UNDERSTANDING INTERNAL CONTROLS

A Reference Guide for Managing University Business Practices

Introduction

As servants of public trust, the University System of Georgia (USG) has a great responsibility to utilize the resources provided in the most effective and efficient ways possible while adhering to laws and regulations. A strong system of internal controls is paramount to properly managing USG's resources within the related business processes. Every employee within the USG has some role in effecting internal controls. Roles vary with responsibility, however, Business Officers play a key role in assuring that high standards of business and ethical practices are followed because they are ultimately responsible for the appropriate use and control of the resources entrusted to them.

The purpose of this section of the BPM is to assist employees in their stewardship role in achieving USG's objectives and to provide guidance for the existence of basic and consistent business controls throughout the USG and to define responsibilities for managing them. It addresses the following five interrelated components of internal control in relation to developing business control systems:

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

This guidance is based upon the internal control guidelines as recommended by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. COSO was formed to support the Commission's recommendation to develop additional, integrated guidance on internal control.

Objectives

The objectives of this Section are as follows:

1) Convey to you that management is responsible for ensuring that internal controls are established, properly documented, maintained and adhered to by each institution from top management all the way down to the Department level.

2) Convey to you that all employees of the USG are responsible for compliance with internal controls.

3) Provide guidance to help managers and staff understand the components of internal control, how those components interrelate when developing a system of internal controls and provide tools to establish, properly document, maintain, and adhere to the Institution's system of internal controls.

Scope

This guidance applies to all of the Institution's departments and operations. The examples of control activities contained in this guide are not presented as all-inclusive or exhaustive of all the specific controls appropriate in each department or unit. Over time, controls may be expected to change to reflect changes in your operating environment.

An effective control system provides reasonable, but not absolute assurance for the safeguarding of assets, the reliability of financial information, and the compliance with laws and regulations. Reasonable assurance is a concept that acknowledges that control systems should be developed and implemented to provide management with the appropriate balance between risk of a certain business practice and the level of control required to ensure business objectives are met. ***As a matter of practical application, the cost of a control should not exceed the benefit to be derived from it, unless mandated by a higher authority.***

The degree of control employed is a matter of good business judgment. When business controls are found to contain weaknesses, we must choose among the following alternatives:

- Increase supervision and monitoring;
- Institute additional or compensating controls; and/or
- Accept the risk inherent with the control weakness (assuming management approval).

The guidance presented here should not be considered to "stand alone." This guidance should be used in conjunction with existing policies and procedures.

Responsibility

All employees of the University are responsible for managing internal controls. Each Group, Business Unit, or Department Head is specifically responsible for ensuring that internal controls are established, properly documented, and maintained in each organization.

There are many resources to assist employees in managing their areas of responsibility for internal control systems and processes. Primary resources include the campus CBO, Controller, and campus auditors. In general, while all employees are responsible for the quality of their internal controls, CBOs and Controllers are responsible for providing campus leadership to ensure that effective internal control and accountability practices are in place. Campus auditors normally assist management in their oversight and operating responsibilities through independent audits and consultations designed to evaluate and promote the systems of internal control.

Balancing Risk and Control

Risk is the probability that an event or action will adversely affect the organization. The primary categories of risk are errors, omissions, delay and fraud. In order to achieve goals and objectives, management needs to effectively balance risks and controls. Therefore, control procedures need to be developed so that they decrease risk to a level where management can accept the exposure to that risk. By performing this balancing act "reasonable assurance" can be attained.

In order to achieve a balance between risk and controls**, internal controls should be proactive, value-added, cost-effective and address exposure to risk.**

Characteristics for Fraud

There are generally three requirements for fraud to occur - motivation, opportunity and personal characteristics. Motivation is usually situational pressures in the form of a need for money, personal satisfaction, or to alleviate a fear of failure. Opportunity is access to a situation where fraud can be perpetrated, such as weaknesses in internal controls, necessities of an operating environment, management styles and corporate culture. Personal characteristics include a willingness to commit fraud. Personal integrity and moral standards need to be “flexible” enough to justify the fraud, perhaps out of a need to feed their children or pay for a family illness.

It is difficult to have an effect on an individual’s motivation for fraud. Personal characteristics can sometimes be changed through training and awareness programs. Opportunity is the easiest and most effective requirement to address to reduce the probability of fraud. By developing effective systems of internal control, you can remove opportunities to commit fraud.

Internal Control Defined

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

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

Several key points should be made about this definition:

1) ***People at every level of an organization affect internal control.*** Internal control is, to some degree, everyone's responsibility. Generally, administrative employees at the department-level are primarily responsible for internal control in their departments. Consequently, the responsibility for controls over accurate financial and reporting primarily falls under the oversight of Institution's Business Officers.

