GETTING STARTED WITH ENTERPRISE RISK MANAGEMENT

A GUIDE FOR NONPROFITS

AMY WARES

Prepared by Amy Wares for the ERM Initiative at NC State University with support from Ericka Kranitz and Dr. Mark Beasley.

We are grateful for the financial support for this project provided by GRF CPAs & Advisors.

NC STATE Poole College of Management
Enterprise Risk Management Initiative

grf CPAs & ADVISORS

INTRODUCTION

The events of 2020 and 2021 have heightened awareness of the need for more and better risk management in the nonprofit sector. The COVID-19 pandemic magnified the imbalance between the demand for the services nonprofits provide and the philanthropic funds available to support nonprofits' ability to respond to that demand. Many nonprofit organizations were already operating with limited reserves. Given the level of uncertainty, nonprofits continue to face unprecedented challenges in achieving their missions and funding their work. Many organizations became overwhelmed as the pandemic strained health care systems and the related economic effects increased demand for social services frequently provided by the nonprofit sector. Other organizations, such as museums and theaters, had to close entirely, while camps and afterschool programs had to reinvent their service delivery models. Simultaneously, fundraising events were canceled, individual donations declined, and earned income from events, retail, and services dried up.

The challenges in the sector have never been so widespread. Even before the pandemic, nonprofit organizations frequently faced highly disruptive risk events. A study of 400 nonprofit organizations and foundations found that 20 percent of the surveyed organizations experienced risk events that caused shortfalls in required funding.[1] Yet, despite operating in high-risk environments with few resources and limited flexibility for responding to risks, only 16 percent of nonprofits rate their organization's risk management oversight as robust or mature.[2]

Enterprise risk management (ERM) integrates strategic planning and risk management to improve nonprofits' responses to change, organizational resilience, and mission fulfillment. **The goal of ERM is to provide an organization's leadership with insights that help them proactively navigate risks that may emerge and impact the delivery of mission critical services and the implementation of new strategic initiatives.** In the end, ERM is designed to increase the odds of an organization's strategic success. The timing has never been better for nonprofits to rethink how they manage risk and strengthen their ability to respond to changes in an uncertain environment.

ERM principles apply to organizations in all sectors, but most guides and resources are oriented toward the private sector. Accordingly, nonprofits may not recognize the potential benefits of ERM and may find it challenging to implement ERM practices. This guide aims to meet the need for ERM resources specifically tailored to nonprofits of all sizes (refer to Appendix A for definitions of terminology used). **The objectives of this guide are to provide practical suggestions for nonprofit organizations just beginning or in the early stages of implementing enterprise risk management.** This guide synthesizes the experiences, challenges, and lessons learned by nonprofit organizations, grant-making organizations, and service providers (see Appendix B: Individuals Interviewed and Appendix C: References). This guide begins with an overview of the ERM cycle and the value nonprofits have realized as a result of implementing ERM. It describes each element of the ERM process, with examples from many types of nonprofit organizations. Finally, the guide summarizes recommendations that practitioners offered for how nonprofit organizations can most successfully get started implementing ERM.

TABLE OF CONTENTS

[1] Open Road Alliance (2016). See Appendix C for citation reference details.
[2] Beasley, et al (April 2021).

THE CASE FOR ENTERPRISE RISK MANAGEMENT FOR NONPROFITS

Enterprise risk management provides a framework for determining an organization's most critical risks and developing plans to manage and mitigate risk events having a significant impact on their financial and operational performance. Nonprofit organizations face threats across multiple dimensions including financial viability, ability to fulfill their mission, and in a worst-case scenario, to the people that they intend to serve.

Nonprofit leaders are accustomed to managing a wide variety of risks, which range from preventing misuse of funds to ensuring the safety of staff and volunteers and protecting their stakeholders. Traditionally, risk management relies on department- and program-level managers to identify and lead responses to risks affecting their area of work. This approach has significant drawbacks. **First**, while department managers may be in the best position to manage risks on a day-to-day basis, risks rarely fall neatly into the mandates of organizational departments. For example, a region's changing demographics may affect demand for services, fundraising opportunities, and personnel needs but may be missed when an organization's risk management structure is siloed and relies on the development director managing fundraising risks, the human resources director managing personnel risks, and program director managing operational risks – none of those may be focused on shifting demographics affecting the entire entity, even though these changes impact them all.

Second, a risk associated with one department may have consequences affecting multiple divisions of the organization. For example, insufficiently vetted partners may jeopardize program implementation, expose the organization to compliance and fiduciary violations, or damage the organization's reputation and trust with donors. In some cases, a risk mitigation strategy implemented by one department creates risks for others. For example, IT staff may tighten security protocols in an effort to protect against cyber attacks, frustrating the development team's ability to hold virtual fundraising events.

Enterprise risk management counters these drawbacks by taking a holistic, enterprise-wide strategic view of risks facing an organization. Building upon knowledge of mission critical deliverables and key elements of an organization's strategic plan, ERM helps management pinpoint issues before they emerge that might impact the success of those mission critical deliverables and strategies. ERM breaks down siloes and supports improved decision-making, increased effectiveness, and greater resilience. ERM requires senior management to lead risk management efforts that span across the entire organization. The result is that the organization can identify emerging risks in a timely manner and coordinate responses to cross-cutting risks and interdependencies.

WHAT IS RISK?

For the purposes of this guide, **risk is defined as uncertainty that materially affects the ability of an organization to achieve its objectives**. It is worth noting that risk, in this definition, does not always have a negative connotation. In fact, a key element of the ERM approach is that risk can be a source of opportunity as well as disruption.

TABLE OF CONTENTS

WHAT IS ENTERPRISE RISK MANAGEMENT?

Enterprise risk management is an integrated approach for managing risks to increase an organization's ability to achieve its objectives. There are multiple variations of the ERM framework,[3] but all generally emphasize that ERM is a continual process that includes the following common elements (Figure 1):[4]

FIGURE 1: ELEMENTS OF AN ERM PROCESS

Culture and Leadership: An organizational culture that supports ERM and the "tone at the top" set by senior leadership and the board of directors provides the foundation that underpins all elements of the ERM process.

Strategy and Objective Setting: The ERM process begins with developing a shared understanding of an organization's mission, vision, and strengths in order to identify the most critical risks to the organization's core value drivers.

Risk Identification: The next step is to identify all types of risks (strategic, operational, financial, external, etc.) that might impact the continued success of key value drivers in the short- and long-term.

Risk Assessment: Once a list of risks is compiled, the organization prioritizes the most critical risks based on their likelihood and potential magnitude of impact.

Risk Response: The objective of the risk response step is often focused on developing plans to lower the likelihood of risks occurring and reduce the impact of risk events should they occur. But sometimes the risk response might be a decision for the organization to take more risks in areas where the organization is currently too risk averse.

Communication and Monitoring: The ERM process recognizes the importance of monitoring risks through key risk indicators (KRIs) and ensuring that the right people receive information about key risks in a timely manner.

This guide discusses each component of the ERM process and provides examples of how various nonprofit organizations have implemented each element.

TABLE OF CONTENTS

BENEFITS OF ERM FOR NONPROFITS

The individuals interviewed for this study represent a diverse set of large and small organizations at various stages of ERM implementation. ERM has been a highly positive experience for all of them. Even organizations that are just beginning to implement ERM are seeing benefits, such as improved communications. Organizations with more advanced ERM programs emphasize the link between effective risk management and achieving the organization's objectives. Bryan Huffman, Chief Financial Officer at the YMCA of the Triangle (NC) explains, "This isn't just a deeper version of our bus safety or lifeguard training. This is about understanding the broad risks that impact the entire association and how we nimbly move through those and make them our strategic focus moving forward toward our mission."

BETTER DECISION-MAKING AND MANAGEMENT PRACTICES

One of ERM's key benefits is that it provides a lens for decision-making that improves management's ability to weigh trade-offs and allocate scarce resources. By taking an organization-wide perspective, leadership can better determine which initiatives are most critical for achieving its mission and require closer management. When management is considering multiple alternatives, ERM contributes valuable information to support prioritization decisions.

Thinking through scenarios in advance and developing plans for dealing with them is particularly important for organizations with limited resources. John MacIntosh, Managing Partner of SeaChange Capital Partners says, "Scenario planning can make all the difference when you don't have large reserves. It will save you time, and if something happens and you do not have large reserves, you do not have a lot of time."

[3] The two most commonly used frameworks are the US-based Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s *Enterprise Risk Management: Integrating with Strategy and Performance* and Switzerland-based International Organization for Standardization (ISO)'s *ISO 31000: Risk Management – Guidelines.*
[4] Beasley (2016).

"When organizations practice risk leadership and consistently and strategically engage with risk, they not only head off potential crises but also position their organizations to successfully fulfill their missions, grow strategically, respond to evolving community needs, and present their organizations as smart investments to savvy donors and funders."[5]

Practitioners also cited improvements in day-to-day operations. Abby Stoddard of Humanitarian Outcomes has seen that ERM can improve relationships between organizations: "organizations that take an expansive view of ERM will view their sub-grantees or contractors as partners with whom risks need to be managed rather than sources of risk." One organization just beginning to implement ERM found that increased attention to risks helped it establish more sound management practices, such as documenting critical operational procedures and cross-training staff so unexpected turnover would not disrupt essential functions. It also conducted a vendor reliance assessment to determine which operational systems depend on third parties. Management used this analysis to create contingency plans for situations when vendors are not able to fulfill their responsibilities.

REDUCED "FIRE-FIGHTING"

A goal of ERM is to think in advance about what could derail a strategy in order to plan for how to minimize the likelihood of the risk occurring and reduce the impact of it should it occur. The ERM manager at a humanitarian relief organization reported that before they started ERM, country program staff would frequently complain that they were tired of "fighting fires." The staff appreciate that ERM helps the organization proactively get ahead of problems. At another organization, staff were initially resistant to ERM, but once they realized it would help them with issues that they were worried about, they were more supportive. Even if an exact risk event is not anticipated, an organization will be more prepared if it has identified risks with similar consequences (see box "Building Resiliency after 2020" on the next page).

BETTER COMMUNICATIONS

Organizations can have internal communication problems if individuals hesitate to identify risks because they fear appearing accusatory or overly negative, doubt whether they will be listened to, or if they are concerned about negative repercussions. Several interviewees said that ERM made it easier to talk about risk by introducing a common vocabulary and normalizing it as a topic of discussion. Shared language encourages conversations across various functions of the organization about risks that may create opportunities as well as risks with negative consequences. One individual noted that the terminology an organization uses does not need to match ERM literature. Most important is using words that are universally understood within the organization and fit the organization's culture.

ALLEVIATED CONCERNS OF THE RISK AVERSE

Several interviewees shared that some individuals at their organizations are particularly risk averse. The process of thoroughly identifying risks and developing risk handling plans helps those staff feel more comfortable. Knowing that risks are considered and managed reduces their resistance to new ideas and makes it easier for the organization to pursue riskier opportunities.

TABLE OF CONTENTS

[5] Leonberger and Ballow (2017).

BUILDING RESILIENCY AFTER 2020

After 2020, there are few people who would challenge the need for risk management. The global pandemic, racial injustice protests, increased cyber attacks, political change, and record wildfires demonstrated that every organization is vulnerable to risk events. Interview respondents reported that their organizations experienced a variety of effects from these events, including dramatic declines in revenues, technology challenges, staff mental health concerns, and unexpected pivots in service delivery.

Despite the increased need for risk management, organizations in the early stages of ERM sometimes found that "building the bus while driving it" was too challenging and slowed down or completely halted plans to implement ERM. Other organizations found that ERM was more valued. Although very few organizations predicted the events of 2020, many had considered risks with similar effects. One interview respondent felt that the credibility of the ERM process was "validated" when the organization experienced 16 out of 34 priority risks and the financial impact was nearly exactly what was estimated. Although the organization reduced its workforce by 25 percent, it never considered laying off its ERM manager because the position is now seen as essential.

Bridges to Prosperity, an international nonprofit organization that builds trailbridges and advocates for investment in rural transport infrastructure, began ERM in 2019 to support an ambitious growth strategy. The COVID-19 pandemic delayed these plans, but their risk management infrastructure and processes better prepared them to deal with the effects of the pandemic. Risk response plans developed to address the risk of Ebola in Rwanda and Uganda enabled the management team to respond quickly to the COVID pandemic to mitigate revenue impact and ensure the safety of expatriate and local staff throughout the world.

NC State University Professor Mark Beasley advises that organizations reflect on their experiences responding to the events of 2020, regardless of the maturity of their ERM program, and document learnings in "playbooks." "These playbooks will guide future leaders and hopefully avoid the need to 'recreate the wheel' in developing appropriate responses to both the immediate threat posed by the next crisis but also build resilience in the organization to best withstand the tragic losses that have been experienced by so many."[6]

RISK AND RELATIONSHIPS WITH DONORS

No interviewees reported having meaningful discussions about risk with donors, whether government agencies or private foundations. Bilateral and multilateral aid organizations, such as the U.S. Agency for International Development and United Nations Development Programme, often require risk assessments in funding proposals, but interviewees from recipient organizations described these requirements as frequently just "check-the-box" activities. As these funders improve the robustness of their own ERM programs, expectations for their implementing partners may increase, but for the time-being, risk is often viewed as merely a "buzzword."

Research by Open Road Alliance, a philanthropic initiative that provides funding to nonprofits and social enterprises facing unexpected roadblocks, found in a survey of 200 funders that 76 percent do not ask applicants to assess the "circumstances that could lead to a need for additional funding."[7]

Open Road Alliance CEO Maya Winkelstein says that philanthropists regularly underestimate risk because "it is not a part of the philanthropic mindset to think that risk exists." The transactional nature of funding projects, unwillingness to fund reserves, and the unbalanced power dynamics that exist between funders and grantees are barriers to candid conversations. As a result, few funders or grantees put sufficient time or resources toward proactively reducing the likelihood of risk events or preparing for situations when something unexpectedly goes wrong.

