Internal Control Program

Carrie A Woodrow
Director Business Compliance and Internal Controls
Introduction to Internal Controls @ UB

Internal control is the integration of the activities, plans, attitudes, policies, systems, resources and efforts of the people of an organization working together to provide reasonable assurance that the organization will achieve its objectives and mission.

The University at Buffalo uses the COSO Internal Control framework as its basis for a comprehensive Internal Control Program.
In order to have a comprehensive Internal Control Program, the University must implement all 5 components of the COSO framework. As the Director of Business Compliance and Internal Controls I have developed a plan to fully implement the framework in 2017.
Control Environment

Establishing a Control Environment at UB
In order to establish a “best in class” Control Environment the following will be performed:

1. Request that president Tripathi distribute a “tone at the top” letter to all employees expressing the importance of Internal Controls at the University.

2. Establish an Internal Control site on the Administrative Services Gateway to include:
   1. The president’s letter
   2. Internal Control Policy
   3. Internal Control Procedures
   4. Internal Control Best Practices
   5. A link to the internal control database (discussed later in this presentation)

3. Author comprehensive training material to be required of all new employees and annually for existing employees.
Risk Assessment

Performing Meaningful Risk Assessments
A sound Risk Assessment will:

- Specify clear University or Unit objectives.
- Identify and analyze risks to the achievement of objectives.
- Assess potential for fraud risk in the achievement of objectives.
- Monitors significant change that could affect internal controls.
Initial Risk Assessment Process

**Identify Risk Areas**
- Input from Internal Audit and the AVP Business Services & Controller

**Communicate**
- Communicate COSO Framework and tools to complete risk assessment to each risk area. Includes 12 schools & 10 academic support units.

**Collaborate**
- Provide collaborative support to each risk area as they complete their risk assessment.

**Compile**
- Compile all risk assessments, creating an inventory of internal controls.
### Risk Assessment Example:

**University At Buffalo - Risk Control Self Assessment**

<table>
<thead>
<tr>
<th>ID#</th>
<th>Risk</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Existing Control Measures</th>
<th>Certification?</th>
<th>Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>What steps do we take to make sure something doesn't go wrong?</td>
<td>How do we confirm that things are under control?</td>
<td>Depending on Likelihood and Impact do we need to take action to either put a control in place or certify an existing control?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **What could go wrong?**
- **What steps do we take to make sure something doesn't go wrong?**
- **How do we confirm that things are under control?**

**University At Buffalo**

*The State University of New York*
## Risk Control Self Assessment Matrix

<table>
<thead>
<tr>
<th>Impact</th>
<th>Human</th>
<th>Monetary</th>
<th>Property</th>
<th>Capability</th>
<th>Information</th>
<th>Reputation</th>
<th>Reputation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor injury or first aid treatment</td>
<td>1% of annual operating budget</td>
<td>Minor damage or vandalism to asset</td>
<td>Minor skills impact - Minimal impact on non-core operations - Impact can be dealt with by routine operations</td>
<td>Compromise of information otherwise available in the public domain</td>
<td>Minor compromise of information sensitive to internal or sub-unit interests</td>
<td>Local mention only. Quickly forgotten. Freedom to operate unaffected</td>
<td></td>
</tr>
<tr>
<td>Injury requiring treatment by medical practitioner and/or lost time from workplace</td>
<td>2-5% of annual operating budget</td>
<td>Minor damage or loss of 5% of total assets</td>
<td>Impact on organizational capability in terms of delays and systems quality. Impact can be dealt with at operational level</td>
<td>Compromise of information sensitive to organizational operations</td>
<td>Scrutiny by executive, internal committees or Internal audit to prevent escalation. Short-term local media concern</td>
<td>Persistent national concern. Scrutiny required by external agencies. Long-term &quot;brand&quot; impact.</td>
<td></td>
</tr>
<tr>
<td>Major injury / hospitalization.</td>
<td>6-10% of annual operating budget</td>
<td>Damage or loss of 20% of total assets.</td>
<td>Impact on the organization resulting in reduced performance such that key targets are not met. Organizations existence is not threatened, but could be subject to significant review.</td>
<td>Compromise of information sensitive to organizational interests</td>
<td>Scrutiny by executive, internal committees or Internal audit to prevent escalation. Short-term local media concern</td>
<td>Persistent intense national public, political and media scrutiny. Major operations severely restricted.</td>
<td></td>
</tr>
<tr>
<td>Single death and/or multiple major injuries.</td>
<td>&gt;10% of annual operating budget</td>
<td>Extensive Damage or loss &gt;50% of total assets.</td>
<td>Breakdown of key activities leading to reduction in performance (e.g. service delays, revenue loss, client dissatisfaction, legislative breach.</td>
<td>Compromise of information with significant ongoing impact.</td>
<td>International concern, government inquiry or sustained adverse national/international media. Significantly affects organizational abilities</td>
<td>Survival of the project/activity/organization is threatened.</td>
<td></td>
</tr>
<tr>
<td>Multiple deaths.</td>
<td>&gt;30% of annual operating budget</td>
<td>Destruction or complete loss of assets.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Likelihood