2) ***Effective internal control helps an organization achieve its operations, financial reporting, and compliance objectives.*** Effective internal control is a built-in part of the management process (i.e., plan, organize, direct, and control). Internal control keeps an organization on course toward its objectives and the achievement of its mission, and minimizes surprises along the way. Internal control promotes effectiveness and efficiency of operations, reduces the risk of asset loss, and helps to ensure compliance with laws and regulations. Internal control also ensures the reliability of financial reporting (i.e., all transactions are recorded and that all recorded transactions are real, properly valued, recorded on a timely basis, properly classified, and correctly summarized and posted).

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

Internal Control Process

Internal control consists of five interrelated components as follows:

- Control (or Operating) environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

All five internal control components must be present to have effective internal controls. Also, when considering the five components of internal control, certain components relate more to the organization as a whole, while other components relate to specific financial reporting areas or transaction classes. The following table illustrates the distinction between organizational (high level) controls and functional (activity/transactional) level controls:

Components of Internal Control	Primary Level of Application	
	Organization Level	Functional(Activity Level)
Control Environment	✓	
Risk Assessment	✓	
Information and Communication	Communication	Information Systems
Control Activities		✓
Monitoring	✓	

The remainder of this document will be devoted to discussing the 5 components of internal control in detail and provide the following:

1) Show interrelationships between the various components of internal controls
2) Provide suggestions to help improve effectiveness
3) Provide sample forms to assist in the documentation of internal controls

ORGANIZATIONAL LEVEL CONTROLS

Control Environment

The control environment sets the tone for the organization and influences how employees conduct their activities and carry out their control responsibilities. The control environment is the foundation for all other components of internal control and provides structure and discipline. Developing a strong culture of control consciousness within the Institution is one of the most cost-effective and efficient ways that internal control over financial reporting can be implemented. Its effect can permeate throughout the Institution, directly impacting each of the other components of internal control. Among the important factors are the attitude, awareness, and actions of management and directors concerning internal control. The personal characteristics, philosophy, and operating style of members of management can have a significant influence on the organization's commitment to reliable financial reporting.

An effective control environment must incorporate the following principles: 1) Integrity and ethical values, 2) Commitment and competence, 3) Attention and oversight provided by Board of Directors or audit committee, 4) Management philosophy and operating style, 5) Organizational structure, 6) Manner of assigning authority and responsibility, and 7) Human Resources policies and procedures.

The following table will provide some guidance on control environment principles (controls) and related control objectives (purpose of controls) as well as possible ways to document that those objectives are being met:

Control Environment Principle	Control Objective	Documentation(*)
Integrity and ethical values.	Management, through its attitudes and actions, demonstrates character, integrity, and ethical values. Sound integrity and ethical values, particularly of top management, are developed and set the standard of conduct for the organization and financial reporting.	Provide employees Code of Conduct. Also provide method for reporting violations through whistleblower provisions. Tone at the top.
Commitment to competence.	The entity is committed to competence in the requirements of particular jobs and in translating those requirements into knowledge and skills.	Employee training and Evaluations
Attention and oversight provided by a board of directors or audit committee (those charged with governance).	The board of directors and/or audit committee is actively involved and has significant influence over the entity's internal control environment and its financial reporting.	Corporate Bylaws and formal policies for financial reporting. Audit committee. Whistleblower program
Management's philosophy and operating style.	Management's philosophy and operating style are consistent with a sound control environment and have a pervasive effect on the entity. Management analyzes the risks and benefits of new ventures, assesses turnover among employees, investigates and resolves improper business practices, views accounting as a means to monitor and control the various activities of the organization, and adopts accounting policies that reflect the economic realities of the business.	Degree of care taken in developing policies and procedures related to financial reporting.
Organizational structure.	The organizational structure of the entity is appropriately designed to promote a sound control environment. Authority and responsibility, appropriate reporting lines, and free flow of information across the organization provide unfettered influence to effectively run the entity and support effective financial reporting.	Organizational charts reflecting roles and responsibilities. Defined job duties of key employees.
Manner of assigning authority and responsibility.	The entity assigns authority and responsibility to provide a basis for accountability and control.	Clearly defined responsibilities and authority limits (Segregation of duties)
Human resources policies and procedures.	Human resource policies and procedures send messages to employees regarding expected levels of integrity, ethical behavior, and competence.	Human resources policy manual. Ethics training. Formal job descriptions. Emphasis on accountability.

(*) Some of the control areas listed above relates more to intrinsic qualities and values of management and therefore they are difficult to evaluate from formal documentation. In those instances, auditors will most likely look at the presence or absence of problems to evaluate operating effectiveness.

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

Suggestions for effective Control Environment

Listed below are some suggestions to enhance a department/business unit's control environment. This list is not intended to be all-inclusive, or applicable for all departments, however, it should be helpful in promoting an effective control environment.