Philanthropists talk a lot about taking risk, but they hardly do anything to define, assess, or manage it.[8]

Although the philanthropic sector often sees itself as taking risks that government and the private sector will not take, these are often little more than vague claims. Few philanthropic organizations seriously consider risk. Winkelstein compares the concept of risk now to where the concept of impact reporting was 15 years ago, "we all claimed it, but nobody measured it."

Open Road Alliance, Rockefeller Foundation, and others are working to educate the philanthropic sector on how to better engage grantees on managing risk.[9] Until it becomes more commonly

[6] Beasley (2020).
[7] Open Road Alliance (2016).
[8] Winkelstein and Whelpton (2017).
[9] See https://openroadalliance.org/resource/risk-management-toolkit/

addressed in the funding process, Winkelstein encourages nonprofit organizations to take the lead in "creating a culture of trust and transparency with funders." Organizations submitting proposals that include honest risk assessments, when accompanied by risk management plans, have a competitive advantage over other grant applicants who face similar risks but have not developed plans for addressing them.

ORGANIZATIONAL CULTURE: THE FOUNDATION FOR ENTERPRISE RISK MANAGEMENT

Regardless of whether an organization is working in social services, humanitarian relief, arts, youth leadership, or other fields, there are common characteristics of organizational culture that support the successful implementation of ERM: committed leadership, willingness to discuss risk transparently and openly, and awareness and capability of staff to engage in the risk management process.

LEADERSHIP AND TONE AT THE TOP

Senior leadership's regular and consistent communication about how ERM supports the organization in fulfilling its mission builds support among staff and counters the view that risk management is bureaucratic and burdensome. Clearly articulating the rationale for undertaking ERM will help staff understand the purpose behind ERM activities and prioritize the aspects of the process that are most critical for the organization. Emphasizing that risk is not always negative encourages staff to search for opportunities created by uncertainty. For example, changes in government or new policies can create opportunities to support new initiatives.

An ERM leader in a humanitarian aid organization recalled that when he joined his organization, staff viewed him as "the person who says no." He worked with the organization's leadership to promote the idea that ERM allows the organization to thoughtfully address challenges in difficult environments that otherwise would not be possible. As a result, he was able to change the perception of ERM from being a roadblock to a tool that allows the organization to take *more* risk.

A senior leader in a health services organization described a turning point for the organization. Previously, staff resisted expanding risk management because they thought it diverted money from programs. Through effectively communicating the purpose of ERM, staff began to understand that risk management was about improving, rather than increasing, oversight, and that it would help them care for their clients better. Management referred to the ERM initiative as "Quality and Risk Management" to help reinforce this link.

TRANSPARENCY AND OPENNESS

Practitioners note that a benefit of a formal ERM process is the depersonalization and depoliticization of talking about risk. Discussing risk becomes more acceptable and comfortable when it is a common and expected topic in meetings and reporting, particularly when an organization adapts terminology to fit the culture of the organization. Encouragement and positive reinforcement by senior management demonstrates that the organization values discussing risk as a contribution to anticipating problems and solving them.

Talking about risk is often difficult, but not talking about it increases the likelihood of bad outcomes and decreases the time the organization has to deal with the consequences. Interview respondents emphasized the importance of transparency and openness. When risk is ignored by senior management (one interviewee referred to it as "willful blindness"), responsibility for addressing risks shifts to front-line staff who frequently do not have the training, information, or resources they need to make the best decisions.

A global humanitarian aid organization staffs its risk management positions largely with residents of the countries where they operate. Not only do they understand the context better, but it is also easier for them to have the necessary difficult conversations.

TABLE OF CONTENTS

ENGAGED STAFF

When ERM is well integrated into everyday processes and activities, staff may not even be aware that they are participating in enterprise risk management. Keys to staff engagement are keeping ERM as simple as possible and incorporating elements of risk management into strategic planning, project proposals and reviews, budgeting, and other existing processes. Flexibility and willingness to adjust and revise approaches in order to respond to staff feedback reinforces the message that the objective of ERM is to improve everyone's ability to contribute to achieving the organization's mission. A goal is "getting staff to see risk management as a proactive management tool rather than something they have to do."

When there is a clear link between ERM and the organization's mission, practitioners report that staff feel that it is their duty to call attention to risks. A risk-aware culture also helps diffuse tension within the organization because there is an avenue for staff to comfortably raise concerns and frustrations.

STARTING WITH A STRATEGIC LENS

The ultimate goal of enterprise risk management is to help organizations continue to provide value and be successful in the future. Accordingly, it is important to clarify how the organization generates value before beginning risk identification. Clarifying value starts with reviewing *what* the organization aims to achieve, as articulated in its mission and vision. Then, the organization reviews *how* it currently provides value through its programs and activities (core value drivers), as well as initiatives planned for the future (strategic initiatives). Viewing risk through this strategic lens helps the organization identify its most important risks, which often cut across functional areas and which traditional risk management approaches may miss.

Gary Love, Senior Director, ERM at the International Rescue Committee, emphasizes the importance of framing ERM in terms of organizational objectives. "People can relate to [ERM] more when they understand that it supports their goals directly rather than being purely an administrative exercise. An objective-centric approach integrated into management processes helps the organization manage risks that matter, and it helps the individual doing the risk identification and assessment to think proactively about how risk is directly affecting what they are trying to do rather than just continually updating a list of perceived 'issues.'"

The organization's core value drivers and strategic initiatives provide the foundation for identifying the most critical current, emerging, and potential risks. Two key questions serve as the link from strategic objectives to related risks:

1. **What must go right for a core value driver or new strategy to succeed?**

   What are the key elements from start to finish? What processes must occur? What are the core systems, resources, and people needed to make the core value driver or new strategy work?

2. **What assumptions related to the core value driver or new strategy are being made by the organization?**

   What is the organization assuming about key resources, processes, and people?

The two questions help identify risks by asking, "What could interfere with what must go right?" and "What if the assumptions are flawed?" For example, a global health services nonprofit determined that it could more effectively and responsibly execute its mission by transitioning from a U.S.-headquartered organization to a network of field-based affiliates with greater autonomy. Reviewing what must go right for this initiative to succeed revealed multiple risks related to the organization's internal management structure and fundraising processes.

WHAT KEEPS YOU UP AT NIGHT?

The common question, "What keeps you up at night?," is helpful for identifying an organization's major risks, but has two main limitations as a starting point for risk identification. First, it focuses on risks that are already known, potentially overlooking critical, previously unconsidered risks, which may lead to underestimating risk exposure. Second, the question may result in answers that are more short-term focused and operational, without considering longer-term and strategic risks.

TABLE OF CONTENTS

In addition to reviewing what may go wrong, it is also useful to consider situations when a program or initiative is more successful than anticipated and that creates additional risk. For example, what would the organization do if it suddenly received an unexpectedly large donation, if demand for its services increased dramatically, or if it was approached by a large number of new volunteers? There may also be opportunities that arise from risks. For example, a region's changing demographics may signal future reduced demand for current programs but may create opportunities to leverage the organization's strengths to reach a new group.

Figure 2 summarizes the process of linking strategy to risk identification (a template is provided in Appendix D).

FIGURE 2: LINKING STRATEGY TO RISK IDENTIFICATION

MISSION: What is the organization's key purpose? Why does it exist?

CORE VALUE DRIVERS: What are the services, knowledge, skills, attributes, etc. that drive the organization's value?

STRATEGIC INITIATIVES: What programs and activities is the organization planning in order to increase the value it provides in the future?

What **must go right** for a core value driver or new strategy to succeed?

What **assumptions** related to the core value driver or new strategy are being made by the organization?

RISK TO: What internal or external events might prevent what must go right for the strategy to succeed? How might assumptions be flawed or based on unreliable or outdated data?

RISK OF: What impact might this strategy have on existing programs and other initiatives?

OPPORTUNITIES: How might a risk the organization is facing turn out to be an advantage?

TABLE OF CONTENTS

In practice, organizations often operate for many years without reviewing their strategies, says Melissa Musser of Washington DC-based GRF CPAs & Advisors, so this process serves as a "useful nudge." She adds that even when a strategic review does not result in identifying new risks, it helps organizations later in the process when they are prioritizing risks and particularly when they are determining how to spend limited resources to manage risks.

A 2016 InterAction and Humanitarian Outcomes study of nonprofits working on humanitarian relief programs described field staff frustration caused by risk management processes that were disconnected from strategic priorities. The study reports, "One senior manager interviewee based in a high-risk setting, for example, felt that the bulk of his focus and mental energy was on the security of his staff, whereas staff in headquarters were more preoccupied with preventing fraud and diversion." The study also reports that respondents lamented differences in the way security risks were mitigated for local staff versus expatriate staff, "including specifically off-hours transportation, communication, and site security." In managing sub-granting, organizations prioritized fiduciary risk and building their partners' capacity in financial management, which led to undermanagement of security risk. The study concludes, "many understood their national NGO partners to be exposed to high levels of security risk, often without sufficient support, training, and discussion."[10]

[10] Stoddard (2016).

Several interviewees noted the reinforcing relationship between strategy and risk; by linking the two, risk management supports better strategic decision-making. An ERM leader at an international nonprofit organization explained that risk is now a critical input into the organization's country expansion plans. Another ERM leader describes the contribution of ERM to long-term planning, "It's made us laser-focused on strategy and what is most important."

IDENTIFYING RISKS

Clarification of strategic priorities carries over to frame the gathering and analysis of other factors affecting risk, including organizational strengths and weaknesses and the external environment in which the organization operates.

UNDERSTANDING CONTEXT

Analyzing contextual factors reveals emerging and potential disruptions to strategy implementation as well as potential opportunities to pursue. Frameworks and tools are helpful for structuring thinking about the factors that affect an organization's ability to achieve its mission. (See Figure 3 for a summary of the tools discussed). Two of the more common frameworks are SWOT (Strengths, Weaknesses, Opportunities, Threats) Analysis and PESTLE (Political, Economic, Social, Technological, Legal, Environmental) Analysis. (See Appendix E and Appendix F for descriptions of the components of these tools). Many nonprofits prefer to organize brainstorming using their own taxonomy of factors including categories such as finance, operations, governance, and reputation. (See Appendix G for a list of commonly used categories).

Expert assessments, surveys, and benchmarking reports provide insights into factors that affect an organization's exposure to risk. Commonly used reports on global, political and economic trends include the World Economic Forum's *Global Risks Report* and Eurasia Group's *Top Risks*. The Protiviti-NC State University *Executive Perspectives on Top Risks* report includes assessments of strategic and operational risks in addition to macroeconomic risks for nonprofit organizations as well as private corporations. BDO's *Nonprofit Standards* is an annual survey of nonprofit performance that can be used to benchmark strategic planning, human resources, operations, impact, and governance. (See Appendix H for more information on these reports.)

A study of risk events experienced by nonprofits during project implementation sheds light on factors organizations might overlook. In 2018, Open Road Alliance analyzed the 102 grants and loans requests it received over a five-year period.[11] It found that nearly half the applications were due to threats inadvertently created by funders, such as changes in funding strategies and delayed disbursements. In many cases, misleading communication exacerbated the consequences of the funder action (or inaction). For example, many applicants indicated that they were informed of the shift in a funder's strategy and were reassured that they would not be affected, only to be denied funding at the last minute. In other cases, funders provided specific dates and timelines for disbursement, but delayed to the point of threatening the viability of a program, or even the organization itself. (See Appendix I for more details on the results of this study.)

TABLE OF CONTENTS

FIGURE 3: COMPARISON OF TOOLS FOR IMPROVING UNDERSTANDING OF CONTEXTUAL FACTORS AFFECTING RISK

TOOL	USE
SWOT Analysis	Identify internal and external factors affecting risk; particularly helpful for identifying potential positive outcomes in addition to negative risks.
PESTLE Analysis	Structure brainstorming of external environment influences to categorize situations and trends affecting risk.
Risk Categories	Classify common risks into groups to identify themes, concentrations of risks, and other commonalities.
World Economic Forum's Global Risk Report	Improve understanding of the likelihood and impact of critical short-term and long-term global threats using results from this annual survey of global business, government and academic leaders.

[11] Open Road Alliance (2018).

FIGURE 3: COMPARISON OF TOOLS FOR IMPROVING UNDERSTANDING OF CONTEXTUAL FACTORS AFFECTING RISK (*CONTINUED)*

TOOL	USE
Eurasia Group's Top Risks	Shape expectations of greatest threats to nations, global politics, industries, and institutions in the next year according to leading experts and analysts.
Protiviti-NC State's Executive Perspectives	Gain perspective of the expected impact of macroeconomic, strategic, and operational risks in the next year and within 10 years with results from this annual survey of business, nonprofit, and government executives.
BDO's Nonprofit Standards	Benchmark performance on strategic planning, human resources, operations, scope and impact, and governance matters.
Open Road Alliance's Roadblock Analysis	Increase awareness of common risk events experienced by nonprofit organizations and social enterprises.

Regardless of the thoroughness of the risk identification process, some risks will remain unknown. It is not necessary, however, to predict a pandemic, earthquake, or volcanic eruption. Rather, it is sufficient to consider any event that is improbable but would have extreme consequences. In these situations, the specific event is less important than identifying highly disruptive impact and ways to address it. Considering the potential effects of any very large, multifaceted unknown risk will prepare organizations to address them, even if details of the plans need to be adapted.

BUILDING CONSENSUS

Depending on the culture and structure of the organization, risk identification may be conducted by the leadership team, delegated to division leaders and teams, or led by the ERM manager. An ERM leader in a large global organization conducts preliminary research and analysis of unit strategic plans and global trends, preparing hypotheses to present to operational leaders as a starting point for discussion. This initial analysis is expanded and refined through review at multiple levels of the organization and across various functions to arrive at consensus on the top priority risks that leadership will present to the board of directors.

