CPAs & ADVISORS

Enterprise Risk Management (ERM)

The Handbook for Association Board Members

CPAs & ADVISORS

Enterprise Risk Management (ERM)

The Handbook for Association Board Members

Index

Dear Association Board Member,

This handbook on Enterprise Risk Management (ERM) has been crafted to offer you a thorough understanding of ERM principles and practices, highlighting the essential role board members play in risk oversight for their association. Our objective is to provide you with the insights and tools needed to effectively navigate the complexities of risk oversight.

Associations today face numerous risks that could impact their objectives, reputation, and long-term sustainability. As custodians of your organization's future, you have a fiduciary duty to ensure resilience and success. Effective ERM enables board members to proactively identify and address risks, thereby enhancing the ability to seize opportunities and address challenges. Integrating ERM into decision-making processes helps cultivate a risk-aware culture, strengthen governance practices, and bolster stakeholder confidence. ERM offers a systematic approach to understanding and managing risks holistically, allowing board members to make informed strategic decisions aligned with the association's mission and goals.

Whether you are a seasoned board member aiming to refine your understanding of ERM or new to the board and seeking a solid foundation in risk management, this handbook will serve as an invaluable resource throughout your journey. Each section delves into the nuances of ERM and provides practical insights and tools to empower you in your role. Let us embark on this crucial journey together, reinforcing risk governance and advancing the success of associations everywhere.

Sincerely,

Melissa Musser, CPA, CITP, CISA, Partner

Susan Colladay, CPA, Partner

Joseph M. Pugh*, CCEP, CFE, RIMS-CRMP, CRMA, CDPSE, Senior Director, ERM, AARP

**Mr. Pugh is writing on his own behalf and the ideas and information shared do not represent those of his employer.*

Topic 1:

Understanding Enterprise Risk Management

In today's fast-paced and often unpredictable environment, effective risk management has become more crucial than ever for associations. The growing complexity of operations, coupled with shifting stakeholder expectations, underscores the need for a structured approach to managing risks. As a board member, your fiduciary duty and role is to provide oversight of the association, and this includes risk oversight.

Consider the following questions:

- How frequently are the association's mission critical risks presented to the board? Annually, quarterly or on a different cadence?
- What methodology is used to identify and evaluate these risks?
- Are your board minutes properly documenting discussions about critical risks?
- Is risk oversight delegated to a specific board committee? If so, which committee, and is this delegation clearly outlined in the committee's charter or bylaws?
- How would the board define a "significant risk"?

It is your responsibility to ensure that robust risk oversight and governance practices are in place. Given the complexities of today's world, many associations are adopting Enterprise Risk Management (ERM) frameworks to effectively fulfill these critical oversight duties. ERM provides a comprehensive approach to managing risks, helping boards meet their responsibilities and navigate an increasingly challenging landscape.

Why ERM is Essential

Comprehensive Risk Understanding - Traditional risk management often focuses on isolated risks—such as IT security breaches or financial mismanagement—without considering their broader implications. Enterprise Risk Management (ERM) offers a holistic view, integrating all potential risks across the organization into a unified framework. This comprehensive approach helps board members understand and connect the dots on how different risks interconnect and impact the association's strategy.

Strategic Decision-Making - ERM empowers board members to make informed strategic decisions by providing a clear picture of the organization's risk landscape. By identifying, assessing, and prioritizing risks systematically, ERM enables you to align risk management with strategic objectives, ensuring that risk considerations are an integral part of your decision-making process.

Enhanced Resilience - Incorporating ERM into your governance practice strengthens the organization's resilience against unforeseen events. It equips board members with tools to anticipate potential challenges, develop effective mitigation strategies, and swiftly adapt to changing circumstances. This proactive approach enhances the association's ability to navigate uncertainties and sustain its operations.

Improved Governance and Accountability - Effective ERM fosters stronger governance by clarifying the roles and responsibilities related to risk management. ERM establishes a framework for accountability, ensuring that risk oversight is embedded into the organizational structure and that risks are managed transparently and systematically.

Increased Stakeholder Confidence - Stakeholders—including members, donors, and regulatory bodies—expect associations to manage risks responsibly. A robust ERM framework demonstrates a commitment to sound governance and responsible risk management, enhancing trust and confidence among stakeholders. This, in turn, supports the organization's reputation and credibility.