1) Make sure that the following policies and procedures are available in your department (hard copy or Internet access):

    Business Procedures Manual
    Employees Purchasing Manual
    Policies and Procedures Manual

2) Make sure that departments have well-written departmental policies and procedures which address its significant activities and unique issues. Employee responsibilities, limits to authority, performance standards, control procedures, and reporting relationships should be clear.
3) Make sure that employees are well acquainted with the Institution's policies and procedures that pertain to their job responsibilities.
4) Discuss ethical issues with employees. If any employees need additional guidance, make sure that it is provided.
5) Make sure that employees comply with the Conflict of Interest policy and disclose potential conflicts of interest (*e.g.*, ownership interest in companies doing business or proposing to do business with the University System).
6) Make sure that job descriptions exist, clearly state responsibility for internal control, and correctly translate desired competence levels into requisite knowledge, skills, and experience; make sure that hiring practices result in hiring qualified individuals.
7) Make sure that the department has an adequate training program for employees.
8) Make sure that employee performance evaluations are conducted periodically. Good performance should be valued highly and recognized in a positive manner.
9) Make sure that appropriate disciplinary action is taken when an employee does not comply with policies and procedures or behavioral standards.

Risk Assessment

The central theme of internal control is (1) to identify risks to the achievement of an organization's objectives and (2) to do what is necessary to manage those risks. Another way of saying this is that Risk Assessment is the process of setting objectives; prioritizing and linking those objectives; and identifying, analyzing, and managing risks relevant to achieving those objectives.

Risk assessment is the identification and analysis of risks associated with the achievement of operations, financial reporting, and compliance goals and objectives. This, in turn, forms a basis for determining how those risks should be managed.

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

A risk is anything that could jeopardize the achievement of an objective. The following are common questions that management should ask themselves to help identify risks:

1) What could go wrong?
2) What assets should we be protecting?
3) How do we protect our assets?
4) What do we do to prevent theft/fraud?
5) What activities are regulated by outside authority (federal or state)?
6) What external exposures do we have?
7) How could someone disrupt operations?
8) How do we know we are achieving our objectives?
9) How would this look to an outsider?

Financial Reporting Risk Assessment Process

From a financial reporting objective, the entity’s risk assessment process involves the identification, analysis, and management of the risks of material misstatement of the financial statements. The institution’s risk assessment process would include the following:

Financial reporting objectives,

Management of financial reporting risks,

And, consideration of fraud risk.

There are basically 4 steps in the risk assessment process. First, objectives need to be set before risk assessment begins. Second, management must identify the risks associated with achieving objectives, next management must perform a risk analysis to determine the extent of the risk and how it should be managed, and finally control activities should be implemented to manage risks. As a follow-up step, institutions should have effective monitoring in place to ensure controls are being consistently performed.

For financial reporting, appropriate control objectives would be:

Entity and financial reporting objectives are established, documented, and communicated.
Accounting principles are properly applied in the preparation of the financial statements.

For management of financial reporting risks, appropriate control objectives would be:

Management has established practices for the identification of risks affecting the entity.
Management considers the entire organization as well as its extended relationships in its risk assessment process.
Management has implemented mechanisms to anticipate, identify, and react to changes.
Management evaluates and mitigates risk appropriately.

For consideration of fraud risks, an appropriate control objective would be:

Management has developed an appropriate fraud risk assessment and monitoring process.

After control objectives are established, management should identify risks that would prevent these objectives from being met. Both external and internal factors affect risk. When an organization identifies and assesses various risks, it is important that the process be comprehensive. In this risk assessment process, the many interrelationships of factors should be considered including relationships between the organization and relevant third parties such as customers, suppliers, regulatory entities, etc.

Risks should also be identified at the activity level. Besides contributing to the risk identification process at the organization level, activity level risks also take into account those risks associated with business operations and activities. Listed below are accounts and other disclosure items that are normally significant to USG institutions at the Financial Statement level:

Balance Sheet Items
Cash (including Petty Cash
if high volumes are processed)
Capital Assets
Payables (Salaries, A/P, Contracts)
Capital Leases
Compensated Absences

Other Items
Financial Statement Presentation
Journal Entries
Accounting Estimates
Special or Unusual Items

Revenues and Expenses
State Appropriations
Tuition and Fees
Grants Accounting
Auxiliary Services
Capital Grants and Gifts
Sales and Services
Operating Expenses/Cash Disb.
Salaries and Benefits
P-Card Expenses
Construction Costs
Scholarships/Fellowships
Utilities

After risks have been identified, management should conduct a risk analysis to determine (1) likelihood or risk occurring, (2) potential impact if risk were to occur (quantitative and qualitative factors should be considered), (3) how the risk will managed (what actions will be taken). Prioritizing risks in this manner helps to direct resources in a manner to properly manage the most significant risks.

