University Audit and Compliance

Risk Assessment Process
Enterprise-Wide Risk Assessment
Risk Assessment Process

Risk Assessment:
- A disciplined, documented, and ongoing process of identifying and analyzing the effect of relevant risks to the achievement of objectives, and forming a basis for determining how the risks should be managed.

Diagram:
- Control Environment
- Risk Assessment
- Control Activities
- Communication
- Monitoring

University Audit and Compliance
Approaches

• Measurement-driven approach
  – Focus on identifying key risk factors
  – Understanding their materiality and probability
  – Manage the most material risks

• Process-control approach
  – Focus on key business processes
  – Manage risk events by achieving consistency and limiting surprises
5 Step Process

1. Identify relevant risks.
2. Assess likelihood and impact of risks identified.
3. Determine risk response.
4. Identify control activities that are needed to help ensure that risk responses are carried out properly and timely.
5. Establish procedures to monitor attainment of goals and identify residual risks.
Process: Identify Risks

1. Identify relevant risks:
   - Obstacles to achievement of goals
   - Limited resources
   - Decentralized systems
   - High turnover
   - Low salaries
   - Outdated policies and procedures
   - Management with limited financial background
   - Employee resistance
Process: Assess

1. Identify relevant risks.

2. Assess likelihood and impact of risks identified.

3. Determine risk response.

4. Identify control activities that are needed to help ensure that risk responses are carried out properly and timely.

5. Establish procedures to monitor attainment of goals and identify residual risks.
Process: Assess

2. Management assesses risk from two perspectives:
   • Likelihood – probability of occurrence
   • Impact – severity of consequence

A combination of two methods is normally used:
   • Qualitative methods - Nominal and ordinal measurement
   • Quantitative methods - Interval and ratio measurement
Process: Assess

Likelihood - Qualitative technique:

• Ordinal measurement
  – Events are listed in order of importance
  – High, medium, low or certain, possible, rare
  – Example: Likelihood of a computer virus disrupting systems is greater than likelihood of staff’s unauthorized transmittal of confidential information
Process: Assess

Impact to institution’s objectives:

- **Strategic** – high-level goals, aligned with and supporting its mission
- **Financial** – safeguarding assets
- **Operational** – processes that achieve goals
- **Compliance** – laws & regulations
- **Reputation** – public image
Impact - Qualitative technique

• Ordinal ranking
  - Level 1 through 5.
  - Insignificant, minor, moderate, major, catastrophic.
  - Example: Impact of unplanned release of hazardous materials ranked from minor (contained on-site) to catastrophic (detrimental effect on environment, significant injuries, etc.).
Process: Response

1. Identify relevant risks.
2. Assess likelihood and impact of risks identified.
3. Determine risk response.
4. Identify control activities that are needed to help ensure that risk responses are carried out properly and timely.
5. Establish procedures to monitor attainment of goals and identify residual risks.
Process: Response

3. Determine risk response.
   • Transfer or avoid unacceptable risks.
   • Reduce threats and control uncertainties.
   • Maximize opportunities.
Process: Response

Choices:

• Avoid
• Transfer
• Minimize consequence
• Reduce the threat
  – Reduce the likelihood or probability
  – Minimize the impact or consequences
• Control uncertainties
• Accept
What to do?

• If an activity is too risky, discontinue it.
• Transfer the risk.
  – Insurance
  – Contractual provisions
  – Bonding
• Reduce level of activity or diversify.
Process: Response

Reducing probability of risk:

- Limit access or role-based access.
- Background checks.
- Independent monitoring.
- Comparisons to benchmarks.
- Separation of duties.
- Establish accountability.
Process: Response

Minimizing Consequence:

• Limit physical access.
• Limit authority.
• Segregate duties.
• Additional approvals for high risk items.
• Limit access to sensitive information/data.
• Independent monitoring.
Process: Response

Controlling uncertainty:

- Disaster recovery planning.
- Awareness of competition.
- Knowledge of industry activities or issues.
- Monitor for presence of unknown.
- Virus scanning.
- Communication with key stakeholders and constituents.
Process: Identify Controls

1. Identify relevant risks.
2. Assess likelihood and impact of risks identified.
3. Determine risk response.
4. Identify control activities that are needed to help ensure that risk responses are carried out properly and timely.
5. Establish procedures to monitor attainment of goals and identify residual risks.
Process: Identify Controls

4. Identify control activities that are needed to help ensure that risk responses are carried out properly and timely.
   • Preventive
   • Detective
1. Identify relevant risks.
2. Assess likelihood and impact of risks identified.
3. Determine risk response.
4. Identify control activities that are needed to help ensure that risk responses are carried out properly and timely.
5. Establish procedures to monitor attainment of goals and identify residual risks.
5. Establish procedures to monitor attainment of goals and identify residual risks.

- Have all threats and uncertainties been identified?
- Are the probability and consequences reasonable?
- Are outcomes compared to goals or benchmarks?
- Are controls working to manage risk?
Potential Threats

• Excessive cost (overpaying).
• Deficit revenues.
• Fraud.
• Conflict of interest or commitment.
• Poor management decisions.
• Inaccurate or untimely financial reporting.
• Excessive regulation.
Potential Uncertainties

- Business interruption.
- Legal action.
- Natural disaster.
- Customer dissatisfaction.
- Competitive disadvantage.
- Government criticism due to politically hot issues.
Potential Opportunities

• Technology
• Untapped markets
• Intellectual property
• Competitive advantage
• Personnel expertise
• Investment management
Who Sets Risk Tolerance

University leadership determines the degree of acceptable risk.

Balance of opportunity versus probability of adverse action.