Consensus building efforts are most effective when they actively seek out diverse staff perspectives, have sufficient depth, and are unbiased. It is essential to have representation across the organization to get the "enterprise" perspective. Methods to gather input from staff include surveys, workshops, and interviews:

- **Surveys** are an efficient way to gain feedback from a large number of people quickly but are less effective for collecting new ideas or understanding reasons behind answers. Consequently, surveys are generally better for prioritization after the initial list of risks has been created.
- **Facilitated workshops** are useful for collecting the input of many individuals at the same time and encouraging discussion and brainstorming.
- **Interviews** conducted by neutral third parties and kept anonymous are helpful for encouraging greater openness and maintaining an unbiased data collection process. It may be necessary to take additional steps to ensure that contributors represent diverse viewpoints and various roles throughout the organization. One practitioner relayed that her organization decided to repeat its baseline risk identification process after realizing that the previous exercise overlooked key issues because it included no non-white perspectives.

TABLE OF CONTENTS

RISK REGISTERS

Many organizations find it helpful to compile all identified risks into a "risk register." Typically, these registers include information about the likelihood and potential impact of each risk as well as how it will be managed and the individual in the organization who has taken responsibility for it.[12] When risk registers work well, they provide an implementation and follow-up structure for the process, improve efficiency, facilitate analysis and reporting, and support decision-making.

[12] A downloadable Excel-based example of a risk register provided by Humanitarian Outcomes: https://www.humanitarianoutcomes.org/publications/risk-register-tool

However, not all organizations find risk registers worthwhile. There is a danger that they become too granular, overwhelming, or an end themselves rather than the means to improving risk management. A risk manager described joining an organization that maintained a register of nearly 400 risks that was updated once a year and rarely considered in between. "It was more a list of complaints than a list of risks." He replaced the register with dynamic, one-page "risk report cards" limited to just those risks directly related to organizational objectives. Managers have access to all the report cards, but generally limit their view to only those risks they can effectively monitor and manage, typically no more than 10. The report cards are regularly updated, and managers can review them to track the status of risks and actions taken to address them.

PRIORITIZING RISKS

The risk identification process generally results in more risks than an organization can – or needs to – manage. Effective risk management requires prioritizing risks and assigning them to the right level of management. Prioritization involves determining which risks are most likely to affect an organization's ability to fulfill its mission. Typically, only the top tier of risks is communicated to senior management and the board of directors and includes no more than 5 to 10 risks.

Assessing and prioritizing risks is the aspect of the ERM cycle that differs most across organizations and requires the most adaptation to the culture and needs of the organization. Some organizations value the consistency and clear outputs that result from applying numerical ratings based on standardized criteria. These quantitative assessments frequently inform risk management plans as well as risk prioritization. Other organizations prefer to avoid scoring completely and rely on qualitative assessments. Regardless of the approach used, assessing and prioritizing risks requires significant judgment.

ASSESSING RISK USING SCALED CRITERIA

The most commonly used approach for assessing risk is rating each risk based on the probability it will occur (likelihood) and the severity of the risk event's consequences if it occurs (impact). Impact may be based on one type of outcome, such as effect on program results, or may be a combination of several factors such as financial, operational, and reputational impact.

For some organizations, likelihood and impact alone do not provide sufficient information for determining the severity of risk. Other commonly used criteria include how quickly the organization would have to react to a risk (speed of onset) or how prepared they feel they are for dealing with the risk (vulnerability). Vulnerability to a risk may consider both an organization's ability to detect a risk occurring and its preparedness to address the consequences of the risk event.

Applying selected criteria in a consistent, comparable way requires defined scales. Some organizations choose low-medium-high for simplicity, but three-leveled scales often do not provide sufficiently differentiated results. Five-point scales are most common because it can be difficult to distinguish between levels when more than five are used. Clear descriptions of each level improve rating consistency. For example, likelihood may be described qualitatively (almost certain, more likely than not, fairly likely, unlikely, and extremely unlikely) or according to probable frequency (once in 3 months, one in a year, once in 5 years, once in 10 years, not in 10 years). Scales to assess impact are typically adapted to meet the needs of the organization. Examples of definitions for five risk categories (strategic, operational, financial, reputational, and compliance) commonly used by nonprofit organizations are presented in Appendix J.

Using scales to develop a preliminary prioritization is relatively straightforward when one criterion is used but is more complicated when there are multiple criteria. Generally, organizations apply a formula such as Likelihood + Impact, Likelihood x Impact, or Likelihood x Impact + Vulnerability.

When two criteria are used, such as likelihood and impact, a visual approach can help determine overall assessment. A common visualization tool is a heatmap (sometimes referred to as a risk matrix) that color-codes combinations of likelihood and impact to signify ratings such as minor risk (green), moderate risk (yellow), and significant risk (red). An example of a heatmap is shown in Figure 4 on the next page.[13]

TABLE OF CONTENTS

[13] GRF CPAs & Advisors.

Although using scales adds complexity to risk assessment, many organizations find it helps staff rate risks consistently and escalate only those risks that require senior management attention.

Clear definitions and templates simplify the assessment process. Relief International, for example, created an Excel tool for staff to input their assessment of risks using well-defined criteria. The tool automatically calculates the overall rating and plots the risk on a heat map. In addition to prioritizing risks, these overall scores also determine the risk monitoring approach and reporting requirements.[14]

A study of risk practices of international non-profit organizations documents the consequences of insufficient risk assessment. An organization working in Turkey to provide cross-border aid to Syria stored humanitarian goods in Syria rather than Turkey in order to comply with Turkish customs regulations. The stock was stolen, and the program had to be suspended. Had the organization evaluated relative negative impact, it would have realized that the negative impacts of risks associated with keeping the goods in Syria were far greater than those associated with keeping the goods in Turkey.[15]

FIGURE 4: EXAMPLE OF A COLOR-CODED LIKELIHOOD AND IMPACT HEATMAP

Impact	Likelihood				
	Rare - 1	Unlikely - 2	Possible – 3	Likely - 4	Certain - 5
Catastrophic - 5	Moderate - 5	Moderate - 10	High - 15	Critical - 20	Critical - 25
Major – 4	Low - 4	Moderate - 8	Moderate - 12	High - 16	Critical - 20
Moderate - 3	Low - 3	Moderate - 6	Moderate - 9	Moderate - 12	High - 15
Minor – 2	Very low - 2	Low - 4	Moderate - 6	Moderate - 8	Moderate - 10
Insignificant - 1	Very low - 1	Very low - 2	Low - 3	Low - 4	Moderate - 5

FORCED RANKING AND OTHER RISK ASSESSMENT APPROACHES

Using scales for likelihood, impact, and other variables provides valuable information for prioritizing risks. However, this approach may not suit some organizations, either because it provides more detail than the organization needs or is not practical to implement.

A forced ranking approach is an alternative method for prioritizing risks that does not require defining scales. Instead, all participants individually select their top ten risks in ranked order. Risks are weighted inversely to their rank (each rank of 1 is assigned 10 points, each rank of 2 is assigned 9 points, and so on). The total points assigned to each risk for all participants determines the final rank order of risks.

The forced ranking approach has some advantages over scale-based approaches. It is simpler and faster to implement because there are no scales involved and individuals do not need to assess each risk on multiple criteria. It also provides a more differentiated ranking when there is concern that too many risks will receive the middle "3" value, resulting in a large number of risks with the same overall score.

A global health services nonprofit found a variation of this approach helpful in the early stage of implementing its ERM program. An external consultant interviewed the executive team, department heads, and a representative sample of the rest of the staff to identify a list of 40 risks. All employees then responded to a survey ranking their top ten risks in order. The consultant aggregated results by respondent type (executive, board, or staff), which informed senior leadership's final selection of its top priority risks.

[14] Relief International (2020). The Excel-based template is available at https://www.ri.org/risk-management-in-fragile-settings-a-toolkit-for-field-practitioners/
[15] Humanitarian Outcomes (2019a).

Other organizations avoid ratings all together. One interviewee said that ratings "give a false sense of security" because risk events rarely occur in isolation. When multiple risks are triggered at once, their combined impact is often more significant than what it would be if one risk alone happened. Instead, the interviewee's organization describes what the actual impact on a specific objective would be. He says that this approach is more helpful when a risk is escalated because leaders have a more direct understanding of the consequences of risks and required responses, especially when they are dealing with multiple, related risks.

APPLYING JUDGMENT TO RISK PRIORITIZATION

Regardless of the approach used, risk assessment is a highly subjective process that requires significant judgment. Even when organizations use quantitative methods, they complement numeric results with qualitative assessments, often using interviews, workshops, surveys, or benchmarking as inputs to the prioritization process. For example, an interviewee described that his organization assesses each risk based on likelihood, impact, and residual risk (the risk that remains after mitigating actions are taken). Then, each senior manager selects the three to five risks most important to the organization as a whole (for a total of approximately 20 risks). The senior management team selects its top tier risks by asking "Is this important to our survival?" and "Does this directly impact strategy?" If the answer to both questions is yes, it is considered highest priority and managed more closely by senior leadership.

Another approach to applying judgment considers "program criticality" or the degree to which the program is urgent, saves lives, relieves suffering, or otherwise fulfills a core element of the organization's mission. Criticality of programs is often considered informally when staff are making decisions, especially since opportunities to help the most in need are frequently accompanied by the greatest risks. Assessing criticality relative to residual risk more intentionally can be useful for decision-making. An organization may be more willing to accept higher residual risk when criticality is also assessed as high or very high. Conversely, it may decide that a certain program activity is not worth the risk it would face.[16]

NC State University Professor Bonnie Hancock suggests that organizations review non-prioritized risks to determine whether they truly have low potential severity or if they are simply well managed by the organization. Low priority risks may still require regular monitoring to ensure that preventive measures are working effectively.

TABLE OF CONTENTS

RISK APPETITE

An organization's risk appetite is the amount and types of risk that it is willing to accept. Risk appetite is a cross-cutting element of risk management because it provides a guide for whether an organization should pursue a certain strategy or project, how it should manage risks, and how it should respond to risk events that occur. For many organizations, risk appetite statements provide useful guidance about the guardrails the organization aims to stay within.

Generally only organizations with relatively sophisticated ERM programs have formal risk appetite statements. Although conceptually important, the reality of articulating an organization's risk appetite is challenging for a number of reasons. First, an organization will likely have many risk appetites. Its willingness to accept legal risks will likely be very different from its willingness to accept program risks. Even across programs, an organization may have different risk appetites. For example, risk appetite for a children's swimming program will be different than a nutrition program for adults. Risk appetite may also vary with the program lifecycle, with willingness to accept risk higher in the early stages of a project than near the end. Risk appetite statements must be carefully crafted, avoiding becoming so caveated that they cease to be helpful. It can also be difficult for staff and board members to distinguish their personal risk appetite from the risk appetite for the organization. This conflation can make coming to consensus complex and possibly contentious.

Even if an organization decides against developing a formal risk appetite statement, discussing risk appetite is useful for developing a common understanding of tradeoffs. A practitioner described the surprise an organization experienced when it surveyed management, staff, and the board of directors. It discovered that management was making assumptions about the level of cash reserves that the board of directors wanted to maintain, but in reality, the board was willing to draw down reserves more if it meant making investments that increased program impact.

If the organization uses a taxonomy for risk identification (such as financial, operational, and reputational), these categories can serve as starting points for discussion. It may be easier – and more useful – to discuss the specific boundaries the organization can accept in each category than a more general and hypothetical risk appetite. For example, an organization may determine that no single donor should provide more than a certain amount of total funding, or that it will not begin operations in a country unless it has a certain number of language speakers.

[16] Haver (2016).

MANAGING RISKS

After identifying and prioritizing risks, the next step is developing risk management plans. A useful starting point is thinking through which of the four general **risk response** strategies is most appropriate for each risk:

- *accepting* the risk without mitigating action,
- *avoiding* the risk entirely,
- *sharing* the risk with others, or
- *reducing* the likelihood and/or impact of the risk.

Reviewing risks at an aggregated level offers a view of the organization's overall exposure to risk. Some organizations task "risk owners" with relevant subject matter expertise to develop initial management plans; others discuss risk response strategies collaboratively in a risk council or working group.

RESPONDING TO RISKS: FOUR STRATEGIES

Assessments used for prioritizing risks can inform an organization's response to those risks. Figure 5 relates assessments of likelihood and impact to the most frequently associated risk response strategy.

ACCEPTING RISKS

Some risks are unlikely to occur and would cause only minimal disruption. Even if there might be some negative impact, it may not make sense from a cost-benefit perspective to take preventative action. For example, inclement weather may affect an outdoor event that could be rescheduled. In these situations, an organization may simply decide to accept the risk without mitigation, though it may still track and monitor the risk.

FIGURE 5: FOUR GENERAL STRATEGIES FOR RISK RESPONSES

Common Approaches to Responding to Risks

	Low Likelihood	High Likelihood
High Impact	***Reduce/Share***	***Avoid***
Low Impact	***Accept***	***Reduce/Share***

AVOIDING RISKS

When risks have unacceptable consequences or the requirements to deal with them are impractical, it may make the most sense to avoid them. For example, an organization operating internationally may decide not to work in certain geographies that pose too many security risks, or where the costs required for effective oversight are too high.

SHARING RISKS

Some situations may involve risks that are unavoidable and greater than an organization can realistically manage itself. In these cases, although the organization still retains responsibility for the risk, there may be opportunities to share risk management with other parties. Insurance and outsourced information technology support services are examples of mechanisms for sharing risk.

For program-related risks, organizations working in high-risk environments may negotiate with their donors for a *force majeure* clause that releases them from contractual obligations when unforeseen risk events occur that make program completion temporarily or permanently unfeasible. These clauses generally require the recipient organization to have clear mitigation measures in place, but also allow the organization to allocate a pre-defined percentage of their budget to manage situations such as forced withdrawals and evacuations when extraordinary events occur.[17] Another approach involves negotiating with a donor to set aside a percentage of a grant in a contingency fund.

