University at Buffalo
The State University of New York

Internal Control Program

Carrie A Woodrow

Director Business Compliance and Internal Controls

University at Buffalo
The State University of New York

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.

University at Buffalo
The State University of New York

COSO Internal Control- Integrated Framework Principles

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.

University at Buffalo
The State University of New York

Control Environment

Establishing a Control Environment at UB

University at Buffalo
The State University of New York

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.

University at Buffalo
The State University of New York

Risk Assessment

Performing Meaningful Risk Assessments

University at Buffalo
The State University of New York

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

University at Buffalo
The State University of New York

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.

University at Buffalo
The State University of New York

Risk Assessment Example:

University At Buffalo - Risk Control Self Assessment

Department Name:	**Completed By:**	**Completed Date:**

ID#	Risk	Likelihood	Impact	Existing Control Measures	Certification?	Action Items
	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?	Depending on Likelihood and Impact do we need to take action to either put a control in place or certify an existing control?

University at Buffalo
The State University of New York

Risk Control Self Assessment Matrix

	Impact				
Human	Minor injury or first aid treatment.	Injury requiring treatment by medical practitioner and/or lost time from workplace.	Major injury / hospitalization.	Single death and/or multiple major injuries.	Multiple deaths.
Monetary	1% of annual operating budget.	2-5% of annual operating budget.	6-10% of annual operating budget.	>10% of annual operating budget.	>30% of annual operating budget.
Property	Minor damage or vandalism to asset.	Minor damage or loss of <5% of total assets.	Damage or loss of <20% of total assets.	Extensive Damage or loss <50% of total assets.	Destruction or complete loss >50% of assets.
Capability	Minor skills impact. Minimal impact on non-core operations. Impact can be dealt with by routine operations.	Some impact on organizational capability in terms of delays and systems quality. Impact can be dealt with at operational level.	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.	Breakdown of key activities leading to reduction in performance (e.g. service delays, revenue loss, client dissatisfaction, legislative breach.	Protracted unavailability of critical skills/people. Critical failure(s) preventing core activities from being performed. Survival of the project/activity/organization is threatened.
Information	Compromise of information otherwise available in the public domain.	Minor compromise of information sensitive to internal or sub-unit interests.	Compromise of information sensitive to the organizational operations.	Compromise of information sensitive to organizational interests.	Compromise of information with significant ongoing impact.
Reputation	Local mention only. Quickly forgotten. Freedom to operate unaffected.	Scrutiny by executive, internal committee or internal audit to prevent escalation. Short-term local media concern.	Persistent national concern. Scrutiny required by external agencies. Long-term "brand" impact.	Persistent intense national public, political and media scrutiny. Major operations severely restricted.	International concern, government inquiry or sustained adverse national/international media. Significantly affects organizational abilities.
	1	**2**	**3**	**4**	**5**
	Negligible	**Minor**	**Moderate**	**Major**	**Extensive**

Likelihood	Chance	Probability	Frequency		
	Is expected to occur in most circumstances.	>95%	Has occurred 10 or more times in the past 10 years in this or similar organization, or circumstances are such it is almost to certain to happen.	**E**	**Almost Certain**
	Will probably occur in most circumstances.	>65%	Has occurred 7 or more times in the past 10 years in this or similar organization, or circumstances are such it is likely to happen in the next few years.	**D**	**Likely**
	Might occur at some time.	>35%	Has occurred 3 or more times in the past 10 years in this or similar organization, or there is a reasonable likelihood to happen in the next few years.	**C**	**Possible**
	Could occur at some time.	<35%	Has occurred 2-3 times per 10 years in this or similar organizations.	**B**	**Unlikely**
	May occur in only exceptional circumstances.	<5%	Has occurred or can reasonably be considered to occur only a few times in 100 years.	**A**	**Rare**

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

University at Buffalo
The State University of New York

Types of Operational Risk:

Clients, Products & Best Practices

- Employment Practices
- Workplace Safety
- Internal Theft, Fraud & Unauthorized activity

Process Related Risks

- Execution, Delivery & Process Management
- Business Disruption & System Failure
- Segregation of duties
- Information security

External Risks

- External Theft and Fraud
- Damage to Physical assets & infrastructure

Risk	Likelihood	Impact	Existing Control Measures	Action Items
What could go wrong?			What steps do we take to make sure something doesn't go wrong?	Depending on Likelihood and Impact do we need to take action to either put a control in place or certify an existing control?
Ineffective cash management including cash, checks, and payment cards	C	4	Documented policies & procedures, segregation of duties, management oversight	Medium - Management responsibility must be specified
Violation of conference rules	C	4	Periodic self-assessment, maintain and advertise a fraud and compliance hotline, knowledgeable personnel	Medium - Management responsibility must be specified
Unruly fans during athletic event	C	3	Trained security personnel, publicize conduct guidelines for fans, crowd control plan	Medium - Management responsibility must be specified
Ticket fraud	C	3	Segregate incompatible duties, peridic ticket audits, documented policies and procedures for controlling and accounting for tickets	Medium - Management responsibility must be specified
Inadequate information systems and IT support to meet business needs--information relating to student-athletes, revenues, expenses, NCAA compliance, etc.	B	4	Knowledgeable personnel and adequate training, strategic IT plan, disaster recovery, periodic audits	Medium - Management responsibility must be specified
Inadequate segregation of duties within the cash handling process	C	3	Staff properly trained in segregation of duties, employees responsible for cash receipts function do not sign checks or reconcile the bank accounts, documented policies and procedures	Medium - Management responsibility must be specified
Data relating to cash transactions is improperly created, altered or deleted	C	3	Monitoring and management review, daily reconciliation of receipts to deposits, supervisors verify cash deposits, voided transactions, and cash overages and shortages, segregation of duties/access controls and limitations, supervisory review and approval of reconciliations	Medium - Management responsibility must be specified
Cash is not adequately safeguarded	B	3	Access controls, checks are restrictively endorsed at time of receipt, locks and combinations changed when personnel change, cash is locked up overnight, surprise cash counts, log receipt and deposit daily	Low - Monitor and manage by routine procedures
Improper management of fundraised accounts	C	4	Supervisory review and approval	Medium - Management responsibility must be specified
Credit Card information not properly safeguarded	C	4	Training and awareness program, documented policies and procedures	Medium - Management responsibility must be specified

University at Buffalo
The State University of New York

Control Activities

Identifying appropriate control activities

University at Buffalo
The State University of New York

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.

