Risk Assessment Survey

What is a risk assessment?

- A risk assessment is not an audit.
- A risk assessment is a method used to identify weaknesses which might prevent a business unit from achieving its goals and objectives.
- Part of the process is a review of mission and goals: Are your unit's mission and goals in sync with the University's mission and goals?
- Part of the process is to identify the activities of the business unit and determine what could prevent the area from achieving its goals or mission.
- A risk assessment is a process that assigns a score to risk based on impact and probability (explained in more detail later in the process).

Why assess risk?

- To identify weak areas within a business unit.
- To direct resources effectively. Too many people or too much time may be spent on processes that do not need that much attention while 'riskier' processes are lacking in attention.
- To communicate risks – an end product that will visually show you and upper management where the problems are.

How do you assess risk?

Risk assessments can be performed on a single function within a major function, or they can be performed on a major function within a larger division. On the following pages is an outline of a risk assessment survey that can be applied to a smaller unit (with a little tweaking) or an entire department.

Please review the process for your own business unit. You will find an example of an already-completed risk assessment of the Business Affairs department at Sample Risk Assessment.*

You may perform the risk assessment on your own, but if you would like to have someone from Internal Audit facilitate a risk assessment survey for your unit, please contact us.

*Disclaimer: *The sample assessment was completed in the spring of 2008 so it does not reflect the business units that have been added to Business Affairs since that time. Also understand that the risks identified at that time may or may not be the same risks that would be identified today should that department repeat this process. This is a process that should be repeated periodically, especially when major changes have occurred.*

** You may copy and save this entire document to your own file **

Proceed to next page

Risk Assessment Survey

University Department: _____

Step 1: Identify the area's mission and goals. If you don't have one now – in writing -
- develop one before proceeding with this assessment. Think about your unit's purpose and
how it ties into the overall mission of the University.

Mission: Click inside the box to begin typing. The box can be enlarged while in edit mode
if more room is needed.

```
[                                                                              ]
[                                                                              ]
[                                                                              ]
[                                                                              ]
[                                                                              ]
[                                                                              ]
```

Long-Term Goals or Objectives: Try to identify at least 3 or 4

1.

2.

3.

Short-Term Goals or Objectives: Try to identify at least 3 or 4

1.

2.

3.

4.

**Step 2: Identify the core processes (major functions) that support this
department's mission and accomplishment of its goals and objectives.**
See Sample Risk Assessment, page1.

**Step 3: List the key activities performed for each of the core processes (major
functions).** See Sample Risk Assessment, pages 2 and 3.

**Step 4: Prepare a list of consequences that may occur if the department is unable
to meet its goals and objectives. Rank the consequences based on the impact
each would have on the department should it occur, no matter the reason.**

With a few exceptions, the consequences listed in the table below represent a set of
consequences identified by a group of senior managers from universities around the
country. This is not a comprehensive list that would apply to every department. Other
consequences can be added; some consequences can be disregarded. Also, if you were

performing a risk assessment on a single function within a major function, e.g., processing a vendor payment in accounts payable, which is a sub-function of the Business Office operations, you would likely have a completely different set of consequences.

The plan here is to review the list – modify or create a new list if necessary -- and to rank the consequences from high to low based on the impact they would have on your unit or department. **An explanation of high, medium, and low is below the table.** The current ranking was used by the Business Affairs, an administrative unit. The current ranking may not be suitable for an academic unit. Don't be hesitant to make changes.

After ranking is complete, renumber each consequence in the far left column. This number is used in other tables as you will see later. The color coding is used for visual effect only.

	CONSEQUENCES	IMPACT VALUE
0	Students unprepared to 'live wisely'	H
1	Loss of significant future revenue stream	H
2	Loss of credibility (long term bad PR)	H
3	Loss of significant assets	H
4	Declining enrollment	H
5	Significant interruption to business continuity	H
6	Death/Major injury	H
7	No awareness of USI - no name recognition	H
8	Decisions based on inaccurate or unreliable information	H
9	Qualified or adverse audit opinion	H
10	Low morale	M
11	Bad PR (short term)	M
12	Civil fines, penalties, or sanctions	M
13	Increased oversight	M
14	Loss of knowledge base (key personnel or data)	M
15	Re-work/Inefficiency	M
16	Lawsuits – individual	M
17	Criminal punishment	M
18	Lawsuits – class action	L
19	Letter of reprimand	L
20	Return funds	L
21	Increased costs	L

High = the consequence of the risk occurring will prevent the organization/unit from meeting its goals and objectives, or to do so will require major damage control.
Medium = the consequence of the risk occurring will only slow, or make inefficient, the organization/unit from meeting its goals and objectives.
Low = the consequence of the risk occurring will have little or no effect on the organization/unit meeting its goals and objectives.