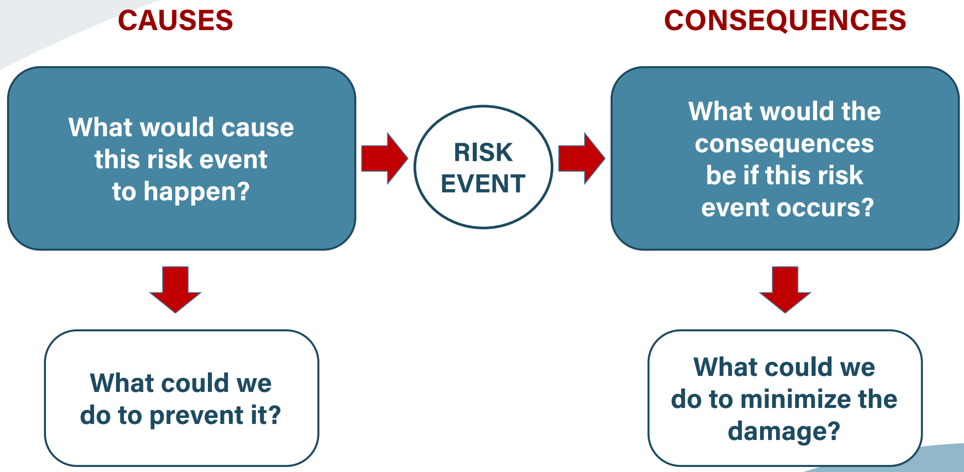
TABLE OF CONTENTS

[17] Humanitarian Outcomes (2019b).

REDUCING RISKS

Unfortunately, most risks are not acceptable, avoidable, or shareable. Consequently, organizations must develop plans to reduce the likelihood that the risk will occur, the impact if the risk does occur, or both. "Bow-tie Analysis" is a framework for identifying risk reducing actions that an organization can take (see Figure 6). It is called "Bow-tie Analysis" because it starts in the middle with the risk event, then determines the potential causes of the risk (left side of the bow-tie) and potential consequences (right side of the bow-tie). A template for Bow-tie Analysis and an example for the risk "Current environment may make it difficult to attract and retain talented workforce" are presented in Appendix K.

FIGURE 6: BOW-TIE ANALYSIS: ADDRESSING CAUSES AND CONSEQUENCES OF RISK EVENTS



Identifying ways to decrease the likelihood of a risk occurring begins with describing the events or circumstances that may cause the risk event. The next step is determining whether any actions can be taken to prevent these events or circumstances from occurring. For example, a dramatic policy shift that occurred in a Central American country would have substantially disrupted the program of a faith-based humanitarian aid organization. But since they had identified the risk in advance and improved their monitoring of legal and regulatory issues, they could adapt their programs before the change took effect. "This is something we would have not been aware of before and would have blindsided us, but since we were looking for it and made the necessary changes, it didn't affect us at all." If an organization is already taking preventive actions, it should evaluate the likely effectiveness of these measures and ways they could be strengthened.

Some events are not preventable, but negative impact can be minimized. By thinking through the potential consequences of risks events in advance, organizations can develop contingency plans. For example, as discussions of a shutdown began at the start of the COVID-19 pandemic, a global health services organization realized that it might have to close all its offices throughout the world. Before the closure became necessary, it held a work-from-home test for all employees simultaneously to discover where problems would arise. It learned that internet connectivity was worse than expected (even in the United States), so the organization purchased hotspots. Since many employees could not scan documents, the organization transitioned to using electronic signature technology. Staff also reported that they missed their large monitors and docking stations. When the official closure orders came in, the organization allowed staff to take home all their personal office equipment and provided boxes and packing materials for that purpose. As a result, even though the organization did not anticipate the length of the time the office would be closed, it could smoothly transition all staff to working from home.

For some risks, there might be both preventive and impact-reduction actions. For example, an organization may have concerns about a partner's capability to manage funds. It could aim to prevent misuse of funds through training the sub-grantee on financial management requirements and could provide clear guidance on expected procedures. It could also reduce the impact of losing funds by providing smaller, more-frequent disbursements of funds and conducting closer oversight. These measures would need to be weighed against the operational risks of putting a heavy compliance burden on the sub-grantee.[18]

TAKING A PORTFOLIO VIEW

A benefit of enterprise risk management over traditional risk management is that ERM's top-down view provides insights that are not as apparent when risk management is disjointed or siloed. When relevant risk information is aggregated, a portfolio view

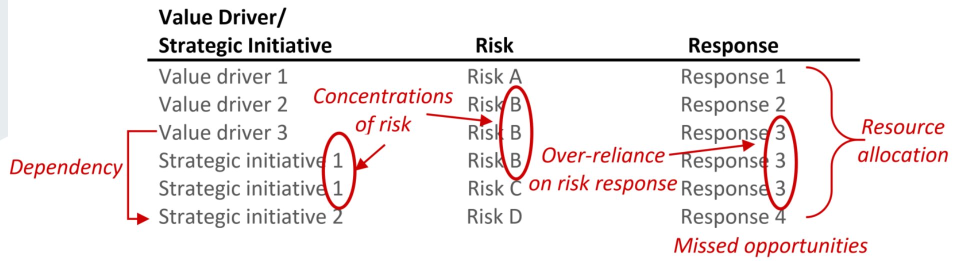
TABLE OF CONTENTS

[18] Stoddard (2016).

supports more effective risk management and resource allocation (see Figure 7).

The following questions are useful for guiding enterprise-wide risk analysis:

FIGURE 7: TAKING A PORTFOLIO VIEW



ARE THERE CONCENTRATIONS OF RISK?

There may be certain risks that affect multiple parts of the organization or a core value driver or strategic initiative that is significantly more exposed to risk. This is illustrated in Figure 7 by Risk B, a risk that is impacting two value drivers and one of the strategic initiatives. The experience of a social services organization provides an example. The organization discovered a problem with a documentation procedure in one of its units that had significant consequences for reimbursement from a government program and revised its procedures to address it. Several years later, the organization discovered a different unit was experiencing the same problem. The organization realized that had they taken an enterprise-level view of risk, they could have addressed both business units' risk at the same time, improving response efficiency and effectiveness.

IS THERE AN OVERRELIANCE ON ANY ONE RISK RESPONSE?

A recurrence of the same or similar response to multiple risks could itself be a risk. In the illustration in Figure 7, the organization is dependent on Response 3 to manage risks associated with a value driver and a strategic initiative. This overreliance can occur, for example, when employee training is a response for several different risks. If something happens that suspends or delays training, it could affect multiple core value drivers and strategic initiatives simultaneously. Similarly, if several responses require action from one staff member or one group of staff members, multiple response strategies may be jeopardized if they are unavailable.

ARE THERE DEPENDENCIES?

If one value driver or strategic initiative is dependent on another, or there are interdependencies among value drivers, the consequences of a risk event could cascade throughout the organization. In Figure 7, Strategic Initiative 2 is dependent on the success of Value Driver 3. For example, a viral negative social media post could damage the organization's reputation, affecting its ability to implement its programs in the community, and its fundraising.

ARE RESOURCES APPROPRIATELY ALLOCATED?

Viewing risks and responses from a portfolio perspective makes it easier to evaluate whether appropriate amounts of time and funds are spent managing risks. For example, it is common for financial and compliance-related risks to be well-managed (and sometimes over-managed) and frequently some of these resources could be reallocated to underfunded risks.

One way to assess resource allocation is to evaluate the extent to which the planned response reduces the risk, and how much risk remains after preventive or ameliorative actions are taken (referred to as "residual risk"). There may be opportunities to improve the effectiveness of risk responses by shifting excess resources from risks with low residual risk, where the resources are less needed, to ones with high residual risk, where additional resources could have greater impact.

ARE WE TAKING ADVANTAGE OF ALL OPPORTUNITIES?

When evaluating risks and responses, it is possible to identify opportunities that result from risk events. For example, one organization noted that previously they were limited in the number of communities they could serve through workshops due to capacity constraints and travel expenses. When all work became virtual and platforms such as Zoom and Google Meet became more widely used during the COVID-19 pandemic, they were able to substantially increase their outreach.

TABLE OF CONTENTS

MONITORING RISKS

When risk monitoring systems and processes are most effective, they maximize the amount of time available for responding to risks. Developing these systems and processes has two elements: determining who will have responsibility for monitoring risks and what information is used to monitor risks.

THE ROLE OF RISK OWNERS

When organizations begin implementing enterprise risk management, they usually designate an individual to be the ERM manager. Frequently ERM will be one aspect of a person's job, particularly in the beginning phases of the ERM process. The ERM manager plays a leadership and coordination role, managing the ERM process rather than the individual risks themselves. The manager educates leadership, the board, and staff about ERM, provides guidance and support when necessary, and champions integrating ERM into strategic planning and operations. The ERM manager may also take responsibility for one or several risks, but it is not practical or desirable for ERM managers to monitor and manage responses to all risks.

Assigning an owner to each risk improves accountability for risk monitoring and accelerates elevating risks to senior leadership when necessary. Typically, the risk owner has a deep understanding of the causes and consequences of their risk and can track signs that its threat level is changing. The risk owner also generally takes responsibility for ensuring that appropriate measures are in place to respond to the risk, even though they may not be responsible for implementing the responses. Organizations usually convene risk owners on a regular basis in a risk council or working group to provide status updates and discuss risk-related issues.

IDENTIFYING KEY RISK INDICATORS

Most risks are not like earthquakes that happen suddenly with minimal advanced warning. There are usually signs that a risk event is becoming more likely or beginning to develop. Identifying and monitoring key risk indicators (KRIs) to provide these early warning signals can buy critical time to implement a risk response strategy. There are two types of KRIs: "leading indicators" provide advanced warning that a risk is imminent or emerging to help an organization take early action to address the risk, and "lagging indicators" measure the effects of a risk that is occurring and are used to determine when certain response actions are necessary.

Selecting key risk indicators is frequently the most challenging element of the enterprise risk management process. In the *2021 State of Risk Oversight* report, only 18 percent of nonprofit organizations surveyed reported that they are very or mostly satisfied with their indicators of key risks. This challenge is not specific to nonprofits; less than half of public companies feel very or mostly satisfied with their key risk indicators.[19]

Since identifying KRIs can be difficult for staff, one risk manager explains that she often conducts preliminary analysis for the organization's top risks, which includes multiple scenarios and the drivers of each outcome. She uses that analysis as well as performance indicators associated with related objectives as a launching point for discussions on KRIs with managers.

A return to Bow-tie Analysis provides a structure for identifying key risk indicators (see Figure 8). At this stage, instead of looking at actions to prevent or reduce the impact of risk events, the focus turns to signs that a risk is imminent or developing. The analysis begins with thinking about the events that might happen immediately before a risk occurs and what the root causes of these events would be (left side of the bow-tie). The next step is identifying signs that the root causes and preceding events are occurring, and the early responses that should be taken. For example, economic policy changes in a country of operation may indicate a future change in exchange rates that could have budgetary consequences. This could trigger an action to prepurchase key supplies or identify sourcing alternatives.

The analysis continues on the other side of the risk event by considering the initial and secondary consequences of a risk event and related indicators. Since it is not always possible to have advanced warning of a risk, it is important to monitor signs that a risk is developing in order to maximize the time available to address it. For example, an organization working on controversial or politically sensitive issues may track local conventional and social media activity to identify warnings of increased threat. (See Appendix L for a template for key risk indicator identification using Bow-tie Analysis.)

TABLE OF CONTENTS

[19] Beasley, et al. (2021).

FIGURE 8: USING BOW-TIE ANALYSIS TO IDENTIFY KEY RISK INDICATORS

Key risk indicators may be quantitative or qualitative, depending on what measures are relevant and observable. Although key performance indicators (KPIs) are backward-looking and risk indicators attempt to signal future events, trends in KPIs, such as changes in program participation or average donation size, can be suitable KRIs.

Once selected, an organization assesses each indicator to determine the thresholds, in the form of values or observable signs, that should trigger informing senior management and taking action. It is critical to establish thresholds in advance because once a risk event is occurring, it can be difficult to gauge the point at which action is required. One organization tracks "mega-issues" at the organization level, defining a mega-issue as one that has the potential to materially affect one of its core priorities such as achieving its mission or ensuring the safety of staff, partners, and beneficiaries. For each of its five organizational priorities, management determined the point at which the priority would be impaired and set thresholds accordingly. For example, if the impact of a risk would affect more than a certain percentage of beneficiaries, it would be seen as jeopardizing the organization's ability to achieve its mission.

TABLE OF CONTENTS

VISUALIZING KEY RISK INDICATORS

In most organizations, risk owners take responsibility for monitoring key risk indicators for changes that signal a need for attention from the risk committee or action. Few organizations currently track indicators centrally, though many risk managers expressed a desire to develop systems to facilitate KRI monitoring and improve communications through visualizations.

One organization with a relatively sophisticated ERM process uses a Tableau[20] dashboard to track risks for countries of operation. The dashboard is not comprehensive, but rather focuses on highest priority categories for management decision-making, such as physical security and legal and regulatory issues. Each category is rated on a one to five scale, with an associated color-rating. Risk owners generally review data once per month, but also update the dashboard intermittently when events occur. Staff use external data sources as input, but rely more heavily on program staff analysis, especially when national-level data does not reflect the conditions faced in the localities where the organization operates. When an indicator value changes, the system automatically notifies leadership and mobilizes the crisis-response team if necessary. Since all staff can access the dashboard, it reduces the number of inquiries to country staff and helps inform travel decisions, such as precautions required for volunteers. (See Appendix M for an example of a Tableau dashboard.)

Another organization uses Microsoft Power BI to visually display all the risks on a chart according to their likelihood and impact. The graphic uses color and marker size to indicate speed of onset and financial impact. The visualization includes links to detailed profiles for all risks. (See Appendix N for an example of a Power BI dashboard).

