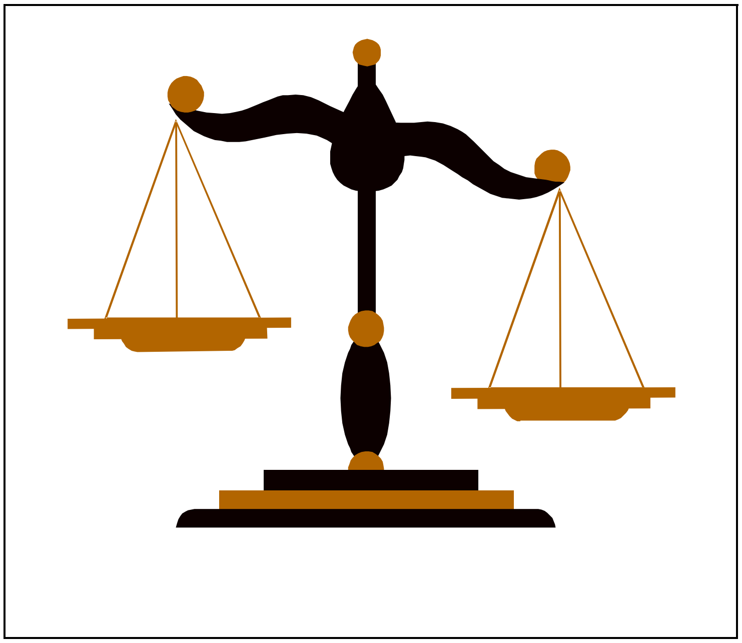
Internal Control Toolkit



THE UNIVERSITY OF TEXAS HEALTH SCIENCE CENTER AT SAN ANTONIO

2002

TABLE OF CONTENTS

1. DEFINITIONS: INTERNAL CONTROL AND RISK

INTERNAL CONTROL is a <u>process</u>—carried out by our administration, faculty, and staff--designed to provide <u>reasonable</u> <u>assurance</u> regarding the achievement of objectives in the following categories:

- **Effectiveness and efficiency of operations,**
- **Reliability of financial and administrative operations, and**
- **Compliance with applicable laws and regulations.**

The above definition of internal control reflects certain fundamental concepts:

- *Internal control must be achieved by people at <u>every</u> level of an organization.* Some people have mistakenly assumed that internal control is the responsibility of the Internal Audit Office, the Office of Accounting, the Office of Legal Affairs and Technology Licensing, the Institutional Compliance Office, or someone else. Internal control is, to some degree, the responsibility of <u>everyone</u> in our organization. At the Health Science Center, administrative officials at the department-level are principally <u>responsible</u> for, and will be held <u>accountable</u> for, internal control in their departments.

- *Effective internal control helps the Health Science Center achieve its operational objectives, its financial and administrative objectives, and its compliance objectives.* Management plans, organizes, and directs the Health Science Center toward the achievement of our objectives. Effective internal control is a built-in part of the management process that applies to all areas of an organization--its operations, its financial and administrative operations, and its compliance with applicable laws and regulations.

- *Internal control can provide only <u>reasonable</u> assurance***--***<u>not absolute</u> assurance***--***regarding the achievement of the Health Science Center's objectives.* Effective internal control helps us achieve our objectives; it does not ensure success or even survival. There are several reasons why internal control cannot provide absolute assurance that objectives will be achieved: cost/benefit realities, collusion among two or more people, faulty judgments, and external events beyond the Health Science Center's control that cause it to fail to achieve its operations objectives.

RISK is the possibility that an organization or an individual will NOT:

- **Achieve goals,**
- **Operate effectively and efficiently,**
- **Protect the area from loss,**
- **Provide reliable reports and other work products, and/or**
- **Comply with applicable laws, rules, regulations, policies, and procedures.**

2. BALANCING RISKS AND CONTROLS

To achieve goals, University employees and management need to effectively balance risks and controls. By performing this balancing act, “reasonable assurance” can be attained. As it relates to financial and compliance goals, being out of balance causes the following problems:

EXCESSIVE RISKS

- Loss of Assets, Donors or Grants
- Poor Business Decisions
- Noncompliance
- Increased Regulations
- Public Scandals

EXCESSIVE CONTROLS

- Increased Bureaucracy
- Reduced Productivity
- Increased Complexity
- Increased Cycle Time
- Increase of Non-value Activities

3. RESPONSIBILITY AND ACCOUNTABILITY

RESPONSIBILITY

Activities, goals, functions, actions, etc. that a person has to account for or answer to. Part of the area of responsibility is to provide reasonable assurance that organizational goals will be accomplished.

