Best Practices in Enterprise Risk Management

A look at how organizations are utilizing Enterprise Risk Management (ERM) best practices to increase efficiency, plan for the future, and achieve strategic objectives

grf

CPAs & ADVISORS

Contents

About GRF CPAs & Advisors

Small-Firm Feel, World-Class Expertise

For 39 years, our full-service accounting firm has provided a wide range of audit, tax and financial solutions. We're headquartered in the Washington, DC metro area with locations in Baltimore and New York, but we work with individuals and organizations of all sizes throughout the world.

GRF CPAs & Advisors' (GRF) expert team has decades of experience helping our clients meet their financial goals. We excel at helping our clients grow and reach their best financial position, which is why we have a robust client base of nonprofit organizations, corporate and business entities, and individuals.

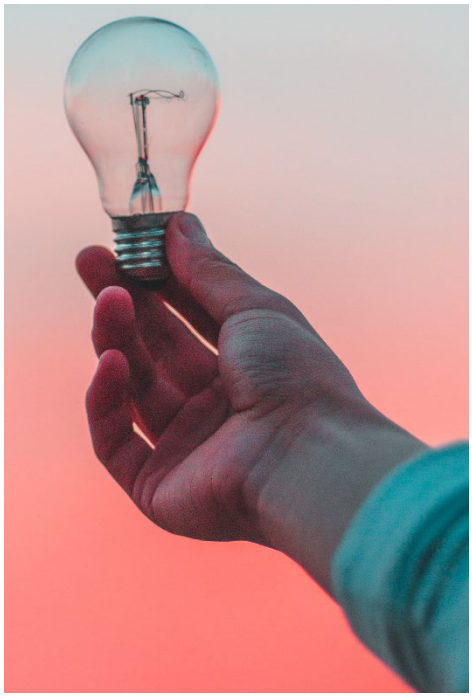
- Traditional Audit & Tax Services
- Enterprise Risk Management & Strategic Risk Identification
- Cybersecurity, Third Party, Disaster Recovery & Privacy Risk
- Internal Audit & International Site Visits
- Fraud & Anti-corruption Risk Management
- Outsourced Accounting & CFO Services

ERM and Nonprofit Organizations

Why Organizations are Thriving with ERM

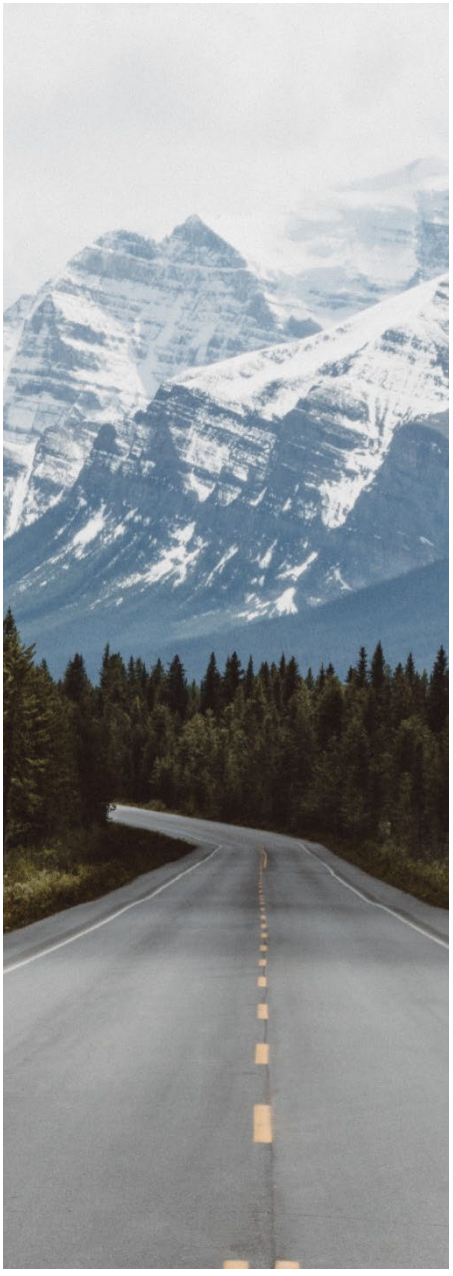
For years, organizations have taken a siloed approach to risk management, focusing on areas like cybersecurity. More are now widening their nets, using ERM to ensure unexpected dangers don't derail their organization. When it comes to risk management, some may think of areas like IT, investment risk management, or risk events that can be covered by insurance, but these are just silos, or pockets, of risk. An increasing number of organizations have embraced ERM, which is a structured and continuous process designed to provide an organization's board and senior leaders a strategic perspective of risks so that they can be managed proactively.