[20] Tableau is a commonly used data visualization software with interactive features.

Vera Solutions, maker of the Salesforce-based Amp Impact software used by many nonprofit organizations, offers a risk module that can be used to create a customized risk management dashboard within an organization's larger information management system. The cloud-based software has the advantages of being user-friendly and providing flexibility to generate custom reports and visualizations. (See Appendix O for screenshot of Amp Impact's risk module).

KRI databases and visualizations are helpful but are not required for monitoring risks. At one organization in the early stages of ERM, the ERM manager tracks trends related to the highest priority risks without formal indicators. She analyzes the risks to know what to listen for in management meetings. Often, she will follow up with individuals after a meeting to get more information. It is an "artform."

COMMUNICATING RISK INFORMATION

Effective enterprise risk management requires communicating risk information to decision-makers clearly, concisely, and comprehensively. Risk information needs to be current and presented using a method of communication suited to decision-makers' needs.

Most organizations assemble risk owners to discuss the status of the risks they are tracking on a regular basis as part of a general management meeting or a specific risk-focused meeting. Management usually briefs the board of directors on the highest priority risks and the actions the organization is taking to respond to them at least once per year.

Organizations also need procedures in place to ensure that risk events can be dealt with quickly when events occur between regular reporting cycles. For an international humanitarian aid organization, the COVID-19 pandemic illustrated the importance of having a process in place to efficiently communicate and quickly escalate risk information to senior leadership. The large, global organization traditionally operated in silos with each region responsible for managing its own risks. Moving to an enterprise-wide risk management system enabled the organization to have a coordinated approach for addressing common risks across the organization. This approach proved effective for addressing broad-based needs such as preventing fraud. It became extremely valuable for managing varying needs across regions for personal protective equipment (PPE) during the COVID-19 pandemic. The ERM Manager explained that having this process in place resulted in "tangible resource savings in terms of people, time, and cost and, in the case of PPE, the speed of organizing in a coordinated fashion probably resulted in saving lives."

A good communications system ensures that information escalates to leadership and also flows back to staff. An ERM manager from a large, global organization highlighted the "initiative fatigue" that many field staff feel. To combat this frustration, he makes concerted efforts to provide information back to field staff. Several risk managers indicated that they check in with risk owners periodically one-on-one in between council meetings both for status updates and to make sure information flows both ways so that employees at all levels see the benefits of ERM.

TABLE OF CONTENTS

The ability to shape the process helps engage staff and improve the efficiency and effectiveness of ERM. An interview respondent described his organization's "ERM Playbook," that provides guidance for staff on topics such as risk identification and assessment, risk management plan development, risk-related communication within the organization and with the board of directors, and roles and responsibilities. The Playbook has helped staff connect theory and practice and institutionalize enterprise risk management within the organization, reducing reliance on him as ERM manager and empowering staff to include ERM into their existing processes. The ERM Playbook is a "flexible, living document rather than a policy" and is frequently updated as staff challenge existing ways of doing things and propose alternatives.

Another organization has made sharing significant mistakes and realized risks from the previous year a regular process. Previously, staff only learned about the organization's missteps through rumor. Formalizing review of mistakes and risks facilitated discussions about what could have been done to avoid or mitigate the consequences, creating learning opportunities.[21]

[21] Stoddard (2016).

RISK COUNCILS

A Risk Council (or Risk Committee or Risk Working Group) is a dedicated internal forum for discussing risks. The council ensures that there is a decision-making body standing by in case a quickly-moving issue arises. It usually meets quarterly or monthly. Some organizations prefer to add risk to the agenda of an existing forum, such as a senior management team meeting or quarterly strategy review, rather than create a new type of forum or group.

Organizations also use these forums to identify risks that cross multiple departments, to better understand where there might be opportunities for and risks associated with common risk responses, to discuss emerging risks, and to prepare briefings for the board of directors. Some organizations use risk council meetings to take "deep dives" into a risk to collaboratively undertake Bow-tie Analysis and brainstorm potential key risk indicators. One interview respondent said staff found the risk council discussions so helpful that each country program requested to have their own council.

Whether they are standalone sessions or part of another forum, the risk council's purpose should be to provide opportunities for updates and discussion. One ERM manager emphasized how important the tone is so it is not perceived as "checking on" but is rather an opportunity to discuss what has changed and gather input collaboratively.

The most effective risk councils periodically reflect on what has worked well and what should be changed or adjusted, either related to specific risks or the risk management process. In addition to reviewing what did not go well, it is also helpful to review what could have gone wrong but did not. Did the organization do something that prevented it or limited its impact? Or was it just luck?

Melissa Musser of GRF CPAs & Advisors warns that the most common pitfall of risk committees is involving too many people. The risk council should limit participation to risk owners and key decision-makers to ensure that decisions are made efficiently, while using other methods, such as periodic updates, for broader staff engagement. The risk council serves as a body that can react, respond, and escalate rapidly changing risks if needed. Musser adds that it is also important to onboard new members so they understand their roles and are prepared for their responsibilities in the process. Some organizations rotate the chair of the council to encourage incorporating new perspectives.

ONE-PAGE RISK SUMMARIES

High-level risk summaries facilitate communicating risk information (see Appendix P and Appendix Q for sample risk summaries). Limiting summaries to one page encourages concise narrative and keeps discussion focused on essential information. Links to other documents can provide more detailed analysis if necessary. Many risk summaries include scores for short-hand assessments. One interviewee instructs staff to view these ratings as discussion starters only and to not "overthink" them. The structure and content vary, but elements are generally a subset of the following:

- *Risk Description:* What is a short (2-3 sentence) summary of the risk?
- *Risk Owner:* Who is responsible for the risk?
- *Relevance to Mission:* To what aspect of the organization's mission or strategy does this risk relate?
- *Underlying Factors:* What are the root causes of the risk?
- *Preventive Measures:* What actions is the organization taking to lower the probability that the risk will occur?
- *Impact Reduction:* What responses is the organization implementing or planning to limit negative impact from the risk?
- *Status:* Are preventive and impact reduction measures complete, on target, or behind schedule?
- *Additional Responses Needed:* Is there anything that the organization needs to do differently, such as modify preventive or response measures to better address the risk?
- *Key Risk Indicators:* How is the organization monitoring whether a risk is becoming more likely or developing?
- *Trigger Points:* At what point will the organization know that it needs to take action?
- *Relevant Metrics:* How does the risk rate on the likelihood, impact, speed on onset, vulnerability, financial impact or other important measures?
- *Trend:* Is the risk becoming more or less likely?

TABLE OF CONTENTS

COMMUNICATING WITH THE BOARD OF DIRECTORS

Many organizations reported that they initiated their ERM processes at the urging of a board member, frequently a new board member who works in the financial services industry. But few organizations report having a board of directors that is actively engaged in risk management. While boards are actively engaged in many aspects of nonprofit stewardship such as fundraising, ERM is an area where additional education and communication is needed. Even when board members are involved in risk management in their professional roles, they often do not recognize risk oversight as part of their fiduciary responsibilities as nonprofit board members.

Involving the board more in ERM is a critically important governance priority. A study by the management consulting firm Oliver Wyman and the nonprofit merchant bank SeaChange Capital Partners found that many of the common characteristics shared by nonprofits in distress after risk events related to board oversight and engagement with risk management:[22]

- The organizations neglected to do explicit scenario planning despite facing inherently uncertain situations and were consequently surprised by crises that could have been foreseen.
- Trustees were not made fully aware of important long-term trends in financial performance or the operating environment.
- Trustees did not get timely, actionable information at the appropriate level of detail before or during the early stages of the crisis.
- Trustees took too long to realize that there was a problem and then delayed taking action even after they had decided it was necessary. Executive directors and trustees suffered from "magical thinking," particularly with respect to fundraising.

Few nonprofit boards of directors are currently engaged in discussions about their organization's risk appetite, but guidance on tolerance for risk in key areas such as finances, programs, and reputation supports management's ERM activities. When management shows the board the value of risk analysis for strategic decision-making, it can encourage the board to take more interest in ERM activities. Some organizations provide risk summaries in board briefing materials for every meeting, regardless of whether discussion of risk is on the agenda. Most organizations provide information on highest priority risks and the planned responses to the board of directors once or twice per year. Frequently, management reports first to the Audit Committee or Executive Committee, which then reviews the analysis and provides feedback before it presents a summary to the full board.

Generally, only risks that are the most consequential for the organization's strategy and operations are presented at the board level. Management's presentation of risks often includes a summary from a portfolio perspective, with an analysis of commonalities across risks, responses, and assumptions. Sometimes risks are grouped into "themes" of related risks that can be tied directly to the organization's mission and strategic objectives. The structure of the presentation should support its purpose, whether it is for awareness only, assistance, or decision-making.

An ERM manager at a large organization described how discussion with the board of directors drives the annual risk review process. The executive leadership team selects the 10-20 highest priority risks for the organization and presents them to the board, accompanied by an analysis of the main assumptions and internal and external drivers (organizational strengths and weaknesses and macroeconomic and geopolitical influences). The analysis highlights changes from the previous year and how the new plan reflects these changes, connecting contextual factors directly to the most urgent three to four critical actions the leadership team proposes to accomplish in the next year. The ERM manager leads a deep-dive refresh annually and provides ad-hoc support and iterative updates, as needed. The organization follows a similar approach for risks that are not in the top tier, at levels of the organization below the board of directors.

TABLE OF CONTENTS

[22] Roberts, et al (2016). Other characteristics were: The organizations were fragile before the crisis occurred, often with several years of deficits that eroded their resources. The organizations had a longstanding challenge in recruiting and retaining a strong chief financial officer. And the crisis was precipitated by an event such the departure of the executive director, non-renewal of an important funder, or a meaningful increase in scale (25-50%).

ERM IN PRACTICE

Many interviewees highlighted that unlike publicly traded companies and regulated industries, nonprofits are not subject to external requirements to implement enterprise risk management programs. Nonprofits have flexibility to determine how to apply ERM principles to benefit their organizations. Accordingly, enterprise risk management systems look very different across nonprofit organizations and from traditional private sector models. Programs vary from informal, with responsibility for coordinating ERM as one aspect of one person's job, to multiple staff members working on ERM full-time. Most important is that ERM principles are woven into the organization in a way that they best contribute to supporting the organization's ability to achieve its mission.

Practitioners recommend taking a long-term approach to implementing ERM, starting with small steps and incrementally adding more. Advice from practitioners for how to adapt the ERM process to meet an organization's needs generally falls into four categories, which combine to form a sequential series of steps for planning an ERM approach (see Figure 9). The pathway starts with clearly defining the objective for ERM, then proceeds to selecting the most important elements of the ERM process to emphasize, customizing those elements to the organization's culture, and developing a long-term vision for ERM in the organization. (A template for ERM process planning is provided in Appendix R.)

FIGURE 9: PATHWAY FOR ADAPTING THE ERM FRAMEWORK

WHY? What do we want to achieve with ERM? → **WHAT?** Which elements of the ERM framework are most important for our objectives? → **HOW?** How do we integrate ERM into our existing processes most effectively? → **WHEN?** How can we increase the value that ERM provides over time?

WHY: WHAT DO WE WANT TO ACHIEVE WITH ERM?

A common piece of advice from nonprofit ERM leaders is to be clear from the outset about the purpose of implementing enterprise risk management and the value the organization hopes to gain from the process. A clearly articulated purpose will improve internal communications and focus the organization's activities on what provides the greatest benefits. One ERM leader commented, "When we get too caught up in the process, we take a step back and remember why we are doing it."

How an organization implements ERM is largely determined by the problem it is addressing. For example, an organization may find that it is frequently blindsided by risks that, in retrospect, could have been avoided or mitigated. Another organization's decentralized structure may lead to inefficient responses to risks and missed opportunities. Or an organization may be concerned that it always seems to be operating in "crisis mode."

Keeping purpose as a north star is the key to adapting the ERM process to add the most value to the organization.

WHAT: WHICH ELEMENTS OF THE ERM FRAMEWORK ARE MOST IMPORTANT FOR OUR OBJECTIVES?

Practitioners emphasize that flexibility in applying ERM is important. A flexible approach selects ERM items from a smorgasbord rather than following a recipe. It is impractical to implement all elements of the ERM framework extensively from the outset.

The guiding purpose determined in the first step helps organizations decide which elements of the process to emphasize. For example, an organization frequently blindsided by foreseeable risk events may find thorough risk identification and monitoring most useful, while a decentralized organization may want to focus more on improving communication and information flow. An organization operating in crisis mode may want to emphasize scenario planning and developing risk response plans. These organizations all start with identifying a central purpose and then selecting ERM activities that best meet the needs of the organization.

TABLE OF CONTENTS

HOW: HOW DO WE INTEGRATE ERM INTO OUR EXISTING PROCESSES MOST EFFECTIVELY?

Once an organization has decided which elements of the ERM framework to prioritize, it needs to determine how to integrate new approaches in a way that fits with the organization's culture and existing processes. Several practitioners recommend first scanning the organization's current practices to leverage what staff are already doing. One respondent commented, "ERM is something we all have been doing to some extent anyway. Formalizing that process gives us a shared language to talk about it and some tools for how to present it." Others emphasize the importance of champions. An ERM leader noted how early enthusiasm from a board member was critical for building momentum. Another suggested pilot programs to build a "coalition of the willing" and enlist peers as advocates.

Practitioners stress the importance of keeping the ERM process as simple for staff as possible, embedding ERM into existing processes and forums rather than adding new ones. For example, a civic action group already had a committee that regularly met to discuss staff and volunteer safety, so this group broadened its scope to be the Risk Committee. The key, says one ERM manager, is to "make risk tools active management tools" to demonstrate the value ERM can provide. Another ERM manager provides standard frameworks and makes sure that staff understand what is expected of them. He offers suggestions for how they should approach risk discussions in management team meetings and stresses that they do not need to use formulas for risk assessments or produce formal reports. "Just the fact that discussions are happening is a big win."

