BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK

Risk Management
Administrative Compliance
Internal Control

# PERFORMING A RISK ASSESSMENT
# (Risk Identification and Analysis)

The following information is designed to provide a comprehensive and repeatable approach for conducting risk assessments.

It is important to have an understanding of the unit before starting an assessment. The following should be among the factors used to analyze the environment:

- a commitment to integrity and ethical values;
- understanding of organizational structure and oversight;
- delegation of authority and responsibility;
- a commitment to competence; and
- accountability.

**Steps**

1) Review the unit's mission, objectives, and functions
   a) Ensure that the unit's mission is up-to-date and reflects the current operations.
   b) Review the unit's strategic plan and/or vision for the future.
   c) Review the unit's operational goals, reporting and compliance requirements and major responsibilities.
   d) Review prior risk assessments or audit materials (if available).
   e) Identify the major functions or activities of the unit.
      i) Review the major functions/processes in place to carry out the mission/strategic plan/goals and objectives.
      ii) Review how the unit is organized and structured.
      iii) Identify the departments or areas that process information and transactions.

2) Using the major functions identified above, identify and analyze the risks facing the unit. A risk is any event or action that adversely impacts the unit's ability to achieve its objectives. Identify events that can cause or result in an adverse effect on operations. Consider all types of risk (financial, operational, health and safety, strategic, compliance, and reputational risks). Identify events/actions that could cause the unit not to be able to achieve the mission or not do it effectively. Consider whether a risk is external or internal, and /or emerging. Asking the following questions will assist in identifying the risks the assessable unit faces when trying to achieve its objectives:
   a) Where are we vulnerable and what could go wrong?
   b) What requirements and laws apply?
   c) What is required to go right for this to succeed?
   d) Are there any new/changed processes or technologies?
   e) What are we trying to protect?
   f) What might be the public perception of this situation?
   g) What keeps me awake at night?

3) Identify the existing control and mitigating activities used to manage the risks.
   a) Review processes/procedures used to manage and/or mitigate the risks. Identify who is accountable for the mitigating activity by documenting the position/person with the responsibility to carry out the procedure.
   b) Record what documentation of the mitigating activity exists or the evidence produced that shows that the procedure was performed (i.e., records, signatures, reports, deposit slips, reconciliations, agenda items, meeting notes, etc.)
   c) Include how supervisors and managers gain assurance that the mitigating procedures are effectively being performed. Document the monitoring and supervisory procedures including the frequency and the position responsible for the monitoring process.
   d) For significant risks, document the reporting and communication to executive management that the mitigation procedures are in place and working as planned.

4) Determine which risks are most significant to the unit by ranking the risks.
   a) Rank the risks considering both the potential impact/consequence and probability/likelihood of the event occurring.
   b) Use (1) Insignificant/Low, (2) Mild/Low-Medium, (3) Moderate/Medium, (4) Significant/Medium High, and (5) Catastrophic/High to rank the probability and impact. Based on this scoring a risk will fall within red, orange, yellow or green areas.
   c) Review the overall rankings – review that the significant risks are captured and that the prioritized risks appropriately reflect the unit's operations/activities and current environment.

5) Recommend subsequent action. Recommendations are derived from consideration of the conclusions reached in the steps above, using previous knowledge and experience, professional judgment, and the overall risk ranking of the unit or activity. Such actions may include establishing or modifying controls to effectively address the identified risks, reduce controls for areas that appear to be over-controlled, or conducting an in-depth internal control review to test the adequacy and effectiveness of the controls in place. Unit management and ERM/Internal Control should agree on the subsequent actions necessary to promote an effective system of internal control.

6) On a periodic basis (i.e., every two years) re-assess and update the risk assessment. For questions or assistance in performing a risk assessment, contact Risk Management and Administrative Compliance at risk@binghamton.edu or 607-777-7475.