Proactive Risk Mitigation - ERM focuses on identifying and addressing risks before they escalate into major issues. By systematically evaluating risks and implementing mitigation strategies, ERM helps prevent potential threats from derailing your association's objectives. This proactive stance reduces the likelihood and impact of adverse events, protecting the organization's interests.

Key Components of an ERM Framework

An effective ERM framework is essential for associations seeking to quickly address uncertainties and capitalize on opportunities while safeguarding their assets. The core components of an ERM framework often draw from established guidance and standards, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM and the International Organization for Standardization (ISO) Risk Management. The key elements of the ERM process are:

Culture and Leadership: The organizational culture needs to support ERM. The tone set by senior leadership and the Board of Directors provides the foundation that underpins all elements of the ERM process.

Linking Risk and Strategy: The ERM process begins with developing a shared understanding of mission, vision, and strategic objectives to identify most critical risks.

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

Risk Assessment: Once a list of risks is compiled, prioritize the most critical risks based on how likely they are to occur, and potential magnitude of impact should they occur.

Risk Response: Depending on the results of the risk assessment, risks may be accepted or managed to affect the likelihood they occur and/or impact should they occur.

Monitoring and Communication: The ERM process recognizes the importance of monitoring changes to current and emerging risks and ensuring that the right people receive information about key risks in a timely manner.

Customized Association ERM Playbook

When an organization aims to implement ERM, it is essential to establish clear definitions, context, and expectations through a formal policy and procedure document tailored to the association's needs. This is often achieved through an ERM Playbook, which incorporates the association's strategic goals and outlines roles, responsibilities, and authorities.

The ERM Playbook should be a dynamic, living document that evolves over time to remain a useful resource in managing the association's ERM processes. In the upcoming sections, we will highlight the key elements to include in your association's ERM Playbook to ensure it effectively supports your risk management efforts.

Topic 2:

Roles and Responsibilities of Association Board Members in ERM

The Board's Role in Risk Oversight

Effective risk oversight is a critical responsibility of an association's board of directors. The board plays a vital role in setting the tone for risk management, establishing the association's risk appetite, and ensuring that appropriate risk management practices are in place. The board's role in risk oversight should include the following:

- **Establishing the Risk Governance Framework:** The board is responsible for approving a risk governance framework, sometimes in the form of an ERM Playbook that defines the roles, responsibilities, and structures for risk management within the association. This includes setting clear risk management policies, guidelines, and reporting mechanisms.

- **Defining Risk Appetite and Tolerance:** The board, in collaboration with senior management, should articulate the association's risk appetite and tolerance levels. This involves determining the level of risk the association is willing to accept in pursuit of its objectives and establishing boundaries for risk-taking activities.

- **Monitoring and Assessing Risks:** The board should regularly monitor and assess the association's risk profile. This includes reviewing risk reports, dashboards, key risk indicators (KRIs), and other relevant information to gain a comprehensive understanding of the critical risks facing the association. It is important to note that the board should have the necessary information to discharge its risk management oversight responsibilities and it the board feels they do not have the appropriate information, management should address.

Aligning Risk Management with Strategy: The board plays a crucial role in ensuring that risk management is integrated into the association's strategic planning process. It should review and approve the association's strategic objectives, considering the risks associated with each objective and evaluating the effectiveness of risk mitigation strategies.

Responsibilities of Individual Board Members

Each board member has a unique set of responsibilities when it comes to risk management. While the board as a whole is responsible for risk oversight, individual board members also have specific roles to play which may include:

- **Active Participation in Risk Discussions:** Board members should actively participate in discussions related to risk management. This involves asking questions, seeking clarification, and providing input to ensure that risks are adequately addressed and managed.
- **Understanding the Association's Risk Profile:** Board members should have a comprehensive understanding of the association's risk profile, including the key risks it faces and their potential impact on the association's objectives. This understanding enables board members to make informed decisions and ask pertinent risk-related questions.
- **Reviewing and Approving Risk Management Policies:** Board members should review risk management policies, guidelines, and frameworks proposed by management. This ensures that risk management practices align with the association's overall strategic direction and risk appetite.
- **Monitoring the Effectiveness of Risk Mitigation Strategies:** Board members should oversee the implementation and effectiveness of risk mitigation strategies for key risks. This includes reviewing progress reports, evaluating the adequacy of controls, and assessing the impact of risk management initiatives. When board members actively engage with risk owners during board meetings, the dynamics in terms of strategic decision-making in the boardroom can be game changing. It's important to note that the ERM lead facilitates the risk process and having the risk owner present who can speak to specific risks and their mitigation activities, sets a strong risk culture. For significant risks, it is a leading practice to seek independent assurance on key risks, which may be provided by an external third party or an internal audit department reporting directly to the board.

