The Roadmap to Risk Management

Risk is a pervasive aspect of business, particularly for nonprofits. If you haven't done so already, consider incorporating risk management into your standard operating procedures. Although there isn't one hard-and-fast method of incorporating this into your organization, the systems are broadly divided into four important phases:

1 Identify the possibilities of risk to your organization.
2 Understand the likelihood of the risk occurring and the magnitude of the ramifications to your organization if the risk occurred.
3 Plan a response before the fact.
4 Put procedures in place to mitigate the risk.

Utilizing the **4 over-arching themes to risk management,** you can create a roadmap to risk management. Here's how to accomplish this:

2 Prior to the meeting, board and management should identify the most significant risks within the following 5 categories: physical assets, financial assets, funding sources, human resources/volunteers, organizational elements, and any other risk not included in these categories.

2. Identify the Risks

4. Prioritize the Risks

4 Prioritize your risks by first addressing those which represents the greatest risks and impact to your organization.

6 Each month, your committees or those responsible for carrying-out the plan, should submit a report updating the board on their progress and action items.

6. Evaluate your progress

[START HERE]

1 Each year, management and board members should plan a meeting to assess risk within your organization.

1. Plan a Meeting

3. Assess the Risks

3 During the meeting, your team can share their list and then use a ranking system of 1-5 to assess the likelihood of occurrence and the financial or reputational impact that it would have on the organization if it did occur. This process may be simplified by creating a survey with Google Docs or Survey Monkey.

5. Create a Plan

5 Create a detailed plan that lists the risk and the response. Your responses might be to create a committee responsible for monitoring grants, consult IT professionals to find vulnerabilities, consult with your auditor for advice on segregating duties, etc.