Enterprise Risk Management for Nonprofits & Associations

WHERE STRATEGY MEETS RISK
Presenters

Melissa Musser, CPA, CITP, CISA  
*Risk & Advisory Services Principal*  
Gelman, Rosenberg & Freedman CPAs

Ricardo Trujillo, CPA, CITP, CISA  
*Nonprofit Audit Partner*  
Gelman, Rosenberg & Freedman CPAs

Derek Symer, CPCU  
*Principal*  
AHT Insurance
Highlights & Objectives

• What is Enterprise Risk Management (ERM)?
• 2019 State of Nonprofit Risk Oversight
• How to Identify Risks to Your Mission/Objectives/Strategic Plan
• Top Forecasted Risks for 2019
• How to Assess the Overall Risk and Develop a Practical Response
• Best Practice Takeaways
What is Enterprise Risk Management (ERM)?
## Traditional vs. ERM

<table>
<thead>
<tr>
<th>Traditional Risk Management</th>
<th>Enterprise Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insurable</td>
<td>Not necessarily covered by insurance</td>
</tr>
<tr>
<td>One-dimensional assessment (potential impact)</td>
<td>Multi-dimensional assessment</td>
</tr>
<tr>
<td>Manages risks one by one</td>
<td>Analyzes material risks and how they relate</td>
</tr>
<tr>
<td>Occurs within one business unit (siloed)</td>
<td>Spans the entire organization (holistic)</td>
</tr>
<tr>
<td>Reactive and sporadic</td>
<td>Proactive and continuous</td>
</tr>
<tr>
<td>Considers only downside (loss)</td>
<td>Considers both upside and downside</td>
</tr>
<tr>
<td>Focuses solely on loss prevention</td>
<td>Focuses on business goals, adding value, and more</td>
</tr>
<tr>
<td>Disjointed activities</td>
<td>Embedded in culture and mindset</td>
</tr>
</tbody>
</table>
ERM Frameworks

[Diagram showing ERM frameworks with COSO and ISO 31000 Risk-Management logos]
2019 State of Nonprofit Risk Oversight
Data was collected during the fall of 2017 through an online survey instrument electronically sent to members of the AICPA’s Business and Industry group who serve in Chief Financial Officer or equivalent senior executive positions.

- 130 large organizations (those with revenues greater than $1 billion)
- 138 publicly-traded companies
- 137 financial services entities
- 103 not-for-profit organizations

https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadedocuments/aicpa-erm-research-study-2018.pdf
Why is ERM on the Rise?

### Percentage of Respondents Selecting “Mostly” or “Extensively”

<table>
<thead>
<tr>
<th>Factors “Mostly” or “Extensively” Leading to Increased Senior Executive Focus on Risk Management Activities</th>
<th>Full Sample</th>
<th>Largest Organizations (Revenues &gt;$1B)</th>
<th>Public Companies</th>
<th>Not-for-Profit Organizations 2017</th>
<th>Not-for-Profit Organizations 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular demands</td>
<td>34%</td>
<td>34%</td>
<td>43%</td>
<td>22%</td>
<td>24%</td>
</tr>
<tr>
<td>Unanticipated risk events affecting organization</td>
<td>36%</td>
<td>44%</td>
<td>44%</td>
<td>37%</td>
<td>37%</td>
</tr>
<tr>
<td>Emerging best practice expectations</td>
<td>36%</td>
<td>37%</td>
<td>39%</td>
<td>41%</td>
<td>53%</td>
</tr>
<tr>
<td>Emerging corporate governance requirements</td>
<td>31%</td>
<td>37%</td>
<td>44%</td>
<td>20%</td>
<td>24%</td>
</tr>
<tr>
<td>Board of Director requests</td>
<td>26%</td>
<td>40%</td>
<td>42%</td>
<td>25%</td>
<td>25%</td>
</tr>
</tbody>
</table>

https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa-erm-research-study-2018.pdf
## Current State of ERM

### Percentage of Respondents

<table>
<thead>
<tr>
<th>Description of the State of ERM Currently in Place</th>
<th>Full Sample</th>
<th>Not-for-Profit Organizations 2017</th>
<th>Not-for-Profit Organizations 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>No enterprise-wide management process in place</td>
<td>17%</td>
<td>17%</td>
<td>9%</td>
</tr>
<tr>
<td>Currently investigating concept of enterprise-wide risk management, but have made no decisions yet</td>
<td>9%</td>
<td>11%</td>
<td>13%</td>
</tr>
<tr>
<td>No formal enterprise-wide risk management process in place, but have plans to implement one</td>
<td>9%</td>
<td>9%</td>
<td>11%</td>
</tr>
<tr>
<td>Partial enterprise-wide risk management process in place (i.e., some, but not all, risk areas addressed)</td>
<td>37%</td>
<td>44%</td>
<td>40%</td>
</tr>
<tr>
<td>Complete formal enterprise-wide risk management process in place</td>
<td>28%</td>
<td>19%</td>
<td>27%</td>
</tr>
</tbody>
</table>

[https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa-erm-research-study-2018.pdf](https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa-erm-research-study-2018.pdf)
Who is Responsible for Risk Oversight?

