Balancing Risks and Controls

Courtesy of Yale University

- Risk Assessment
- Internal Control Tools
- Control Conscious Environment
- Segregation of Duties
- Authorizations/Approvals
- Reviews
- Reconciliations
- Asset Security
- Information and Communication
- Monitoring
- Balancing Risks and Controls

Risk Assessment

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

With management team members, ask the following questions:

- What can go wrong?
- Where are we most vulnerable?
- Where is our greatest exposure?
- What types of transactions in our area provide the most risk?
- Do we have "liquid" assets or assets which have alternative uses?
- How can someone bypass the internal controls?
- What potential risk areas could cause adverse publicity?

Benchmark with others in similar situations. Are there risks in their areas that could occur in your area?

Analyze financial data. (Where is the high volume or large dollars?)

- Below are some types of transactions that may pose higher risks to departments/colleges:
  - Assets with Alternative Uses (i.e., computers)
  - Cash Receipts (continuing education programs, gifts, endowments, special events, bookstore, athletic programs, performances, etc).
  - Consultant Payments and Other Payments for Services
Travel Expenditures
Scholarships
Payments to Non-Vendors
Equipment Delivered Directly to Department
Purchase Exemptions (sole source)
Payroll (rates, changes, terminations)
Equipment on Location
Software Licensing Issues
Intellectual Property
Confidential Information
Grants (meeting terms, not overspending)

These are transaction types that deserve a conscious risk review.

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 a 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

Internal Control Tools

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 need to focus on their high risk, high priority areas. The next section will present the tools managers can use to design their internal control systems.

Think of internal control as a map that helps managers to get to their destination. Obviously, just because managers have a "map", there is no "guarantee" that they will get there, but it does provide "reasonable assurance". Internal controls help keep a company 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.

In the same way that managers are primarily responsible for identifying the financial and compliance risks for their operations, they also have line responsibility for designing, implementing and monitoring their internal control system. Internal Audit and the Accounting and Financial Services are available to provide advice and expertise. Managers are encouraged to consult with these offices when evaluating internal controls, especially with
regard to areas deemed to be high risk.

Trust is a key component in managers' interactions in the academic and medical environments. Employing honest, trustworthy personnel is critical; however, trusting employees is not a replacement for an 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. Any override of controls provides an "opportunity" for someone to take advantage of the system which management is responsible for.

The following internal control tools will be discussed in this section:

- Creation of a Control-Conscious Environment
- Separation of Duties
- Authorization/Approval
- Reviews
- Reconciliations
- Asset Security
- Information and Communication
- Monitoring

Controls can be either preventive or detective. The intent of these control types is 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 providing evidence that the preventive controls are functioning and preventing losses.

Control Conscious Environment

The control environment is the control consciousness of an organization; it is the atmosphere in which people conduct their activities and carry out their control responsibilities. An effective control environment is an environment where competent people understand their responsibilities, the limits to their authority, and are knowledgeable, mindful, and committed to doing what is right 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.

Corporation members and management enhance an organization's control environment when they establish and effectively communicate written policies and procedures, a code of ethics, and standards of conduct. Moreover, corporation members and management enhance the
control environment when they behave in an ethical manner - creating a positive "tone at the top" - and when they require that same standard of conduct from everyone in the organization.

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

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

- The highest levels of integrity and personal and professional leadership
- A leadership philosophy and operating style which promote internal control throughout the organization;
- An assignment of authority and responsibility which ensures the highest possible level of accountability.

The following action steps will help to encourage ethical behavior:

- Communicate to employees that fraud (embezzlements, stealing, etc.) and conflicts of interest will not be tolerated.
- Communicate that University policies and procedures are important and will be followed.
- Make employees fully aware of their responsibilities (including internal controls).
- Document key department/college/school policies and procedures.
- Send employees to ethics and internal control training.
- Evaluate personnel based on performance related to internal controls.
- Take disciplinary or other actions for non-performance.
- Monitor the internal control system on an on-going basis.

Case Study

Laura is a new employee in XYZ Department at Wahoo University. It is her first day on the job and her Supervisor offers to introduce Laura to people in the department.

First, Laura meets the office secretary who informs Laura that after she meets everyone in the department, she needs to go down to Human Resources and fill out a bunch of forms. The secretary says to Laura, "Don't worry about reading any of it, just tell them you want automatic everything and you can be back in time for us to take you to lunch."

While walking down the hall to meet the next person, Laura asks her supervisor about department policies and procedures, especially those that pertain to her job. The supervisor informs her that there are not any department policies and procedures and that she should just look around her office and figure out the way the previous guy did her job. The supervisor says to Laura, "I think we have something called Regents' Rules and Regulations and BPMs, but I've never seen them. If you have a question, ask me and I'll call Frank. He's been with this place for years and he knows all the ways to get around the bureaucracy around here."

Next, Laura meets the office accountant. As she walks into the accountant's office, she notices that he is playing a golf game on his computer. Obviously embarrassed, he explains
that he just got the game from a guy in Information Resources. As he exits the program, she notices that a Federal income tax return pops up on the screen. He explains that he does a few personal income tax returns on the side to make a few extra bucks. "After all," he explains, "they don't pay a person what he's really worth around here."

