also have the ability to enter or change transactions in R*Stars. Persons performing the 89 user class approval, i.e., from the 35 or 39 screen, should carefully review supporting documentation for 100% of the transactions to ensure that the related goods or services were received, and their review should be evidenced on the underlying documents.

If the person assigning the 123, i.e., user class 89 which creates the transmittal, or the person with user class 99, with accounting transaction indicator > 0, also has access to the 32 screen, which appends the 456 for transmission to GAD, this person must not also have the ability to change disbursement transactions in R*Stars. The ability to create and change disbursement transactions in R*Stars is given through user classes 01, 11, 21, 80, and 99, with accounting transaction indicator > 0. Specifically, this segregation requires that the individuals who have user class 01, 11, 21, or 80, should not also have user class 89, release ability, (release flag = 1), and update ability on the 32 screen, which appends action code 456 to transmit the payment transactions to GAD. Also, persons with user class 99, with accounting transaction indicator > 0, which allows disbursement transaction entry and change, and also appends the 123 action code when it interfaces from ADPICS, should not have update ability on the 32 screen. Note that corrected transactions remove the 123 action code, which can only be replaced using the 89 user class.

The Legislative Auditor strongly advises that even in the smallest of agencies no one individual should have the ability to create and change disbursement transactions, append the 123 action code and release the batch via the 32 screen. Having the transmittal thoroughly reviewed and approved by the individual authorized to sign the transmittal's cover sheet provides no control. Employees with the aforementioned incompatible accesses can forge transmittal cover sheet signatures keeping the transmittals from ever being seen by the authorized signer. Agencies must carefully monitor the approval process and establish internal control procedures to minimize the risk associated with incompatible user class combinations.

While the aforementioned procedures should apply to many of the internal control situations encountered by State agencies, the indicated procedures are not meant to be all inclusive. These specific internal control techniques should be further developed and expanded by management personnel as is deemed necessary under the circumstances in order to minimize the vulnerability of the State's assets to fraud, waste and abuse.

Manuals Issued by State Control Agencies

Control Departments Promulgating Authority	Title of Manual
Department of Budget and Fiscal Planning	• Department of Budget and Fiscal Planning Manual • Personnel Manual • Data Processing Manual • R*STARS Manuals • ADPICS Manuals • TESS Manuals • ADHOC Documentation • Security Manual • View Direct Manual
Comptroller of Maryland General Accounting Division	• Accounting Procedures Manual for Use by State Agencies • Internal Control Manual • Corporate Purchasing Card Program Policy and Procedures
Comptroller of Maryland Central Payroll Bureau	• Payroll Procedures Manual for Use by State Agencies
State Treasurer's Office	• Insurance Manual
Office of the Attorney General	• Maryland Tort Claims Act Manual
Department of General Services	• Procurement Manual for Using Agencies • Inventory Control Manual • Records Management Manual

Glossary

Activities - Specific and distinguishable services provided by an organizational unit to accomplish a function for which the government is responsible.

Assessable Entity - A manageable subdivision, segment, department or institution subject to a risk assessment or internal control review.

Assurance Statement - Management's assessment of the effectiveness of the agency's internal control over financial reporting as of March 31 of that fiscal year.

Control Departments - The principal responsibility of control departments is to exercise control over or promulgate policies concerning the operations of the State's departments and independent agencies. Examples are the Department of Budget and Fiscal Planning, the Comptroller of Maryland, and the Department of General Services.

Control Objectives - The goals or targets to be achieved for a specific event cycle. The objectives should be tailored to fit the specific operations in each entity and be consistent with the overall objectives of internal controls.

Control Techniques - Procedures, processes, or documents that are being relied on to efficiently and effectively accomplish a control objective and thus help safeguard an activity from error.

Department - Generally refers to any Executive Branch department, independent agency, office, commission, board, bureau, or other establishment of the State government, including independent regulatory commissions and boards, which are directly responsible to the Governor of the State of Maryland.

Department Component - An agency, a major organization, a program, or a functional subdivision of a department.

Department Head - The chief executive officer of a department who is directly accountable to the Governor.

Event Cycle - Logical work flow pattern which initiates and achieves an end product, creates the necessary documentation and gathers and reports related data.

General Control Environment - Organizational structure and culture created by management and employees to sustain organizational support for effective internal control.

Inherent Risk - The potential for fraud, waste, and abuse due to the nature of an activity. For example, activities conducted within severe time constraints have greater inherent risk than those which are not subject to time constraints.

Internal Accounting Controls - The controls on authorizing, processing, recording, and reporting transactions and which operate within the broader control environment of administrative controls.

Internal Administrative Controls - Broad controls on all activities carried out by officials to accomplish their objectives. Primarily, these activities concern planning, organization, productivity monitoring, improvement, and quality control activities. Administrative controls can be divided into two groups: organizational and operational.

Internal Control - The organization, policies, and procedures which are tools to help program and financial managers achieve results and safeguard the integrity of their programs. The three objectives of internal control are to ensure the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. The safeguarding of assets is a subset of all of these objectives.

Internal Control Report - A comprehensive report prepared by department heads summarizing the results of the risk assessments and, if required, the results of the detailed internal control reviews. For any internal control weaknesses identified, the plans and related schedules for correcting the weaknesses and the status of actions taken to correct weaknesses identified in prior years' reports are given.

Internal Control Review - Examining existing internal controls to determine whether existing measures are adequate to prevent or detect the occurrence of potential risks in a cost effective manner. An internal control review cannot be equated to an audit since the latter is much more comprehensive and requires the application of standards not appropriate for the internal control review.

Materiality - The significance of an event, amount, or error, when measured in the light of surrounding circumstances by a reasonable person. In making a decision or judgment, an event, amount, or error would be material if it affects the reasonable person's decision.

Operating Departments - The principal responsibility of operating departments is the delivery of programmatic services to the general public.

Operational Controls - The controls which provide assurances that the goals and objectives of a department are met effectively, economically and efficiently, and that only authorized activities are carried out.

Organizational Controls - The controls on how the department assigns responsibility and defines authority through its organization structure and delegates authority and supports human capital policies within the structure.

Reasonable Assurance - A satisfactory level of confidence considering costs, benefits, and risks. Reasonable assurance recognizes that the cost of internal control should not exceed the benefit derived.

Report on the Status of Internal Control - See "Internal Control Report".

Risk Assessment - A review of the susceptibility of a department or program to loss or unauthorized use of resources, errors in reports and information, illegal or unethical acts, and/or adverse or unfavorable public opinion.

Segregation of Duties - Assigning duties to individuals so that no one individual controls all phases of the processing of a transaction, thereby permitting errors of omission or commission to go undetected.

Standards of Internal Control - These include control environment, risk assessment, control activities, information and communications, and monitoring.

References

1. Audit of State and Local Governmental Units, American Institute of Certified Public Accountants

2. CARE Audit Methodology, United States General Accounting Office

3. Comptroller's Internal Control and Accountability Directive, City of New York

4. Commonwealth of Virginia, Internal Control Guidance Manual

5. Governmental Auditing Standards, United States General Accounting Office

6. How to Evaluate and Improve Internal Controls for Governmental Units, Government Finance Officers Association of the United States and Canada

7. Miller Comprehensive GAAS Guide

8. State of Tennessee, Guidelines for the Evaluation of Internal Accounting and Administrative Controls

9. OMB Circular No. A-123, Revised

10. Federal Managers' Financial Integrity Act

11. Evaluating Internal Controls, A Local Government Manager's Guide by Stephen J. Gauthier