Assessing the Effectiveness of Your Risk Management Program

James B. Yard
Internal Audit and Risk Advisory Services

Schneider Downs & Co., Inc.
October 22, 2013
Learning Objectives

During our time together, we will explore:

• Evolution of risk management
• How are not-for-profits addressing risk management?
• How does an organization identify strategic risks in today’s environment?
• How do we go about implementing and executing an effective risk management program?
• Best practices and pitfalls
Enterprise Risk Management (ERM) Overview

**COSO** - The Committee of Sponsoring Organizations of the Treadway Commission

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 is Enterprise Risk Management?

My 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.
Evolution of Risk Management

Traditional risk management can be characterized by fragmented responsibility, rather than a holistic approach; a focus on discrete events; a perception of risk management being a product of transaction (insurance/hedge) or a reaction to events.

The move to today’s ERM is strategic and focused. Today’s ERM model allows organizations to integrate business managers with risk managers, increase non-financial risk awareness, and increase involvement from all areas of the organization - executive management, board members, and business managers.
Traditionally risk was viewed more from a financial risk perspective. The new standard is to look at risk throughout the enterprise.
Board Members Should Be Asking

- Is there an established mechanism that addresses key risks across the organization and which elevates risk discussions to the strategic level?
- Has the organization conducted an in-depth, prioritized analysis of the top risks that can really make-or-break the organization?
- Do we understand the “big bets” we are taking as an organization?
- Is there a clear understanding of risks that management can measure and track?
- Do we have an established risk review process and get from management insightful risk reports?
- Do we have ownership, accountability and the right resources on risk matters?
Board Members Should be Asking

- Do our strategic planning, capital allocation, and financing activities consider risk factors?
- Is risk governance and risk-related committee structures at the board level defined?
- Is top management’s compensation structured to ensure performance in light of risks taken?

Asking these tough questions enable directors to fulfill their fiduciary duties and ultimately help their organizations prosper.
Survey Results - What the Non-Profit Community Has to Say

Sent to over 600 Non-Profit Leaders

Responses rate of 12%
What is the size of your organization?

- 0-25 employees (20%)
- 26-50 employees (14%)
- 51-100 employees (11%)
- 101-500 employees (31%)
- 500+ employees (23%)

What is your organization’s annual revenue?

- Less than $2 million (12%)
- $2-10 million (28%)
- $10-25 million (19%)
- $25-50 million (19%)
- $50-100 million (11%)
- Greater than $100 million (11%)
### Identification and Consensus on Top Risks

<table>
<thead>
<tr>
<th>Rating</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor</td>
<td>5%</td>
</tr>
<tr>
<td>Below Average</td>
<td>6%</td>
</tr>
<tr>
<td>Average</td>
<td>44%</td>
</tr>
<tr>
<td>Above Average</td>
<td>35%</td>
</tr>
<tr>
<td>Excellent</td>
<td>10%</td>
</tr>
</tbody>
</table>

### Education and Training on Risk Matters

<table>
<thead>
<tr>
<th>Rating</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor</td>
<td>3%</td>
</tr>
<tr>
<td>Below Average</td>
<td>27%</td>
</tr>
<tr>
<td>Average</td>
<td>44%</td>
</tr>
<tr>
<td>Above Average</td>
<td>21%</td>
</tr>
<tr>
<td>Excellent</td>
<td>5%</td>
</tr>
</tbody>
</table>
### Linking Risk Management with Organizations Strategy and Decision Making

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor</td>
<td>2%</td>
</tr>
<tr>
<td>Below Average</td>
<td>29%</td>
</tr>
<tr>
<td>Average</td>
<td>38%</td>
</tr>
<tr>
<td>Above Average</td>
<td>30%</td>
</tr>
<tr>
<td>Excellent</td>
<td>2%</td>
</tr>
</tbody>
</table>

### Ensuring Individuals Know Their Role in Managing Risk

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor</td>
<td>2%</td>
</tr>
<tr>
<td>Below Average</td>
<td>30%</td>
</tr>
<tr>
<td>Average</td>
<td>41%</td>
</tr>
<tr>
<td>Above Average</td>
<td>22%</td>
</tr>
<tr>
<td>Excellent</td>
<td>5%</td>
</tr>
</tbody>
</table>
Anticipating and Managing Risks

- Poor: 0%
- Below Average: 16%
- Average: 48%
- Above Average: 30%
- Excellent: 6%
Please assess your individual knowledge of Enterprise Risk Management (ERM):

- 50.0% have a basic understanding
- 29.7% have been personally involved in an ERM initiative
- 20.3% have never heard of it
To what extent has your organization adopted or considered an ERM program?

- 34.9%: Don't know
- 22.2%: Are investigating or plan to consider an ERM program in the next 1 to...
- 19.0%: Do not have and do not plan to consider an ERM program
- 17.5%: Have a fully integrated ERM program
- 6.3%: Have a partially integrated ERM program
What was the primary motivator for adopting ERM in your organization?

