University of Alabama System

THE UNIVERSITY OF ALABAMA
THE UNIVERSITY OF ALABAMA AT BIRMINGHAM
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE
THE UAB HEALTH SYSTEM

Understanding Internal Controls

Office of Internal Audit

July 2015

Objectives for this manual

- Provide guidance to help management understand their responsibility to ensure that internal controls are established, properly documented, maintained, and followed by everyone from senior management down to the staff level.
- Ensure faculty and staff understand their responsibility for compliance with internal controls.
- Provide guidance for faculty and staff about the components of internal control and tools to establish, properly document, maintain, and follow an effective system of internal controls.

Scope of this manual

Understanding internal controls applies to all areas. The examples of internal control activities in this manual should not be interpreted as an all-inclusive guide of all control activities appropriate for each department. With time, control processes should change to reflect changes in the operating environment.

How much control to employ is a business decision. When a weakness is identified in a control, management must choose among the following alternatives.

- Additional supervision and monitoring
- Additional or compensating controls
- Accept the risk(s) associated with the identified control weakness(es). This alternative should be considered after an evaluation of the costs and risk exposure. Decisions to accept significant risk, rather than address the control weakness, requires approval by senior management and a disclosure to the audit committee.

This manual is not a substitute for existing policies and procedures. The guidance provided in this manual should be used in conjunction with existing policies and procedures.

Table of Contents

Introduction to Risk Management

The concept of risk management is included in the internal control manual because risk and internal control are interrelated. When a risk is identified management may implement a control(s) that will mitigate the risk - the control(s) should be cost effective and reasonable.

All activities of the University involve risk. There is no uniform risk management framework but the management of risk usually involves the following:

- Identifying the risk
- Assessing the impact of the risk and the probability of occurrence
- Determining the risk treatment
- Determining the risk owner

Identifying the risk is the process of recognizing and describing the risk. For example, with regard to cash, an identifiable and recognized risk is the "inappropriate safeguarding of cash."

Assessing the impact of the risk and the probability of occurrence is the process of assessing the potential severity of impact (generally a negative impact, such as damage or loss) and the likelihood of occurrence. For example, without the proper internal controls cash could be stolen, which would result in a loss to the University and the probability of occurrence could be high.

Determining the risk treatment is the process of deciding to avoid the risk, mitigate the risk, or accept the risk. In the example above, the process of avoiding the risk would result in not accepting cash, which may not be an acceptable alternative as it could affect customer service. Accepting would not be appropriate because of the high risk of loss. So the best treatment would be to implement the proper internal controls to ensure that cash is properly safeguarded.

Determining the risk owner is the person who has the accountability or the authority to manage the risk. Normally, this is the person that has the overall responsibility of determining the risk treatment.

What Are Internal Controls?

Mission of the University requires a wide variety of tasks and assignments, completed by employees in numerous physical locations and with many diverse skill sets and backgrounds. Each of us has some level of University resources available to us as we complete our day-to-day tasks and projects. "Internal Controls" are the mechanism that allows us to minimize risk and protect the University's resources to ensure that they are used for legitimate purposes.

Internal controls enable the University to accomplish the following:

- Achieve goals
- Carry out management directives
- Reduce unpleasant surprises
- Enhance the reliability of information
- Promote effectiveness and efficiency of operations
- Safeguard assets
- Comply with rules and regulations

Internal controls may be preventive, detective, or directive.

- Preventive controls are considered proactive controls and are intended to prevent loss, errors, or omissions.
- Detective controls provide evidence after-the-fact of a loss or error, but do not prevent an occurrence. Detective controls play a critical role in providing evidence that preventive controls are working as intended.
- Directive controls are designed to establish desired outcomes.

A control conscious environment (preventive control) is a critical element of internal control and conveys an attitude of honesty and accountability at all levels. Management is responsible for "setting the tone at the top" for their areas and encouraging the highest level of integrity and ethical behavior, as well as exhibiting leadership behavior that promotes internal control and accountability.

Common internal control activities and objectives include the following:

- Authorization and Approval
- Continuity of Operations
- Documentation
- Management Oversight
- Monitoring
- Policies, Standards, Process, and Procedures
- Reconciliation
- Safeguarding Assets
- Segregation of Duties

The following pages discuss in more detail the above internal control activities and objectives.

