May 30, 2018

Risk Assessment: A Template for Nonprofit Boards

- Written by Nick Price

What is risk? According to the Business Dictionary, risk is defined as:

"A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action."

While it's not possible for boards to eliminate every potential risk, it's prudent for nonprofit boards to conduct a thorough risk assessment annually to mitigate risks for the protection of the organization and its donors.

All organizations face some degree of risk, which is usually necessary to realize growth. The degree of risk that organizations choose to accept is called the "risk appetite." A risk assessment is a formal process for identifying, evaluating and controlling risks.

Risk Assessment Template

The following is a seven-step process for conducting a risk assessment:

Step #1: Identify the Risks

Risks exist in various areas of nonprofits' operations. Reviewing your organization's strategy and main objections will start you off in the right direction toward identifying risks. Each organization has different objectives and different needs, and the types of risk will reflect them.

Start by listing categories that risk may fall into, such as the following:

- Governance
- External
- Regulatory
- Financial
- Operational

Develop questions for each of these categories. For example, you may have questions under the financial category about whether the organization has enough financial reserves, or if they can begin investing some of their funds. Under operational risks, you may want to know if there is enough staff to operate safely.

Step #2: Analyze the Risks

Two main questions lie at the base of analyzing risks:

1. What is the likelihood that the risk will happen?
2. What would the impact be on the organization if the risk occurred?

It takes a team that's familiar with the workings of the organization to brainstorm about all of the possible implications of each risk. It's important to take some time to complete this portion of the assessment and to think beyond the obvious impacts that risks can create.

Impact from risk may affect the organization or the people in it.

After analyzing the risks, score them first according to the likelihood of occurrence and then according to the degree of impact on the organization on a scale from 1 to 5, similar to the following:

Scores for Likelihood

Score 1 Rare—unlikely to happen, may happen only under special circumstances.

Score 2 Unlikely—don't expect it will happen, but there is some possibility of it occurring.

Score 3 Possible—likely to occur some of the time, but not frequently.

Score 4 Likely—likely to occur, happens more often than not.

Score 5 Certain—occurs in the majority of cases.

Scores for Impact on the Organization

Score 1 Insignificant impact—little or no impact on the organization's operations or reputation. Complaints are unlikely, and there is only a remote possibility of litigation.

Score 2 Minor impact—potential for slight impact on the organization's operations or reputation. Complaints and litigation may be possible.

Score 3 Moderate impact—could lead to moderate disruption of operations or moderate negative publicity. Complaints and litigation are probable.

Score 4 Significant impact—operations would be disrupted, and adverse publicity would be certain. Formal complaints and litigation would be almost certain.

Score 5 Major impact—interrupts operations for a lengthy period and generates major negative publicity. Major litigation would be likely and senior management and/or resignations would be anticipated. This category may also reduce confidence in the organization's beneficiaries.

Now you have the proper information to be able to calculate the initial risk score.

Multiply the likelihood score by the impact score.

For example, if you assigned a risk with a likelihood of 4 and an impact of 3, the initial risk score for that risk would be 12.

The next step is to assign an action level according to the following definitions:

Levels 1–8 Low risk. Accept the risk and manage it at this level.

Levels 9–16 Medium risk. Manage the risk with the goal of taking action to recategorize it to a low risk.

Levels 17-25 High risk. Alert the rest of the board to this risk and discuss options for mitigating it.

Step #3: Prioritize the Risks

Don't expect to manage every risk. This step, prioritizing risks, will show you what to focus on most heavily and to establish important priorities.

Board discussion on this step will focus on what steps they're willing to take to mitigate risk versus accepting the risk on its face.

Step #4: Determine the Appetite for Risk

It helps to take a hard look at the top-10 risks and determine the board's appetite for assuming risks. The willingness to accept risk may increase if the board can find a way to mitigate it, which is called "residual risk."

Step #5: Reduce and Control the Risks

Make a final determination as to whether risks are acceptable, too high or too low. The board may decide not to take action on risks that fall in the acceptable level. Board directors should be taking a more in-depth look at risks that fall into the high-risk category and making decisions about how to further reduce the risk or stopping the activities that lead to the risk.

Step #6: Give Assurance

Boards are responsible for oversight of the operations. This step requires board directors to ensure that the risk controls are performing as they expect them to. Board directors may ask internal or external auditors to provide assurance that internal controls are in place and working.

