March 2012 (updated April 2013)

**Risky Business: Why All Not For Profits Should Periodically Assess Their Risk**

By Joshua J. Mintz[1]

Many for profit companies consider a comprehensive risk assessment to be a critical part of their overall risk management process. Regrettably, many not for profit organizations do not take the time to perform a risk assessment for a variety of reasons: they do not understand or appreciate the benefits of such an exercise; they believe they adequately understand their risk profile; or they may feel they lack the resources to adequately perform the job. Fortunately, this trend seems to be moving in the right direction, that is, more not-for-profits are understanding why a risk assessment is necessary.

This article provides a framework that all not for profit organizations can use as a starting point to implement a periodic risk assessment.[2] It describes the goals of a risk assessment, identifies the nature of the broad risks facing many organizations, suggests a proposed approach, and offers suggested steps to mitigate and control the risks. While the mechanics of a risk assessment may be undertaken by staff or consultants, the role of the Board in understanding, evaluating, and assessing risk cannot be understated. It is executive leadership and the Board that must set the appropriate tone, understand the dynamics of risk for any given organization and articulate a clear philosophy on an organization's approach to risk.

**Goals**

Not for profit organizations face different types of risks than for profit companies, but the goals of a risk assessment should be similar:

- To identify, analyze and prioritize legal/ethical misconduct and compliance risks specific to the operations and culture of the organization;
- To provide a basis for possible compliance, training and ethics programs;
- To refine or develop risk mitigation and monitoring strategies;
- To identify areas where deeper reviews internal reviews would be warranted; and
- To develop a benchmark for ongoing risk assessment and measurement of the effectiveness of mitigation steps that may be taken.

---

[1] Joshua Mintz is the Vice President and General Counsel of the John D. and Catherine T. MacArthur Foundation. The views expressed herein reflect his own views and not necessarily the views of the MacArthur Foundation.

[2] There are many resources and proposed approaches for risk assessment in the for profit corporate context. These are not so easily transferable to not for profits in many cases. An organization will have to adapt proposed approaches to its particular circumstances. The chart attached is one starting point but a number of foundations and other not for profits have adopted or created their own forms or methods of approaching the question of risk assessment.

**Who Should Undertake the Risk Assessment?**

A comprehensive risk assessment can be done by staff if competent to do so or by outside consultants, such as a law or accounting firm. Even if staff is capable of performing the risk assessment, there is value to having outsiders perform this task occasionally. This assures a fresh perspective is brought to risk evaluation and allows all parts of the organization to be evaluated without any potential for self interest of staff to color the assessment. These benefits must be weighed against the additional costs of an outside review. A useful compromise is to have an outside reviewer evaluate the work of staff at the end of the process or consult during the process. Some outside firms will undertake a risk assessment pro bono, others may discount fees.

**One Methodology for In-House Risk Assessment**

A risk assessment should identify a broad parameter of risks within specific categories, analyzing the probability of occurrence and the severity of impact, identify mitigating factors to various risks, and suggest a process for tracking or monitoring risk. All of these steps require the exercise of judgment based on the knowledge of the organization and in general is as much art as science

**Identify Risks**

Step one is to carefully consider the types of risks faced by the organization. Think broadly and do not constrain yourself to solely legal risks. Risks can be broadly conceptualized into two categories: risks an organization should usually seek to avoid (what I will refer to as "threat risks"); and the risk of failure, the type of risks an organization may choose to embrace. Threat risks can result in fines, penalties, liabilities or even loss of tax exemption and can be operational, legal, financial, or related to the investments of the organization.

Risks of failure include the risk that an underlying program objective or strategy may not succeed or that investment or financial performance necessary to sustain the organization cannot be achieved. For many not for profit organizations, particularly foundations, failing to embrace risk in their programs or grants may result in a cautious, unimaginative organization. Foundations, in particular, have the freedom to take risks that other types of organizations or government may be unable or unwilling to take. An organization may wish to adopt a risk philosophy that articulates how it views the risks it will embrace and how it approaches threat risks. An interesting take on this risk question and another definition of programmatic risk can be found in an article by Gabriel Kasper & Justin Marcoux of Monitor Group in the Stanford Social Innovation Review, Spring 2012 edition, The Re-Emerging Art of Funding Innovation, p. 28 and in particular on page 31.