Select control objectives (not discussed in detail in this manual) include the following:

- *Accuracy* – to ensure transactions are properly calculated
- *Classification* – to ensure transactions are properly classified
- *Completeness* – to ensure all valid transactions are recorded
- *Existence* – to ensure recorded transactions actually occurred and were recorded only once
- *Timeliness/Cutoff* – to ensure transactions are recorded in correct period
- *Valuation* – to ensure appropriate measurement and recognition principles are applied

Key Controls

A key control is a significant control that provides assurance that the organization is achieving key business objectives.

- These are the controls that management is most dependent upon to make certain that things get completed the right way.
- These controls may mitigate a number of risks.
- Absence of these controls would increase risk.

Management Override of Internal Controls

Management may be in a position to override internal controls. Override may be considered by someone who feels they have "too many important things to do" to comply with established procedures or someone with intent to avoid detection for wrongdoing.

The risk of management override is most effectively mitigated by creating a culture where integrity is held in high esteem and practiced every day. The message must be clear – internal control procedures apply to every individual in the organization.

In a strong control environment, timely and appropriate actions are taken when problems are discovered and employees feel comfortable reporting issues without fear of retaliation.

Established internal controls should be followed by everyone – left unchecked, management override can negate the effectiveness of other internal control measures.

Authorization and Approval

Preventive Controls

Authorization is a control activity that assures transactions are only permitted in accordance with management's directives. Approval of a transaction means that the approver has reviewed the supporting documentation and is satisfied that the transaction is appropriate, accurate, and complies with policies, procedures, laws and other applicable requirements. Before a transaction is approved the following should be performed.

- Review original supporting documentation to ensure that necessary information is present to justify the transaction.
- Verify the accuracy of the classification of the expense (i.e., object/account code is correct, amount is accurate).
- Question unusual items.
- Ensure unallowable expenses are not charged to grants, contracts, or state accounts.
- Ensure business purpose is clearly documented.
- Ensure expenses are consistent with donor intent and restrictions, if applicable.
- Ensure that the payee name and address on disbursement transactions match the supporting documentation.

Additional Best Practices for Authorization and Approval Controls

- Give approval authority only to individuals with sufficient authority and knowledge to recognize and challenge unusual transactions.
- Link approval authority to specific dollar levels – transactions that exceed the specified dollar amount should require approval at a higher level. Transactions should never be split to avoid higher approval limits.
- A person should never approve a transaction for which they are the payee (or are related to the payee).
- A person should not approve transactions to, or for the benefit of, their supervisor.

Continuity of Operations

The goal of continuity of operations is to ensure that essential functions can be continued throughout, or resumed rapidly after, a disruption following a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.

The **Business Continuity Plan** should outline how an area will complete its critical tasks during an emergency, or in the absence of a critical information system or other critical resource. The plan should include employee roles during an emergency, computer hardware and other critical electronic equipment such as two-way communications, alternate backup hardware, backup activities and system recovery, including expected recovery time. The business continuity plan should be tested to determine viability and to identify weaknesses in the plan, which can be corrected and re-tested before an actual emergency situation arises. All personnel should be familiar with their roles in business continuity.

The **Disaster Recovery Plan** specifies procedures an area is to follow in the event of a disaster. It is a comprehensive statement of consistent actions to be taken before, during, and after a disaster. A disaster recovery plan should include the following:

- Alternative processing method for both critical and noncritical applications
- IT and user personnel requirements and special skills needed in the event of an unanticipated processing disruption
- Storage of critical replacement forms, supplies, and documentation off-site
- Recovery priority for all applications to determine the sequence of restarting critical systems following an unanticipated processing disruption
- Assessment of the lead time between loss of application processing and adverse impact on operations to determine acceptable downtime

Detailed disaster recovery plans should be documented and tested periodically to ensure recovery can be accomplished. Where tests of the full disaster recovery plans are impractical due to business conditions or the cost of testing, test plans should be developed and implemented to test portions of the plan. Custodians of computer systems, in conjunction with application owners, should review and update the disaster recovery plan annually or after significant changes. Updates should reflect changes in application, hardware, and/or software.

Select controls related to business continuity and disaster recovery include the following:

- Maintain adequate surge protection and uninterruptible power supplies for critical equipment and systems – test equipment periodically.
- Provide adequate environment, including heat and air condition, for critical equipment and systems.
- Protect critical assets from exposure to water, smoke, chemicals, and dust.
- Maintain up-to-date fire suppression equipment for critical assets – test equipment periodically.
- Conduct fire and other emergency procedure drills with all personnel.
- Protect power and data cables from disruption, interference, or interception of data.