NOTE: There is no significance to the order of consequences within each category.

Step 5: Identify risks or challenges associated with each core process based on the activities identified in step 3.

This is a brainstorming session. Ask "What would cause this process to fail?" Don't get carried away with this part. Identify your most likely or significant risks first and stop after identifying 15 or so risks. More than that is information overload and impossible to work with later on.

Step 6: Using the ranked consequences, assign an IMPACT value to each risk/challenge based on the most likely consequence(s) should that risk happen.

As defined earlier, impact is the effect on the achievement of goals and objectives when the risk happens.

Step 7: Assign a PROBABILITY value (High, Medium, Low) of the risk happening.

Assume there are only operating controls in place -- which are those embedded in day-to-day operations, guided by policies and procedures, segregation of duties, and routine reconciliations -- but disregard any supervisory or oversight controls that may exist when assigning a probability value.

High probability = It will happen often.

Medium probability = It is likely to happen, but not often.

Low probability = It is unlikely to happen at all

Sort the risks from high to low as shown in the 'Ranking' column of the table below.

The results of steps 5, 6, & 7 are reflected in tables like the one below. See Business Affairs, pages 5 – 7, for more examples.

Core Process: **Budgeting**	Impact	Prob	Ranking	Consequences
1. Decreasing State appropriation	H	M	HM	1, 4, 10
2. Competing budget priorities	M	H	MH	10, 11
3. Insufficient budget staff	M	H	MH	10, 11, 13, 14, 15
4. Understated expenditure and/or overstated revenue budgets (significant variances)	M	M	MM	8, 11, 13, 15
5. Inability to prevent end-of-year spending to 'use up' available budget	M	L	ML	11, 13, 15, 21

Point values: H = 3; **M** = 2; **L** = 1
Impact based on average score of Consequences listed: **H =** 2.5 and above
M = 1.5 thru 2.49
L = < 1.5

Ranking scores:

HH, HM	🟥	Critical Risk
HL, MH	🟨	Near-Critical Risk
MM, ML, LH	🟩	Moderate Risk
LM, LL	⬜	Low Risk

Step 8: Generate a Risk Footprint matrix based on the risks and associated ranking for each core process.

This step may or may not be necessary. If you are performing a risk assessment of one or two smaller departments, you may be able to visualize where the riskier areas are from the tables created in steps 6 and 7 above. However, if you are performing a risk assessment of a larger unit, such as the entire Business Affairs division in the example, you will be better served to create the risk footprint. A segment of the Business Affairs Risk Footprint is shown below. Click on these links -- page 1A and page 1B -- for full display.

Layout of the Risk Footprint matrix:
- The core processes are listed down the left column (vertical axis). Those with the most critical risks are listed first.
- The risks identified in the steps 6 and 7 are listed across on the same row as the core process to which they pertain (horizontal axis).
- The footprint is designed so that core processes with the highest risk items (red) are presented first at the top left, moving right and down with lesser risk items. The lowest risk items would be at the far right and/or at the bottom right.

Management should use the footprint to allocate resources to managing the risks that can affect the achievement of goals and objectives.

Business Affairs		RISKS ⟶					
CORE PROCESSES		1		2		3		4
Physical plant operations	HH	Dependency on city and Vectren for water and electricity	HL	Failure to maintain capacity to operate campus boilers, chillers, electrical, or HVAC	MH	Failure to attract qualified people for key positions	MH	Inability to control utilities costs
Budgeting	HM	Decreasing State appropriation	MH	Competing budget priorities	MH	Insufficient budget staff	MM	Significantly understate expense and/or overstate revenue budgets
Computer & telecom Services	HM	Failure to protect/ recover data from man-made or natural disasters	MM	Attracting and/or retaining qualified staff	MM	Failure to keep pace with technology changes	MM	Failure to maintain secure IT environment
Finance & investing	HL	Inability to make timely payment of principal and interest	HL	Failure to ensure that cash flow is adequate to meet daily needs	MH	Market values affected by change in interest rate	MM	Rating change of underlying credit instruments
Internal auditing	HL	Restricted independence/scope/ access	HL	Lack of management or audit committee support	MH	Inadequate audit coverage	MM	Insufficient audit staff

Step 9: Construct a Control Footprint matrix for each core process, identifying controls that are in place, or should be in place, for each of the risks identified.