University at Buffalo
The State University of New York

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.

University at Buffalo
The State University of New York

Information & Communication

Creating an environment of transparency

University at Buffalo
The State University of New York

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.

University at Buffalo
The State University of New York

The database will allow for reporting on trends and metrics.	Quantity of issues by priority level.
	Aging of issues to resolution date
	Concentration by unit or issue type

University wide information sharing-best practices.	Identify potential for efficiency through resource sharing
	Use best practices for mitigation of similar risks
	Identify subject matter experts

University at Buffalo
The State University of New York

Monitoring Activities

University at Buffalo
The State University of New York

Ongoing Monitoring

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.

University at Buffalo
The State University of New York

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

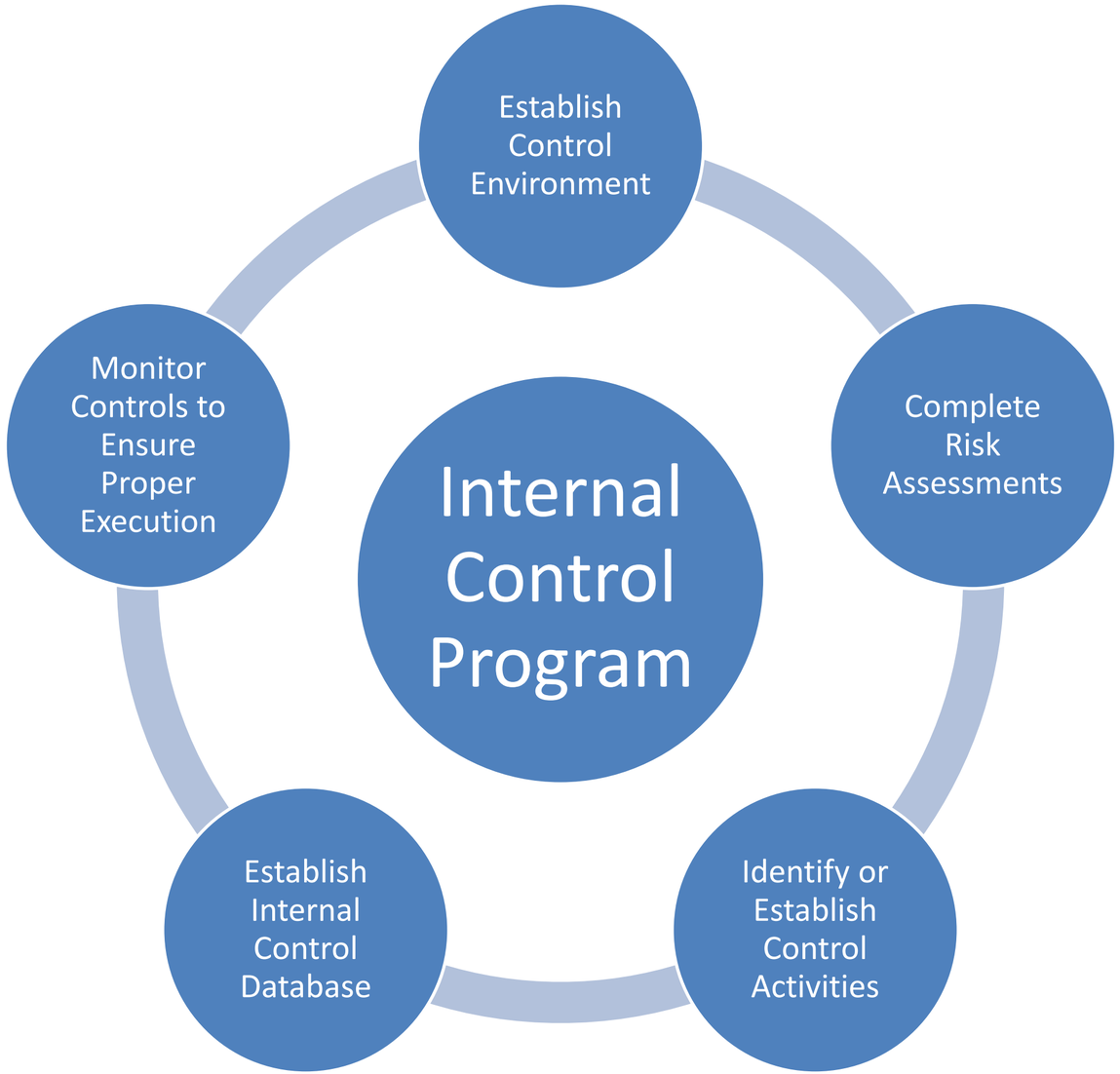
Second Line of Defense

- Compliance Activities
- Internal Control Monitoring and Follow Up

Third Line of Defense

- Internal and External Audit
- Regulators

University at Buffalo
The State University of New York



University at Buffalo
The State University of New York

Comments/Questions?