Step #7: Monitor and Review Risks

The risk assessment is a valuable tool. Boards need to be aware that circumstances around risk may change continually. Risks come and go. The impact of risks can change as other circumstances change. It's best for boards to implement some plan for monitoring and reviewing risks on a regular basis.

Some boards find it helpful to select one risk to add to their agenda at each meeting. This provides time to discuss and review each risk on an ongoing basis. Boards should look for assurance that nothing has changed, and that the proper controls remain in place.

Risky Business: Why All Nonprofits Should Periodically Assess Their Risk

By Joshua Mintz | May 8, 2012

Many for-profit companies consider a comprehensive risk assessment to be a critical part of their overall risk management process. Regrettably, some not-for-profit organizations do not take the time to perform a risk assessment for a variety of reasons: some do not understand or appreciate the benefits of such an exercise; some believe they adequately understand their risk profile; or some may feel they lack the resources to adequately perform the job.

This article provides a framework that all not-for-profit organizations can use as a starting point to implement a periodic risk assessment.[i] 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 of Risk Assessment

Nonprofit 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 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.

Who Should Undertake 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 the 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 to consult with staff during the process. Some outside firms will undertake a risk assessment pro bono, while 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. It should also 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 knowledge of the organization. In general, this process is as much art as science.

1. 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, which 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 the investment or financial performance necessary to sustain the organization cannot be achieved. For many nonprofit 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.

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 as to how and where to use scarce resources.

Most nonprofit 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 of 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 can be found here. Of course, not all of these risks will apply to every organization.

2. 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 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.

3. Rate the Risk to Assess Likelihood and 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. Here is an example of one such chart.

The following scale may be useful in categorizing the probability of a risk's occurrence[ii]:

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.

4. Take Steps to Address or Mitigate Risk

There are steps any organization, regardless of its size or sophistication, can take to address or mitigate risks. These steps are outlined below.

Segregate duties

It is important that duties regarding oversight of assets, reporting, and payments be segregated so that there are sufficient checks and balances to protect against one party or department orchestrating a fraud or misusing assets. 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 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.

Set 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 department has the ability to shield payments from other departments or parties. Payment controls can include requiring two signatures on checks as 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 nonprofit 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.

Conduct due diligence and legal review

With respect to most transactions, contracts or investments, an organization must perform adequate due diligence and ensure that there has been legal review of contracts or other agreements. Whether the organization is a grantmaking organization, a 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 are available from a variety of sources.

Conduct 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. A well governed institution should at least have the following policies in place (and should periodically review the implementation of compliance with these policies): conflicts of interest, whistleblowers, payment controls, a code of ethics, and zero tolerance for sexual or other harassment.

Set the right 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 does 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. No matter the size of the organization, period risk assessments are one way for boards and upper management to walk the walk of risk management and to avoid complacency. If your organization hasn't done one recently or at all, now is the time to implement one. Hopefully this article and related resources will give you the tools to start.

The Mark of Good Nonprofit Stewardship

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. 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.

Joshua Mintz is the vice president and general counsel of the John D. and Catherine T. MacArthur Foundation. The views expressed herein are his own and not necessarily the views of the MacArthur Foundation.

Jeff Wallop August 19, 2014

Risk Management Best Practices for Non-Profits

Posted in: Risk Management Consulting

Are you aware of the exposures that may threaten your non-profit organization? I had the opportunity to speak on a webinar organized by the non-profit team at McGladrey where we exposed commonly faced risks and shared best practices to help non-profit organizations avoid facing costly and disruptive issues. I've distilled down the main points into what I hope will be a helpful post for organizations looking to limit exposure to risk.

This post will cover four areas of concern for non-profit executives:

- Cyber liability;
- Employee handbook "Do's and Don'ts";
- D&O Insurance, and;
- Fraud.

How do you protect your non-profit from Cyber Liability?

If you're not already familiar with cyber liability, it is the risk posed by conducting business over the internet, over other networks or using electronic storage technology. So if your organization has a website, a shared network or saved data in the cloud then you are at risk. There are two types of breaches:

1) **First party**, which includes employee data, and occurs when your own information is breached or compromised, and

2) **Third party**, which includes former and current donors, clients, students and consumers, and occurs when their information that your organization has promised to keep safe, is compromised.

We find that third party breaches are more common than first party. And as a non-profit you are vulnerable due to financial constraints as well as the type and number of records you have stored.

