GLENMEDE

Mission Possible—Due Diligence for Foundations, Endowments and Nonprofits

In the 21st century, we conduct due diligence and reconnaissance on nearly every aspect of daily life. We swear by Yelp ratings, scour Amazon product reviews and research people and opportunities using Google. In a world with unprecedented access to information, and at a time when increased scrutiny is placed on all businesses and organizations, it is important that nonprofit trustees, board members and staff conduct ongoing due diligence on all areas of the organization, including reviews of insurance policies and providers, auditors, software systems, equipment and cybersecurity.

Due Diligence Matters

Trustees and board members are legally bound to a series of duties and responsibilities that may be classified as:

- Duty of Care: Emphasizes active participation in organizational planning and decision-making to achieve sound and informed judgments.[1]

- Duty of Loyalty: Places the interests of the nonprofit before personal or professional concerns and avoid potential conflicts of interest.[2]

- Duty of Obedience: Ensures that the organization complies with applicable federal, state and local laws and remains committed to its mission.[3]

Beyond these requirements, boards and trustees must also act as a fiduciary, maintain oversight of the assets and ensure the organization has the necessary resources. Ongoing due diligence is a means to help board members and trustees remain prudent in meeting their fiduciary responsibilities, and will also expose potential organizational risks as well as highlight opportunities for improvement.

Factors to Consider

Who: One of the first considerations in developing a due diligence plan is to determine which vendors or processes will be reviewed. Some may choose to evaluate service providers, while others may focus on marketing or fundraising protocols. Along the way, internal as well as external personnel, either staff, committee members, vendors, consultants or volunteers, should participate in the review process.

What: When reviewing third-party providers, organizations should assess business operations, as well as relevant embedded processes. In the case of fundraising, for example, an organization may choose to evaluate the merchant services provider. Beyond the history, capabilities and stability of the provider's operations, organizations should thoroughly review cyber-security and fraud prevention programs, problem resolution procedures and escalation policies. During an appraisal, organizations should also consider the following material factors: consistency of performance, fees, client service, willingness to collaborate and ability to innovate.

[1] http://grantspace.org/tools/knowledge-base/Nonprofit-Management/Boards/legal-duties-of-the-nonprofit-board
[2] Ibid
[3] Ibid

When: Policies should be established concerning timing and frequency of third-party provider reviews. While some organizations implement time-based reviews by calendar intervals — every two, three or five years are common choices — others may plan evaluations based on board or staff tenure and turnover, grantmaking programs, fundraising cycles or signature events.

Why: Trustees, board members and staff should establish criteria for scheduling impromptu reviews. Reviewing an external auditor, for example, may become necessary if there is overall dissatisfaction or if there has been a change in the provider's leadership, processes or service levels.

How: Discussion about how the due diligence process will be implemented and how reviews will be conducted should result in tangible procedures. Will the organization implement a formal RFP process? Will providers be invited to interview in person or will there be a combination of approaches? Who from the organization will participate in the review process and who will have the authority to make the final decision?

What's the Risk?

Beyond a failure to meet legal and fiduciary obligations, poor due diligence practices can render organizations vulnerable. If, as an example, an organization does not adequately monitor cybersecurity procedures, then donor and volunteer data, such as name, contact, credit card or bank information, may become compromised, along with organizational assets and monies. These events carry legal, reputational and financial risks that may jeopardize a charity's growth and stability, potentially causing past donors to end their support and making new donors wary of offering future contributions.

These areas of vulnerability are not exclusive to cybersecurity. All operational areas, from marketing to grantmaking and volunteer management, require regular, periodic review.

Partnering with Professionals

Professional associations can be a helpful resource in developing and implementing due diligence plans. Industry leaders with expertise in the areas under evaluation are another important resource. Partnering with experts provides an organization's leaders with valuable guidance regarding the type of information they should be gathering as well as the questions they should ask during due diligence reviews.

Although each organization's due diligence program will vary, it is important that foundations, endowments and nonprofits institute ongoing review processes. Professional associations and other industry leaders offer valuable help when developing the insights and practices to safeguard an organization's financial and reputational well-being, paving the way for future success. A carefully planned due diligence program will instill corrective measures to prevent