This article focuses primarily on threat risks. It is important, however, for an organization conducting a risk assessment to recognize the different types of risks and their attendant consequences. Ultimately, in assessing any action or inaction that carries risk an organization must balance the benefits to be achieved against the downside. An organization may also consider adopting a risk management philosophy that would entail, among other things, defining the risk appetite of the organization,

determining how to implement a comprehensive risk management process, and building the process into the many facets of the organization. Incorporating an agreed upon framework regarding risk management into the DNA of an organization helps align the balance between risk and reward, reduces the potential for unwelcome surprises, permits better planning and response time, enhances the ability to take advantage of opportunities and more effectively allows the organization to make decisions how and where to use scarce resources.

**Talk to Other Staff**

A useful risk assessment will include discussions with staff at varying levels of and in different areas of the organization. Staff members interviewed should be asked to identify what they see as the principal areas of risk within their areas, how the risk is currently addressed or mitigated, and ideas for more effectively addressing or mitigating the risks.

Particular care and attention should of course be paid to those risks that have a higher likelihood of occurrence and a more significant impact. Those that are less likely to occur but still would have significant impact should also be carefully reviewed.

**Broad Risks**

Most not for profit organizations will share the same type of broad risks that can be generally described as follows:

- Internal or External Fraud
- Misuse of Assets
- Inadequate Monitoring or Understanding of Investments
- Incomplete, unreliable or improperly reported information
- Damage to Reputation caused by a variety of potential factors
- Violation or Failure to Comply With Legal requirements
- Government investigations or Audits

Within these broad categories there are a host of specific risks that should be considered and analyzed. A listing of many of these risks is attached in appendix 1, not all of which of course will apply to every organization

## Rating the Risk: Assessing Likelihood and the Severity of Impact

In assessing the **likelihood** of a particular risk occurring, the following factors might be considered:

- your organization's culture and ethics;
- Ongoing compliance;
- Policies;
- Internal controls;
- Workforce awareness and knowledge;

- History; and
- Employee intent.

There are different methodologies and charts that can be used to present the risk assessment and which one you choose is dependent on your organization's needs, culture, and sophistication. Appendix 1 is an example of one chart.

The following scale may be useful in categorizing the probability of occurrence[3]: Rare; unlikely, possible, likely and almost certain as defined below.

| **Likelihood** | **Description** |
|---|---|
| Almost Certain | Highly likely, this event is expected to occur. |
| Likely | Strong possibility that an event will occur and there is sufficient historical incidence to support it. |
| Possible | Event may occur at some point – typically, there is history to support it. |
| Unlikely | Not expected but there is a slight possibility it may occur. |
| Rare | Highly unlikely, but it may occur in unique circumstances. |

A judgment on the **severity** of impact can be made using the following scale: Minor, moderate or severe, or some combination thereof. In assessing the severity of a particular risk, the following factors might be considered:

- Possible fines and civil or criminal penalties;
- Impact on the manner and ability of the organization to continue to operate;
- Impact on the reputation of the organization;
- Impact on employees and possible loss of employees; and
- Costs of compliance.

**Steps to Address or Mitigate Risk**

For each of the risks there are steps any organization, regardless of its size or sophistication, can take to address or mitigate the risks. These include the following with a brief explanation of each.

Segregation of duties

It is important that duties regarding oversight of assets, reporting, and payments be segregated so there are sufficient checks and balances to protect against one party or department from orchestrating a fraud or misusing assets. So, for example, a department that orders purchases, whether computer equipment or other goods, should not control all aspects of the procurement. There should be an independent department or person checking the purchase and making the payment in accordance with

[3] See Framework For Conducting Effective Compliance and Ethics Risk Assessments (Association of Corporate Counsel / Corpedia 2008). This is a useful reference and methodology for approaching a risk assessment.

policies and controls instituted by the organization. For many smaller organizations this can be a challenge as they might feel they lack the people power to differentiate functions. Nevertheless, establishing segregation of duties to some degree, even if that means using outside resources is critical to the prevention of fraud

Due diligence and legal review

With respect to most transactions, contracts or investments, an organization must perform adequate due diligence and ensure there has been legal review of contracts or other agreements. Whether the organization is a grant making organization, provider of services or has varying levels of investments, each organization should have agreed upon protocols in place for what they believe is adequate due diligence and legal review. Due diligence checklists for investments, grants and vendors may be obtained from the author.