The final step in the risk assessment process will be to establish control activities in response to perceived risks. For the purposes of financial reporting, those "risks" relate to the following assertions inherent in financial statements:

1) Existence or occurrence – states that assets, liabilities and ownership interests exist at a particular date (balance sheet date) and that recorded transactions are those that have actually occurred during a given period.
2) Completeness – indicates that all transactions and events that have occurred during the period have been recorded in the financial statements.
3) Rights and obligations – states that as of a given date, assets are the rights of the organization and the liabilities are the obligations of the organization.
4) Valuation or Allocation – indicates that assets, liabilities, revenues and expenses are recorded in the financial statements at the appropriate amounts in accordance with accounting principles and that they are mathematically correct and summarized properly.
5) Presentation and Disclosure – addresses that items appearing in the financial statements are properly described, sorted and classified.

External Auditors Consideration of Risk

Auditing Standards require the external auditor to obtain a sufficient knowledge of management's risk assessment process to evaluate how management considers risks relevant to financial reporting objectives. Auditors normally focus on the following issues:

1) How does management identify risks relevant to financial reporting?
2) How does management estimate the significance of the risks?
3) How does management assess the likelihood of their occurrence?
4) How does management decide on actions to manage those risks?

Since auditors take this approach, it is imperative that management conduct a risk analysis to prioritize risks and make sure that organizational resources are properly utilized to manage significant risks to reduce the likelihood of occurrence.

The auditor is also required to evaluate whether the entity's controls sufficiently address the identified risks of material misstatement due to fraud and the risks of management override of other controls. Such controls might include those relating to:

1) Significant or unusual transactions.
2) Journal entries and adjustments made in the period-end financial reporting process.
3) Related party transactions.
4) Significant management estimates.
5) Incentives for and pressures on management to falsify or inappropriately manage financial results.

Communication

Communication is one part of the information and communication component of internal control. Just as all organizations need information to operate a business, communication is an essential aspect of information systems. Communication of expectations, responsibilities, and other matters is necessary for the business to operate effectively.

Communication relates to providing a clear understanding of financial reporting and safeguarding controls, how they work, and the responsibilities of individuals within the organization related to those controls. Effective communication also includes communication of organization standards of conduct to third parties with whom the institution conducts business. Communication may take the form of policy manuals, memoranda, letters, oral communications, etc. The form of communication depends on the size and structure of the organization.

Communication is another way that management conveys the tone at the top. Management should communicate the information necessary for employees to perform their assigned tasks, for managers to supervise, and for responsible parties to make key operating and financial decisions. In particular, it is important that management clearly communicate:

1) That internal control responsibilities are a critical part of employees' job duties,
2) The roles and responsibilities that each employee has in the internal control system,
3) That unexpected events should be investigated, including determining the cause of the event,
4) How job activities relate to the work of others.

Monitoring

Since institutions and their personnel continuously change, it is essential that controls be monitored over time to determine whether they continue to be relevant and are able to address new risks to the institution. Monitoring is a process that assesses the quality of an organization's internal control over time and involves assessing the design and operation of controls on a timely basis and taking actions as necessary. Monitoring activities can also reveal evidence or symptoms of fraud.

There are a number of reasons that an internal control system may change over time. The manner in which controls are placed in operation may change. This may be because controls are applied differently as control processes continue to evolve, or controls that were previously effective may no longer be performed, or just may not be effective. Among the reasons that control procedures may no longer be effective are changes in personnel, less effective training or supervision, limitations on time or resources, or other pressures. In addition, the risks and conditions that control procedures were designed to address may change, which would impact control effectiveness.

A good monitoring process helps ensure that control activities and other planned actions to affect internal controls are carried out properly and in a timely manner sufficient to ensure that the end result is effective internal controls. Ongoing monitoring activities should include various management and supervisory activities which evaluate and improve the design, execution, and effectiveness of internal controls. Periodic monitoring activities, such as self assessments by various departments and internal audit appraisals, also provide helpful information.

Managers, like auditors, don't need to look at every piece of information to determine if controls are functioning properly. Managers should focus their efforts on high risk areas. They can use spot checks of transactions or basic sampling techniques to gain a reasonable level of confidence that the controls are functioning as intended.

FUNCTIONAL (ACTIVITY LEVEL) CONTROLS

As discussed earlier when looking at the 5 components of internal control process, certain components relate more to the organization as a whole while others relate more to specific financial reporting areas or transaction classes. This subsection discusses those components that relate to the flow of information specific to a given area, transaction, or account balance. Those components are referred to as functional (activity) level controls. They are comprised of the information systems component of Information and Communication and Control Activities.

Information Systems

Information systems are used to generate information necessary to carry out many control activities. An information system may be computerized, manual, or a combination of the two, depending on the size and complexity of the organization. The information system relevant to financial reporting (the "financial reporting system") consists of automated and manual procedures and records established to initiate, record, process, and report organization transactions (as well as events and conditions) and to maintain accountability for the related assets, liabilities, and equity.