For about half of the organizations, the board has delegated risk oversight to a committee, with most delegating to the audit committee, risk committees are on the rise from the prior year.

<table>
<thead>
<tr>
<th>If board delegates formal responsibility of risk oversight to a subcommittee, which committee is responsible?</th>
<th>Full Sample</th>
<th>Largest Organizations (Revenues &gt;$1B)</th>
<th>Public Companies</th>
<th>Financial Services</th>
<th>Not-for-Profit Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Committee</td>
<td>46%</td>
<td>56%</td>
<td>48%</td>
<td>31%</td>
<td>54%</td>
</tr>
<tr>
<td>Risk Committee</td>
<td>31%</td>
<td>24%</td>
<td>34%</td>
<td>51%</td>
<td>15%</td>
</tr>
<tr>
<td>Executive Committee</td>
<td>8%</td>
<td>4%</td>
<td>2%</td>
<td>6%</td>
<td>8%</td>
</tr>
</tbody>
</table>

https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa-erm-research-study-2018.pdf
Strengthening Risk Management Infrastructure

- Higher percentages of organizations are appointing individuals to lead the organization’s risk management process
- Even higher percentages of organizations are creating management-level risk committees
- Boards of Directors continue to delegate risk oversight to a board committee, which is most often the audit committee
Who Does the Chief Risk Representative Report to?

<table>
<thead>
<tr>
<th>To Whom Does the CRO Formally Report?</th>
<th>Full Sample</th>
<th>Largest Organizations (Revenues &gt;$1B)</th>
<th>Public Companies</th>
<th>Financial Services</th>
<th>Not-for-Profit Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board of Directors or Committee of the Board</td>
<td>23%</td>
<td>11%</td>
<td>24%</td>
<td>25%</td>
<td>19%</td>
</tr>
<tr>
<td>Chief Executive Office or President</td>
<td>42%</td>
<td>40%</td>
<td>39%</td>
<td>59%</td>
<td>32%</td>
</tr>
<tr>
<td>Chief Financial Officer</td>
<td>20%</td>
<td>29%</td>
<td>22%</td>
<td>12%</td>
<td>23%</td>
</tr>
</tbody>
</table>

https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa-erm-research-study-2018.pdf
Managing risks in today’s environment isn’t getting easier
Demands for greater management focus on risks are increasing
Risk management practices in most organizations remain relatively immature
Organizations are formalizing their risk management leadership structures
Most struggle to integrate risk management with strategy

Organizations have some elements of risk management processes
Boards receive written reports annually about top risks, but the underlying process may not be robust
Opportunities exist for improvement in the nature of risk information being reported to senior management
Few organizations are linking risk management responsibilities to incentive compensation

https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa-erm-research-study-2018.pdf
How to Identify Risks to Your Mission/Objectives/Strategic Plan
Determine Organization Context

- Industry
- Strategic Objectives
- Culture
- Structure
- Processes
- Systems
- People
Risk Identification Techniques

- Objectives Based
- Past Events
- Internal Analysis and Surveys
- Process Flow Analysis
- Scenario Based
- Current Events
- Facilitated Workshop and Interviews
Risk Universe – Categories

- Management and Operational Risk
- Financial and Fraud Risk
- External, Collaboration and Reputation Risk
- Legal and Compliance Risk
- Personnel and Volunteer Risk
- IT Risk
- Strategic and Governance Risk
- Third-Party Vendor Risk
- Environmental, Health and Human Safety
Top Forecasted Risks for 2020
Top Forecasted Risks for 2020

- Digital Transformation/Big Data
- Cyber Threats / Privacy and Information Security Management
- Culture/HR/Talent Management
- Fraud/Corruption
- Regulatory Changes/Scrutiny Over Compliance
How to Assess the Overall Risk and Develop a Practical Response
# Example Likelihood and Impact Matrix

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>25</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
</tbody>
</table>

*Impact*
Types of Risk Impact

- Strategic
- Reputation
- Financial
- Operational
- Compliance
- Technology
Determine Risk Response

Reduce/Mitigate Risk
Eliminate/Avoid Risk
Transfer Risk
Accept Risk
## Risk Register Tracking Technique