Documentation

Directive Controls

Documentation furnishes evidence or information regarding a decision, event, transaction, policy or system. Documentation should be clear, complete, accurate, and recorded timely. Documentation facilitates the performance of processes and procedures in an efficient, consistent, and reliable manner and serves as a method of training (i.e., manuals and guides).

Documentation should enable management to trace each transaction from its inception through its completion. This means the entire life cycle of the transaction should be recorded. For example, the purchase of equipment would begin with an authorized purchase request, continued with a purchase order, vendor invoice, receiving confirmation, and final payment documentation. Stages of documentation include the following:

- Initiation and authorization
- Progress through all stages of processing and receiving
- Final classification in financial and supporting records

The following is an example of cash receipt process.

- Collect payment.
- Prepare a pre-numbered receipt including the date, method of payment, amount of payment, and purpose for payment.
- Provide receipt to payer and retain a copy in the department (use later for reconciliation procedures by someone not involved in the collection or deposit process).
    - Use receipts in numerical order and account for all pre-numbered receipts including voided receipts.

Management Oversight

Detective Controls

Management usually has time constraints that prevent analysis of every piece of information. For this reason management should assign these tasks to others and concentrate on exercising appropriate supervision and oversight of the process. The foundation for an effective internal control environment is leadership establishing the right "tone at the top" and demonstrating that it is a priority by example.

The following is a short list of activities related to exercising appropriate management oversight:

- On a monthly basis, confirm that all required account reconciliations, reviews, and periodic analyses of risk areas have been completed. Inquire of personnel responsible for reviewing/monitoring reconciliations as to whether there were issues or items of significance. Follow up on such items to ensure appropriate explanation or resolution.
- Review monthly financial information and statements and activity reports, including budget to actual and comparison to prior year. Consider whether the amounts appear reasonable and in line with expectations, based on your knowledge and understanding of the department's operations and activities. Make inquiries as appropriate regarding unexpected results and matters of potential significance.
- Regarding human resources compliance:
  - Annually communicate the importance of performance appraisals and your expectation that supervisors complete appraisals by a stated deadline. Assign someone to verify completion and report to you regarding non-compliance.
  - Annually request a report from HR verifying whether employees have completed required training and communicate to those not in compliance your expectation that required training be completed.
  - Verify that personnel in your area are aware of procedures to report sexual or other forms of harassment and that management understands how to handle such reports in compliance with policy.
- Ensure completion of an annual process to maintain and update departmental policies and procedures, verify that none conflict with University policy, and communicate updates to employees.
- Establish and maintain a simple method to document management's oversight activities. Completing the Management Oversight portion of the internal controls checklist provides a resource to help develop this activity. Documentation of follow up on issues or significant matters should be documented.

Monitoring

Detective Controls

Monitoring is an ongoing evaluation of an organization's activities and transactions to determine whether the components of internal control are working as intended. Proper monitoring will identify control deficiencies and determine whether controls are effective in addressing risks.

Management's role is crucial in establishing effective internal controls by ensuring the monitoring conducted is objective and is performed by personnel with sufficient knowledge to understand how the controls should operate. Internal controls evolve over time and become less effective due to factors such as new personnel, varying levels of training and supervision, time and resource constraints, and changes in procedures that have occurred since the initial controls were designed.

Individual employees should routinely monitor and evaluate internal controls affecting their areas since they are involved in the daily activity and are more attune to changes/situations that may potentially influence the effectiveness of the internal controls.

Some examples of monitoring include the following:

- Ensure employees have training and resources they need to perform their responsibilities effectively and efficiently.
- Ensure departmental policies and procedures are maintained up to date and provided to employees.
- Review reconciliations for accuracy and confirm that all discrepancies are explained and resolved appropriately.
- Review procurement card reconciliations for reasonableness.
- Conduct surprise cash counts.
- Ensure special account analysis occurs for high-risk accounts and to identify outlier transactions or unusual trends.
- Randomly pull a transaction's supporting documentation to ensure accuracy, reliability, appropriate approval, and reasonableness.
- Compare budgeted to actual expenses.
- Compare current to prior period results.
- Periodically review sample of donor restricted funds to ensure transactions are consistent with donor intent.
- Compare expenditures charged to a grant/contract to ensure they are allowable and allocable to the project.