Payment controls

Payment controls are the first cousin to segregation of duties. The greatest mischief or fraud often arises from a lack of adequate payment controls where one party or document has the ability to shield payments from other departments or parties. This can include requiring two signatures on checks to an appropriate reconciliation process. Accounting firms can be helpful in suggesting the appropriate controls for the nature of the specific organization. What might be appropriate for a large private foundation with a robust finance department may not be practical for a small not for profit organization. Yet in each case there should be thoughtful consideration of an appropriate control over payments, keeping track of inventory, reimbursements for travel and expenses, and similar matters

Audits (external and internal)

In addition to an annual audit of financial statements, even the best set of controls or processes should be subject to periodic review and audit. The use of an independent outside firm to perform periodic audits on specific processes or controls is advised, but even an internal review is better than doing nothing.

Implement and follow strong internal policies

An ad hoc approach to risk management is almost always doomed to failure to one degree or another. A well governed institution should have at least the following policies as well as a process in place to periodically review the implementation of compliance with the policies: conflict of interest, whistle blower, payment controls, code of ethics, zero tolerance for sexual or other harassment.

Board and executive oversight:  The tone at the top

No risk control environment can succeed in the long run if the leaders of the organization, senior staff and the board, do not reflect high ethical and professional behavior. The board of an organization must maintain vigilant oversight of the organization directly or through committees with specific roles and

responsibilities. Committee charters should be strongly considered to be clear about roles and responsibilities.

For most organizations compliance and risk management starts at the top, with the executive and the board. The tone set by top management and the board will permeate the organization. If the president or board do not show respect for the law, compliance and risk management through their actions and words, a culture of compliance and strong ethical practices will not grow.

Avoid complacency

Even well run organizations need to avoid complacency and the notion that bad things only happen to other organizations. Period risk assessments are one way for boards and upper management to walk the walk of risk management and to avoid complacency no matter the size of the organization. If your organization hasn't done on recently or at all, now is the time to implement one. Hopefully this article and related resources will give you the tools to start.

**Conclusion**

The notion of performing a comprehensive risk assessment may seem daunting to many organizations, but it is an integral part of the responsibility of the stewards of any charitable organization large or small. Each organization should undertake an assessment that fits its size, sophistication and needs. Hopefully, this article offers guidance to allow any organization to initiate, continue, or improve its own risk assessment process.

| RISK AREAS | LIKELIHOOD | SEVERITY | MITIGATION / AGGRAVATING | TRACKING / REPORTING |
|---|---|---|---|---|
| | | | | |
| **LEGAL** | | | | |
| lobbying by foundation (§4945) | | | | |
| self-dealing (§4941) | | | | |
| private benefit/inurement (§501(c)(3)) | | | | |
| political campaigning (§501(c)(3)) | | | | |
| foreign corrupt practices act (15 U.S.C. §§ 78dd-1, et seq.) | | | | |
| excess business holding (§4943) | | | | |
| grants to individuals outside approved proc (§4945) | | | | |
| minimum distribution requirement (§4942) | | | | |
| jeopardizing investment (§4944) | | | | |
| breach of fiduciary duty / conflict of interest (IL law) | | | | |
| Sarbanes (whistleblower/document retention) | | | | |
| Violation of Intellectual Property/Copyright | | | | |
| | | | | |
| **OPERATIONAL/FINANCIAL** | | | | |
| improper tax returns | | | | |
| flow of funds | | | | |
| violation of anti-terrorist financing regs | | | | |
| fraud/theft (internal) | | | | |
| physical disaster / act of terrorism / war | | | | |
| unauthorized payments | | | | |
| foreign office compliance (tax/human resources) | | | | |
| environmental claims | | | | |
| financial statement misstatements | | | | |
| personal use of cell phone | | | | |