- **Very High (VH)**: Immediate action required by Executive with detailed planning, allocation of resources and regular monitoring
- **High (H)**: High risk, senior management attention needed
- **Medium (M)**: Management responsibility must be specified
- **Low (L)**: Monitor and manage by routine procedures
- **Very Low (VL)**: Managed by routine procedures

### Chance

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Probability</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is expected to occur in most circumstances.</td>
<td>&gt;95%</td>
<td>Almost Certain</td>
</tr>
<tr>
<td>Will probably occur in most circumstances.</td>
<td>65%</td>
<td>Likely</td>
</tr>
<tr>
<td>Might occur at some time.</td>
<td>35%</td>
<td>Possible</td>
</tr>
<tr>
<td>Could occur at some time.</td>
<td>35%</td>
<td>Unlikely</td>
</tr>
<tr>
<td>May occur in only exceptional circumstances.</td>
<td>5%</td>
<td>Rare</td>
</tr>
</tbody>
</table>

---

### Impact

- **Negligible**: Monitor and manage by routine procedures
- **Minor**: Managed by routine procedures
- **Moderate**: High risk, senior management attention needed
- **Major**: Immediate action required by Executive with detailed planning, allocation of resources and regular monitoring
- **Extensive**: High risk, senior management attention needed
## Types of Operational Risk:

<table>
<thead>
<tr>
<th>Clients, Products &amp; Best Practices</th>
<th>Process Related Risks</th>
<th>External Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employment Practices</td>
<td>Execution, Delivery &amp; Process Management</td>
<td>External Theft and Fraud</td>
</tr>
<tr>
<td>Workplace Safety</td>
<td>Business Disruption &amp; System Failure</td>
<td>Damage to Physical assets &amp; infrastructure</td>
</tr>
<tr>
<td>Internal Theft, Fraud &amp; Unauthorized activity</td>
<td>Segregation of duties</td>
<td>Information security</td>
</tr>
<tr>
<td>Risk</td>
<td>Likelihood</td>
<td>Impact</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
<td>--------</td>
</tr>
<tr>
<td>Ineffective cash management including cash, checks, and payment cards</td>
<td>C</td>
<td>4</td>
</tr>
<tr>
<td>Violation of conference rules</td>
<td>C</td>
<td>4</td>
</tr>
<tr>
<td>Unruly fans during athletic event</td>
<td>C</td>
<td>3</td>
</tr>
<tr>
<td>Ticket fraud</td>
<td>C</td>
<td>3</td>
</tr>
<tr>
<td>Inadequate information systems and IT support to meet business needs -- information relating to student-athletes, revenues, expenses, NCAA compliance, etc.</td>
<td>B</td>
<td>4</td>
</tr>
<tr>
<td>Inadequate segregation of duties within the cash handling process</td>
<td>C</td>
<td>3</td>
</tr>
<tr>
<td>Data relating to cash transactions is improperly created, altered or deleted</td>
<td>C</td>
<td>3</td>
</tr>
<tr>
<td>Cash is not adequately safeguarded</td>
<td>B</td>
<td>3</td>
</tr>
<tr>
<td>Improper management of fundraised accounts</td>
<td>C</td>
<td>4</td>
</tr>
<tr>
<td>Credit Card information not properly safeguarded</td>
<td>C</td>
<td>4</td>
</tr>
</tbody>
</table>
Control Activities