Short- and long-term benefits to implementing ERM include prioritizing limited resources, making timely decisions, accomplishing strategic objectives, integrating varying views of risk management (i.e., eliminate silos), increasing member and stakeholder confidence, enhancing governance, and aligning strategy and culture. In ERM, organizations conduct a risk-rating analysis, where they identify and evaluate all risks to achieving the their objectives. This builds a "risk universe." To facilitate the risk evaluation process, organizations can use risk surveys, risk workshops, interviews, past risk events, and industry risk events.



ERM and Nonprofit Organizations

Why Organizations are Thriving with ERM (continued)



To implement ERM, organizations should begin by securing buy-in and approval from the board and then designating a champion or committee dedicated to and responsible for risk mitigation. Logically, a growing number of chief financial officers are leading ERM initiatives for their organizations since most have already been designated to oversee financial, IT, and HR risks. Many organizations are also instituting internal risk councils consisting of executive management and "risk owners," such as representatives from HR, IT, marketing, and so forth.

With ERM, the risks with the highest 'likelihood' and 'impact' score are those the board should be monitoring. This helps the organization focus on the risks that truly impact the organization rather than a single stakeholder's view of priorities.

Although managing risk is a serious endeavor, there is no right or wrong way to formalize ERM. You can start simply with an assessment of risks and progress to more sophisticated models of risk management as your organization grows and evolves.

Report Process

In order to assemble the Best Practices in ERM report, GRF CPAs and Advisors performed the following procedures:

- Utilized our extensive knowledge of ERM across the nonprofit and association industry;
- Held nonprofit specific workshops to identify the policies and procedures utilized by organizations throughout the world to administer effective ERM;
- Conducted interviews with individuals leading ERM initiatives at organizations across multiple industries; and

- Reviewed best practices issued by the International Organization for Standardization (ISO), the Committee of Sponsoring Organizations of the Treadway Commission (COSO), NC States ERM initiative and other respected industry resources.

Critical Success Factors for ERM

1 BOARD ADVOCACY FOR THE ERM PROGRAM

2 ALIGNMENT OF ERM WITH STRATEGY

3 ACCOUNTABILITY AND TRANSPARENCY

Board Advocacy

Board and executive leadership support for the ERM initiative is critical to the success of the program. This was attained through various measures:

- Implementing Board training on risk management and education on ERM initiatives, which encourages active Board engagement in risk management
    - In some instances, Risk Officers partnered with various Board members, one at a time to educate them on risk management. This resulted in a cascading effect where the entire Board learned risk intelligence through the process
    - Consistent, periodic reporting to the Board over ongoing risk mitigation efforts and emerging risks
- Conducting annual **governance satisfaction surveys** with the Board and upper management requesting feedback on overall satisfaction, need for training, reporting formats, etc.

Critical Success Factors for ERM

Alignment of ERM with Strategy

In a historical context, it typically has not been a compliance incident or operational breakdown that has caused organizations to collapse. Rather, organizational breakdown can be tied to strategic failures related to reputation, employee misalignment, brand management, cultural barriers, and communication missteps, to name a few examples. Strategy is the driving force of decision-making, budgeting, and the determination of critical mission goals. Accordingly, leading teams are working to align ERM with strategic objectives in order to be effective in identifying the organizations most critical risks.

- Risk identification should be tailored to identify short-term and long-term strategic objectives of the organization, as well as the effect of potential risks that may arise in the next 1-3 years

- **Questions to Ask**
  - Which risks or opportunities will emerge?
  - How will they be managed?

Alignment of ERM with Strategy (continued)

For organizations that were not able to align ERM with the strategy department, the ERM function took a strategic approach to risk management. Examples are as follows:

- Used strategy as reference point for interviews and surveys
- Focused on strategic initiatives to gain most useful insights
- Refreshed the risk register and prioritization based on strategic perspective. Presented top risks with reference to strategic objectives or strategic initiatives

TOP RISKS	STRATEGIC INITIATIVE #1	STRATEGIC INITIATIVE #2	STRATEGIC INITIATIVE #3	STRATEGIC INITIATIVE #4	STRATEGIC INITIATIVE #5
Risk #1	X	X			
Risk #2				X	
Risk #3	X				
Risk #4	X	X	X	X	X
Risk #5	X				
Risk #6		X		X	
Risk #7	X		X		
Risk #8			X		
Risk #9		X			
Risk #10	X				

Source: NC State ERM Initiative

Critical Success Factors for ERM

Alignment of ERM with Strategy (continued)

Example: Five Key Questions to Ask Regarding Strategic Initiatives	
1	What is the business objective; who is the owner?
2	Which risks does the strategy present: Regulatory? Reputation? Customer? Alignment?
3	What are your mitigation strategies?
4	What are your contingency plans if risks occur or circumstances change?
5	How will you monitor and re-assess strategy?

