Conducting an Enterprise Risk Assessment and Building a Program Tailored to Your Institution’s Needs
August 23, 2017

Presented by:
Jim Yard and Heather Haemer

Big Thinking. Personal Focus.
<table>
<thead>
<tr>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>James B. Yard, Shareholder</strong></td>
</tr>
<tr>
<td>Risk Advisory Services</td>
</tr>
<tr>
<td>CPA, CIA, CISA</td>
</tr>
<tr>
<td>Schneider Downs &amp; Co., Inc.</td>
</tr>
<tr>
<td>One PPG Place, Suite 1700</td>
</tr>
<tr>
<td>Pittsburgh, PA 15222</td>
</tr>
<tr>
<td><a href="mailto:jyard@schneiderdowns.com">jyard@schneiderdowns.com</a></td>
</tr>
<tr>
<td>Work Phone: (412) 697-5345</td>
</tr>
<tr>
<td>Cell Phone: (724) 822-3915</td>
</tr>
<tr>
<td><strong>Heather A. Haemer, Senior Manager</strong></td>
</tr>
<tr>
<td>Risk Advisory Services</td>
</tr>
<tr>
<td>CPA, CIA</td>
</tr>
<tr>
<td>Schneider Downs &amp; Co., Inc.</td>
</tr>
<tr>
<td>One PPG Place, Suite 1700</td>
</tr>
<tr>
<td>Pittsburgh, PA 15222</td>
</tr>
<tr>
<td><a href="mailto:hhaemer@schneiderdowns.com">hhaemer@schneiderdowns.com</a></td>
</tr>
<tr>
<td>Work Phone: (412) 697-5433</td>
</tr>
<tr>
<td>Cell Phone: (412) 596-3387</td>
</tr>
</tbody>
</table>
Disclaimer

IRS CIRCULAR 230 DISCLOSURE: Any tax advice contained in this communication (or in any attachment) is not included or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code, or (ii) for promoting, marketing or recommending to another party any transaction or other matter addressed in this communication (or in any attachment).

The views expressed by the presenter do not necessarily represent the views, positions, or opinions of Schneider Downs & Co., Inc. These materials, and the oral presentation accompanying them, are for educational purposes only and do not constitute accounting, tax or legal advice or create an accountant-client or attorney-client relationship.
Agenda

- What’s the Value in ERM?
- ERM in Higher Education
- Conducting an Enterprise Risk Evaluation
- Best Practice to Consider
What’s the Value in ERM?

The **COSO** “Enterprise Risk Management - Integrated Framework” defines ERM as ...

A process, effected by an entity’s board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.
What’s the Value in ERM?

Accountability Guide for University and College Boards

ERM is a business process led by senior leadership that extends the concepts of risk management and includes:

• Identifying risks across the entire enterprise;
• Assessing the impact of risks to the operations and mission;
• Developing and practicing response or mitigation plans; and
• Monitoring the identified risks, holding the risk owner accountable, and consistently scanning for emerging risks.
What’s the Value in ERM?

Our definition - A discipline of understanding risk for the purpose of appropriately allocating an organization’s resources on business activities that present high risk and exposure to the organization’s strategic purpose and ability to prosper. ERM offers a framework for effectively managing uncertainty, responding to risk and harnessing opportunities as they arise.

By focusing on, dedicating resources to, and continuously monitoring these business activities, an organization continuously improves its operations and value is derived.
ERM in Higher Education

Recent history indicates that the pace of change in Higher Education is unprecedented; however, institutions are only seeing a modest increase in the use of risk-based decision making—

- Boards and senior administrators **not yet fully committed**
- **No shortage of recent events** that impact reputations of institutions
- **Highly competitive environment** means that colleges and universities are under intensifying pressure to attract and retain faculty and students and maximize their assets — something that cannot be achieved without tight control of risks across the board.
ERM in Higher Education

• Association for Governing Boards of Universities and Colleges and United Educators says -

“Now more than ever, governing boards and senior leaders need to be attentive to risks. This is no time for complacency and the assumption that incidents with tragic financial or reputational impact couldn’t happen at our college or university.”
Many institutions are not adequately prepared to address risks that may impact their –

- Mission
- Strategy
- Financial Condition
- Student Experience
ERM in Higher Education

More integrated process on top risks areas (both upside and downside risk) can enable better decision making and resource allocation -

• Achievement of strategic objectives and goals
• Protection of reputation
• Financial preservation/viability
• Board transparency
• Compliance with laws and regulations
## Life Is Simple, Isn't It?