ACCOUNTABILITY

If a person is responsible for an action, he or she is also accountable for that action. Responsibility and accountability are linked. In terms of the delegation of duties, management can delegate some of the duties they are responsible for, but cannot delegate responsibility or accountability.

List some of the activities that you are responsible and accountable for at the Health Science Center:

-
-
-
-
-
-
-
-

4. RISK ASSESSMENT

- **REASONABLE ASSURANCE**

The objective of a risk assessment is to attain a “reasonable” level of assurance that the organization’s financial and compliance goals will be achieved. Trying to attain an absolute level of assurance is not possible due to the following reasons:

--It is **cost-prohibitive**. The objective is to find an optimal level of control for an acceptable level of risk.

--**Management** can bypass or **override** the internal controls.

--Employees may **collude** with each other.

--**Human error** may occur.

- **WHAT SHOULD I DO TO ASSESS RISKS IN MY AREA(S) OF RESPONSIBILITY?**

□ Identify all significant activities or processes for which you are responsible.

□ Read and complete the ***Internal Control Review Questionnaires***. (Appendix A)

□ Complete the ***Risk Assessment Worksheets***. (Appendix B). First, identify each possible risk related to all your significant activities or processes. Higher risk transaction types include:

Accounts Reconciliation
Billings and Accounts Receivable
Cash Receipts
Chemical Inventory
Confidential Information
Consultant Payments or Other Payment for Services
Departmental Organization and Staffing
Departmental Manual
Equipment Delivered Directly to Department
Equipment Inventory
Expenditures
Grade processing
Grants (meeting terms, overspending etc.)
Information Security
Intellectual Property
Inventories for Resale
Long Distance
Medical Charge Capture
Office Supplies
Office Furniture
One Person “Financial” Staff
Payments to Non-vendors (i.e., experimental patient payments)
Payroll
Performance Evaluations
Personnel File Maintenance
Petty Cash
Scholarships
Segregation of Duties
Sole Source Purchases
Software Licensing
Travel Expenditures
Turnover in Key Personnel
Video Equipment

□ Make sure that the activities (or processes) for which you are responsible have clear and measurable objectives--operations, financial and administrative, and compliance objectives.

□ Ask yourself the following questions:

- What could go wrong?
- How could we fail?
- What must go right for us to succeed?
- Where are we most vulnerable?
- What assets do we need to protect?
- Do we have liquid assets or assets with alternative use?
- How could someone steal from the department?
- How could someone disrupt our operations?
- On what information do we most rely?
- On what do we spend the most money?
- How do we bill and collect our revenue?
- What decisions require the most judgment?
- What activities are most complex?
- What activities are regulated?
- What is our greatest legal exposure?
- What types of transactions in our area provide the most risk?
- How can someone bypass our internal controls?

□ Consider various external and internal risk factors such as:

- Changing economic and political conditions
- New technology
- New accounting standards
- Changing customer demands
- Competitor actions
- New personnel
- The threat of outsourcing
- New or modified information systems
- Past performance
- Vendor/Contractor performance and reliability
- New products or activities
- Reorganization

□ Secondly, for each identified risk, estimate on the ***Risk Assessment Worksheet***, the potential impact (high, medium, or low) that such an event might happen. Then estimate the probability (high, medium, or low) that such an event might happen. Based on these two estimates, rank the risks so that you can identify which risks should be addressed first. In evaluating the potential impact of risk, both quantitative and qualitative costs need to be addressed. Quantitative costs include the cost of property, equipment, or inventory; cash dollar loss; damage and repair costs, cost of defending a lawsuit, etc. Qualitative costs can have wide-ranging implications to the University. These costs may include:

--Loss of public trust

--Loss of future grants, gifts and donations

--Injury to the school's reputation

--Increased legislation

--Violation of laws

--Default on a project

--Bad publicity

--Decreased enrollment

□ Remember it is management's responsibility to assess risks for the department as a whole--at both the department level and the activity or process level. Management's risk assessment may alter the risk assessment of a particular activity or process.

5. OVERVIEW OF INTERNAL CONTROL TOOLS

- **THE NEXT STEP**

  After assessing and prioritizing the financial and compliance risks, the next step of the process is to identify the appropriate controls to manage the risks. Managers and employees need to focus on their high risk, high priority areas.