At a large global humanitarian relief organization, risk management is an "integrated management core competency" and ERM is "close to having zero footprint." Two important elements of integrating ERM are to include it in the budget process and strategy development process.

Discussing risk can be important for budgeting, particularly for showing the importance of a particular budget request. An interviewee whose organization links ERM and the budget process describes that risks are updated during the budget cycle so the analysis can feed into the budget. For example, it informs how many and what type of people the organization needs to hire and ensures that there is budget available for the proposed risk mitigations.

Another interviewee says that it is helpful to use the risk taxonomy as part of performance assessments around the annual budget planning and strategy processes. This makes it easier to identify common themes across the large organization, particularly when there are new requests or when teams are asking for guidance or assistance. Other organizations report that it is helpful to align top risks and objectives and request discussion of risk as part of the strategy process.

Many organizations struggle with determining how much they should try to implement themselves and whether engaging consultants would be helpful for accelerating ERM implementation. External assistance is most beneficial when it plays a supporting, rather than leading, role. Several organizations found it helpful to bring in fresh perspectives when they were feeling stuck at a step of the process and needed new ideas and suggestions. Others felt an independent third party was beneficial for conducting interviews, facilitating workshops, and training staff. One ERM leader commented that a benefit of engaging consultants was that it reassured the board of directors that they were following best practice.

Reliance on consultants can be problematic, however, when there is insufficient ownership of the process within the organization. One organization hired consultants to prepare an ERM strategy. The strategy's success hinged on the consultants' recommendation to hire a new executive Chief Risk Officer to lead the ERM implementation. The vacancy announcement was retracted at the start of the COVID-19 pandemic. There is continued interest in ERM in the organization, but without someone on staff able to keep it moving forward, implementation was indefinitely postponed.

WHEN: HOW CAN WE INCREASE THE VALUE THAT ERM PROVIDES OVER TIME?

Many practitioners emphasize that implementing ERM should be viewed as an incremental, long-term process and that it is helpful to continually think through how to increase value from the process. An ERM leader at an organization starting its second annual ERM cycle commented that risk identification was a time-intensive process the first year, but updating identified risks was easier the second year and they could do more to integrate ERM into other processes, such as preparing the annual budget and strategic planning.

TABLE OF CONTENTS

It is helpful to keep expectations modest and view some actions as planting seeds for the future. An ERM leader describes, "I always have a three to five year plan. I'll raise something that I think will not make it into the formal risk reporting mechanisms yet, such as the Enterprise Risk Register, but from that moment, it is on the table for discussion and might be raised by leadership the next year. Or maybe it will be addressed and go away. If the risk is better understood, given appropriate attention, or even mitigated within appetite, it is a win, regardless of formalities."

CONCLUSION

Enterprise risk management is a long-term investment that improves an organization's financial strength, operational efficiency, program effectiveness, and resilience during uncertain times. Most importantly, ERM catalyzes mission achievement by linking risk management to strategic objectives. Although ERM is a nascent practice in the nonprofit sector, the nonprofit practitioners and experts interviewed for this guide expect that it will become more prevalent in the near future. Four recurring themes on the outlook for ERM emerged from interviews:

ERM REQUIRES CULTURAL CHANGE

Currently, most nonprofit organizations view risk management as a compliance activity rather than an integral element of strategic planning and management. Staff and boards of directors do not prioritize ERM because they either fear it will become a bureaucratic burden or do not see it as critical to their role. While changing organizational culture to support ERM requires some creativity and effort, organizations that achieve it find that they deliver higher quality services and more effective programs, have more efficient operations, and discover new opportunities for mission achievement.

MINDSETS ABOUT RISK ARE CHANGING

A positive outcome of the COVID-19 pandemic is that it has destigmatized risk and shown that everyone is vulnerable to factors outside their control. However, nonprofits can be more prepared to manage these factors. Organizations that began ERM activities before 2020 reported increased appreciation for ERM within their organizations because it improved their response to the effects of the pandemic and guided decision-making. Donors are increasingly valuing resilience.

ENGAGING BOARDS OF DIRECTORS MORE IS A PRIORITY

Boards of directors play a critical role in risk oversight, but few nonprofit boards are currently engaged in a significant way. Boards should discuss their appetite and tolerance for risk and reporting on the status of key risks and management's risk response plans should be a regular element of board discussions. Many directors may need training on how to better fulfill their risk oversight roles in a way that shifts views on risk from a compliance lens only to ERM as a tool for fulfilling an organization's mission and achieving strategy objectives.

THE NONPROFIT SECTOR NEEDS MORE TAILORED RESOURCES

There is significant demand for resources to assist nonprofits in each step of the ERM process. Many practitioners reported that they appreciated the opportunities they have had to share their experiences and learn from each other but expressed frustration about the lack of ERM guidance for nonprofit organizations. Practitioners and experts emphasized that, while the absence of a "right way" to implement ERM for nonprofits presents opportunities to adapt ERM to best suit an organization's needs, it also presents challenges, especially related to managing relationships with funders. In addition to more resources to support management and risks owners, practitioners suggested that they would find the following additional guidance most useful:

- Board members require materials that would help them understand and fulfill their governance responsibilities related to risk oversight and to demonstrate the value that ERM provides.
- Funders would benefit from guidance on how to assess the risk management practices of the organizations they support (as well as how to implement it within their own organizations). If ERM becomes as commonplace as monitoring and evaluation, as many practitioners expect, there will need to be standards on how to right-size risk oversight to ensure that it is proportionate to what is needed.

TABLE OF CONTENTS

APPENDICES A-R

Templates provided in the appendices are available at https://erm.ncsu.edu/library/article/getting-started-with-enterprise-risk-management-templates. Additional resources, including an extensive library of ERM-related articles, interviews, and research papers, are available on the NC State University ERM Initiative website (erm.ncsu.edu/library).

APPENDIX A	DEFINITION OF TERMS
APPENDIX B	INDIVIDUALS INTERVIEWED
APPENDIX C	REFERENCES
APPENDIX D	CORE VALUE DRIVER/STRATEGIC ANALYSIS TEMPLATE
APPENDIX E	SWOT ANALYSIS TEMPLATE
APPENDIX F	PESTLE ANALYSIS TEMPLATE
APPENDIX G	RISK IDENTIFICATION USING RISK CATEGORIES TEMPLATE
APPENDIX H	ANNUAL GLOBAL RISK AND BENCHMARKING REPORTS
APPENDIX I	OPEN ROAD ALLIANCE ROADBLOCK ANALYSIS
APPENDIX J	EXAMPLE OF IMPACT SCALES
APPENDIX K	BOW-TIE ANALYSIS EXAMPLE AND TEMPLATE
APPENDIX L	KEY RISK INDICATOR (KRI) IDENTIFICATION USING BOW-TIE ANALYSIS TEMPLATE
APPENDIX M	EXAMPLE OF A TABLEAU DASHBOARD
APPENDIX N	EXAMPLE OF POWER BI DASHBOARD
APPENDIX O	SCREENSHOTS OF VERA SOLUTIONS' AMP IMPACT RISK MODULE
APPENDIX P	RISK PROFILE TEMPLATE
APPENDIX Q	EMERGING RISK SUMMARY TEMPLATE
APPENDIX R	ERM PROCESS PLANNING TEMPLATE

TABLE OF CONTENTS

APPENDIX A: DEFINITIONS OF TERMS

Bow-tie Analysis: A visual method of analyzing root causes and consequences of a risk event that is used to aid formulating risk responses and identifying key risk indicators. It gets its name from the shape that is generated when multiple causes (left side) feed into a single risk event (center), which generates multiple consequences (right side).

Business context: The existing and emerging events, trends, and other factors that influence an organization's ability to achieve its objectives.

Culture: The shared beliefs, values, and attitudes that shape decision-making, behavior, and interactions within an organization.

Dashboard: An interactive, at-a-glance view of key risk indicators and/or status of risks. Typically used for monitoring changes.

Enterprise risk management: An integrated approach for managing risks to increase an organization's ability to achieve its objectives.

External environment: Factors originating outside an organization that influence its ability to achieve its objectives.

Heat map: A visual representation of an organization's overall risk profile that plots each risk according to its potential impact and the likelihood of it occurring, using color coding to signify overall risk ratings.

Impact: The effect or result a risk event would have on the organization.

Inherent risk: The risk to an organization before it takes any action to alter the risk's severity or likelihood.

Internal environment: Factors originating within an organization that influence its ability to achieve its objectives.

Key risk indicator: A quantitative or qualitative measure that a risk event is imminent or emerging to help an organization take early action to address the risk (leading indicator) or is occurring to help determine when certain response actions are necessary (lagging indicator).

Likelihood: The probability a risk event will occur.

Portfolio view: A composite view of risk across the entire organization that facilitates analysis of concentrations of risks and responses, commonalities, and interdependencies.

Preparedness: The degree to which the organization has steps in place to manage a risk should it occur.

Residual risk: The risk that remains after risk response and management actions have been taken.

Risk: Uncertainty that materially affects the ability of an organization to achieve its objectives. It is worth noting that risk, in this definition, does not necessarily have a negative connotation. In fact, a key element of the ERM approach is that risk can be a source of opportunity as well as disruption.

Risk appetite: The amount and types of risk that an organization is willing to accept.

Risk register: A risk management tool that compiles all risks across the organization (or department) with relevant descriptive information such as risk owner, expected impact, and actions being taken to prevent or mitigate the risk.

Speed of onset: How quickly a risk may emerge.

Strategy: An organization's plan for achieving its mission.

Velocity: Synonym for speed of onset.

Vulnerability: How susceptible an organization is to a risk. It may include preparedness as well as an organization's ability to detect a risk.

APPENDIX B: INDIVIDUALS INTERVIEWED

Thank you to the following individuals who generously shared their time so that others can learn from their experience.

ORGANIZATION	NAME, POSITION
Bridges to Prosperity	Alex McNeill, Director of Operations
Catholic Relief Services	Sergey Hayrapetyan, Director, Global Compliance & Risk
GRF CPAs & Advisors	Melissa Musser, Principal, Risk & Advisory Services
Humanitarian Outcomes	Abby Stoddard, Partner
International Rescue Committee	Gary Love, Senior Director of ERM
The Jewish Board	David Rivel, former Chief Executive Officer John Kastan, Interim Chief Executive Officer
NC State University	Bonnie Hancock Professor of Practice and Executive Director, ERM Initiative
Open Road Alliance	Maya Winkelstein, Chief Executive Officer Aaron Kotler, Director of Partnerships
SeaChange Capital Partners	John MacIntosh, Managing Partner
Vera Solutions	Zak Kaufman, Co-Founder & Chief Executive Officer
YMCA of the Triangle	Bryan Huffman, Chief Financial Officer

APPENDIX C: REFERENCES

Beasley, Mark. "What is Enterprise Risk Management." North Carolina State University Enterprise Risk Management Initiative. 2016.

Beasley, Mark S., Bruce C. Branson, Bonnie V. Hancock. *2021 The State of Risk Oversight: An Overview of Enterprise Risk Management Practices.* April 2021.

Beasley, Mark. "How to Leverage ERM Principles to Better Respond to COVID-19-Related Risks." North Carolina State University Enterprise Risk Management Initiative. 2020.

Beasley, Mark and Jeff Lovern. "Tools for Escalating Risk Issues to the C-Suite and Board." ERM Professional Insights. NC State University Enterprise Risk Management Initiative. December 2020.

Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management: Integrating with Strategy and Performance*. June 2017.

GRF CPAs & Advisors. "Best Practices in Enterprise Risk Management."

Haver, Katherine. "Tug of War: Ethical Decision-Making to Enable Humanitarian Access in High-Risk Environments." *Humanitarian Practice Network Paper* Number 80. November 2016.

Humanitarian Outcomes. "NGO Risk Management: Principles and Promising Practice." 2019a.

Humanitarian Outcomes. "NGOs and Risk: Managing Uncertainty in Local-International Partnerships." 2019b.

Institute of Risk Management. *Risk Management for Charities: Getting Started: Supplementary Guidance*. 2018.

International Organization for Standardization. ISO 31000: *Risk management – Guidelines*. 2018.

Leonberger, Katie and Jeff Ballow. "Risk and Reward: Positioning Your Nonprofit for Sustained Impact." *Nonprofit Quarterly*. Summer 2017.

Open Road Alliance. *Roadblock Analysis Report: An Analysis of What Goes Wrong in Impact-Focused Projects*. 2018.

Open Road Alliance. *Contingency Funding in Philanthropy: Open Road Alliance Survey Full Report*. 2016.

Relief International. *Risk Management in Fragile Settings: A Toolkit for Field Practitioners*. February 2020.

Roberts, Dylan, George Morris, John MacIntosh, and Daniel Millenson. "Risk Management for Nonprofits." Oliver Wyman and SeaChange Capital Partners. March 2016.

Stoddard, Abby, Katherine Haver, and Monica Czwarno. "NGOs and Risk: How International Humanitarian Actors Manage Uncertainty." February 2016.

United Nations Development Programme. *UNDP Enterprise Risk Management (ERM) Policy and Procedures*. November 2018.

Winkelstein, Maya and Shelley Whelpton. "Foundations Don't Know What They're Risking." *The Foundation Review* Vol 9:2. 2017.

APPENDIX D: CORE VALUE DRIVER/STRATEGIC ANALYSIS TEMPLATE

MISSION: *What is the organization's key purpose? Why does it exist?*	• •
CORE VALUE DRIVER/STRATEGIC INITIATIVE: *Select a core value driver (service, knowledge, skill, attribute, etc. that drives the organization's value) or a strategic initiative (program or activity the organization is planning to increase the value it provides in the future)*	• •
WHAT MUST GO RIGHT*: *What must go right for this core value driver or strategic initiative to succeed?*	• •
RISKS TO THE CORE VALUE DRIVER/STRATEGIC INITIATIVE: *What internal or external events might prevent what must go right for the strategy to succeed?*	• •
ASSUMPTIONS*: *What assumptions is the organization making related to the core value driver or strategic initiative?*	• •
RISKS OF ASSUMPTIONS: *How might assumptions be flawed, based on unreliable data, or outdated?*	• •
RISKS OF THE CORE VALUE DRIVER/STRATEGIC INITIATIVE: *What impact might this strategy have on existing programs and other initiatives?*	• •
OPPORTUNITIES: *How might a risk the organization is facing turn out to be an advantage?*	• •

*It may be difficult to distinguish between what must go right and assumptions. It does not matter what goes in which box, as long as both boxes combined capture all factors. Asking the questions differently helps identify more factors.