So how should you protect yourself? Your property and crime policy only covers the loss of tangible property. You will need to:

- Segregate and restrict access to sensitive data.
- Establish user control password protection procedures.
- Review security access to network and server.
- Encrypt private data on database, laptops, mobile.
- Implement and maintain a firewall.
- Apply intrusion detection software systems.

Failure to protect could result in litigation, loss of business, and decreased client and donor satisfaction. Don't be lulled into a false sense of security when saving information in the cloud. Make sure you are asking your cloud service provider the right questions such as:

- Who owns the data once it resides in the cloud?
- Does your cloud provider guarantee the security and privacy of your data?
- Will you be alerted if there is a breach of your data within the cloud?
- Will you have the right to investigate the breach?
- Who will be responsible for notifying your customers of a breach incident?

What are the "Do's and Don'ts" of your employee handbook?

If your organization chooses to have an employee handbook, it must be both effective and adhered to by the organization. A poorly written handbook can cause just as many issues as not having one.

Essential handbook policies to include are:

- Introduction Provisions/Disclaimer
- EEO Statement
- Sexual Harassment Policy
- Non-Harassment Policy
- Problem Solving Procedure

When there has been a violation, it is vital that you define the problem and then follow those exact procedures as outlined in the handbook. Always have an attorney review your employee handbook before disseminating to employees.

Why do non-profits need D&O Insurance (Directors and Officers Insurance)?

Thirty-five percent of non-profits have D&O claims as compared to 29 percent for publicly traded companies and 26 percent for privately held companies. D&O Insurance does not replace responsible governance, however it will protect you from exposures that are driven by the specific nature of what your organization does day to day, personal liability, your duties as a director, volunteer protection and indemnification. D&O Insurance will not only protect directors and officers but employees, volunteers and committee members as well. It also includes Employment Practices Liability Coverage and provides third party liability extension.

What is Occupational Fraud and how can it impact your non-profit?

Occupational fraud is the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets. Eighty-nine percent of occupational fraud cases are the misappropriation of assets such as skimming cash or misusing inventory. Other types of occupational fraud include corruption such as bribes or conflicts of interest and fraudulent statements. The median duration of fraud is between 18 and 24 months and it is most often committed by accounting staff or upper management. Non-profits who have been victims of occupational fraud have seen a median loss of $109,000 per claim. Outside of the obvious financial consequences, fraud can also lead to bad PR, a loss of public trust, increased oversight and operating costs and damaged employee morale.

To help prevent occupational fraud:

- Develop and implement a code of conduct, ethics policy and fraud policy.
- Document policies and procedures for core functions.
- Offer employee assistance programs.
- Protect proprietary and confidential information.
- Create a fraud hotline.
- Rotate responsibilities and cross train.
- Trust but don't over delegate.
- Perform background checks.
- Protect vendor and proprietary information (i.e. donors).
- Audit committee involvement and external audit assurance.
- Secure assets and document custody transfer.
- Segregate duties: record the transaction, authorize the transaction, custody of the transaction and execute the transaction.

Fraud can be detected from independent or external audits, financial management or internal control or employee tips or complaints.

For more detailed information on each of these areas of concern, please click below to view the webinar in its entirety. Also, please feel free to contact me at jeffw@psafinancial.com with any questions relating to controlling risk exposures at your non-profit organization.

Effective Risk Prioritization Is Key to Effective Risk Mitigation

Author: Steven Minsky

A big mistake in risk management, especially when it comes to companies with newer programs, is underestimating the importance of standardized risk prioritization. Diving into identification and assessments without a sufficient framework inhibits prioritization. This can result in ineffective risk mitigation and duplicate work across departments, or even serious risks flying under the radar. The possibility of "missing" a serious risk is a disturbing one, but it's impossible to be completely certain about *everything* that touches your business.

Understanding Risk vs. Uncertainty

This is why thinking about *risk* versus *uncertainty* is important. They are closely related, but are not one and the same; "uncertainty" has a broader scope. It is the lack of knowledge about a particular event's outcome, and exists for every individual and every organization. Part of a risk manager's job is to evaluate those uncertainties and determine which ones are likely enough and could have a serious enough impact to warrant mitigation. When an uncertainty reaches a particular threshold of likelihood and impact, the company recognizes it as a risk that needs to be mitigated.

Enterprise risk management is the best way of quantifying and preparing for an uncertain future, or in other words, *Managing Tomorrow's Surprises Today*®. Rather than being too conservative with risk identification and assessments (a dangerous practice) to avoid wasting resources, it is best to instead improve the processes' efficiency and effectiveness.