- **IMPORTANCE OF INTERNAL CONTROLS**

  Think of internal control as a map that helps us get to our destination. Obviously, just because we have a map, there is no 'guarantee' that we will get there, but it does provide "reasonable assurance". Internal controls help keep an organization on course to achieve goals, carry out management directives, reduce surprises, increase reliability of information, promote effectiveness and efficiency, safeguard assets and comply with rules and regulations.

- **WHO IS RESPONSIBLE?**

  Chairs and directors are primarily responsible for identifying the financial and compliance risks and internal controls for their operations. In addition, individual employees have responsibility for evaluating, establishing and/or improving, and monitoring internal controls for their areas of responsibility and accountability.

- **THE ISSUE OF TRUST**

  Trust is a key component in our interactions in the academic and medical environments. Employing honest, trustworthy personnel is critical; however, trusting employees is not a replacement for a manager's internal control system. An internal control system does not rely solely on trust but is an "objective" set of procedures to help ensure that goals are met, whether at a department level or at an individual's workstation. Any override of controls provides an "opportunity" for someone to take advantage of the system.

- **KEY CONTROL TOOLS**

  --Creation of a Control-Conscious Environment

  --Separation of Duties

  --Authorization/Approval

  --Control over Physical and Intellectual Assets/Records

  --Monitoring

- **PREVENTIVE AND DETECTIVE CONTROLS**

  Controls can be either preventive or detective. The intent of these control types are different. Preventive controls attempt to deter or prevent undesirable acts 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 by providing evidence that the preventive controls are functioning and preventing losses.

6. TOOL #1: CONTROL CONSCIOUS ENVIRONMENT

- **WHAT IS IT?**

  It is an environment that supports ethical values and business practices. (It is a preventive control.)

- **WHO IS RESPONSIBLE?**

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

  --The highest levels of integrity and personal and professional standards

  --A leadership philosophy and operating style which promote internal control throughout the organization, and,

  --An assignment of authority and responsibility which ensures the highest possible level of accountability.

  Each individual employee is responsible for adhering to the institutional Standards of Conduct. We are all expected to conduct ourselves in an ethical and professional manner as we do our work at the University.

- **WHAT SHOULD I DO TO CONTRIBUTE TO A POSITIVE CONTROL ENVIRONMENT?**

  □ Read the *Institutional Compliance Program and Standards of Conduct.*

  □ Visit the homepage for ethics at the UT System (http://www.utsystem.edu/OGC/Ethics/).

  □ Visit the homepage of the UTHSCSA Office of Institutional Compliance at http://www.uthscsa.edu/compliance.

  □ Familiarize yourself with departmental policies and procedures.

  □ If you work in a support position, develop a desk manual if you do not already have one. The Office of Employee Development and Training offers classes on this topic.

  □ Make sure that you understand your job responsibilities, the limits to your authority, performance standards, and reporting relationships.

  □ Disclose ownership interest in companies doing business or proposing to do business with the department; communicate this information to the administrative officials in your department.

  □ Make sure that your dealings with your supervisor, other employees, vendors, contractors, and all other parties are based on honesty and fairness.

□ Ask yourself the following three questions each time you are about to make an ethical decision:

> ***Is it legal?*** This question incorporates laws, regulations, and UT System policy.
>
> ***Is it fair?*** This question considers the fairness of the decision to all parties involved.
>
> ***How will it make me feel about myself?*** This question taps into your own personal beliefs about right and wrong.

□ When in doubt, seek clarification and direction from management (chair, director, manager, supervisor, etc.)

7. TOOL #2: SEPARATION OF DUTIES

- **WHAT IS IT?**

  Functions are divided so that no one person has control over all parts of a transaction.

- **ACTIVITIES TO SEPARATE**

  --Initiating/Authorizing (Approving)/Recording/Reconciling/

  --Physically Controlling (Custody)

- **EXAMPLES**

  --Cash Receipts/Recording Transactions/Bank Deposits/Bank Account Reconciliations

  --Supplier Database/Requisition/Order/Receipt of Goods (services)/Reconciling Accounts

  --Order/Receipt of Inventory/Maintenance of Inventory Records/Physical Inventory Count

- **IN OTHER WORDS--**

  The same person should not perform the following duties:

  --Initiating and approving a purchase and receiving the goods directly,

  --Collecting money and recording the payment on the books, or

  --Issuing checks and reconciling bank accounts

- **ISSUES**

  --Two key questions are:

  - Does one person perform all parts of the transaction from initiating to reconciling the account?
  - Does someone have access to “information systems” that create a separation of duties problem?