Critical Success Factors for ERM

Accountability and Transparency

The goal of ERM is to establish a sustainable and integrated risk culture that supports and aligns with strategic objectives and encourages the attraction and retention of employees. This requires accountability and transparency on the part of the Board, its subcommittees, and the organizations' employees. This includes clear designation of responsibilities and consistent reporting to allow for all parties to be informed and up-to-date on risk management efforts. In leading ERM organizations the following are commonalities:

- The risk management duties are added to council members' (and beyond) respective job descriptions. The annual employee evaluation process considers adequacy and quality of participation on the Risk Council and/or related risk management duties
- Ongoing educational campaigns are taking place:
    - **Onboarding and consistent training**
    - **Internal marketing campaigns (i.e. brochures, email blasts, newsletters focused on risk)**
- Risk owners report on the status of risks themselves instead of the risk liaison or ERM leader. This aids in ownership, accountability and transparency of highly effective and successful ERM teams. The risk owner can delegate risk mitigation to multiple committees or persons, but the owner is ultimately responsible for the individual risk/task assigned

Resourcing and Structuring an Effective ERM Program

Organizational Accountability and Reporting Structure for ERM

Organizational accountability and reporting structure is typically broken down as follows:

ROLE	RESPONSIBILITY
Board of Directors/ Audit Committee	Responsible for risk management oversight and approving the risk management strategy. Monitor and review risk register.
President/CEO/CFO/ General Counsel/ Internal audit	Champion of the risk management process and ensures risks are managed effectively, holding managers accountable.
ERM Committee/ Risk Council	Develops the risk management strategy and supporting framework. Executes risk management objectives. Reports to the "President/CEO" on the effectiveness of the strategy and the enterprise risk register. Oversees administration of the ERM program and policy.
Chief Risk Officer/Risk Coordinator/Facilitator/ ERM Liaison	Acts as the lead risk ERM contact and assists in facilitating the process. Has expertise in ERM and is often Chair of the risk council
Risk Owner(s)	Serves as a Subject Matter Expert (SME) on the risk(s) issue. • Assesses risk exposure, causes and consequences • Develops and coordinates the implementation of mitigation activities and controls in accordance with risk action plan • Monitors related risk indicators and related risk events • Maintains risk documentation required by ERM • Owns and reports out on risk mitigation status
Risk Team/ Subcommittees	Individuals / committees assigned to assist in the mitigation plans headed by the risk owner
Employees	Manages risk effectively in their roles and reports risks to management.

In leading ERM programs, the ERM council should report directly to the Board of Directors and CEO. This ensures that the risk function is given proper visibility in the organization and does not get lost within the finance function or another department.

There is increasing discussion about having ERM report into the strategy function, although there have been minimal examples of this in current practice. Instead, CEOs are working to have the strategy and ERM cycles converge over time to produce the most effective results.

Resourcing and Structuring an Effective ERM Program

Employee Dedication and Participation

- Number of full time employees dedicated to ERM facilitation ranged from 1.5 to 3. Chief Risk Officer (or equivalent position) fully devoted to enterprise risk management was rare among interviewees. Most organizations pushed duties down to risk owners and aligned job descriptions accordingly
- Risk Councils made up of cross functional representatives typically assume the role as the global umbrella governance body. These entities properly assist with the management of key holistic risks and opportunities that align with the organization's strategic goals and objectives

Risk Awareness Training

- In order to enhance the effectiveness of the ERM Program, an organization's risk education campaign is crucial for all levels of management, including the Board. Approximately 70% of interviewees established some type of onboarding and ongoing training campaign specific to risk
- Participants agreed that educating the organization on risk management expectations produced an improvement in:
  - Information turn-around
  - Meeting efficiency
  - Accuracy of risk data and risk evaluation
  - Organization members (both the Board and staff) understanding the strategic value of risk management
  - Overall positive risk culture

Governance, Risk and Compliance (GRC) Tools

GRC tools are a rising technology that organizations are utilizing to help manage risk

Most leading ERM teams interviewed have found keeping it "simple" a priority and that a GRC tool would add minimal value to the ERM cycle. Benefits could be gained in continuous monitoring and data visualization which is often pushed down to individual risk owners to determine mitigation, monitoring and reporting techniques.