A taxonomy framework, which you can read more about in another blog post, will standardize each department's approach to risk prioritization. Using the same criteria and scale enables information to be collected, aggregated and compared enterprise-wide in a manner that is accessible and understandable to previously uninvolved personnel. A standard scale and common root-cause library will also reveal high-level risks that *do* affect multiple business areas, making prioritization systematic.

How Standardized Assessments Support Risk Prioritization

When assessing identified risks, we recommend a scale that provides as much detail as possible. Consider the following risk matrix (adapted from a Wikipedia page):

		Impact				
		Insignificant	Minor	Moderate	Serious	Catastrophic
Likelihood	Certain					
	Likely					
	Possible					
	Unlikely					
	Rare					

Even with criteria assigned to each "tier," some ambiguity remains. A risk with a score of "Likely x Minor," for example, may warrant less mitigation effort than a risk with a score of "Unlikely x Serious." The reverse might also be true, but neither reality is reflected by the matrix.

For greater insight into your risk register, consider the next matrix, which is the most frequent scale used by LogicManager customers:

			Impact									
			Insiginificant		Minor		Moderate		Serious		Major	
			1	2	3	4	5	6	7	8	9	10
Likelihood	Major	10										
		9										
	Serious	8										
		7										
	Moderate	6										
		5										
	Minor	4										
		3										
	Insignificant	2										
		1										

Breaking each impact and likelihood "bucket" into two options makes it possible to think about risk in a more dynamic manner, and enables users to select the high or the low of each category. This makes risk prioritization easier and more specific, which in turn allows for more targeted resource allocation.

The key is implementing a level of granularity that makes sense for your business and that assists with prioritization.

Nonprofits & NGOs

A Call for Nonprofit Risk Management

Nonprofits have a duty to apply risk management principles—a look at when organizations should adopt a risk management program and how they can begin.

- share
- comment
- print
- order reprints

By Ted Bilich Jul. 13, 2016

High-profile nonprofit failures and scandals have increased scrutiny of the nonprofit sector in recent years. In late 2014, the largest social services agency in New York, the Federation Employment and Guidance Service, suddenly closed due to financial mismanagement. In January 2016, Goodwill Industries of Toronto declared bankruptcy, leading its CEO and board of directors to resign. And in March, the Wounded Warrior Project fired its CEO and COO after reports of wasteful spending.

According to a 2013 investigative report from the *The Washington Post*, between 2008 and 2012, more than 1,000 major US nonprofits disclosed in federal filings that they had suffered a "significant diversion" of assets from internal wrongdoing.

It's no secret that nonprofits are ill-equipped to address risk. In 2015, for example, the Utah Food Bank announced that a data breach exposing donor names, addresses, credit card information, and security codes may have impacted eight percent of its donors. Technology often requires significant capital, and nonprofits do not have the same access to capital resources as their for-profit peers.

As with the Sarbanes-Oxley Act of 2002, which ushered in regulations to enhance corporate responsibility and combat fraud, leading organizations committed to nonprofit advancement have begun to emphasize that nonprofit risk management—a defined, routine commitment to gather, evaluate, and respond to threats and opportunities—is a nonprofit duty. Some examples:

Select Standards on Nonprofit Risk Management

Independent Sector:
"A charitable organization's board should ensure that the organization has adequate plans to protect its assets – its property, documents and data, financial and human resources, programmatic content and material, and its integrity and reputation – against damage or loss. The board should review regularly the organization's need for general liability and directors' and officers' liability insurance, as well as take other actions necessary to mitigate risks."

Standards for Excellence Institute:
"Organizations should make every effort to manage risk and periodically assess the need for insurance coverage in light of the organization's activities and its financial capacity. A decision to forego general liability insurance coverage or Directors and Officers liability insurance coverage should be made only by the board of directors. The decision should be reflected in the minutes for the meeting at which the decision was made."

District of Columbia Bar and Public Counsel:
"Every nonprofit organization needs to create a risk management plan and review it annually. The organization should also review its plan after making a significant change to the types of activities it engages in, or when acquiring a piece of property, a new computer system, or other significant asset."