Identifying appropriate control activities
Control Activities Resulting From Risk Assessments

| The risk area identifies existing controls in place to mitigate the risk to the achievement of objectives, bringing risk to an acceptable level. | The risk area develops new controls in order to mitigate the risk to the achievement of objectives, bringing risk to an acceptable level. | The risk area accepts the risk based on the parameters of risk acceptance and the University’s risk appetite established by ERM. |
Existing Controls

- Identify Responsible Person
- Ensure proper documentation in either policy or procedures.

New Controls

- Establish action Plan with:
  - Clear Objective
  - Responsible Person
  - Resolution Date
  - Priority Level

Accepting Risk

- Ensure compliance with ERM Framework for risk acceptance.
- Document Accepted Risk.
- Set parameters for establishing a new control in the event of change to the risk environment.
Information & Communication

Creating an environment of transparency
In order to properly evaluate the internal control environment at the University at Buffalo, we will establish a database housing and inventory of all internal controls and any internal control issues. These issues may be identified by:

- Internal Audit
- Compliance
- External Auditors
- Regulators
- Internal Controls
- Management Self Identified in the Risk Assessment Process

The database will serve as the central location for an internal control inventory as well as any outstanding issues and will include, responsible party, a comprehensive action plan, resolution date, priority level and contact person. Resolution dates will be tracked to completion before issues can be closed in the database. The compilation of this information will allow for comprehensive reporting to senior management and the ERM Steering Committee to ensure that the University hasn’t surpassed establish risk limits.
<table>
<thead>
<tr>
<th>The database will allow for reporting on trends and metrics.</th>
<th>Quantity of issues by priority level.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Aging of issues to resolution date</td>
</tr>
<tr>
<td></td>
<td>Concentration by unit or issue type</td>
</tr>
<tr>
<td>University wide information sharing-best practices.</td>
<td>Identify potential for efficiency through resource sharing</td>
</tr>
<tr>
<td></td>
<td>Use best practices for mitigation of similar risks</td>
</tr>
<tr>
<td></td>
<td>Identify subject matter experts</td>
</tr>
</tbody>
</table>
Monitoring Activities
Annually, Risk Assessments will be revisited to ensure that identified controls remain accurate and that new controls have been put into place for any process, system, procedural, or structural change in the unit.

On an as needed basis, work with units to ensure proper controls are in place. Act as a partner in risk mitigation across the university.

Internal Audit will be able to reference the Internal Control Inventory for use of developing a risk based audit plan and for the planning stage of their audits.

Action plans will be tracked to resolution dates to ensure timely risk mitigation.
Monitoring Responsibilities

First line of Defense
- Regular Business Certifications on internal controls
- Using due diligence during business processes
- Business Identifies changing risk profile
- Following established policies and procedures

Second Line of Defense
- Compliance Activities
- Internal Control Monitoring and Follow Up

Third Line of Defense
- Internal and External Audit
- Regulators
Internal Control Program

- Establish Control Environment
- Complete Risk Assessments
- Identify or Establish Control Activities
- Establish Internal Control Database
- Monitor Controls to Ensure Proper Execution
Comments/Questions?

I know, right?! It's so shocking that we have internal controls to prevent the fraud I silently think you're committing...

your ecards
someecards.com