APPENDIX E: SWOT ANALYSIS TEMPLATE

STRENGTHS	WEAKNESSES
What do we do well? What internal resources do we have? What advantages do we have over similar organizations?	*What factors in our control detract from our ability to be more effective? What areas need improvement? What does our organization lack?*
OPPORTUNITIES	**THREATS**
What opportunities exist in our area of expertise that we can benefit from? Is the opportunity sustainable or one-time?	*What might threaten our effectiveness? What factors exist that are beyond our control?* *Are there any anticipated unfavorable trends?*

APPENDIX F: PESTLE ANALYSIS TEMPLATE

COMPONENTS	RELEVANT ISSUES AND EFFECTS
POLITICAL FACTORS *Elections, change of government leadership, potential policy changes, rule of law, etc.*	
ECONOMIC FACTORS *Economic growth or stagnation, interest rates, exchange rates, inflation, unemployment, etc.*	
SOCIAL FACTORS *Population and demographic changes, health conditions, level of education, social mobility, social attitudes, religious beliefs, socio-cultural changes, etc.*	
TECHNOLOGICAL FACTORS *Changes in the availability or price of new technologies, technological infrastructure, potential changes in technological standards, etc.*	
LEGAL FACTORS *Labor laws, relevant court cases, employment regulations, etc.*	
ENVIRONMENTAL FACTORS *Climate, weather, energy consumption regulations, etc.*	

APPENDIX G: RISK IDENTIFICATION USING RISK CATEGORIES TEMPLATE

RISK CATEGORIES	
FINANCIAL/FIDUCIARY *e.g., fraud/theft/bribery, accuracy/sufficiency of financial information, adequacy of reserves/cash flow, dependency on limited income sources, currency fluctuations*	
IMPACT/OPERATIONS/PROGRAMS AND SERVICES *e.g., service delivery, staff recruitment, training and retention, contracts, volunteers, disaster recovery and continuity*	
LEGAL/COMPLIANCE *e.g., legislation and regulations, reporting requirements, taxation, conflicts of interest, codes of conduct*	
GOVERNANCE/LEADERSHIP/STRATEGY *e.g., oversight, decision-making, organizational structure, theory of change, accountability*	
EXTERNAL ENVIRONMENT/SOCIAL AND ENVIRONMENTAL/POLITICAL *e.g., demographics, government change, natural resources, climate change, human rights*	
INFORMATION TECHNOLOGY *e.g., data loss or corruption, breach or misuse of confidential/sensitive data, reliability of essential technology, business continuity/disaster recovery*	
REPUTATIONAL *e.g., media coverage, stakeholder relations, social media*	
SECURITY/SAFETY *e.g., violence or crime, civil unrest, accident or illness*	

APPENDIX H: ANNUAL GLOBAL RISK AND BENCHMARKING REPORTS

WORLD ECONOMIC FORUM'S GLOBAL RISK REPORT

The World Economic Forum is an international non-governmental organization best known for its annual convening of global business, government and civil society leaders in Davos, Switzerland. Its annual risk report provides results from its survey of affiliated leaders and expert analysis of top identified risks. The survey asks respondents to assess whether 35 risks (as of 2021) in five categories (economic, environmental, geopolitical, societal, and technological) are critical threats in the short-term (0-2 years), medium-term (3-5 years), or long-term (5-10 years). It also asks for assessments of the likelihood and impact of each of these risks within 10 years, which are most concerning, which the current global response falls short in addressing ("blind spots"), and which a coordinated global response has the most potential to prevent or mitigate ("opportunities"). In 2021, most questions were answered by 600-700 respondents, of whom 73 percent were men and 46 percent were European. Thirty-nine percent of respondents were business leaders, 18 percent academics and 16 percent government leaders.

https://www.weforum.org/global-risks

EURASIA GROUP'S TOP RISKS

The Eurasia Group is a political risk advisory and consulting firm primarily serving the investment community and corporate decision-makers. Its annual report ranks and describes the top ten risks its experts and analysts predict to be the greatest threats to nations, global politics, industries, and institutions in the coming year.

https://www.eurasiagroup.net/

PROTIVITI-NORTH CAROLINA STATE UNIVERSITY'S EXECUTIVE PERSPECTIVES ON TOP RISKS

Protiviti is a global consulting firm that partners with the Enterprise Risk Management Initiative at NC State University to conduct and present the results from an annual survey of over 1,000 executives and members of boards of directors in corporate, nonprofit, and government sectors. Survey respondents rate the expected impact of 36 macroeconomic, strategic, and operational risks on their organizations in the next year and within 10 years (on a 10-point scale from "No Impact at All" to "Extensive Impact.")

https://erm.ncsu.edu/library/article/report-executive-perspectives-on-top-risks-for-2021-2030

BDO'S NONPROFIT STANDARDS

BDO is a global professional services firm providing assurance, tax, and financial advisory services. Its annual survey of 200 nonprofit organizations representing a variety of sectors provides organizations with an opportunity to benchmark their performance on strategic planning, human resources, operations, scope and impact and governance matters.

https://www.bdo.com/insights/industries/nonprofit/nonprofitstandards

APPENDIX I: OPEN ROAD ALLIANCE ROADBLOCK ANALYSIS

The table below presents the roadblocks nonprofit organizations and social enterprises faced that led them to request grant funding from the Open Road Alliance (2012-2017).[23]

46%	**Funder-Created Obstacles**	13%	Change in strategic direction or allocation priorities
		12%	Delayed disbursement of approved funds
		9%	Funder policy inflexibility (inability to adapt to/make exceptions for situations outside of the funding recipient's control)
		5%	Funder misfortune (such as unexpected reduction in endowment)
		3%	Change in grant amount
		2%	Change in funder policy (such as shift from advancing funds to reimbursing funds)
		2%	Change in grant cycles
		<1%	Change in personnel
27%	**Acts of God/Economics**	9%	Weather events
		8%	Government policy and regulatory changes
		4%	Market changes/economic crisis
		4%	Violence/conflict
		2%	Public health crisis
		<1%	Foreign exchange rate changes
27%	**Organizational Misfortune**	9%	Partner problem (such as underdelivering or pulling out of the relationship)
		4%	Fraud or theft
		4%	Personnel issues (such as departure or change)
		3%	Errors by credible experts (such as underestimating costs or project requirements)
		2%	Change in price/costs
		2%	Equipment failure
		2%	Property damage
		1%	Timeline acceleration

[24] Institute of Risk Management (2018)

APPENDIX J: EXAMPLE OF IMPACT SCALES[24]

CATEGORY	VERY HIGH	HIGH	MEDIUM	LOW	VERY LOW
STRATEGIC	Would require a fundamental change in organizational strategic/ critical objectives.	Would require a significant shift from organizational strategic/ critical objectives that would require Board of Trustees input.	Would impact the organizational strategic/ critical objectives and would require management discussion.	May have an impact on achieving organizational strategy but this could be resolved.	Little impact on the organizational strategy.
OPERATIONAL	Fundamental organizational changes would need to be implemented. Delay of > 1 year in delivery of project.	A significant amount of work would need to be done at all levels to resolve the matter. Delay of 6-12 months delivery on the project.	A significant amount of work would be required by a team to repair operational systems. Delay of 3-6 months in delivery of project.	Low level processes would need to be revised but the matter could be resolved. Delay of 1-3 months in the delivery of project.	Has no impact on the day-to-day operation of the charity. Less than 1 month delay in delivery of project.
FINANCIAL	If the risk materialized, the cost to the charity would be > £3 million.	If the risk materialized, the cost to the charity would be between £1 million and £3 million.	If the risk materialized, the cost to the charity would be between £500,000 and £1 million.	If the risk materialized, the cost to the charity would be between £100k and £500k	If the risk materialized, the cost to the charity would be no more than £100k.
REPUTATIONAL	Significant and irreparable damage to reputation. Sustained negative publicity resulting in loss of public/ professional/ political confidence in the charity.	Significant and irreparable damage to reputation. High negative impact on the charity's reputation. Could impact charity's ability to influence public/ professionals/politicians. Generates significant number of complaints.	Minor damages but widespread. Significant localized low level negative impact on the charity's reputation/ generates limited complaints.	Minor damages in a limited area. May have localized, low level negative impact on the charity's reputation/generates low level of complaints.	Has no negative impact on the charity's reputation/no media interest.
COMPLIANCE	Serious breach of governance regulations that would lead to status of the charity being reviewed.	Significant breach of governance regulation requiring immediate notification of regulatory bodies.	Breaches governance regulations and would require significant work to rectify.	May breach low level governance regulations but can be rectified.	No impact on the charity's governance structures.

[24] Institute of Risk Management (2018)

APPENDIX K: BOW-TIE ANALYSIS EXAMPLE[25] AND TEMPLATE

The following questions can be used to guide the analysis:

1. What are the top 3-4 root causes that might cause the organization to be vulnerable to the risk?
2. What risk responses does the organization already have in place to prevent the root causes of the risk from occurring?
3. How confident is the organization that these actions will be effective at minimizing risk exposure?
4. What else might the organization do to more effectively prevent this risk from occurring?
5. Assuming the risk occurs, what are the specific responses the organization would implement should the risk begin to occur?
6. How confident is the organization that these responses would be effective at minimizing the consequences of the risk?
7. What else might the organization want to do to more effectively prevent this risk from occurring?

CAUSES	RESPONSES TO PREVENT RISK	RISK	CONSEQUENCES	RESPONSES TO MINIMIZE IMPACT
Compensation and benefits not competitive	Conduct benchmarking with entities that compete for same talent	**Current environment may make it difficult to attract and retain talented workforce**	Key operations are interrupted for period of time	Prioritize functions that need staffing most and boost compensation packages to secure longer employment
Younger people do not view industry as favorable	Develop awareness campaign of importance of industry		Existing employee base has to work overtime	Provide incentives and rewards to recognize extra efforts
Unclear career path options	Develop a leadership development program to layout career path options		Over-taxed workforce continues to leave at faster pace	Seek opportunities to outsource key functions to third parties
Physical workplace locations unappealing	Upgrade facilities; offer remote work opportunities		Certain initiatives have to be placed on hold	Prioritize initiatives to place on hold first

[25] NC State University ERM Initiative

APPENDIX K: BOW-TIE ANALYSIS EXAMPLE AND TEMPLATE (*CONTINUED)*

RISK IDENTIFICATION: ______________________________

RISK OWNER: ______________________________

Root Causes – Vulnerabilities That Might Precede Risk Event	Current Responses That Lower Probability of Root Cause Occurring	Assessment of Effectiveness of Response (1=Not Effective; 10=Extremely Effective)	What Else Might Be Done to Prevent the Risk		Responses to Minimize Impact of Risk	Assessment of Effectiveness of Response (1=Not Effective; 10=Extremely Effective)	What May Be Done Differently to Lessen the Impact of the Risk
				Risk Event			

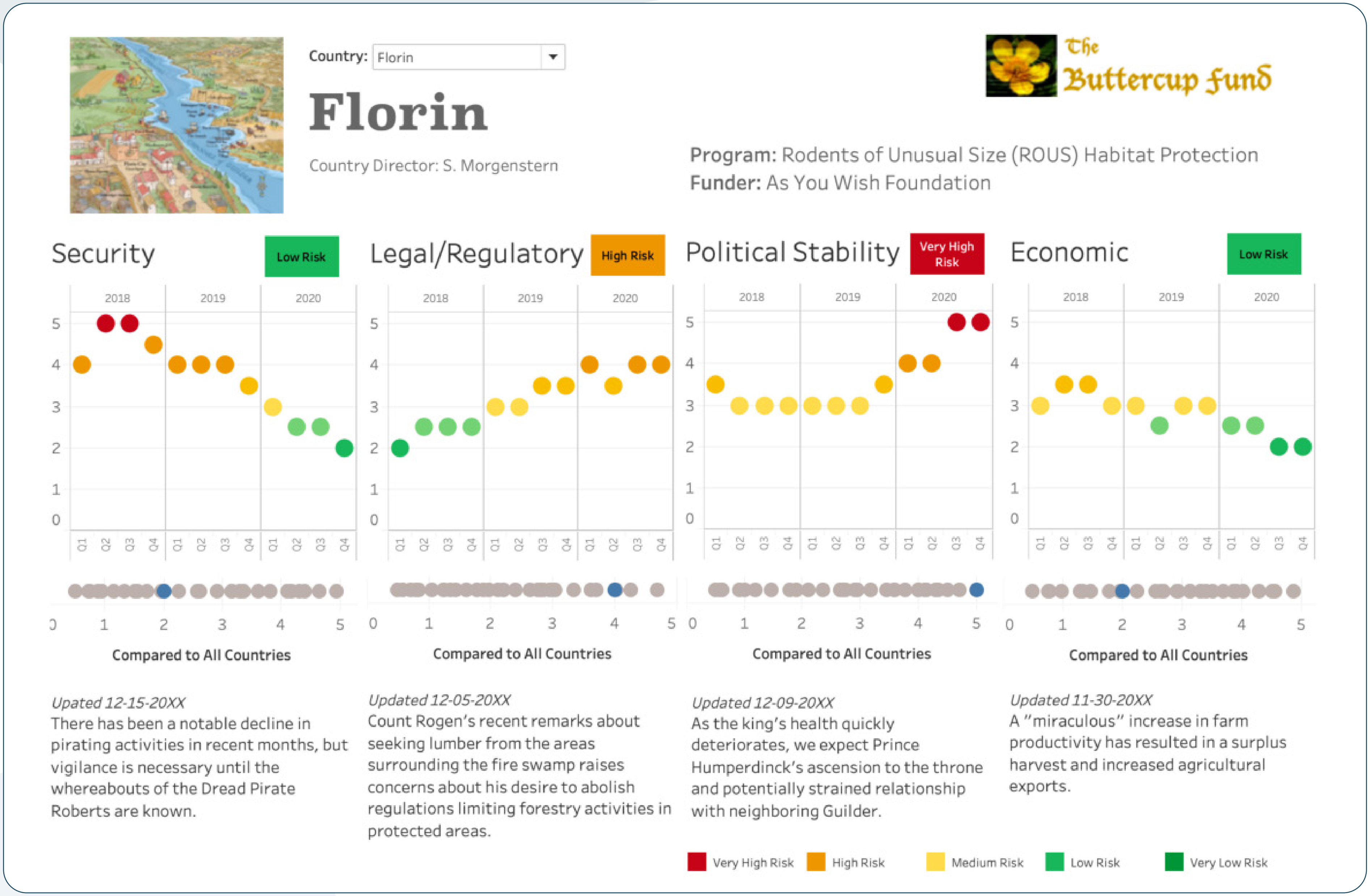
APPENDIX L: KEY RISK INDICATOR (KRI) IDENTIFICATION USING BOW-TIE ANALYSIS TEMPLATE