Human Services Council of New York:
"Providers must implement financial and programmatic reporting systems that enable them to identify and quantify the financial impact of changes in the operating environment. Private and governmental funders must underwrite the development of robust financial and performance monitoring systems necessary for long-term sustainability and program quality. Provider boards, in conjunction with staff, must be engaged in risk assessment and implement financial and programmatic reporting systems that enable them to better predict, quantify, understand, and respond appropriately to financial, operational, and administrative risks. Private and governmental funders should help build their capacity to do so by facilitating access by nonprofit staff and board members to professional development, technical assistance, and coaching."

The call for nonprofit risk management is clear. But although nonprofits are increasingly aware of the need to adopt risk management, there's still little guidance about when and how they should adopt such a program, or what it should look like in its early stages. Having trained and counseled large and small organizations for more than 25 years, I now work with nonprofits to use risk management principles to enhance sustainability. Based on this work, I urge the following basic approach.

When to Start

During the "idea" and "start-up" stages of a nonprofit's lifecycle, when the focus is on viability, risk management programs are not cost-effective. If founders focus on process—even a virtuous one like risk management—it diverts resources from critical early-stage efforts. It can also undermine the experimentation and "creative destruction" that fuels early-stage nonprofits. At the beginning, risk management will likely begin and end with insurance, which can shift some of the responsibility to a third party and provide some safety net for many potential exposures.

Toward the end of the start-up phase, however, nonprofits reach distinct milestones. They begin to undergo regular independent audits to attract and retain high-quality donors. They consider whether to engage in strategic planning. They face the challenges of expanding the board of directors' skill set (from "working" to "governance"), formalizing job responsibilities, and adopting policies and procedures throughout the organization. At this juncture, which marks a transition toward the "growth" phase of the nonprofit lifecycle, developing a risk management process becomes essential for at least five reasons:

1. **Priorities:** Organizations can't understand their true priorities until they understand the negative risks (threats) and positive risks (opportunities) they face throughout the organization.
2. **Planning:** Nonprofits can't effectively engage in strategic planning until they understand the risks they face.
3. **Performance:** Organizations need donors to trust that they're exercising effective stewardship over funding resources.
4. **Sustainability:** Although nonprofits may focus on services to current users, during the growth phase, they become increasingly aware of the need to provide service to recipients into the future.
5. **Insurance Insufficient:** Insurance, which merely shifts the impact of defined risks to others, fails to provide any early warning or practical response mechanisms for emerging threats and opportunities.

How to Start

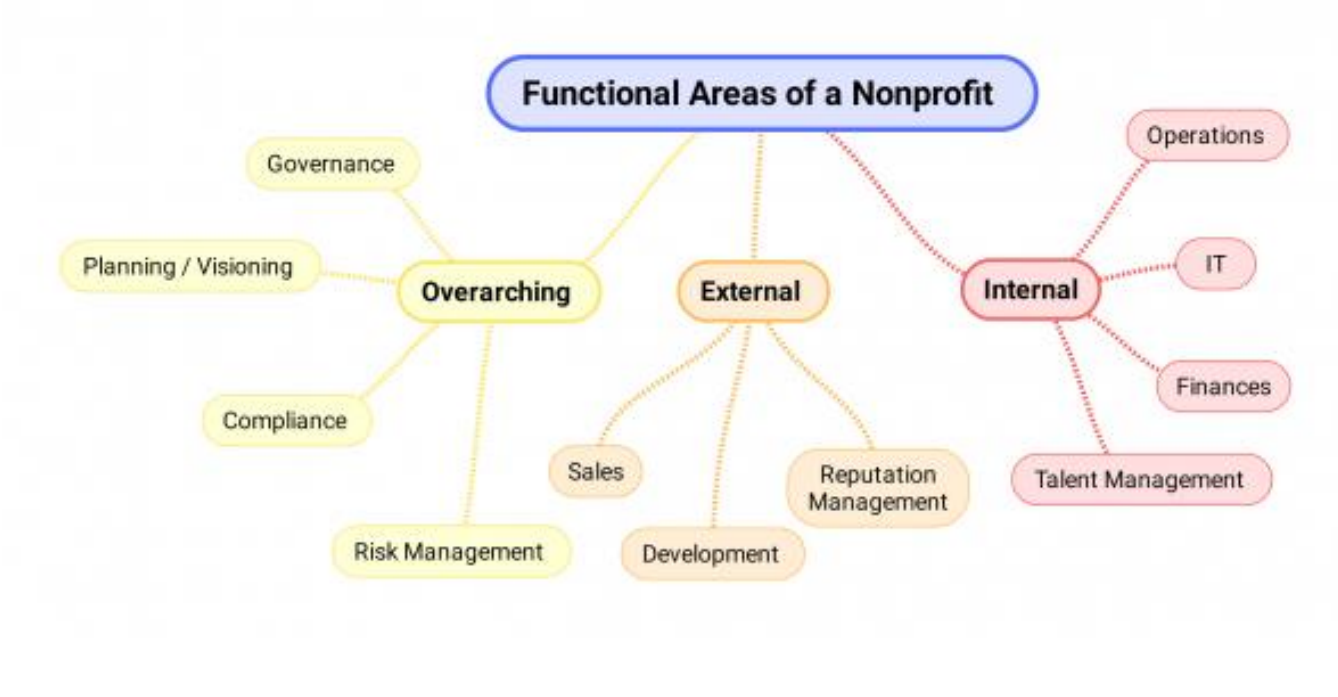
These steps can help nonprofits make risk management a standard operating procedure:

Understand context. Gather together current strategic and operational plans, and mission and value statements so that everyone involved in implementation can clearly assess where the organization stands, what it stands for, and what it wants to accomplish. These documents may change after exposure to the risk management process, but they can help frame priorities.

Develop a timeline and set goals. An effective risk management program isn't something organizations adopt overnight. Nonprofit should develop a phased, deliberate process with metrics to measure success. Year one may focus on training a core senior management group, year two on building out risk management capacity on the board, and year three on training for line personnel.

Perform a risk inventory. Nonprofits should survey threats and opportunities across all functions of the organization (see below).

Senior staff, one or more "line" personnel, and possibly one or more board members and/or stakeholders should take part in this initial risk inventory. Line personnel help senior staff avoid groupthink and tunnel vision, and provide additional insight into how the organization is performing its work on a daily basis.



Create and use a risk register. Nonprofits should engage in prioritization exercises to rank identified risks, then gather them in a "risk register"—a prioritized punch list of threats and opportunities that describes who within the organization "owns" any given risk, what responses are they are applying, and when the organization should follow up. That risk register should become a standard agenda item in staff meetings to focus staff on the most pressing, high-value issues facing the organization.

Implement a risk cycle. After identifying and prioritizing risks, the third step is to proactively respond to them. Responding includes researching and measuring emerging issues, mitigating

threats, developing opportunities using pilot programs (for example, beginning a new programmatic initiative or modifying a current program to see whether results improve), and declaring certain activities off-limits (through policies and procedures, and documented processes). The fourth step involves periodic evaluation of those responses to see what works, what needs improvement, and what else can be done. And then—critically—a risk cycle requires looping back through the process perpetually to institutionalize a culture of learning, improvement, agility, and responsiveness.

Seek funder support. The Human Services Council of New York has noted, "Private and governmental funders should help build [nonprofits'] capacity to [to perform risk management] by facilitating access by nonprofit staff and board members to professional development, technical assistance, and coaching." Funders are increasingly receptive to the important role of risk management in nonprofit sustainability. Ultimately, it's in funders' interests to ensure that grantees are spending money with an eye toward long-term resilience and stability.

Increase sophistication incrementally. After implementing basic risk management tools, nonprofit teams can consider ways to improve effectiveness. This could include:

- Developing staff positions dedicated to risk management, process improvement, and quality assurance within the organization
- Improving data gathering processes to better inform decisions
- Improving prioritization processes by training personnel to more effectively estimate the likelihood and effect of potential events
- Increasing the sophistication of modeling the potential financial impacts of different scenarios

Expense and Competing Priorities

Nonprofits may argue that risk management costs too much—but a single liability incident can easily cost tens of thousands of dollars, not to mention reputational damage and staff distraction. A nonprofit with a $1 million budget should be willing to allocate one or two percent of that budget to initial risk management efforts. Starting the process above doesn't require substantial budget outlays, and efforts can grow or change over time.

Others may argue that risk management isn't a priority, but unless organizations perform a risk inventory, they can't really assess their true priorities. Effective stewardship demands reality-based decision-making, and that requires risk management.

An effective risk management program can provide reasonable assurance that an organization remains agile and responsive in the face of uncertainties. It's unsurprising, therefore, that risk management is an emerging nonprofit best practice. Indeed, as in the for-profit sector, where publicly traded organizations are increasingly held to account for their risks, an effective risk management program will soon become a minimal criterion for nonprofit credibility in the marketplace.

