GENERAL COUNSEL / CHIEF FINANCIAL OFFICER ROUNDTABLE: Risk Management Tools to Prepare for the Unexpected[1]

Katherine Karl, General Counsel & Chief Legal Officer
The Humane Society of the United States
1255 23rd Street, N.W., Suite 450
Washington, D.C. 20037
Email: kkarl@humanesociety.org

Ellen Taus, Treasurer & Chief Financial Officer
The Rockefeller Foundation
420 5th Avenue
New York, New York 10018
Email: etaus@rockfound.org

Nicola Fuentes Toubia
Fuentes Toubia, PLLC
2450 Louisiana, Suite 400
Box 936
Houston, Texas 77006
Email: nicola@toubialaw.com
Office: (713) 589-2138
Cell: 202-288-8268

Ellen D. Willmott, Corporate Secretary
The Susan G. Komen Breast Cancer Foundation, Inc.
5310 Harvest Hill Road, Suite 120
Dallas, Texas 75230
Email: ewillmott@komen.org

I. Proactively Minimizing Risk.

Effective risk management of a nonprofit organization begins at the strategic level by evaluating organizational risk and examining the total operations of the organization. Organizational risk includes all types of risk, such as budgetary, reputational, cybersecurity, employee, legal, investment, funding, etc. It is everywhere, as evidenced by the corporate scandals that constantly make headlines. Corporate scandals – large and small – may also plague nonprofits. Today's disgruntled employee may be tomorrow's whistleblower or #MeToo follower.

---

[1] The information contained in this outline is presented for educational purposes only and is not intended to be and should not be relied upon as legal advice. This outline is an overview of the risk areas that most nonprofits face and is designed to alert nonprofit executives to areas of concern and how best to manage them.

Because nonprofit organizations are not exempt from traditional corporate risks, nonprofit leaders should ensure that their organization has an ongoing plan to assess and diminish risk. Executive communication and cohesive systems, processes, and methodologies can do a lot to mitigate organizational risk. For example, nonprofit executives can implement anonymous reporting channels, communicate policy and procedure updates on a formal and timely basis, and emphasize the importance of compliance so that employees are more likely to adhere to the policies and controls that a nonprofit implements.

Hurricane Harvey's devastation of southeast Texas highlights the risk that nonprofits face from natural disasters – both to their organizations and the communities that they serve. While good risk management cannot prevent historic flooding, it can minimize the damage and the recovery time.

While this outline discusses risk management components that are common to all nonprofits, it is important to recognize that effective risk management must be tailored to each organization. There is not a one-sized-fits-all/off the shelf approach that will work for your organization. Further, risk management is a journey, not a moment in time. The best way to manage risk is to build methodically on what your organization currently has in place and add or subtract risk management tools as you continue your journey.

a. **High risk areas.**

i. **Lack of financial oversight**. Failing to provide adequate financial oversight can result in significant losses to an organization's finances and reputation. Moreover, with the recent changes to Federal tax laws and fear that an increased standard deduction may reduce charitable giving, nonprofits would be wise to closely monitor their finances to quickly identify any shortfalls.

ii. **Founder or employee misdeeds and/or negligence**. Employee misdeeds can also have a detrimental effect on a nonprofit. In the three years since this risk management presentation was last given, Ms. Toubia has been represented several nonprofits that are battling problems created by "founder-itis". In addition, many non-profits are thinly staffed, particularly in the area of financial oversight, in order to provide maximum resources for programmatic activity. This can mean an open door to certain employees inviting malfeasance or fraud. It has been our experience that a door left open long enough means that someday someone will walk through it.

iii. **Cybersecurity**. Today's risk management programs must assess cybersecurity risk because nonprofits cannot operate well without managing donor and client data. The AICPA recently released System and Organization Controls ("SOC") for Cybersecurity. Nonprofits can use these SOCs to evaluate their cybersecurity program because cybersecurity has moved beyond just the realm of the information technology department. It is more than just a firewall – cybersecurity involves communicating with stakeholders about who should have access to certain data and what is data is utterly essential to the organization's operations. Management must understand and monitor cybersecurity. If the nonprofit does not have sufficient expertise in-house, cybersecurity risk management may involve contracting with external security managers to protect the organization's data.

A nonprofit should consider the type of data it is collecting, the sensitivity of that data, how the data is stored, who has access to the data, and how to mitigate against data breaches. On-line fundraising and e-commerce activities most likely will subject the nonprofit to cybersecurity regulations. For example, the Texas Business and Commerce Code requires a nonprofit to notify a donor if there has been a breach of the nonprofit's security of computerized data.[2]

iv. **Reputational Risk**. Unlike traditional risk assessment approaches which tend to be inward focused, assessing reputational risk requires a nonprofit to step outside its four walls and ask how it appears to others. What is the message that its brand conveys and have there been any external attacks on that brand? It is not enough for the nonprofit to ask its own board and management about its performance and brand. The nonprofit must seek input from other stakeholders like donors, clients, regulatory bodies, and community leaders. It should be savvy as to how it collects these stakeholders' opinions. Moreover, it should be very proactive about managing reputational risk because the time to ask outsiders to rate your nonprofit is not in the midst of, or just after, a crisis. A good reputational risk assessment will provide leadership with the means to anticipate threats, analyze trends that may affect reputation, and implement new strategies to maintain a positive brand.

v. **Lack of operational oversight**. Nonprofits with large employee populations and/or higher-risk missions, such as those that provide services to individuals or operate internationally may face higher operational risk. Further, most nonprofits' programs are funded with taxpayer dollars or charitable contributions. Managing operational risk helps a nonprofit ensure that it is conducting its programs in the way its government funders or donors intended.

b. **Assessing and Articulating Organizational Risk Tolerance.** It is essential to establish the organization's attitude toward different risks that are present or could present themselves in the course of business. The organization may want to establish a risk committee (see section in Establishing Internal Controls) that would from time to time scan the landscape for significant risks, and determine the level of tolerance that the organization is willing to assume, which may be

[2] TEX. BUS. & COMM. CODE §521.002, §521.052; §521.053 (Vernon's 2017).

Title search: GC/CFO Roundtable: Risk Management Tools to Prepare for the Unexpected

Also available as part of the eCourse
2018 Nonprofit Organizations eConference

First appeared as part of the conference materials for the
35th Annual Nonprofit Organizations Institute session
"GC/CFO Roundtable: Risk Management Tools to Prepare for the Unexpected"