Why Prioritized Risk Management is Critical for Nonprofits

Guest Authors *Donna Galer, Al Decker*

When a 60-year-old nonprofit in New York City placing volunteers in schools closed its doors a few years ago, it recognized a sizeable fundraising risk it faced: its major donor, the City, was giving less and giving inconsistently. The nonprofit did take steps to address this, such as reducing expenses and asking schools for a "partnership fee." Unfortunately, that was not enough to avoid closure.

This outcome points to some open questions that all nonprofits can benefit from asking: 1) Did the organization see the risk early enough? 2) Did it act quickly enough? 3) Were the actions comprehensive enough? 4) Were there other risks feeding into this risk that were not identified or addressed?

Anticipating the Risks

Whenever I ask executive directors of nonprofits what keeps them up at night, the most common answer is "a shortfall in donor funding." This answer comes even from board members of well-funded organizations, such as large universities and hospitals.

Although lack of adequate or consistent funding is a risk nonprofits face, it's not generally thought of in the same way as other risks. Yet swings in donations are as unpredictable as a lightning strike, car accident, or cyber hacking—they're not under the **direct** control of the nonprofit.

This article is about the various strategic and operational risks that nonprofits face that are neither transferable to an insurer nor easily avoided. It's about how any sized nonprofit should evaluate the organization to identify existential risks and apply specific mitigation actions to address those risks.

Enterprise Risk Management is the way to do this. ERM is not new, but many nonprofits are new to it. Without this systematic, holistic, and detailed approach to addressing risks, organizations typically fall into a pattern of knowing there are uncertainties and issues to address but never taking any concerted action (or enough action) to protect themselves.

ERM has several steps:
1) Identify risks
2) Prioritize risks
3) Mitigate risk
4) Monitor risks and mitigation plans
5) Report on risks and mitigation plan status to the board of directors (board) and other stakeholders

The prioritization of risks allows the organization to focus only on the top risks that are not already handled in some way. So, the risk of losing the value of an owned building due to a fire may be significant, but if the organization already has adequate property insurance coverage, this risk is not going to make the top 10 or 20 risk list.

However, if the inability to attract and retain volunteers is a major risk for the organization, then maintaining an adequate number of volunteers may be on the list. An organization governs in a way that truly promotes sustainability when the organization understands its strategic and operational risks (current and emerging) and makes detailed plans to address top risks.

Some common strategic risk areas for nonprofits:

- Insufficient funding
- Unclear mission
- Lack of visibility in community served
- Competition from similar organizations for funding, volunteers, clients

Some common operational risks for nonprofits:

- Lack of acceptable fiscal management
- Late/forgotten filings, e.g. 990, other required permits, licenses, etc.
- Insufficient cyber security protocol
- Errors due to lack of training volunteers/staff

To find out what risks are the most serious to an organization, it is not enough for the board, alone, to make a list. There should be input from some wider group of participants to the identification process. The mass of input is not as important as the diversity of the input. For example, some number of staff members, volunteers, donors as well as board members should be polled via personal interviews, group workshops, or questionnaires.

Those risks that have the potential to cause the most negative impact are prioritized on an impact scale, typically 1-5 with 5 being the most impact. The top 10-20 risks warrant assignment of a risk owner and a mitigation plan. The mitigation plan likely needs multiple actions since the risks are serious and often complex.

ERM does not guarantee success at averting or minimizing risk thereby shielding an organization from loss, but it offers a much greater chance of doing so.

In summary, ERM enables an organization to do the following:

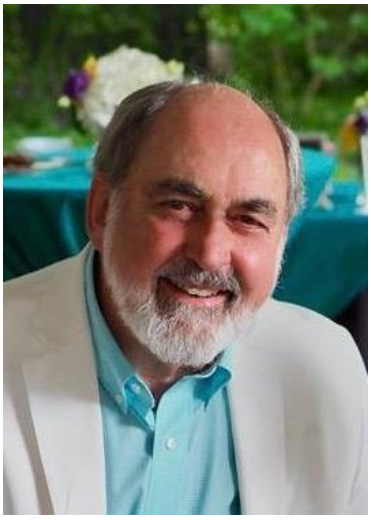
- Identify and address risks earlier than the organization would otherwise identify and address them
- Assign risk owners with clear and individual accountability versus organization-wide accountability: unspecified or generally assigned accountability often leads to finger-pointing about who is really responsible for a mitigation action

- Create comprehensive mitigation action plans rather than a one-shot attempt to deal with a major risk
- Show stakeholders, including donors, that the organization manages risk seriously

All of these benefits combined make ERM a worthwhile expenditure of time and effort for any nonprofit.

Authors

Donna Galer is a consultant, author, and lecturer. Currently, she is Senior Advisor at Hanover Stone Solutions where she provides companies with strategy and risk management consulting. From 2006 to 2010, she served as the Chairwoman of the Spencer Educational Foundation. Ms. Galer held many senior executive positions with Zurich Insurance, including Executive Vice President and Chief Administrative Officer for Zurich's worldwide General Insurance business, both in the U.S. and in Switzerland. She is the co-author of *Enterprise Risk Management – Straight Talk for Nonprofits* and an active contributor to Insurance Thought Leadership. She has given presentations at Risk and Insurance Management Society, The Institutes CPCU Society, and university events; served on numerous industry and academic boards; and published articles on strategy, ERM, human resource issues, and cyber risk. In 2000, she was named among the Top 100 Insurance Women by *Business Insurance*. Among the boards on which Ms. Galer recently served was NC State's Poole School of Business' Enterprise Risk Management's Advisory Board. In addition to having attended executive education classes at Northwestern's Kellogg School and IMD in Lausanne, Switzerland, Ms. Galer holds an MA from Rutgers University and a BA from Wagner College.



Al Decker is a nationally recognized authority on enterprise risk management (ERM), information security and privacy, and internal controls. Al is the co-author of several books on ERM including *Enterprise Risk Management – Straight talk for Nonprofits* and is currently a consultant with the Executive Service Corp of the Triangle in North Carolina. He has more than 30 years of professional experience in private industry and public accounting. A former worldwide executive for security and privacy services at IBM, he has also been Executive Director of Enterprise Risk Management at Electronic Data Systems (EDS) and the National Partner-in-Charge of IT Security Services and National Director of IT Assurance Services at Coopers & Lybrand, LLP (now PWC). Al holds an MBA from Rutgers University and a BA from William Paterson University.