- Leading ERM teams most commonly use Microsoft Office (**Excel, Word, and Access**) in place of a formal GRC tool
  - Risk registries and on-going mitigation activities are maintained in excel spreadsheets and reports formatted in word or PowerPoint documents
- There are various online GRC tools that provide basic functionality that can help to organize risks, push tasks down to risk owners, and track progress. Some of the advantages of these online tools are that they:
  - Provide some basic GRC functionality for free
  - Assist in the flow down of risk responsibility by assigning tasks to risk owners to help solidify their respective responsibilities and duties
  - Help to reduce some of the manual processes currently undertaken by the ERM facilitator with automated surveys, risk ranking, and reporting

Governance, Risk and Compliance (GRC) Tools

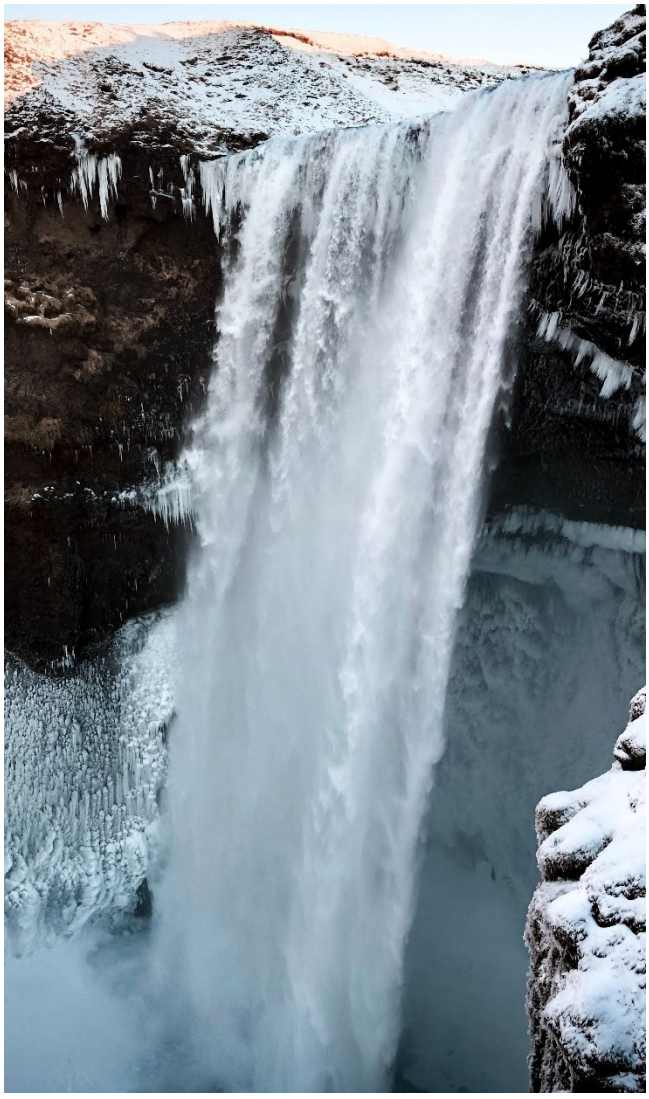
GRC tools are a rising technology that organizations are utilizing to help manage risk (continued)

- There are also more comprehensive solutions utilized by organizations due to their compliance requirements of the heavily regulated industries in which they operate. These tools can provide:
  - IT & security management
  - Enterprise and operational risk management
  - Regulatory & corporate compliance management
  - Audit management
  - Business resiliency
  - Third-party governance

ERM Process

Like many aspects of ERM, risk assessment methodologies are not "one size fits all," however, practices found in the majority of the leading ERM programs were as follows:

- Most used anonymous surveys to gather assessment information
- Interviewed all the top levels of management
- Assessed both impact and likelihood using 5-point scales
- Identified top 5 to 10 risks (aggregated across the entire organization)



ERM Process

Practices (continued)

- Majority of organizations' ERM process was annual
    - A higher frequency was seen as too resource heavy and anything less was perceived as not valuable
    - Average reporting structure was quarterly to leadership and annually to the Board
- In some instances, organizations maintain separate risk cycles for reporting on existing risks vs. emerging risks
    - Emerging risk cycle was separate from the annual process of reevaluating existing risks. The results of the emerging risk cycle then flowed into the annual risk reevaluation cycle

Capturing Risk Data and Key Elements of the Risk Assessment Process

Prior to assessing risks, leading organizations develop and/or review the "risk register" and/or "risk universe" that lists all identified risks facing an organization

Defining these risks accurately enhances the risk assessment process as the ERM liaison moves between different stakeholders – board, management, and those tasked with risk management. This is crucial to the development of a complete range of risk survey data and helps to prioritize risk response efforts.

Other common risk elements in capturing risk data for leading ERM teams are listed to the right.

