NONPROFIT TRENDS

ENTERPRISE RISK MANAGEMENT- A VALUABLE PROCESS

BY MITCH LEWIS AND ROBERT CUMMINGS

May 2017

MAZARS

Boards and senior management of not-for-profit organizations recognize that identifying risks and managing those risks are a critical responsibility.

Enterprise risk management (ERM) is a process which the board and senior management are proactively involved. Risk is managed and assessed across the entire organization. Identifying, considering and developing responses to potential events, both internal and external that may negatively impact the organization is the basic definition of ERM.

ERM formalizes an approach that many organizations perform informally. A board or senior managers regularly meet and discuss various issues, some of which may relate to risk; for example damage to property and related insurance, a member of senior management decides to retire and a search for a replacement is discussed, a staff person leaves their lap top computer on a train and sensitive data is at risk. Just 3 examples of risk an organization may encounter.

Formalizing the process of documenting the key organizational risks and identifying the mitigation strategies is a valuable exercise. When the risk becomes a reality, having identified the mitigation strategy in advance will reduce the stress involved in rectifying the situation.

An effective ERM process can be led by senior management personnel and documented by internal associates. As an alternative, or in concert with management, utilizing an outside professional as a facilitator to lead the process can add efficiency and industry expertise.

Recent financial scandals and organizational errors cause damage to the reputation the specific not-for-profit and the sector overall.

Many not-for-profits believe reputational risk is a primary risk area. We believe reputational risk is the outcome of many potential risks and can result from economic risks, fraud, I/T risks or public scrutiny.

The impact of reputational damage can have long-term effects, causing multiple problems. For example, the Volkswagen diesel emission scandal is not only leading to current litigation and settlements, but the reduction in sales of other Volkswagen models currently being sold.

There are a broad range of not-for-profit organizations and as a result their risks can also vary. Some of the more common risks we have seen are as follows:

- Succession planning for senior management, department heads or board members
- Social media risks
- Cyber security risks
- Major donor risks
- Funding risks
- Program compliance risks
- Property risks

There are 6 key components to an ERM process:

1. Have a Risk Management Governance Structure
2. Follow a Risk Management Framework (e.g. COSO, ISO 31000)
3. Continuously Identify Risk and Risk Event Universe
4. Create and Manage a Risk Profile
5. Establish Risk Responses
6. Monitor and report

1. Develop a risk management governance structure which includes:

- Alignment with organization strategy and goals
- Clarity of risk management roles and responsibilities
- Risk policy statement
- A defined risk appetite
- Universal risk language
- Defined ethical standards
- Defined communication strategy
- Commitment to internal and external stakeholders

2. Follow a framework (e.g. COSO, ISO 31000)

The 2004 COSO ERM Framework introduced the following important enhancements to the Original COSO framework which are a key to having a value added ERM process:

- A focus on “Strategic” risks
- Extending the financial reporting objective to all “Reporting”
- Including the additional components of objective setting, event identification and risk response.

3. Continuously identify risk and risk event universe through creation of a risk register. Execute this through the use of

- Risk surveys
- Board level and Management interviews and/or brainstorming sessions
- Comparison of risks to risk tickler list of similar type organizations
- Collaboration with outside organizations where appropriate
- Risk event universe should not include ALL possible risks. The focus is on material and realistic risk events

Be cognizant that new risks are developing continuously especially in our adoption and use of evolving technologies.

4. Create a risk profile which includes:

- A defined risk tolerance
- Quantification and prioritization of risk events
- Identification of:
    - Risk Event Trigger
    - Risk Event Consequence
    - Key Risk Indicators

The risk profile should align with the organizational strategy and goals to prevent the acceptance of risks that do not further the organizational mission.

5. Establish risk responses which include:

- Accepting, sharing, or avoiding risks
- Implementing controls and procedures to mitigate risk impact
- Implementation plan for specific response activities
- Pre-risk event communication plan – what to do in case of emergency
- Communication plan to implement risk response
- Social media and public relations response plan to mitigate reputational harm.

6. Develop a monitoring and reporting process which includes:

- Key Risk Indicators (KRIs), Key Performance Indicators (KPIs) and related reports
- Use of Internal Audit as a monitoring and Board reporting component of the process

This process should be performed at intervals appropriate to the risk universe your organization is operating in.

ERM is a process affected by the Board and management to identify and address risks and risk events. While organizations may be aware of their key risks, a formal ERM process to regularly evaluate and monitor risks may not be in place. With Board oversight, not-for-profit entities are moving toward having formal ERM processes in place. Implementing ERM is a journey which includes multiple phases and steps. One size does not fit all.

FOR MORE INFORMATION CONTACT:

MITCH LEWIS, CPA
PARTNER
NOT-FOR-PROFIT GROUP
+1 212.375.6723
mitchell.lewis@mazarsusa.com

ROBERT CUMMINGS, CPA
PARTNER
CONSULTING GROUP
+1 732.205.2011
robert.cummings@mazarsusa.com

VISIT US AT www.mazarsusa.com

MAZARS