Next, Laura meets the Assistant Director. He requests a private meeting with Laura to introduce himself to her. While in his office, he asks, "Well Laura, I noticed that you aren't wearing a wedding ring. Are you seeing anyone right now?" Surprised by his question, she doesn't say anything. He says, "You are a very attractive woman and I like to encourage all our people to get to know each other inside and outside the office. I look forward to our working together and if you ever need anything, just come by and see me."

After meeting several other people in the office, she meets the Director of the department. He seems very nice and apologizes for not being able to go to lunch with her and everyone else. He explains that he has made lunch plans to meet an old buddy who is bidding on one of the department's requests for proposal (RFPs).

After filling out the forms in Human Resources, Laura returns to the office and finds that everyone is waiting for her to go to lunch. Laura explains that she brought her lunch and that she needs to cash a check to go out for lunch. The office secretary says, "Don't worry, Laura, just get $20 out of the petty cash fund for your lunch. It's an unofficial benefit for first day employees. I'll write it up as a "miscellaneous expense." Laura is stunned; she does not know what to do.

**Required:**

1. Underline everything in the case study that contributes negatively to the Department's control environment.

2. What does this Department's control environment communicate to Laura?

---

**Segregation of Duties**

No one person should:

- Initiate transaction
- Approve transaction
- Record transaction
- Reconcile balances
- Handle assets
- Review reports
Segregation of duties is critical to effective internal control; it reduces the risk of both erroneous and inappropriate actions. In general, the approval function, the accounting/reconciling function, and the asset custody function should be separated among employees. When these functions cannot be separated, a detailed supervisory review of related activities is required as a compensating control activity. Segregation of duties is a deterrent to fraud because it requires collusion with another person to perpetrate a fraudulent act.

Specific examples of segregation of duties are as follows:

- The person who requisitions the purchase of goods or services should not be the person who approves the purchase.
- The person who approves the purchase of goods or services should not be the person who reconciles the monthly financial reports.
- The person who approves the purchase of goods or services should not be able to obtain custody of checks.
- The person who maintains and reconciles the accounting records should not be able to obtain custody of checks.
- The person who opens the mail and prepares a listing of checks received should not be the person who makes the deposit.
- The person who opens the mail and prepares a listing of checks received should not be the person who maintains the accounts receivable accounting records.

Authorizations/Approvals

An important control activity is authorization/approval. Authorization is the delegation of authority; it may be general or specific. Giving a department permission to expend funds from an approved budget is an example of general authorization. Specific authorization relates to individual transactions; it requires the signature or electronic approval of a transaction by a person with approval authority. 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 applicable laws, regulations, policies, and procedures. Approvers should review supporting documentation, question unusual items, and make sure that necessary information is present to justify the transaction - before they sign it. Signing blank forms should not be done.

Approval authority may be linked to specific dollar levels. Transactions that exceed the specified dollar level would require approval at a higher level. Under no circumstances should an approver tell someone that they could sign the approver's name on behalf of the approver. Similarly, under no circumstance should an approver with electronic approval authority share his password with another person. To ensure proper segregation of duties, the person initiating a transaction should not be the person who approves the transaction. A department's approval levels should be specified in a departmental policies and procedures manual.
Reviews

- Budget to actual comparison
- Current or prior period comparison
- Performance indicators
- Follow-up on unexpected results or unusual items

Reviewing reports, statements, reconciliations, and other information by management is an important control activity; management should review such information for consistency and reasonableness. Reviews of performance provide a basis for detecting problems. Management should compare information about current performance to budgets, forecasts, prior periods, competitors, or other benchmarks to measure the extent to which goals and objectives are being achieved and to identify unexpected results or unusual conditions which require follow-up. Management's review of reports, statements, reconciliations, and other information should be documented as well as the resolution of items noted for follow-up.

Reconciliations

Broadly defined, a reconciliation is a comparison of different sets of data to one another, identifying and investigating differences, and taking corrective action, when necessary, to resolve differences. Reconciling monthly financial reports from the Web Statements to file copies of supporting documentation or departmental accounting records is an example of reconciling one set of data to another. This control activity helps to ensure the accuracy and completeness of transactions which have been charged to a department's accounts. To ensure proper segregation of duties, the person who approves transactions or handles cash receipts should not be the person who performs the reconciliation.

A critical element of the reconciliation process is to resolve differences. It does not do any good to note differences and do nothing about it. Differences should be identified, investigated, and explained - corrective action must be taken. If an expenditure is incorrectly charged to a department's accounts, then the approver should post a correcting journal entry; the reconciler should ascertain that the correcting journal entry was posted. Reconciliations should be documented and approved by management.

Asset Security

- Security of physical and intellectual assets
- Physical safeguards
- Perpetual records are maintained
- Periodic counts / physical inventories
- Compare counts to perpetual records
- Investigate/correct differences

Liquid assets, assets with alternative uses, dangerous assets, vital documents, critical systems, and confidential information must be safeguarded against unauthorized acquisition,
use, or disposition. Typically, access controls are the best way to safeguard these assets. Examples of access controls are as follows: locked door, keypad systems, card key system, badge system, biometric system, locked filing cabinet, guard, terminal lock, computer password, menu protection, automatic call-back for remote access, smart card, and data encryption.