Assessment Methodology
Likelihood x Impact (most common)
Likelihood + Impact
Likelihood + Impact – Preparedness (most public companies)
Forced Ranking (No dimensions used) (not common)

Dimensions (example provided)
Likelihood
Impact
Velocity (not common)
Persistence (not common)
Preparedness (mostly public companies)

Capturing Risk Data and Key Elements of the Risk Assessment Process

Risk Universe (Continued)

Assessment Scales	Execution
1. 3-Point	Assessments based on interviews of top leadership and surveys of a sample of leaders at lower levels.
2. 5-Point	

Data Retention

Having a centralized source of risk information or risk register is key to leading ERM teams. Many organizations utilize Microsoft Office Suite to inventory their "risk universe." This is used even in cases where organizations have implemented established GRC systems. Many systems export to Word or Excel for ease of manipulating data and performing data analytics. Here is a list of the metadata that could be included in a risk register:

• Name	• Velocity (not often used)
• Definition	• Current Mitigation/future mitigation
• Status (active, inactive)	• Risk response (avoid, transfer, mitigate and accept)
• Cause	• Strategy
• Effect	• Owner
• Impact	• Risk score
• Likelihood	• Applicable departments
• Outlook (not often used)	

Capturing Risk Data and Key Elements of the Risk Assessment Process

Key Risk Indicators and Key Performance Indicators

- Key Risk Indicators (KRIs) help to predict or measure risks against a defined risk threshold. When triggered, these indicators provide alerts to the appropriate personnel in order to take corrective action before a risk event takes place. Utilization of KRIs assists with:
    - Continuous monitoring of controls
    - Risk assessment and measurement
    - Regulatory compliance

- Key Performance Indicators (KPIs) allow risk practitioners to measure the operating effectiveness of a particular process/control as it relates to its risk management objective. Achievement of KPIs can indicate that controls are operating effectively and/or whether or not mitigation efforts have been successful. Utilization of KPIs assists with:
    - Benchmarking
    - Determining effectiveness of controls/processes and mitigation efforts
    - Assessment of overall success of ERM Program

KRIs and KPIs can be maintained in the risk register with the risks to which they apply. They should be monitored and reviewed along with the risk as part of the normal ERM process.

Capturing Risk Data and Key Elements of the Risk Assessment Process

Example Risk Strategies

Leading ERM organizations use a combination of strategies in responding to risks. Below is an example excerpt from a policy manual of an international organization.

STRATEGY	AVOID	MITIGATE	ACCEPT	TRANSFER
Expected Risk Impact	Reduce to $0	% or $ amount less than status quo	Status quo	% or $ amount less than status quo
Upfront Investment	Up to status quo	> $0, < status quo	$0	> $0, < status quo
Risk Identification	A strategy to eliminate the possibility of a negative impact by exiting any activity that would expose the organization/ project to a loss	A strategy to reduce the probability and/or negative impact of a risk to an acceptable level	A strategy to maintain the negative impact and probability of a risk within an acceptable level	A strategy to share the negative impact of a risk event in order to reduce the risk to an acceptable level
Sample Risk Response Plan	• Divest by existing market • Stop specific activities • Transfer all of the risk • Insure against the risk • Develop contingency plans	• Disperse/diversify • Manage risk through internal processes (e.g. training, control, SOPs)	• Set specific risk thresholds and monitor risk to ensure it does not reach unacceptable levels • Develop contingency plans	• Obtain insurance policy to cover potential losses • Enter into a strategic partnership • Develop contingency plans

Capturing Risk Data and Key Elements of the Risk Assessment Process

Example Risk Mitigation Template

RISK STATEMENT			DATES	
Cause			Status	**Open**
Risk			Opened	
Impact			Approved	
Management effectiveness score			Closed	

RISK CLASSIFICATION			HANDLING PLAN		
Executive Owner			Description of Task	Owner	Status
Risk Manager					
Handling Approach	**Mitigate**				
INHERENT RISK RATING	**CURRENT**	**TARGET**			
Impact Rating (1-5)					
Likelihood Rating (1-5)					
Risk Score					
INTERRELATED TOP ENTERPRISE RISKS					

Capturing Risk Data and Key Elements of the Risk Assessment Process

Scoring Risks

There is a wide variety of practices around compiling all of the ratings into an overall "score." The most common risk scoring methodology used focuses primarily on multiplying likelihood times impact, calculating the result as a score, and plotting it on a heat map. See examples provided below.