Inherent Risk vs. Residual Risk Explained in 90 Seconds

Sep 7, 2017 3:18:43 PM / by Rachel Slabotsky

I recently had a conversation with clients around a risk analysis they conducted and noticed as they walked me through it that they seemed to get hung up on the terms “inherent risk” and “residual risk” and what inherent risk represented in that particular scenario.

They could not get comfortable with the current state of their control environment without having a firm grasp on the assessed inherent risk for that scenario. This stemmed from their experience in conducting risk assessments where the first step is to identify the inherent risk, then factor in controls to arrive at residual risk.

Here are the standard definitions of the two concepts:

- **Inherent risk represents the amount of risk that exists in the absence of controls.**
- **Residual risk is the amount of risk that remains after controls are accounted for.**

Sounds straightforward. But these two terms seem to fall apart when put into practice.

Applying the above definitions to the clients’ scenario uncovered the fact that the “inherent” risk being described was not a “no controls“ environment, but rather, one that only excluded some controls.

The flaw with inherent risk is that in most cases, when used in practice, it does not explicitly consider which controls are being included or excluded.

A truly inherent risk state, in our example, would assume no employee background checks or interviews are conducted and that no locks exist on any doors. This could lead to almost any risk scenario being evaluated as inherently high. Treating inherent risk therefore can be quite arbitrary.

According to Jack Jones, author of *Measuring and Managing Information Risk: A FAIR Approach* and creator of the FAIR model, much more realistic and useful definitions would be

- **Inherent risk is current risk level given the existing set of controls rather than the hypothetical notion of an absence of any controls.**

- **Residual risk would then be whatever risk level remain after additional controls are applied.**

How FAIR can help

Applying the FAIR model to risk analyses, such as the scenario described above, can help rid the ambiguity around the "no controls" notion of inherent risk by focusing on explicitly identifying and evaluating key controls in the current state environment.

Specifically, when measuring the current level of risk for a given scenario, controls are factored into either the frequency or magnitude side of the model based on their nature (avoidance, deterrent, response, etc.). Doing so allows you to be more intentional about the controls that you chose to include or exclude from your analysis, and ultimately identify which controls appear to have the greatest effect on the loss scenario.

Learn more in Jack's blog post Using the FAIR Model to Measure Inherent Risk.

- April 14, 2016

The Role of the Board in Risk Management

- Written by Jeremy Barlow

In decades past, boards could rely solely on management to oversee and manage risk. The 2008 financial crisis, also known as the global financial crisis, was considered to be the worst financial crisis since the Great Depression. Harsh economic times hit boards of directors squarely, as they came face to face with complex legal issues and failing businesses. The financial downfall, along with the subsequent fallout, was an abrupt wake-up call for boards of directors to delve deeper into their organization's risk management practices.

The pervasiveness of risk in the workings of everyday business means that boards must factor risk as an integral part of organizational strategy. Technology has increased the pace of business transactions globally, which has increased the volume and speed of product cycles. Today's businesses are wrought with complexities and litigiousness like never before—issues that hold the potential to destroy organizations overnight.

Increased Scrutiny Over Risk

In addition to management, boards are increasingly being held accountable for managing risk. Corporate governance rules and credit rating agencies are taking a stronger role in corporate risk by forming policies that address risk management policies. These emerging trends are forcing boards to assess past organizational exposures to risks. Economic trends also demand boards to be forward-thinking with regard to overseeing current financial risks and exposures to minimize the impact of financial crises.

Since the 2008 financial crisis, the New York Stock Exchange's corporate governance rules now require that risk assessment and risk management be included in audit committee discussions. Corporate credit ratings now include an assessment of commercial risk management processes,

as required by commercial credit rating agencies, such as Standard and Poor's. These changes mean that risk management items are becoming staples of board agendas.

Potential Loss Areas

Exposures to financial loss can include real and personal property, as well as property that is tangible and intangible, and personnel losses. Revenues can be lost by profit margins or expense increases. Poor risk management exposes organizations to civil and statutory offences, which can result in fines or other legal complications. The result of not managing risks can quickly deplete an organization's reserves. Examples of risks with financial impact include:

- Retained losses—insurance deductibles, retention amounts, or exclusions
- Net insurance proceeds
- Costs for loss control measures
- Claim management expenses
- Administrative costs to manage programs

Finding the Balance Between Taking and Managing Risks

Board members, executive directors, managers, and stakeholders know that there are strategic advantages to taking risks and that realizing growth requires some degree of risk. While managing complex business transactions, managers struggle to strike a balance between adding value while managing risks.