An effective financial reporting system includes methods and records for:

Identifying and recording all valid transactions,
Describing the transactions on a timely basis and in enough detail to permit proper classification in the financial statements,
Valuing transactions in a way that allows them to be reported at their proper amounts in the financial statements,
Providing sufficient information to permit recording of transactions in the proper accounting period, and
Properly presenting the transactions and related disclosures in the financial statements.

The quality of information generated by an institution's information systems is critical to the institution's operations and success. Whether the information stems from automated or manual systems, the quality of the information affects whether management will be able to make appropriate decisions relating to managing and controlling the organization's activities. The important factors to consider in determining the quality of an information system are:

Whether the needed information is provided,
Whether the needed information is provided on a timely basis,
Whether the information is current,
Whether the information is accurate, and
Whether the information is easily accessible by the appropriate persons.

While the focus here is on Information systems at the functional level because of the significance information systems have on the flow of information for significant transaction classes and processes that relate to key financial reporting areas, information systems have implications at the organizational level as well. The consideration of the information process at the organization level focuses on making an overall evaluation of whether the institution has established an overall process or structure to ensure that financial reporting objectives as a whole has been achieved.

When evaluating the effectiveness of information systems the following factors should be considered:

(1) Does external and internal information obtained from the information systems provide management with necessary reports on the organization's performance relative to ensuring reliable financial reporting and safeguarding of assets?
(2) Do the information systems provide the right information on time to the right people, so that they may fulfill their responsibilities effectively and efficiently?
(3) Are information systems developed and revised under a strategic plan that is linked to the organization's overall objectives and strategies?
(4) Does management show their commitment to developing appropriate information systems by assigning appropriate resources?

The evaluation for controls of information systems is largely based on the flow of information for significant transaction classes and processes that relate to key financial reporting areas which take place at the control activities level.

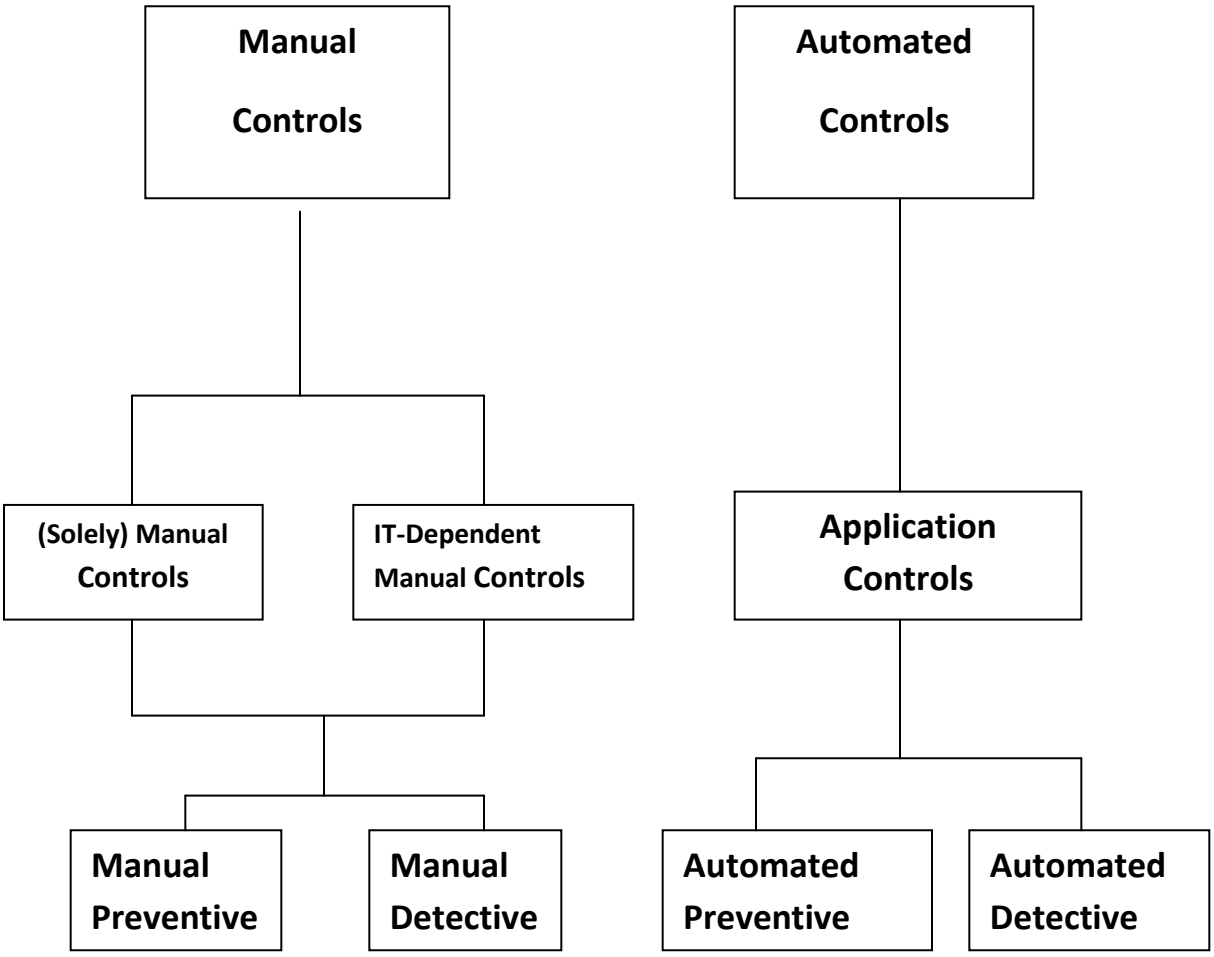
Since the effectiveness of information systems is inherently connected to how Control Activities are designed and implemented, specific applications will be discussed in the following section on Control Activities.