  --A simple way of looking at separation of duties is to have at least “two sets of eyes” look at a transaction.

  - Remember trust should not prevent a manager from separating duties. Often it is the long-time, trusted employee who commits fraud because he/she knows the system and how to circumvent it.
  - Banks will cash most checks presented for payment. Checks received and issued should be viewed like cash.

  -- In small departments, it is often difficult to separate duties. To compensate for this problem, some of the following actions could be employed:

- Place greater emphasis on monitoring.
- Require employees to take vacation.
- Use the Dean’s office as a level of separation if feasible.
- Use the information system to analyze activities.
- Make sure cash transactions are recorded ASAP.
- Make sure that checks are restrictively endorsed upon receipt.

- **POTENTIAL KEY AND HIGH RISK TRANSACTION TYPES** USING SEPERATION OF DUTIES

Transaction Type	**Initiates**	**Authorizes**	**Records**	**Reconciles**	**Control (Custody)**
Purchase of Goods	Issues Requisition **Person A**	Approves P.O./ Invoice **Person B**	University Records **Accounting**	Budget Report **Person B or C**	Receives Goods **Person A or C**
Purchase of Services (1)	Issues Requisition **Person A**	Approves Payment & Verifies Receipt of Services **Person B**	University Records **Accounting**	Budget Report **Person B or C**	Disburses Check **Accounting**
Cash Receipts (2)	Opens Mail, Lists Check, Restrictively Endorses **Person A**	Makes Deposit **Person B**	University Records & Department Records **Accounting &** **Person B**	Bank Acct/Budget Report & Deposits to Checklist **Person A or C**	N/A
Payroll	Employee's Time Report	Approves Time Report and Payroll Data Changes **Person A**	University Records **Accounting**	Budget Report Review **Person B**	Distribute Payroll Check **Person B or C**
Inventory (3)	Issues Requisition **Person A**	Approves P.O./ Invoice **Person B**	University Records & Department Records (Issues & Receipts) **Accounting & Person B**	Departmental Records to Budget Reports & Physical Counts **Person B or C**	Receives Distributes Goods **Person A**

(1) If the same person authorizes and reconciles, additional monitoring is necessary.

(2) No receipts should be received directly by Person B.

(3) Physical counts should not be under the **control** of persons responsible for custody or recording.

8. TOOL # 3: AUTHORIZATION

- **WHAT IS IT?**

  Transactions are executed and access to assets is permitted only in accordance with management's directives. This is a preventive control.

- **ISSUES**

  --Signature authority or delegation of that authority should be limited to a "need to have" basis. It's like giving someone signed blank checks. Consequently, managers should judiciously limit authorization authority.

  --"Rubber stamping" documents circumvents this control. Managers should question what they sign, at least on a sample basis. Where appropriate, supporting documentation should be attached to the signature form or at least made available. Questioning various transactions and requesting additional information enhances a control conscious environment.

  --Written procedures outlining the delegation guidelines should be developed.

- **INFORMATION AUTHORIZATION**

  --Access to, and use of, computing resources is restricted to appropriately authorized users.

  --All means of access to automated information resources, such as passwords, are confidential and proprietary to the university. Passwords authenticate a user's identity and establish accountability. An employee is required to maintain the privacy of his or her password(s) and is accountable for the unauthorized use. Sharing user identification codes or revealing passwords is prohibited.

9. TOOL #4: CONTROL OVER ASSETS/RECORDS

- **WHAT IS IT?**

Establishing control procedures to prevent loss of physical and intellectual assets/records and assuring that assets/records are physically secured; these are preventive controls. Taking a physical inventory, on the other hand, is a detective control.

- **ISSUES**

--Managers are personally responsible for the assets in their organization. Assets have a way of "walking off" if physical controls don't exist.

--Equipment moved between labs or classrooms needs to be monitored.

--Separation of duties should be maintained between the person who has custody of the assets/records and the person who takes the physical inventory.

- **ASSET CONTROL ACTIVITIES**

--Periodic asset counts

--Use of perpetual records

--Periodic comparisons of the accounting records to the perpetual records

--Investigation of discrepancies

--Periodic summaries of inventory usage

--Physical safeguards against theft and fire

--Proper authorization of purchases

10. TOOL #5: MONITORING

- **WHY IS IT IMPORTANT?**

--Monitoring ensures that the internal control system is operating as expected. Just because a control exists does not mean that it is properly functioning. Effective controls may be designed into the system, but are not effective unless they are functioning properly.