Once the risk assessment is complete, you are now faced with the task of determining what to do next. A mitigation strategy will help you determine how to manage risk. There are several choices depending on the criticality of the risk and management's tolerance for risk. Options for managing risk include the following:

- *Accept the risk* – Do nothing to manage it. This may be a suitable action for low risk activities where the cost of adding a control would outweigh the benefit.

- *Avoid the risk* – Do not do the activity which generates the risk. This may not be possible if the activity causing the risk is an activity that's critical to accomplishing the unit's goals.

- *Control the risk* – Establish policies and procedures to manage the risk. Review existing policies and procedures to determine where they might be strengthened to better control the risk.

- *Manage the risk* – Do something to lower the probability to an acceptable level. Be aware that managing a risk will affect the *probability* of the risk occurring, but the *impact* will remain the same should the risk occur anyway.

- *Share the risk* – Partner with another entity who has a stake in the success of the unit accomplishing its goals. If another party takes responsibility for some portion of the activity, the risk level could be lowered.

- *Transfer the risk* – Let someone outside the organization be responsible for the activity or be the control. An example of this is the coverage provided by an insurance policy.

For purposes of this exercise, identify an existing control or a potential control that could be implemented for each risk identified in the preceding steps. This might be a brainstorming session, or you might draw from some of the controls found in General Controls.

Using the Control Footprint matrix. . .
1. Document the controls down the left side that are currently in place for each risk (entered across the top) within each core process.
2. Document which risks a control mitigates by placing an "X" in the matrix. Keep in mind that one control can mitigate more than one risk.
3. Document any controls within a core process that are currently being performed that are not tied to a risk. The reason for this is because you may have a control that is unnecessary – or perhaps another risk that was forgotten.
4. In the far left column, indicate the level of the control identified.
   a. 1 = Operating control – generally performed as part of the process itself by the staff performing the activity.
   b. 2 = Supervisory control – performed as a quality check on the process by supervisors or others who do not originate the event or transaction.
   c. 3 = Oversight control – status reports, analytical reviews, etc. performed by representatives of executive management.

Notice on the Control Footprint matrix, on the far right hand side, there is a section entitled 'Monitoring Plan'. The following instructions pertain to this section.
5. Document the responsible person and evidence of control for each control listed.
6. Decide on which controls to monitor.
   a. Controls shaded in peach are chosen to monitor because they provide the most coverage for critical (red) or near critical (yellow) risks, or because management has the experience and available resources to monitor.
   b. Controls shaded in blue are managed outside the authority of this unit.
   c. Controls shaded in purple are being considered for implementation in the future.

A portion of the Control Footprint matrix for the budgeting process is illustrated below. Unfortunately, there is no example of a completed control matrix at this time to reference. If you should complete one – including the monitoring plan – Internal Audit would greatly appreciate receiving a copy to use as an example with this risk assessment survey process.

Core Process:	Budgeting				
Control Footprint Matrix					
L E V E L	**RISKS** ➡ **CURRENT CONTROLS** ⬇	Decreasing State appropriation	Competing budget priorities	Insufficient budget staff	Significantly understate expense and/or overstate revenue budgets
3	Effectively lobby legislators	X			
1	Provide budget training and awareness programs		X	X	X
1	Hire qualified staff			X	
3	Monitor state legislation	X			
2	Assign responsibility		X	X	X
3	Monitor budget to actual		X		X
3	Performance evaluations			X	
1	Training and professional development			X	

Congratulations!

If you have completed the Risk Assessment Survey all the way to the end, you are to be congratulated. If you didn't complete the process, don't fret. This is a very time consuming process, and you may have better success assessing smaller areas than trying to assess an entire division at once.

As we said earlier, if you want help from the Internal Audit department on any part of the process, just contact us.