Control Activities

Control activities are those actions that are taken to address risks that threaten the entity's ability to achieve its objectives, one of which is reliable financial reporting. Control activities are usually supported by (1) a policy that established what should be done, and (2) the procedure that implements the policy.

Nature of Controls

Controls can generally be broken down into 2 broad categories: (1) manual controls, and (2) automated controls. Those two categories can be broken down further as follows:



Manual Controls are controls that are manually performed by individuals. They may be solely manual where no IT generated reports are used or they may be IT Dependent whereby an employee is using a system generated report to test the validity of a particular control.

Application controls are performed entirely by the computer system. These controls are discussed in more detail in item 6 below.

Preventive controls attempt to deter or prevent undesirable events from occurring. They are proactive controls that help to prevent a loss. Examples of preventive controls are separation of duties, proper authorization, adequate documentation, and physical control over assets.

Detective controls, on the other hand, attempt to detect undesirable acts. They provide evidence that a loss has occurred but do not prevent a loss from occurring. Examples of detective controls are reviews, analyses, variance analyses, reconciliations, physical inventories, and audits.

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

Types of Control Activities

Control activities occur throughout the organization, at all levels and in all functions. They include a range of detective and preventive control activities as described below:

1) ***Approvals, Authorizations, and Verifications (Manual and/or IT-Dependent, Preventive).*** Management authorizes employees to perform certain activities and to execute certain transactions within limited parameters. In addition, management specifies those activities or transactions that need supervisory approval before they are performed or executed by employees. A supervisor's approval (manual or electronic) implies that he or she has verified and validated that the activity or transaction conforms to established policies and procedures.

   Authorization and approval are the most important elements of this control activity. Some specific control aspects should be observed. For example, appropriate limits should be established for approval authority, blank approval forms should never be signed, passwords for electronic approval authority should never be shared, person initiating transaction should not also approve transaction, and written policies and procedures should be available with documents approval levels and limits.

2) ***Reconciliations (Manual and/or IT Dependent, Detective).*** An employee relates different sets of data to one another, identifies and investigates differences, and takes corrective action, when necessary.

   This Control Activity helps ensure accuracy and completeness of transactions. Examples would be monthly bank reconciliations, monthly financial report reconciliations, etc. **A critical element to remember is that a reconciliation is no good unless the variances identified are researched, explained and resolved.**

3) ***Reviews of Performance (Manual and/or IT Dependent, Detective).*** Management compares information about current performance to budgets, forecasts, prior periods, or other benchmarks to measure the extent to which goals and objectives are being achieved and to identify unexpected results or unusual conditions that require follow-up.

   This Control Activity also includes management's review of reconciliations, reports and other information generated from item (2) above which substantiates the accuracy of the reconciliations performed.

4) ***Security of Assets (Manual and IT Dependent Manual, Preventive and Detective).*** Access to equipment, inventories, securities, cash and other assets should be restricted. Also, assets should be periodically counted and compared to amounts shown on control records.

   This Control Activity is critical because liquid assets, vital documents, critical systems and confidential information must be safeguarded against unauthorized acquisition, use or disposition. Generally limiting access to these assets is the best way to protect them whether by physical controls such as locked doors or alarm systems or by IT controls such as passwords, data encryption, etc. Periodic inventory counts should be made and perpetual inventory records should be maintained.

5) ***Segregation of Duties (Predominately Manual, Preventive).*** Duties are segregated among different people to reduce the risk of error or inappropriate action. Normally, responsibilities for authorizing transactions, recording transactions (accounting), and handling the related asset (custody) are divided.