- Regulatory requirements: 54.0%
- Board directive: 19.0%
- Insurance requirements: 4.8%
- Management directive: 12.7%
- Response to an adverse event: 9.5%
- Not applicable
Outsourcing Risk Management Activities

- 7% of respondents surveyed outsource their risk management program
- An additional 9% are considering outsourcing within the next 1 to 5 years
Does your organization have an employed individual dedicated to overseeing and identifying risk management?

- Yes (33%)
- No (67%)

If yes, how long has your organization had this position?

- 64.9% of respondents do not have this position
- 17.5% of respondents have had the position in place more than 5 years
- 10.5% have had the position 1-5 years
- 7% have had the position less than 1 year

If no, are there plans to add a position?

- 0% - yes
- 63.2% - no
- 36.8% - N/A, we have this position
Does your risk management professional hold other responsibilities or are they 100% dedicated to risk management?

- 45.0%: Do not have an individual but have a risk management committee
- 15.0%: N/A - do not have this position
- 3.3%: Shared responsibilities
- 36.7%: 100% dedicated to risk management
What department within your organization is primarily responsible for directing ERM?
Who was the primary advocate for implementing ERM within your organization?

- Board: 48.3%
- CEO: 21.7%
- Board and CEO: 10.0%
- General Counsel: 11.7%
- Other: 8.3%
- Not applicable: 0%
To whom does your risk management professional-administrative report?

- Board: 32.8%
- CEO: 29.5%
- CFO: 14.8%
- Legal Counsel: 9.8%
- Other: 13.1%
- Not applicable: 0%
How often does your Board discuss the risks to your organization?
13% of respondents stated that their organizations have adopted a formal Enterprise Risk Management framework.

9% of respondents answered that their framework was approved by the Board or a Board committee.
What software tools does your organization utilize to enable your risk management function?

- Vendor developed risk management software
- In-house developed risk management software
- Microsoft Excel
- Other
- Not applicable

Percentage:

- Vendor developed risk management software: 0%
- In-house developed risk management software: 0%
- Microsoft Excel: 10%
- Other: 5%
- Not applicable: 85%
What criteria does your organization utilize for quantifying risk within your organization? Please select all that apply.

- Impact
- Likelihood
- Velocity
- Not applicable
Does your organization utilize risk appetite to make informed decisions on risk matters?

- Yes: 52.8%
- No: 26.4%
- Not applicable: 20.8%
Is your organization satisfied with its risk management practices?

- Yes: 59.6%
- No: 40.4%
Implementation – It is really not that hard to do

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

**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

**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

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

<table>
<thead>
<tr>
<th>Key Outputs</th>
<th>Project plan</th>
<th>Policy</th>
<th>Defining risk</th>
<th>Defining reporting relationships and resource requirements</th>
<th>Risk workshop advance prep</th>
<th>Ranking criteria</th>
<th>Standard templates</th>
<th>Completed risk model</th>
<th>Gap analysis</th>
<th>Risk reports</th>
</tr>
</thead>
</table>
Risk Management Principles

Risk Management 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
- Be based on the best data
- Be tailored to your environment
- Consider human factors
- Be transparent and inclusive
- Be responsive and iterative
- Support continuous improvement
Choosing a Framework

Which Framework do you use?

- Anyone you want, however ...
  - COSO ERM
  - AS/NZS 4360:2004
  - The Turnbull Guidance
  - ISO 31000-2009
My Take on ERM in Non-Profit World

- Keep it focused, simple and easy to understand or it will fail
  - Commitment, involvement and consensus
  - Link it to your strategy
  - Looks 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
Leading Practices

- Establish a risk management policy for your organization
- Communicate your risk management policy
- Fully engage your board of directors
- Involve risk management into strategic planning
- Integrate risk management into your business functions
- Assign risk ownership and accountability for risk management
- Communicate and ensure transparency
- Gather intelligence (benchmarking, trend analysis)
- Continuously monitor
- Evaluate scenarios (stress testing, disaster recovery)
- Allocate time and resources
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
Common Pitfalls

- Not linking strategic planning and risk management
- Not positioning ERM as a management practice
- Procedural approach (restrictive/limiting)
- Many failures explained by challenges of responding to an unanticipated event, Black Swan event, or combination of events
- Placing risk management oversight with the audit committee
- Diminishing transparency
- Lack of support at the executive level
- Not looking beyond impact and likelihood
- Lack of understanding on the “Big Bets” being taken
- Failure to assess industry and peer dynamics
Key Takeaways

- Understand your organization’s culture, strategies and objectives
- It is not that hard - keep it simple
- Involve your board and key business advisors
- Dedicate resources and train them
- Develop a common risk language
- It should improve your organization
- Continuously monitoring and reporting
"We've considered every potential risk except the risks of avoiding all risks."
James B. Yard
Internal Audit and Risk Advisory Services
CPA, CIA, CISA

Contact Information:
jyard@schneiderdowns.com
One PPG Place, Suite 1700
Pittsburgh, PA 15222
Phone: 412-697-5345