RISK IDENTIFICATION: ______________________________

RISK OWNER: ______________________________

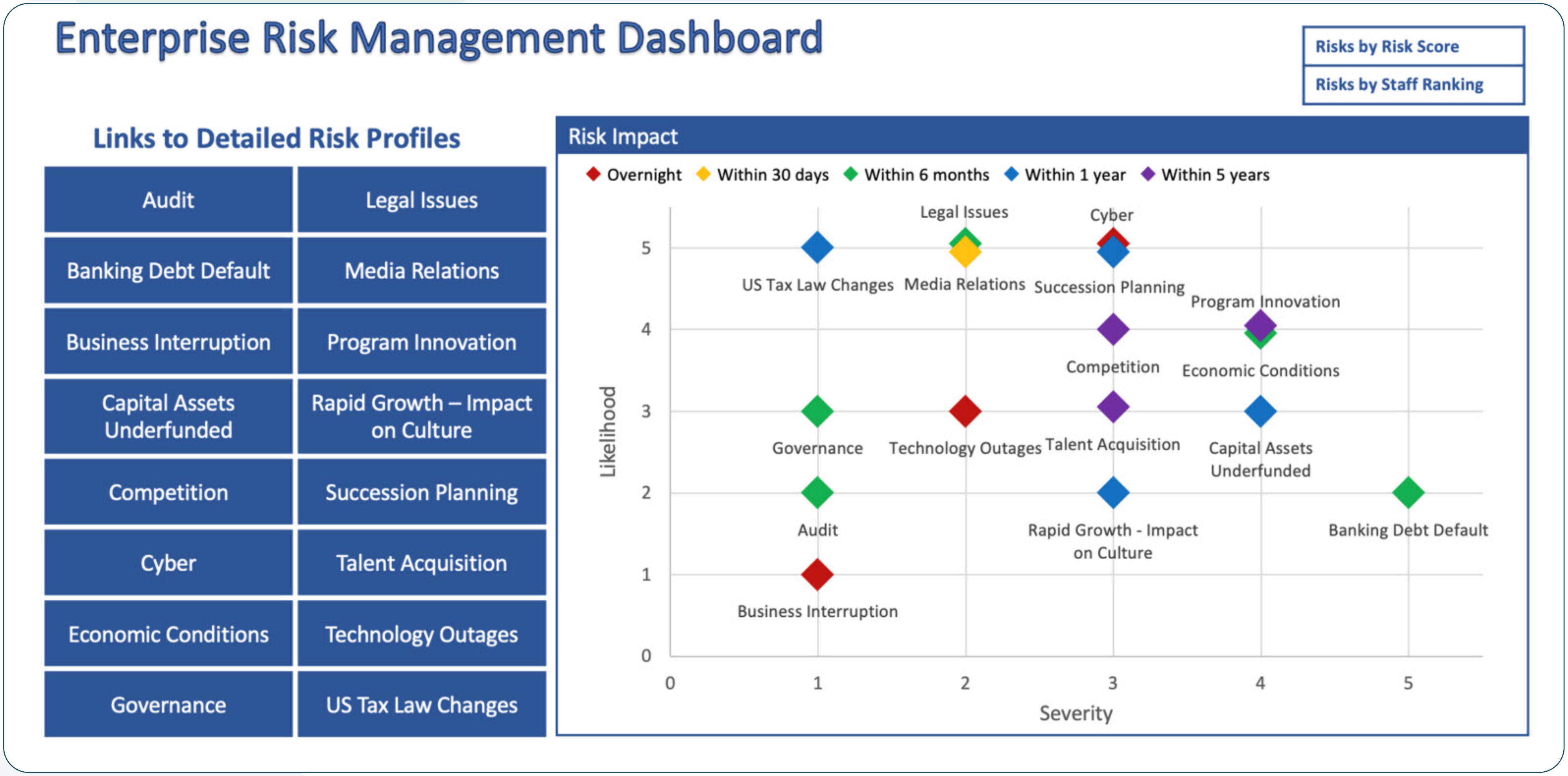
ROOT CAUSES THAT WOULD START PATH TOWARDS RISK EVENT	LEADING KRIs	INTERMEDIATE EVENTS THAT WOULD PRECEDE OCCURRENCE OF RISK EVENT	LEADING KRIs	RISK EVENT	INITIAL SIGNS OF RISK CONSEQUENCE	LAGGING KRIs	ULTIMATE CONSEQUENCE OF GREATEST CONCERN

APPENDIX M: EXAMPLE OF A TABLEAU DASHBOARD[26]

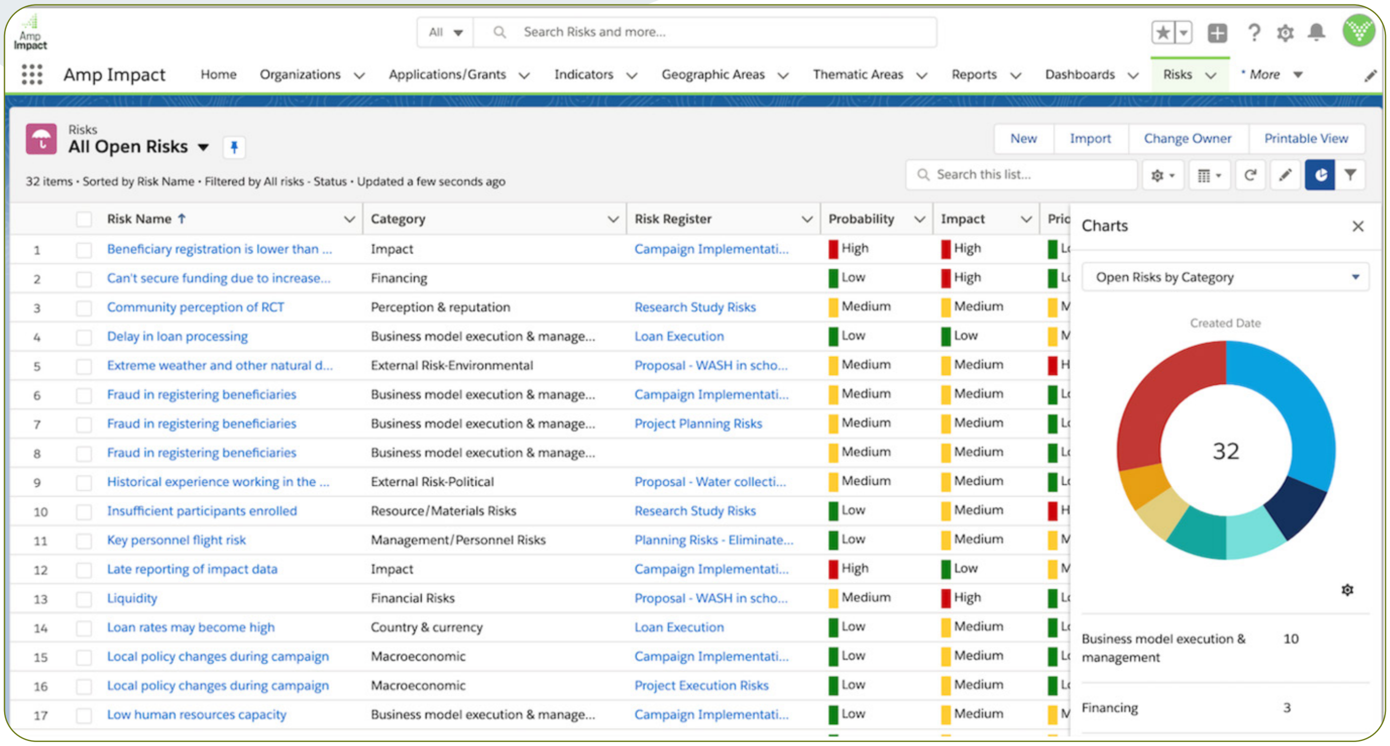


[26] Map image credit: https://blogtarkin.wordpress.com/tag/princess-bride/

APPENDIX N: EXAMPLE OF A POWER BI DASHBOARD



APPENDIX O: SCREENSHOTS OF VERA SOLUTIONS' AMP IMPACT RISK MODULE



APPENDIX P: RISK PROFILE TEMPLATE

<table>
<tr><td rowspan="2">RISK:</td><td colspan="3">DESCRIPTION:</td></tr>
<tr><td colspan="3">RISK OWNER:</td></tr>
<tr><td colspan="2">WHAT ARE WE DOING TO PREVENT RISK FROM OCCURRING? (PREVENTIVE RESPONSE):</td><td>WHAT ARE WE DOING TO MINIMIZE CONSEQUENCES OF RISK IF IT OCCURS? (REACTIVE RESPONSE):</td><td>NEED FOR ADDITIONAL RESPONSES:</td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td>SPEED OF ONSET:</td><td></td><td colspan="2" rowspan="3">INFORMATION HELPFUL FOR MONITORING RISK (KEY RISK INDICATORS):</td></tr>
<tr><td>LIKELIHOOD:</td><td></td></tr>
<tr><td>SEVERITY:</td><td></td></tr>
<tr><td>PREPAREDNESS:</td><td></td><td colspan="2" rowspan="2">WHEN WILL WE KNOW DIFFERENT ACTION SHOULD BE TAKEN (TRIGGER POINT)?</td></tr>
<tr><td>FINANCIAL IMPACT:</td><td></td></tr>
</table>

APPENDIX Q: EMERGING RISK SUMMARY TEMPLATE[27]

PREPARED BY: ______________________________

RISK ISSUE:		
WHAT IS HAPPENING RIGHT NOW?		
WHAT FACTS DO WE CURRENTLY KNOW?	**WHAT DO WE CURRENTLY NOT KNOW?**	**HOW MIGHT THIS RISK IMPACT OUR ORGANIZATION?**
HOW FAST IS IT MOVING?	**WHAT SEEMS TO BE DRIVING THIS RISK?**	
WHAT DATA CAN WE TRACK TO MONITOR THIS RISK?		
WHAT RESPONSES DO WE HAVE IN PLACE?		**WHAT ELSE SHOULD WE CONSIDER?**

[27] Beasley, Mark and Jeff Lovern 2020.

APPENDIX R: ERM PROCESS PLANNING TEMPLATE

GUIDING PURPOSE	*Why are we implementing ERM? What do we aim to achieve? What benefits are we hoping to see?*
MOST CRITICAL ELEMENTS OF THE ERM PROCESS FOR OUR ORGANIZATION	*Which elements of the ERM framework are most important for our objectives?*
APPROACH FOR ADAPTING ERM PRINCIPLES TO OUR ORGANIZATIONAL CULTURE AND NEEDS	*How can we integrate ERM into our existing processes most effectively? Will we form a new risk council or use an existing forum for risk discussion? How will we train risk owners? How will we include ERM into budgeting and strategic planning? How will we engage our board of directors?*
PLAN FOR INCREMENTALLY INCREASING THE VALUE OF ERM TO OUR ORGANIZATION	*How and when will we expand ERM to increase the value it provides our organization?*

ABOUT THE AUTHOR

Amy Wares is a consultant with 20 years' experience in the social sector. She served as Research Director at the Social Progress Imperative, a Washington, DC-based non-profit organization committed to supporting data-driven advocacy, and Senior Competitiveness Advisor at the U.S. Agency for International Development. She holds a Master of Business Administration degree from Harvard Business School and a Master of Accounting degree from NC State University.

AWARES@NCSU.EDU

ABOUT THE ERM INITIATIVE

NC STATE Poole College of Management
Enterprise Risk Management Initiative

The ERM Initiative is an internationally recognized thought leadership initiative in the Poole College of Management at NC State University. The ERM Initiative seeks to advance ERM knowledge and practices to assist leaders of organization with the integration of risk insights with strategic planning and corporate governance. Faculty in the ERM Initiative frequently work with boards of directors and senior management teams helping them link ERM to strategy and governance, and the ERM Initiative's website contains an ERM Library with abstracts of over 600 research studies, articles, benchmarking surveys, and interviews of ERM professionals.

WWW.ERM.NCSU.EDU

ABOUT GRF CPAS & ADVISORS

GRF CPAs & Advisors' legacy is helping nonprofit organizations and associations of all descriptions achieve new heights through compliance, financial stability, and increased accountability and transparency. The firm provides audit, tax, and advisory services to over 600 nonprofit organizations and associations annually, to help clients stay focused on their mission and reach their financial goals.

grf CPAs & ADVISORS

WWW.GRFCPA.COM