Board-Level Risk Committees and Structures

To support effective risk oversight, associations may establish board-level risk committees or structures. These committees are dedicated to overseeing and managing risks on behalf of the board and are typically supported by a committee charter. For many associations, this responsibility often falls within the **audit committee** if not its own committee. Associations may need to review and update their committee charter and or by-laws to confirm if the board has formally delegated this authority. See the appendix for an example of a simple risk committee charter.

- **Risk Committee Composition:** The composition of a risk committee may include board members who have diverse backgrounds, skills, and expertise relevant to the association's context and risk profile. This ensures a comprehensive perspective when addressing risks and enables the committee to make well-informed recommendations to the board. It is important to note that

this board-level committee is not to be confused with a management-level risk committee, which may be formed at the organizational level to execute and oversee the day-to-day ERM functions.

- **Responsibilities of the Risk Committee:** The risk committee is responsible for providing guidance, advice, and recommendations to the board and association management on risk-related matters. Activities include reviewing risk reports, assessing the effectiveness of risk management practices, and advising on risk mitigation strategies. The focus is on strategic oversight rather than day-to-day risk management activities, which are the purview of management-level committees.
- **Reporting to the Board:** The risk committee should regularly report its findings, recommendations, and updates to the board. These reports should provide a comprehensive view of the association's risk landscape, highlight emerging risks, and communicate the status of risk mitigation efforts. This reporting helps the board maintain a high-level understanding of the association's risk profile and ensures that significant risks are being managed appropriately.
- **Integration with Other Board Committees:** The risk committee should collaborate and coordinate with other board committees, such as the audit committee (if not included as part of the audit committee) or finance committee, to ensure a holistic approach to risk management. This integration helps avoid duplication of efforts and promotes a unified approach to risk oversight. Effective collaboration ensures that all aspects of risk, including financial, operational, and compliance risks, are considered in the decision-making process.

Management-Level Risk Committees (Risk Councils):

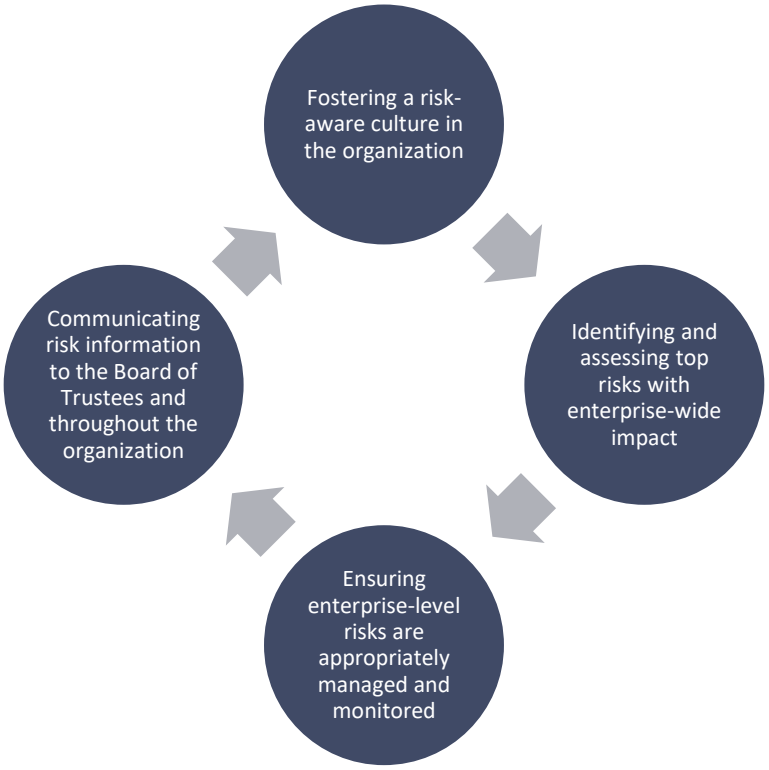
To support the board's oversight role, management-level risk committees are often established to handle the operational aspects of risk management. These committees play a critical role in the execution and day-to-day management of the ERM framework, and are sometimes referred to as Risk Councils to avoid confusion with the board level risk committees. The Risk Council should meet regularly discuss emerging risks, changes to enterprise-level risk exposures, and priorities for risk response activities.