<table>
<thead>
<tr>
<th>Risk ID #</th>
<th>Title</th>
<th>Impact Description</th>
<th>Status</th>
<th>Strategic Objective</th>
<th>Risk Category</th>
<th>Impact 1=Lo, 5=Hi</th>
<th>Likelihood 1=Lo, 5=Hi</th>
<th>Risk Rank</th>
<th>Owner</th>
<th>Risk Response</th>
<th>Risk Response Summary</th>
<th>Date Closed</th>
<th>Closed Reason</th>
</tr>
</thead>
</table>
# What Your Peers Are Doing

<table>
<thead>
<tr>
<th>Percentage of Respondents</th>
<th>Full Sample</th>
<th>Largest Organizations (Revenues &gt;$1B)</th>
<th>Public Companies</th>
<th>Financial Services</th>
<th>Not-for-Profit Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage that maintain risk inventories at enterprise level</td>
<td>43%</td>
<td>58%</td>
<td>62%</td>
<td>58%</td>
<td>48%</td>
</tr>
<tr>
<td>Provides explicit guidelines to assess risk:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Probability</td>
<td>38%</td>
<td>61%</td>
<td>62%</td>
<td>46%</td>
<td>38%</td>
</tr>
<tr>
<td>• Impact</td>
<td>42%</td>
<td>63%</td>
<td>68%</td>
<td>51%</td>
<td>36%</td>
</tr>
</tbody>
</table>

[https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadedocuments/aicpa-erm-research-study-2018.pdf](https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadedocuments/aicpa-erm-research-study-2018.pdf)
## What Your Peers Are Doing – Continued

### Percentage of Respondents

<table>
<thead>
<tr>
<th>Frequency of Going Through Process to Update Key Risk Inventories</th>
<th>Full Sample</th>
<th>Largest Organizations (Revenues &gt;$1B)</th>
<th>Public Companies</th>
<th>Not-for-Profit Organizations 2017</th>
<th>Not-for-Profit Organizations 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all</td>
<td>25%</td>
<td>11%</td>
<td>7%</td>
<td>29%</td>
<td>29%</td>
</tr>
<tr>
<td>Annually</td>
<td>36%</td>
<td>51%</td>
<td>41%</td>
<td>42%</td>
<td>45%</td>
</tr>
<tr>
<td>Semi-Annually</td>
<td>12%</td>
<td>12%</td>
<td>13%</td>
<td>13%</td>
<td>11%</td>
</tr>
<tr>
<td>Quarterly</td>
<td>19%</td>
<td>19%</td>
<td>30%</td>
<td>12%</td>
<td>11%</td>
</tr>
<tr>
<td>Monthly, Weekly or Daily</td>
<td>8%</td>
<td>7%</td>
<td>9%</td>
<td>4%</td>
<td>4%</td>
</tr>
</tbody>
</table>

[https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa-erm-research-study-2018.pdf](https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa-erm-research-study-2018.pdf)
Monitor and Report

Management Handling Plans

<table>
<thead>
<tr>
<th>Risk #</th>
<th>Risk Statement</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Open</td>
</tr>
</tbody>
</table>

**Risk Classification**
- Internal Review
- Risk Register
- Category 1
- Category 2
- Category 3
- Category 4
- Mitigate

**Handling Plan**
- Description of Task
- Owner
- Target

Independent Assurance

![Diagram](image)
Best Practice Takeaways
Critical Success Factors

1. Obtain Board approval and involvement
2. Designate committees or individuals to champion
3. Involve business and technical experts
4. Create a risk aware culture
ERM Implementation and Maturity

Develop ERM committee charter

Develop ERM policy, procedures (ERM playbook), risk universe/register and classification

Develop Board reporting tools such as heat maps and risk reporting and mitigation dashboard

ERM training for stakeholders
Develop and document procedures for conducting risk assessments and develop templates and tools to facilitate and standardize the process.

- Who is responsible for initiating and conducting risk assessments?
- Who will participate?
- What steps will be followed?
- How disagreements will be handled and resolved?
- What approvals will be needed?
- How assessments will be documented?
- How documentation will be maintained?
- To whom reports will be provided?
Benefits of ERM

- Increasing the range of opportunities
- Identifying and managing risk entity-wide
- Increasing positive outcomes and advantage while reducing negative surprises
- Reducing performance variability
- Improving resource deployment
- Enhancing enterprise resilience
Questions?

Melissa Musser, CPA, CITP, CISA
Gelman, Rosenberg & Freedman CPAs
Risk & Advisory Services Principal
mmusser@grfcpa.com | 301-951-9090

Ricardo Trujillo, CPA, CITP, CISA
Gelman, Rosenberg & Freedman CPAs
Nonprofit Audit Partner
rtrujillo@grfcpa.com | 301-951-9090

Derek Symer, CPCU
AHT Insurance
Principal
dsymer@ahtins.com | 703-669-1121