Development of Policies, Procedures, and Awareness

The board should not take a direct role in managing risks. The board's role should be limited to risk oversight of management and corporate issues that affect risk. Without becoming directly involved in managing risk, boards can fulfill their role in risk oversight by:

1. Developing policies and procedures around risk that are consistent with the organization's strategy and risk appetite.
2. Following up on management's implementation of risk management policies and procedures.
3. Following up to be assured that risk management policies and procedures function as they are intended.
4. Taking steps to foster risk awareness.
5. Encourage an organizational culture of risk adjusting awareness.

Areas of Risk Management Oversight

Boards should be looking at areas that either may be subject to risk or may be out of compliance with established best practices on risk management, from a domestic and global standpoint. Specific areas that boards should review include:

- Fiduciary duties
- Federal and state laws and regulations
- Stock exchange listing requirements
- Established and evolving best practices—domestic and worldwide

Risk management may fall under more than one committee, which may be the risk management committee or the audit committee. To effectively cover all areas of risk, committees should be coordinated so that communication between them regarding risk occurs horizontally and vertically. Committees report back to the board regarding the adequacy of risk management measures so that the board has confidence that management can support them.

Risk Management Oversight from a Broad Perspective

Board members need to have a good understanding of risk management, even when they lack expertise in that area. Boards may lean on the expertise of outside consultants to help them review company risk management systems and analyze business specific risks. Boards should perform a formal review of risk management systems, annually.

As part of the annual review, boards should review risk oversight policies and procedures at the board and committee levels and assess risk on an ongoing basis. It's helpful to familiarize the board with expectations within the industry or regulatory bodies that the organization operates in by arranging for a formal annual presentation on risk management best practices. The annual risk management review should include communication from management about lessons learned from past mistakes.

Risk management issues have been at an all-time high. Boards can continue to expect risk management to be an increasingly challenging part of board decision-making. There is a lot at stake with poor risk management practices. The impact will be felt from the top to the bottom and transcend across the board, management, and stakeholders. Taking a focused approach to risk management should be more than a compliance mechanism. Risk management needs to be an integral part of the organization's culture, strategy, and day-to-day business operations. Of all the risk management challenges that boards face, the greatest challenge is in navigating organizational growth while protecting the organization from unnecessary risk, so that it doesn't impact the business negatively. Today's commercial and economic climate demands that boards step up their game with an intense focus on risk management.

Sources:

Risk Assessment: A Template for Nonprofit Boards

Author: Nick Price

https://www.boardeffect.com/blog/risk-assessment-template-nonprofit-boards/?utm_source=marketo&utm_medium=email&utm_content=blog&utm_campaign=BEblogsubscribers&mkt_tok=eyJpIjoiTmpKbE1XVXlPV0ptT0dKbSIsInQiOiI1MlNIdXk1OWpha3NvSGF1bHlyQm5JOFdudnRSQnFEc0NZaXAyZ3JUZXA0SGFsUVVJQXkwK0ZaZnB2bkpzT1ROb3IzdFwva0t1aHd0MjJLejhmaFhVWk5iNU42VlpnUFJEMmppSXVcLzIyMU1FelwvOGxUUUZiZkpGakdNS2d3MlJqeSJ9

Risky Business: Why All Nonprofits Should Periodically Assess Their Risk

Author: Joshua Mintz

https://nonprofitquarterly.org/2012/05/08/risky-business-why-all-nonprofits-should-periodically-assess-their-risk/

Risk Management Best Practices for Non-Profits

Author: Jeff Wallop

https://www.psafinancial.com/2014/08/risk-management-best-practices-for-non-profits/

Effective Risk Prioritization Is Key to Effective Risk Mitigation

Author: Steven Minsky

https://www.logicmanager.com/erm-software/2016/03/15/risk-prioritization-is-key-to-risk-mitigation/

A Call for Nonprofit Risk Management

Author: Ted Bilich

https://ssir.org/articles/entry/a_call_for_nonprofit_risk_management

Inherent Risk vs. Residual Risk Explained in 90 Seconds

Author: Rachel Slabotsky

https://www.fairinstitute.org/blog/inherent-risk-vs.-residual-risk-explained-in-90-seconds

The Role of the Board in Risk Management

Author: Jeremy Barlow

https://www.boardeffect.com/blog/role-of-the-board-in-risk-management/