Key components of a management-level risk committee include:

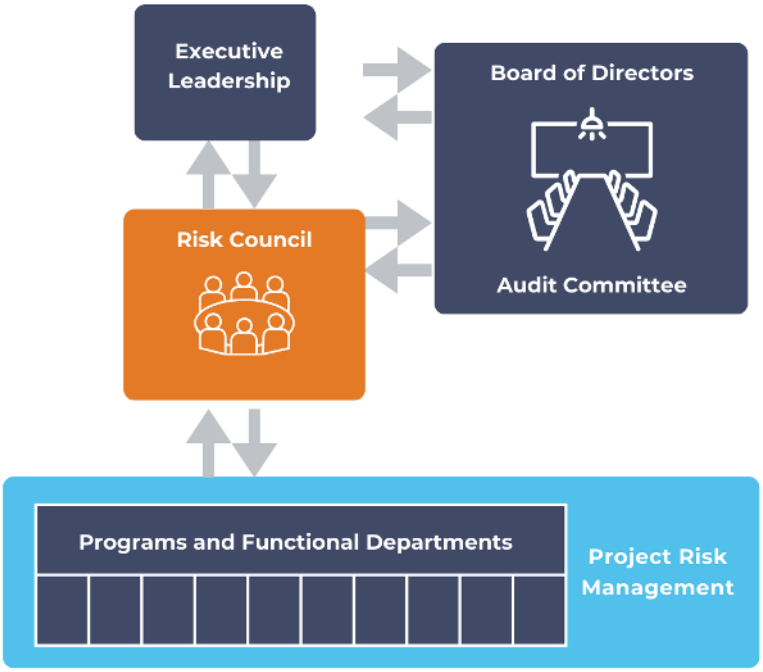
- **Composition and Structure:** Management-level risk committees are typically comprised of senior executives and risk managers from various departments within the association. These individuals bring operational insights and expertise, ensuring a thorough understanding of the association’s risk profile. They serve to spearhead the implementation of risk management strategies. The committees are often chaired by a designated ERM champion or lead at the association. ERM champions can come from a variety of backgrounds including Accounting, IT, Insurance, Internal Audit, or Legal.
- **Responsibilities:** Management-level risk committees are responsible for fostering a risk aware culture at the association. They are tasked with identifying, assessing, and managing risks on an ongoing basis and often leverage their association’s ERM Playbook to execute their duties, which can include:
  - Risk Identification and Assessment: Continuously identifying and evaluating risks that may affect the association’s operations and strategic objectives.

- Risk Mitigation: Developing and implementing risk mitigation plans, controls, and policies to manage identified risks.
- Monitoring and Reporting: Regularly monitoring risk indicators and reporting findings to the board-level risk committee. Ensuring timely and accurate risk reporting to support informed decision-making by the board.
- Communication: Communicates regularly with risk owners and provides guidance to all staff on risk management policies and procedures.

- **Governance Structure and Coordination with Board-Level Committees:** Management-level risk committees and councils should maintain open lines of communication with board-level risk committees, ensuring alignment and consistency in risk management practices. This collaboration helps bridge the gap between strategic oversight and operational execution, facilitating a comprehensive and integrated approach to risk management.



By understanding the distinct roles and responsibilities of board-level and management-level risk committees, associations can effectively manage risks at both strategic and operational levels. Establishing appropriate structures and processes for both levels enhances the association's ability to address risks comprehensively and systematically.



Topic 3:

Identifying and Assessing Risks

Risk Identification Techniques

Understanding and documenting the association's risk universe is a critical step in the ERM process. This involves systematically identifying potential risks that could impact the achievement of objectives across the association, covering key categories such as Strategic, Financial, Operational, Technology, Compliance, and Reputation.

Depending on the maturity of the ERM program, the association’s culture, as well as overall management engagement, identifying enterprise risks without duplicating existing risk management activities in other departments or teams can be challenging. One area ERM can collaborate with is Internal Audit. Often Internal Audit will have a “continuous risk assessment” process, which in most cases means they are interviewing a cross-section of roles and levels throughout the association to gain a better understanding of the risks and challenges that stakeholders/business units are facing.