   Typically no one person should initiate a transaction, approve the transaction, record the transaction, reconcile balances, handle assets, and review reports. Segregation of duties is one of the best fraud deterrents and if the size the staff prevents adequate segregation of duties, then a compensation control activity such as supervisory reviews must be implemented. See **Appendix A** to assist in determining proper Segregation of Duties for institutions with limited business office staff. **Completion of the Segregation of Duties Matrix will help identify areas where compensating controls are needed.**

6) ***Controls over Information Systems (IT Dependent Manual and Automated, Preventive and Detective).*** Generally speaking there are 4 types of IT controls: General controls, IT dependent manual controls, Application controls, and End-User Computing controls.

   General Controls – set the tone within the IT control environment by supporting the functioning of Application Controls and IT Dependent Manual Controls. These commonly include controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance.

   IT Dependent Manual Controls – These are processes that are manually performed by individuals, but rely on computer generated information. To ensure the effectiveness of IT Dependent Manual Controls, one must validate the accuracy and completeness of the system-generated report and the effectiveness of the manual portion of the control.

IT Application Controls – These are "computer controls" based on the Institution's business rules (system settings). These controls determine how transactions will be input, processed and output by the computer system.

Input controls ensure the complete and accurate recording of authorized transactions by only authorized users; identify rejected, suspended, and duplicate items; and ensure resubmission of rejected and suspended items. Examples of input controls are error listings, field checks, limit checks, self-checking digits, sequence checks, validity checks, key verification, matching, and completeness checks.

Processing controls ensure the complete and accurate processing of authorized transactions. Examples of processing controls are run-to-run control totals, posting checks, end-of-file procedures, concurrency controls, control files, and audit trails.

Output controls ensure that a complete and accurate audit trail of the results of processing is reported to appropriate individuals for review. Examples of output controls are listings of master file changes, error listings, distribution registers, and reviews of output.

End-User Computing Controls – This type of IT control comes into play when using departmentally developed spreadsheets or data bases as tools for performing work which extends to the information reported in the financial statements. Important control elements would be employee access, accuracy and process integrity, backup and review. An example would be Nvision reports that are used in financial reporting.

Control activities must be implemented thoughtfully, conscientiously, and consistently. A procedure will not be useful if performed mechanically without a sharp continuing focus on conditions to which the policy is directed. Further, it is essential that unusual conditions identified as a result of performing control activities be investigated and appropriate corrective action be taken.

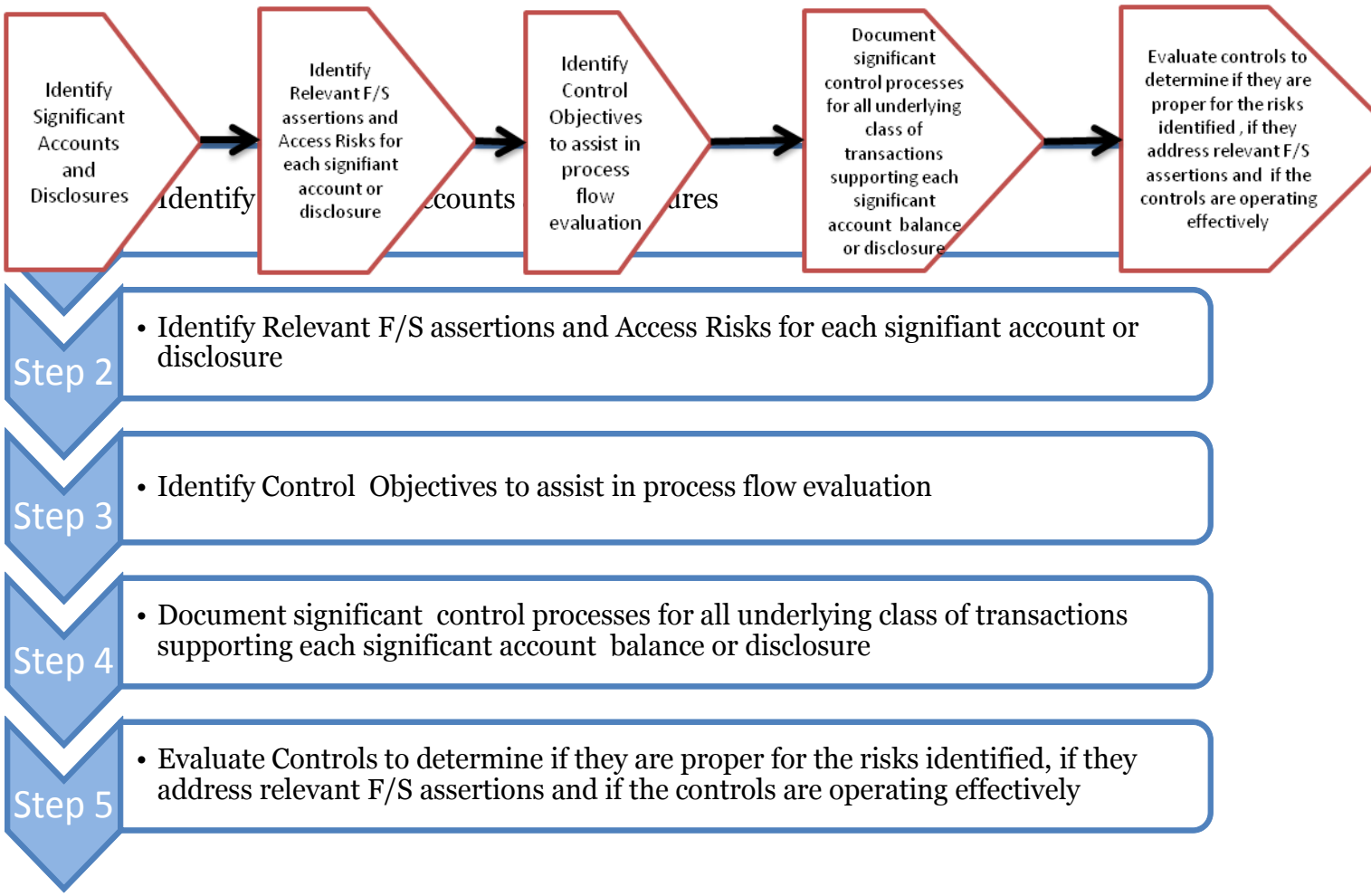
Integration of Control Activities with Risk Assessment Process