| RISK AREAS | LIKELIHOOD | SEVERITY | MITIGATION / AGGRAVATING | TRACKING / REPORTING |
|---|---|---|---|---|
| document retention policy | | | | |
| credit card fraud | | | | |
| use of credit card by other person | | | | |
| employee v. contractor | | | | |
| pandemic | | | | |
| expense reimbursement (accountable plan) | | | | |
| reporting (federal/state)** | | | | |
| matching gift abuse/ fraud | | | | |
| altered checks | | | | |
| consultant agreements | | | | |
| | | | | |
| **INVESTMENT** | | | | |
| failure to achieve return objective | | | | |
| fraud by insiders (loss/reputation) | | | | |
| market risk | | | | |
| breach of pship agree (confidentiality; cap call) | | | | |
| loss on investment | | | | |
| fraud by outsiders | | | | |
| liquidity risk | | | | |
| loss of key personnel | | | | |
| loss of key data | | | | |
| tax structure/foreign funds | | | | |
| valuation risk (external / internal) | | | | |
| excess trades beyond authority | | | | |
| violation of ethics policy | | | | |
| bad press b/c investment (contrary to mission / bad actors) | | | | |
| calculating/rept investment performance | | | | |
| counterparty risk | | | | |
| | | | | |

| RISK AREAS | LIKELIHOOD | SEVERITY | MITIGATION / AGGRAVATING | TRACKING / REPORTING |
|---|---|---|---|---|
| **HUMAN RESOURCES** | | | | |
| employment claims (fed/state)* | | | | |
| ERISA claims (retiree/health plans) | | | | |
| leadership succession | | | | |
| HIPPA/Privacy claims | | | | |
| FLSA | | | | |
| improper time recording | | | | |
| defamation / libel | | | | |
| unauthorized payroll changes | | | | |
| | | | | |
| **TECHNOLOGY** | | | | |
| infiltration of system (virus/worms) | | | | |
| system crash | | | | |
| access to restricted data | | | | |
| loss of privacy/information | | | | |
| data errors | | | | |
| system down / system hacked | | | | |
| unauthorized network access | | | | |
| sharing of logins/passwords | | | | |
| | | | | |
| **GRANT MATTERS** | | | | |
| conduct inconsistent with grant (Fdn or grantee) | | | | |
| inaccurate press release re grant structure | | | | |
| lobbying by grantees | | | | |
| earmarking/pass through | | | | |
| third party liability (human subject) | | | | |
| violations of foreign law | | | | |
| failure to exercise ER | | | | |
| lack of impact of grants/strategy | | | | |

| RISK AREAS | LIKELIHOOD | SEVERITY | MITIGATION / AGGRAVATING | TRACKING / REPORTING |
|---|---|---|---|---|
| individual grants (purpose not achieved) | | | | |
| controversial grantee positions | | | | |
| copyright infringement | | | | |
| grant v. admin expense | | | | |
| breach of grant agreement | | | | |
| misconduct by grantee | | | | |
| misuse of funds by grantee | | | | |
| regranting done ineffectively | | | | |
| tax reporting (1441) | | | | |
| grant approvals in excess of budget | | | | |
| | | | | |
| **REPUTATIONAL** | | | | |
| failure to abide by conflicts of interest policy | | | | |
| controversial positions by foundation | | | | |
| inaccurate press release | | | | |
| tax avoidance strategies | | | | |
| use of foundation assets by individuals | | | | |
| conflicts of interest within policy parameters | | | | |
| board compensation | | | | |
| board/President expense | | | | |
| board travel | | | | |
| director outside affiliations | | | | |
| senior compensation | | | | |
| level of investment expense | | | | |
| mission-related investments | | | | |
| lack of diversity | | | | |
| misuse of social media | | | | |
| corporate apartments | | | | |
| | | | | |

| RISK AREAS | LIKELIHOOD | SEVERITY | MITIGATION / AGGRAVATING | TRACKING / REPORTING |
|---|---|---|---|---|
| **REGULATORY** | | | | |
| limitation on activities | | | | |
| new taxes | | | | |
| new penalties | | | | |
| | | | | |
| **OWNED REAL ESTATE** | | | | |
| fire/catastrophe | | | | |
| union strikes | | | | |
| building permits / code violations | | | | |
| equipment failures (includes elevators) | | | | |
| contractor claims / mechanic's liens | | | | |
| employment claims | | | | |
| defaulting tenant | | | | |
| personal injury | | | | |
| tenant claims | | | | |
| bomb scares | | | | |