Example Likelihood Scale

	1 RARE	2 UNLIKELY	3 POSSIBLE	4 LIKELY	5 ALMOST CERTAIN
Description	The event may occur only in exceptional circumstances	This event could occur at some time	The event should occur at some time	The event will probably occur in most circumstances	The event is expected to occur in most circumstances
Frequency	Less than once in 10 years	Will occur once every 5 to 10 years	Will occur once every 1 to 5 years	Will occur once every year	Will occur more than once a year

Capturing Risk Data and Key Elements of the Risk Assessment Process

Example Impact Scale

	1 INSIGNIFICANT	2 MINOR	3 MODERATE	4 MAJOR	5 CATASTROPHIC
Injury	No injuries	Employee loss time injury	A single event involving serious injury and/or multiple employee lost time injury	A single event involving death and/ or multiple injuries as a direct result of ORG negligence and/or single employee death or multiple injuries	Two or more events involving death and/or multiple injuries as a direct result of ORG negligence and/or multiple employee deaths
Financial	Loss of assets or revenue less 4%	Loss of assets or revenue of 5% to 9%	Loss of assets or revenue of 10% to 24%	Loss of assets or revenue of 25% to 49%	Loss of assets or revenue exceeding 50%
Media / Reputation	Local newspaper headline (not front page)	Local television/ newspaper headlines (front page)	State television/ newspaper headlines	In-country television/ newspaper headlines	Global television/ newspaper headlines
Compliance		Regulatory Inquiry	Regulatory Investigation	Government Investigation	Global Agency Investigation
Operational	Minor service disruption	Business interruption over 12 hours	Total service cessation for a period of 1 to 2 days and subsequent interruption over several days	Total service cessation for a period of 2 to 3 days and subsequent interruption over several weeks	Total service cessation for more than 1 week

Capturing Risk Data and Key Elements of the Risk Assessment Process

Example Risk Matrix / Heat Map

With ERM, the risks with the highest "likelihood" and "impact" score are ones the board should be monitoring, for example in the chart anything in red or orange color coding. This helps the organization focus on the risks that truly affect the organization, rather than a single stakeholder's view of priorities. Ultimately, ERM is based on board and management's expectations regarding acceptable levels of risk (i.e., the organization's risk appetite) for those that directly affect the organization's strategic goals and objectives.

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

Summary and Next Steps

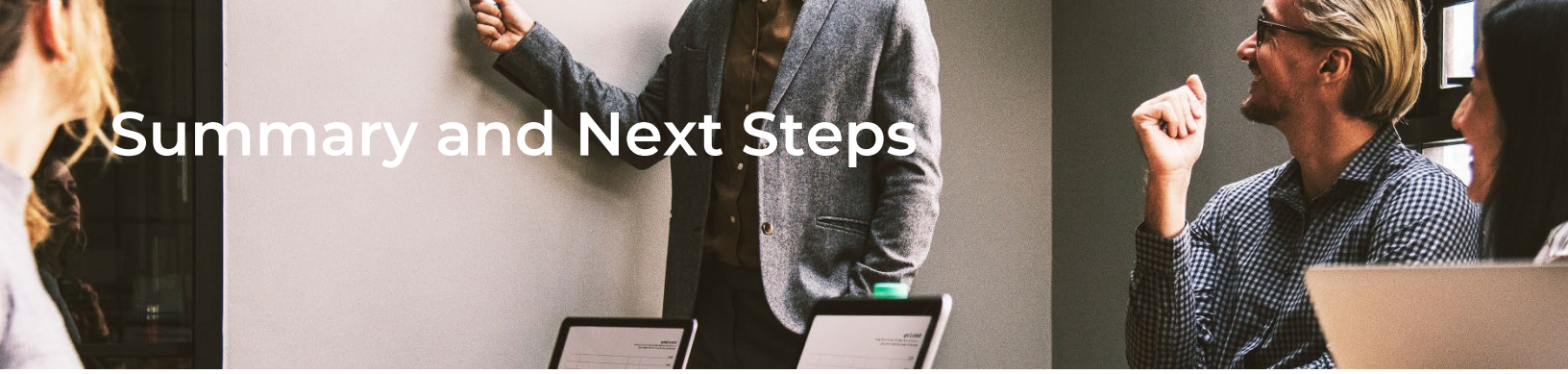
In Summary

There is no right or wrong way to formalize ERM. Organizations should educate the board, management, and staff on ERM goals and objectives and begin with what makes the most sense within their organization. You can start simply with an assessment of risks and progress to more sophisticated models of risk management as your organization grows and evolves.