Control activities are the mechanism for managing risks, therefore, institutions should integrate Control Activities with the Risk Assessment Process. Control activities should be established in response to perceived risks, and for the purpose of financial reporting, which relate to assertions inherent in financial statements (existence or occurrence, completeness, rights and obligations, valuation and allocation, and presentation and disclosure) as well as actual risks of safeguarding assets from unauthorized acquisition, use, or disposition.

Controls Assessment

Most guidance provided recommends a **top-down approach** to internal control evaluation. That basically means that you should begin with an identification and assessment of risks at the financial statement level, and then move down to the significant account and disclosure level to determine whether controls have been placed in operation to address those risks. By taking this approach you can more easily identify items at the financial statement level that are highly risky and/or have significant or material balances which much be addressed from a control perspective to ensure that financial statements are fairly presented. Likewise, when risks are minimal and account balances are relatively insignificant, management would not have to expend extensive resources over controls for those reporting areas.

The following diagram depicts how a top-down internal control process evaluation would work:



Note: If you have decentralized business units that perform financial operations related to significant accounts you must consider the scope of the work performed and if significant to an account balance or class of transactions you should consider the risks to financial reporting to determine if an internal control process evaluation would be necessary for those decentralized

operations.

The Internal Control Documentation Worksheet (Appendix "B") has been developed to assist Institutions in documenting the internal control process(es) related to significant accounts and disclosures. You are not required to use this particular form if you already have one developed that meets documentation requirements of the external auditors, however, this form has been reviewed by the auditors and they are in agreement that it includes the elements needed to properly document your internal controls. As with any document, it must be accurately completed and properly documented for all significant accounts, processes and disclosures.

APPENDIX "A"

Separation of Duties for Primary Accounting Functions
Cash Receipts, Cash Disbursements, Payroll

Two-Person Office

Business Manager	Chief Financial Officer
Mail checks	Approve and Sign checks
Write checks	Sign employee contracts
Approve payroll	Distribute payroll
	Process vendor invoices
Record accounts receivable entries	Complete deposit slips
Receive cash	Reconcile petty cash
Disburse petty cash	Perform interbank transfers
Reconcile bank statements	Receive, open and review bank statements
Authorize purchase orders	
Authorize check requests	Review Bank reconciliations
Authorize invoices for payment	
Record credits/debits in accounting records	
Record G/L entries	

Three-Person Office

Bookkeeper	Office Manager	Chief Financial Officer
	Mail checks	Sign checks
Record accounts receivable entries	Disburse petty cash	Complete deposit slips
Reconcile petty cash	Approve invoices	Perform interbank transfers
Write checks	Authorize purchase orders	Sign employee contracts
Record general ledger entries	Approve payroll	Receive, open, and review bank statements
Reconcile bank statements	Receive cash	
Process vendor invoices	Distribute payroll	
Record credits/debits in accounting record	Authorize time sheets	Review Bank reconciliations

Four-Person Office

Bookkeeper	Clerk	Office Manager	Chief Financial Officer
Record A/R entries	Distribute payroll	Complete deposit slip	Sign checks
Reconcile petty cash	Receive cash	Approve invoices	Sign employee contracts
Write checks	Disburse petty cash	Approve payroll	Approve time sheets
Record G/L entries	Authorize POs	Process Vendor	Perform interbank transfers
Reconcile bank statements	Authorize ck requests	Invoices	Receive, open, & review bank statements
Record credits/debits in accounting records	Mail checks		Review Bank reconciliations