Policies, Standards and Procedures

Directive Controls

A policy and standard establishes what should be done and is the basis for procedures. Procedures describe specifically how the policy or standard is to be implemented.

An organization must establish policies, standards, and procedures for the following reasons.

- To facilitate achievement of objectives
- To ensure staff members know what has to be done
- To guide actions of the area
- To increase efficiency, reduce errors, and make training of new personnel easier and faster
- To ensure compliance with policies, standards, procedures, and regulations/other requirements

Reconciliations

Detective Controls

Broadly defined, reconciliation is a comparison of different sets of data to one another to ensure the accuracy and completeness of transactions. The reconciliation process includes the following key steps.

- Identifying differences
- Investigating differences
- Taking corrective action to resolve differences

Reconciliations are a critical detective control. Without timely reconciliations there may be an increase in the risk of fraud, theft or compliance violations. Reconciliations should be documented, performed timely, and approved by management. To ensure appropriate segregation of duties, the person who approves transactions or handles cash receipts should not be the person who performs the reconciliation.

Select examples of reconciliations that should be performed include the following.

- Compare original departmental receipt records (dollar amount of cash, checks, and credit card payments received) to deposit amounts per financial records (Banner/Oracle/ Lawson).
- Compare expenditures charged to department or grant/contract account to supporting documentation.
- Record cash receipts when received.
- Count and balance cash receipts daily.
- Perform periodic surprise cash counts.

Safeguarding Assets

Preventive Controls

Access to assets, including logical access to data and systems should be granted only to individuals with a legitimate business need to perform their assigned responsibilities. In general an individual should have the lowest level of access that allows them to perform their duties.

Access controls include the following (not intended to be an exhaustive list).

- Restrictively endorse check upon receipt.
- Restrict access to select areas, such as patient care areas – all visitors should be escorted and unrecognized persons should be challenged as to reason for their presence.
- Control the issue of keys and access badges with frequent review to ensure access is granted to only those with a business need.
- Terminate all physical and electronic access immediately when an employee is terminated.
- Terminate or change access appropriately when an employee transfers to new area or has a change in job responsibility.
- Ensure all sensitive or protected information is not visible or accessible to those with no business need.
- Evaluate mail drops, printers and fax machines to ensure they are protected appropriately.
- Configure computers to time out and require password when inactive for period of time.
- Place computer monitor displaying protected or sensitive information so it is not visible to others.
- Maintain assets in accordance with manufacturer or vendor guidelines.
- Ensure all computers have active anti-virus and spyware software.
- Encrypt all laptops, portable computers, and flash drives.
- Ensure all installed software is properly registered to avoid licensing issues and enable identification of recovered equipment.
- Record serial numbers of all computer hardware and other assets.
- Ensure computers/assets are disposed of via University surplus procedures.

Segregation of Duties

Preventive and Detective Controls

Segregation of duties is a control that aids in the timely detection of errors and irregularities in the normal course of business by providing adequate checks and balances. A simple way to look at segregation of duties is to have at least two sets of eyes look at a transaction.

The following functions should be separated among employees and no individual employee should handle more than one of the functions below.

- Custody of assets
- Record keeping
- Authorization
- Reconciliation

For example, the same person should not maintain custody of cash and record the deposit. The same person should not record the deposit and reconcile deposits to the financial system.

Examples of segregation of duties among employees include the following:

- The person who approves purchases should not reconcile monthly financial reports.
- The person who maintains accounting records or reconciles financial reports should not have custody of checks.
- The person who opens mail and receives payments should not make the deposit.
- A computer programmer who makes programming changes should not have access to publish the changes in the production environment.

Maintaining segregation of duties is especially challenging for departments and units with a small numbers of employees. To compensate for this problem, some of the following should be considered.

- Place greater emphasis on monitoring by someone not involved in the process.
- Require all employees to take vacation and require someone else to perform their duties (rather than letting them wait to be completed when employee returns).
- Use transaction and activity reports to identify outlier transactions or unexpected trends.
- In a clinical area, an employee with no cash handling responsibilities should verify that all original fee tickets are collected, including those for cancellations and no-shows.
- In a clinical area, persons who receive cash and check payments should not enter patient charges or be responsible for clearing missing charge items.