Final Take Away

The best ERM programs keep risk management simple by focusing on the following:

- Understanding the organization's context (industry, strategy, culture, structure, processes, system, and people)
- Identifying the organization's risk universe through surveys, workshops, industry trends, and so forth
- Using a logical method to rank risk (likelihood and impact scales)
- Deciding who is responsible for actions, whether a risk council, ERM champion, or risk owners
- Monitoring and learning, including board reporting and cultivating a risk aware culture



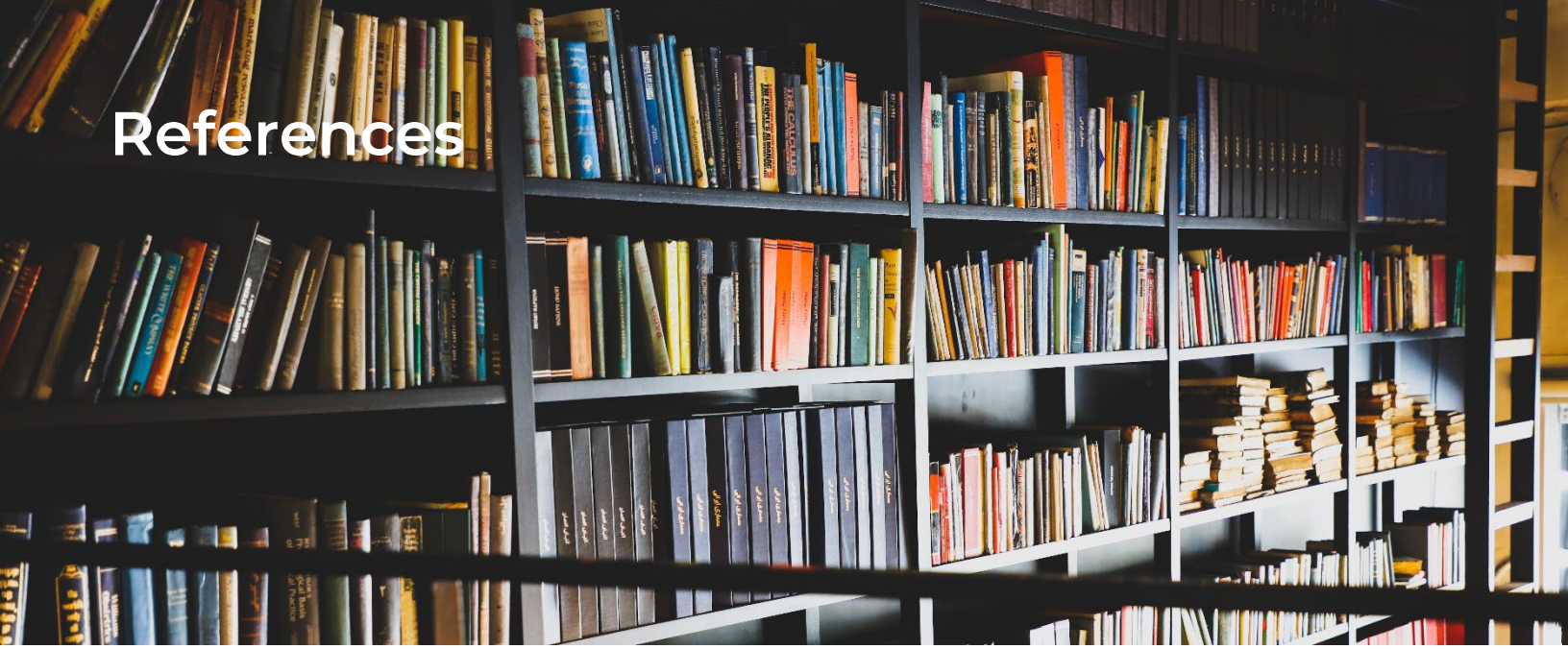
Summary and Next Steps

Next Steps

If not already implemented, the organization should determine who leads and participates in the risk assessments, what action steps to include, how best to resolve conflicts, and what documentation and reporting are preferred. Incorporating technical experts and consultants in the process helps develop sound ERM procedures, mitigation plans, and effective board reporting tools.

For Guidance

- Consult frameworks such as the Committee of Sponsoring Organizations (COSO) ERM – Integrated Framework and the International Organization for Standardization (ISO 31000) ERM. (add links)
- Attend ERM workshops and Seminars (add link to our ERM Event Page with NC State)
- Engage ERM practitioners to assist on your journey



References

1. https://erm.ncsu.edu/az/erm/i/chan/library/2019_Current_Report_on_State_of_Risk_Oversight.pdf

2. https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

3. https://www.iso.org/iso-31000-risk-management.html

4. https://www.smartsheet.com/comprehensive-project-management-guide-everything-raci

Who We Are

Risk & Advisory Services

GRF's Risk & Advisory Services advisors collaborate with management, board members and staff to help organizations develop a holistic Enterprise Risk Management framework, connect strategy to risk and improve the processes around risk governance.