--Managers, for their areas, and individual employees, for their workstations, should perform ongoing monitoring activities to determine whether the control system can be relied on to provide reasonable assurance that financial and compliance goals can be accomplished and to address new risks.

--Monitoring is a detective control that aids in identifying losses, errors or irregularities.

- **BUT I'M SO BUSY . . .**

All of us are, of course, extremely busy. However, management's role in the internal control system is critical to its effectiveness. Managers, like auditors, don't have to look at every single piece of information to determine that the controls are functioning and should focus their monitoring activities in high-risk areas. The use of spot checks of transactions or basic sampling techniques can provide a reasonable level of confidence that the controls are functioning. Individual employees should routinely review and evaluate internal controls affecting their area of responsibility and accountability.

- **REPORTS**

--Financial reports are a key monitoring tool. Below is some information that managers should obtain from their reporting system to use to monitor controls:

- Comparison of actual to budget
- Comparison of the current month to the previous month
- Comparison of the current month to the previous year's month
- Year-to-date totals
- Special account analysis for high risk accounts
- Reconciliation of department/college balances to a monthly account statement

--For easy use, the above reports should include a variance column (where appropriate) and totals should be consistent among the reports. Also, reports should be summarized to the proper level of detail. Thick reports are useless if they are not read.

- **MONITORING ACTIVITIES**

  --Review and evaluate financial reports for propriety and trends

  --Review reconciliations, ensuring that reconciling items are investigated

  --Verify the propriety of supporting documentation

  --Have Internal Audit review high risk areas

  --Have periodic asset counts performed

  --Make surprise cash counts

  --Follow-up on complaints, rumors, allegations

  --Send out periodic confirmation of accounts receivable

- **MONITORING BY TRANSACTION**

  --PAYROLL

  - Review and approve initial pay and any “changes”
  - Review procedures for additions/deletions
  - Review terminations to ensure they are taken off the system
  - Review for nonstandard hours
  - Monitor sick/vacation leave

  --TRAVEL

  - Review supporting documents
  - Personally approve
  - Analyze by employee and related expenses

  --CONSULTANTS

  - Review supporting documentation of brochure, airline ticket or hotel
  - Make a “call” if support is not available

11. CHANGE MANAGEMENT

- **CHANGE MANAGEMENT**

We all are operating in a constantly changing environment that requires continuous review and monitoring. In such an environment, financial and compliance goals are more challenging to achieve and demand more attention. As external and internal events occur, an organization's risks may significantly change. All employees must re-evaluate risks and internal controls when circumstances change.

- **EXTERNAL FACTORS AFFECTING RISK**

--Increased regulatory requirements

--New technology

--Political changes

--Intense public and journalistic scrutiny

- **INTERNAL FACTORS AFFECTING RISK**

--Management turnover

--Decentralization

--Inherited staff

--University policy

--Limited resources

- **THE PROCESS**

As the above risk factors occur, they may dramatically affect the organization's risk. Therefore, we should review risk factors on a periodic basis. It should be part of our on-going monitoring process.

12. THE “RED FLAGS” OF FRAUD

Although fraud is an infrequent occurrence on campus, we should each be aware of its possible existence. Here are some of the factors that can result in the occurrence of fraud:

MOTIVE	JUSTIFICATION	OPPORTUNITY
• Greed • Financial crisis • Gambling/drinking/ drugs • Living beyond means • Affairs • Mid-life crisis • Revenge • Unappreciated • Workaholic • Family Problems	• “It was so easy.” • “They don’t pay me enough.” • “My child is sick.” • True crisis, divorce, etc. • “My boss circumvents the rules.” • “I’ll pay it back.”	• Poor or weak internal control system • Lack of monitoring the controls • High management turnover

Below are some indications that fraud might be or is actually occurring:

1. Employee won’t take a vacation.
2. Unexplained variances.
3. Complaints.
4. No reconciliation to university accounting records.
5. Even amounts on checks/documents.
6. Missing reports/documents.
7. Failure to investigate reconciling items.
8. One employee “does it all”.
9. Duplicate payments or documentation is not original.
10. Using “exemptions” to use particular vendor over and over.

13. RESOURCES

Institutional Compliance Office
567-2014

Office of Internal Audit
567-2370

http://www.uthscsa.edu/compliance/