Departments which have capital assets or significant inventories should establish perpetual inventory control over these items by recording purchases and issuances. Periodically, the items should be physically counted by a person who is independent of the purchased authorization and asset custody functions and the counts should be compared to balances per the perpetual records. Missing items should be investigated, resolved, and analyzed for possible control deficiencies; perpetual records should be adjusted to physical counts if missing items are not located.

Information and Communication

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

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

When assessing internal control over a significant activity (or process), the key questions to ask about information and communication are as follows:

- Does our department get the information it needs from internal and external sources - in a form and timeframe that is useful?
- Does our department get information that alerts it to internal or external risks (e.g., legislative, regulatory, and developments)?
- Does our department get information which measures its performance - information that tells the department whether it is achieving its operations, financial reporting, and compliance objectives:
  - Does our department identify, capture, process, and communicate the information that others need (e.g., information used by our customers or other departments) in a form and timeframe that is useful?
  - Does our department provide information to others that alerts them to internal or external risks?
  - Does our department communicate effectively - internally and externally?
Information and communication are simple concepts. Nevertheless, communicating with people and getting information to people in a form and timeframe that is useful to them is a constant challenge.

Monitoring

Monitoring is the assessment of internal control performance over time. It is accomplished by ongoing monitoring activities and by separate evaluations of internal control, such as self-assessments, peer reviews, and internal audits. The purpose of monitoring is to determine whether internal controls are adequately designed, properly executed, and effective. Internal control is adequately designed and properly executed if all five internal control components are present and functioning as designed. Internal control is effective if the Corporation Members and management have reasonable assurance that:

- They understand the extent to which operation objectives are being achieved.
- Published financial statements are being prepared reliably.
- Applicable laws and regulations are being complied with.

While internal control is a process, its effectiveness is a state of condition of the process at one or more points in time.

Just as control activities help to ensure that actions to manage risks are carried out, monitoring helps to ensure that control activities and other planned actions to effect internal control are carried out properly and in a timely manner and that the end result is effective internal control. Ongoing monitoring activities include various management and supervisory activities which either validate or invalidate the design, execution, and effectiveness of internal control. Separate evaluations, on the other hand, such as self-assessments and internal audits, are periodic evaluations of internal control components resulting in a formal report on internal control. Self-assessments are performed by department employees; internal audits are performed by internal auditors who provide an independent appraisal of internal control.

Balancing Risks and Controls

To achieve goals, management needs to effectively balance risks and controls. By performing this balancing act "reasonable assurance" can be attained. As it related to financial and compliance goals, being out of balance causes the following problems:

<table>
<thead>
<tr>
<th>Excessive Risks</th>
<th>Excessive Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Assets</td>
<td>Donors or Grants Increased Bureaucracy</td>
</tr>
<tr>
<td>Poor Business Decisions</td>
<td>Reduced Productivity</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Noncompliance</td>
<td>Increased Complexity</td>
</tr>
<tr>
<td>Increased Regulations</td>
<td>Increased Cycle Time</td>
</tr>
<tr>
<td>Public Scandals</td>
<td>Increase of Nonvalue Activities</td>
</tr>
</tbody>
</table>

Internal controls should be proactive, value-added, and cost-effective. In summary, properly balancing risks and controls makes good business sense.

**Internal Controls**

A process effected by a university's governing board, administration, faculty and staff 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.

**Risk**

The possibility that an organization will **NOT**:

- Achieve its goals.
- Operate effectively and efficiently.
- Protect itself from loss.
- Provide reliable financial data (reports).
- Comply with applicable laws/regulations and defined policies/procedures.

The university environment has some unique inherent risks that make the job of managing financial and compliance risks more challenging. Below are some of the inherent risks faced by university managers:

- Decentralized accounting and reporting system.
· Rotation of key management positions.
· Tight budgets.
· Managers with limited financial background.
· Intense public and journalistic scrutiny.

**Reasonable Assurance**

The objective 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:

1. **It is cost-prohibitive.** The objective is to find an optimal level of controls for an acceptable level of risk.
2. **Management can bypass or override** the internal controls.
3. Employees may **collude** with each other.
4. **Human error** may occur.

**Note:** With a decentralized accounting system, controls cannot, by themselves, provide reasonable assurance that departments/colleges/schools are adequately controlled. Certain of these controls (authorization and approval process), if followed, will reduce the risk of loss. However, these controls are easily circumvented or ignored at the department level when adequate emphasis is not placed on internal controls and/or the controls are not being monitored to see that they are functioning properly.

**Responsibility**

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

**Accountability**

By definition, if a person is responsible for an action, he/she is therefore 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". A much stronger emphasis is currently being placed on responsibility and accountability than was in the past.

Duties and responsibilities must be carried out with the full knowledge and understanding of the implications of actions being taken by each employee at all levels within the organization.

[^ Back to Top]