<table>
<thead>
<tr>
<th>Compliance</th>
<th>Oversight/Outside Forces</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Higher Education Opportunity Act</td>
<td>• NCAA/NAIA</td>
</tr>
<tr>
<td>• Title IX</td>
<td>• Accreditors</td>
</tr>
<tr>
<td>• Clery Act</td>
<td>• Lenders</td>
</tr>
<tr>
<td>• Whistleblower Protection Act</td>
<td>• Department of Justice</td>
</tr>
<tr>
<td>• Occupational Safety and Health Act</td>
<td>• Department of Labor</td>
</tr>
<tr>
<td>• Equal Employment Opportunity Act</td>
<td>• Department of Education</td>
</tr>
<tr>
<td>• Fair Credit Reporting Act (FCRA)</td>
<td>• Immigration and Customs</td>
</tr>
<tr>
<td>• Uniform Guidance</td>
<td>• Occupational Safety and Health Administration</td>
</tr>
<tr>
<td>• Equity in Athletics Disclosure Act</td>
<td>• IRS</td>
</tr>
<tr>
<td>• Gramm-Leach-Bliley Act (GLBA)</td>
<td>• National Labor Relations Board</td>
</tr>
<tr>
<td>• HIPAA</td>
<td></td>
</tr>
<tr>
<td>• Family Educational Rights and Privacy Act (FERPA)</td>
<td></td>
</tr>
</tbody>
</table>
WHAT IS ERM? It is the capability to effectively answer the following questions:

- What are all the risks to our business strategy and operations?
- How much risk are we willing to take?
- How good are we at overseeing risk taking?
- How do we ensure we have the right information to manage risk?
- How do we determine the size and scope of the risks?
- How well do we manage the risks?
- What are we doing about the risks?
- What else can go wrong and how are risks interconnected?

• Circular depiction is highly intentional
• Components are meant to be dynamic (reviewed back/forth in any sequence)
• Having the right culture is key

Source: The Risk Management Association
implementation

1. Phase 1: Project governance
   - Develop project plan
   - Assign executive sponsor
   - Define leadership team
   - Approval of risk policy and framework

2. Phase 2: Conduct the initial enterprise-wide risk assessment & develop an action plan
   - Define risk universe
   - Develop and define ranking criteria
   - Risk assessment advance communication sent to management

3. Phase 3: Inventory the existing risk management strategies and controls
   - Conduct executive interviews – data gathering and documentation
   - Evaluate management’s responses on risk
   - Perform gap analysis

4. Phase 4: Reporting and Sustainability
   - Develop initial risk reporting
   - Develop ongoing monitoring
   - Final Plan to organization management
   - Develop appropriate executive management & board communications

Key Outputs

<table>
<thead>
<tr>
<th>Project plan Policy</th>
<th>Risk workshop advance prep</th>
<th>Completed risk model Gap analysis</th>
<th>Risk reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining risk</td>
<td>Defining reporting relationships and resource requirements</td>
<td>Standard templates</td>
<td></td>
</tr>
</tbody>
</table>
Applicability to Higher Education

• Focus attention on key business activities such as:
  – Enrollment and admissions
  – Construction and facilities management
  – Campus safety and business continuity
  – Faculty and curriculum management
  – Data privacy and security
  – Registrar and degree conferral
  – Tuition billing and financial aid
  – Grant management
  – Compliance
Identifying and Measuring Risk

- The concept of risk
  - is not easily quantified.
  - is not expressible in a neat, numerical package that all can understand.
  - can be highly subjective, having both qualitative and quantitative elements.
Identifying and Measuring Risk

• Identify and assess risk
  – Institutional knowledge
  – Industry/peer knowledge
  – Subject-matter knowledge

• Arriving at a universal “risk formula” to apply to events, occurrences and/or opportunities is very challenging.
  – TRUTH: every organization, within and outside of a given industry, has its unique applications of risk management policies and practices.
Example Risk Areas

- Succession planning
- Strategic plan
- Maintaining mission and identity
- Competition
- Marketing/differentiation
- Economic downturn
- Changes in funding
- Diversification of student body
- Tuition dependency
- Low endowment