We provide consulting to support our clients' most challenging business decisions. Our deep bench of expert CPAs and advisors provide guidance to clients through a wide range of business and financial issues. Visit our website at https://www.grfcpa.com/.

Melissa Musser,

CPA, CITP, CISA

Risk & Advisory Services Principal

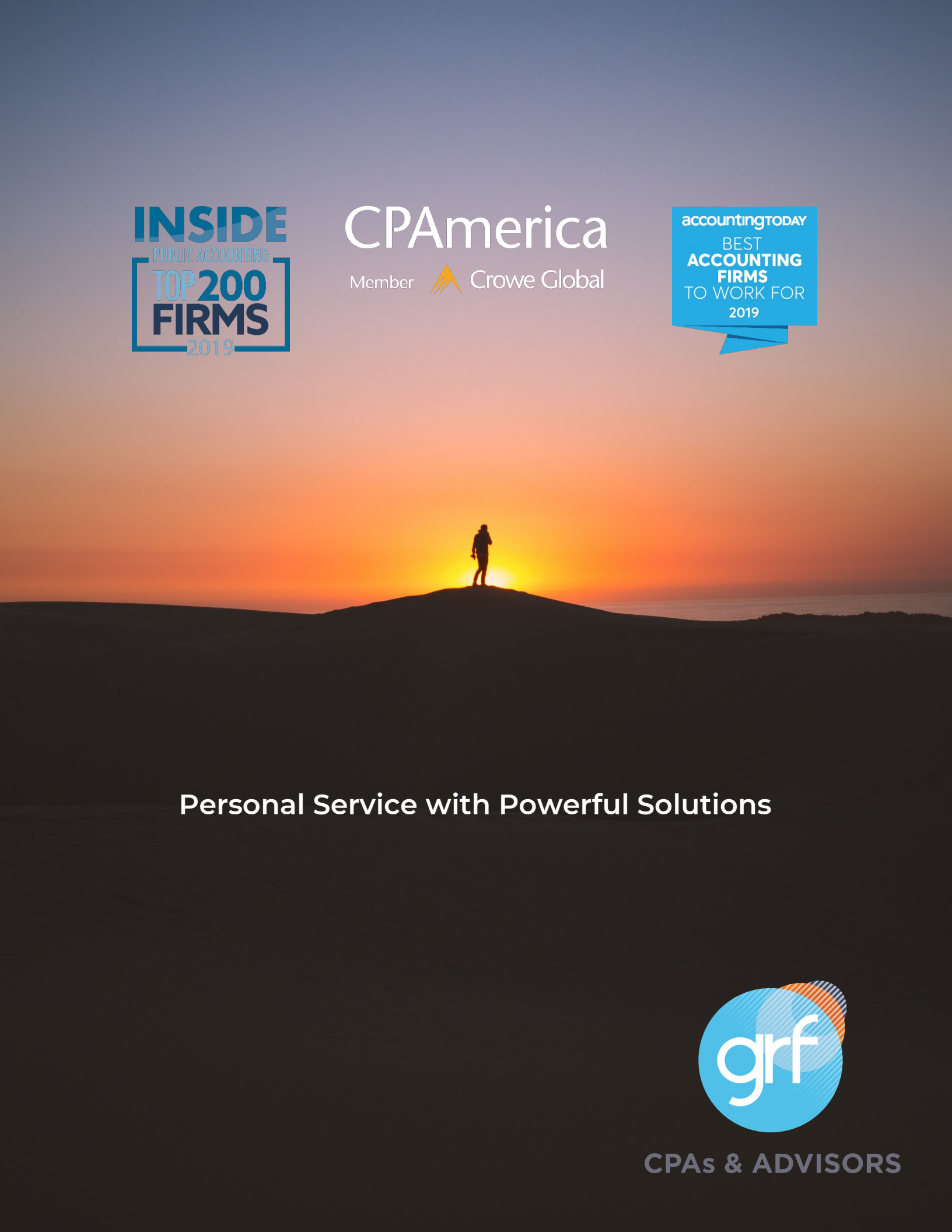
mmusser@grfcpa.com

Mac Lillard, CPA, CFE, CISA,

CRISC, CITP, PCP

Risk & Advisory Services Supervisor

mlillard@grfcpa.com


INSIDE
PUBLIC ACCOUNTING
TOP 200
FIRMS
2019
CPAmerica
Member
Crowe Global
accountingTODAY
BEST
ACCOUNTING
FIRMS
TO WORK FOR
2019
Personal Service with Powerful Solutions
grf
CPAs & ADVISORS