- Unionization
- Faculty shortage
- Enrollment decline
- Cyber attack/technology breaches/failures
- e-Learning/hybrid learning
- Aging infrastructure
- Loss of facilities
- Campus safety/security crisis
- Compliance violation
- Student support services
Rating Risks

- Probability/Likelihood/Vulnerability – risk threat level absence controls
- Impact/Severity/Loss Magnitude – measurements include financial, threat to human life, environmental, etc.
  - Also consider future repercussions/secondary effects (prime effects and the secondary effects ... quake/aftershocks/longer-term ramifications)
Rating Risks

- Velocity/Speed – speed at which the risk occurs, and will management have sufficient opportunity to react to its onset
- Frequency/Persistence – one-time event or recurring and at what rate
- Direction of Risk/Threat
Measuring and Monitoring Risk

- Inherent and residual risk measurements
  - Risk Acceptance (risks in the normal course of business)
  - Risk Appetite (determined based on strategy/long-term business plan)
  - Risk Tolerance (point at which potential impairment occurs, entering crisis mode)
Measuring and Monitoring Risk

• Assigning accountability (e.g., Risk Owner)
• Determining your key risk indicators
• Consequences if you do nothing
• Action plans - steps to reduce/respond
• Evaluation frequency
• Target dates and milestones
Most organizations are familiar with key performance indicators (KPIs) as a way of monitoring and measuring success or progress towards business goals.

Key risk indicators (KRIs) can perform a similar role with regard to exposures.

- KRIs are leading indicators of potential threats and should be proactively monitored and tracked.
- KRIs could be thresholds that measure success and failure and are used to reward and trigger alerts.
Key Risk Indicators

- One of the challenges of embedding ERM in an organization is to gain agreement to include KRIs alongside KPIs in the balanced scorecard or other management reporting tool that the board and senior executives use for assessing performance.

- By monitoring and assessing KRIs together with KPIs, an organization will have a better understanding of the context of its performance, as well as potential threats and opportunities that might impact that performance.
ERM – Embracing Analytics

DATA and the Digital World:

- Continuous monitoring of key risk indicators
- Quantifiable risk measurements
- Ability to assess entire populations
- Create risk dashboards

Challenges:

- Technology and talent
- Quality of data and its availability
- Access to comparable external data sources
ERM Best Practices

• ERM should:
  – Be linked and embedded in your strategy
  – Create and protect value
  – Be part of all processes
  – Be part of your decision making
  – Be used to handle uncertainty
  – Be systematic and timely
ERM Best Practices

- ERM should:
  - Be based on the best data
  - Be tailored to your environment
  - Consider human factors
  - Be transparent and inclusive
  - Be responsive and iterative
  - Support continual improvement
ERM is an Enabler

- Culture Change
- New Expectations
- Improved Response
- Increased Reporting
- Compliance
What Is the Value?

• More effective strategic and operational planning
• Planned risk-taking and the proactive management of risks
• Greater confidence in decision making and achieving operational and strategic objectives
• Greater stakeholder confidence
• Enhanced organizational resilience
• Dealing effectively with disruptions and losses, minimizing financial impact
• Avoid surprises through forward planning
• Regulatory compliance and director protection
Key Takeaways

- Keep it focused, simple and easy to understand or it will fail
  - Commitment, involvement and consensus
  - Link it to your strategy
  - Look outside your walls (industry and peer analysis)
  - Consider ‘Black Swan’ events
  - Get to a top 10 or 20, but also evaluate scenarios where multiple risks could have substantial impact
  - Manage, monitor, and improve in areas where greatest value can be achieved
  - Manage progress and enforce accountability

- Often the most significant risks and opportunities for value reside in areas threatening your key/strategic business objectives:
  - Strategy
  - Competition
  - Reputation
  - Mission/Program Differentiation
Resources

• Association of Governing Boards of Universities and Colleges
• Higher Education Compliance Alliance
• United Educators Insurance
• The Risk Management Association
• COSO
• ISO
As one of the largest certified public accounting and business advisory firms in the region, Schneider Downs serves clients throughout the country and around the world. By integrating high-quality resources, systems and personnel, Schneider Downs has built a reputation of delivering individualized services built on insight, innovation, and experience to meet each client’s specific needs.

For more information, visit us at www.schneiderdowns.com