Some typical questions included in a continuous risk assessment interview process might be:

1. What part of your area might land us in the Wall Street Journal if not executed well?
2. What risks threaten your business unit's priorities/goals and how are those risks managed/monitored?
3. What are you doing in your business unit from a transformation/innovation perspective and how might that generate new risks or escalate existing risks? Do you have what you need to manage these risks?
4. Is there any information you need to help better manage risks/take more strategic risks?
5. Do you see any emerging risks that may impact the association that we are not currently monitoring?
6. Have interviewees rate the following statements choosing either "often", "sometimes" or "always":
    a. I have the information I need to manage risks.
    b. My management supports taking informed, thoughtful risks.
    c. My business unit does a good job managing risks.

Partnering with Internal Audit allows ERM to cast the risk identification process more holistically across the association. It provides an opportunity to see the interview results and key risk themes from across the association - helping to inform the enterprise-level risk profile. Furthermore, leveraging information from the continuous risk assessment process allows ERM to have insight into risk culture and validate some of the most critical risks that could affect the association as a whole. Enterprise-level risks have the potential to impact the association's mission, vision, and long-term sustainability, often cutting across various functions, divisions, and locations and affecting multiple facets of the association, so the more visibility ERM has regarding risks to the association, the better risks can be identified and mitigated as appropriate.

Example Risk Categories: Categorizing risks based on common attributes provides a structured and systematic approach for identifying, managing, and monitoring risks. Categories create a common language for discussing and analyzing risks across the organization, making it easier to understand and communicate potential threats and opportunities. These categories, impact scales and other important attributes based on the associations context should be laid out in an ERM playbook or policy to help define the taxonomy used within the association.

Risk Category	
Strategic	events or circumstances that could affect the effectiveness of mission-related activities
Financial	events or circumstances that could affect financial resources or the accuracy of financial reporting
Operational	events or circumstances that could affect the day-to-day management of activities
Reputational	events or circumstances that could affect standing or credibility with external stakeholders
Legal and Compliance	events or circumstances that could affect adherence with laws, regulations, grant agreements, contracts, or other legal requirements
Safety and Security	events or circumstances that could cause harm to people or physical assets
Human Capital	events or circumstances that could affect the wellbeing, productivity, hiring, or retention employees
Information Technology	events or circumstances that could affect the processing, security, stability, capacity, performance, or resilience of information technology

To build the risk universe, there are various risk identification techniques that association can employ:

- **Objectives Based:** Focus first and foremost on the association's strategic objectives and the risks that could prevent those objectives from materializing. These objectives are often discovered well in facilitated workshops and interviews.
- **Brainstorming Sessions:** Conduct collaborative brainstorming sessions to identify risks. This technique encourages open discussion, creativity, and the exploration of various perspectives to uncover risks that may not be immediately apparent.
- **SWOT Analysis:** Strengths, Weaknesses, Opportunities, and Threats analysis helps identify internal strengths and weaknesses of the association, as well as external opportunities and threats. By focusing on the "T" component, the association can identify potential risks that could hinder the association's objectives. Linking ERM to the strategic planning cycle can be very beneficial and can help reduce redundancy and increase success in strategic planning process.
- **PESTEL Analysis:** PESTEL (Political, Economic, Social, Technological, Environmental, Legal/Regulatory) analysis offers another approach to identifying risk and opportunities that may disrupt the assumptions of the association's business strategy. This approach can pinpoint and address future strategic risks, minimize surprises, and identify and exploit opportunities. This approach is typically done in a workshop setting where participants leave with a common understanding and alignment of current and potential risk factors/key issues that could derail the association's business model.
- **Process Mapping:** Visually illustrate the association's key processes and workflows. By analyzing each step and potential decision points within the processes, board members can identify risks that may arise from process inefficiencies, bottlenecks, or inadequate controls.

- **Scenario Analysis:** Develop plausible scenarios and assess the impact of each scenario on the association. By considering multiple future scenarios, associations can gain insights into the potential risks and develop contingency plans accordingly.
- **Surveys:** Ask stakeholders to identify risks from their unique perspectives. The surveys can be flexible and designed based on the organization context. They can include open ended questions or more structured questions that can be used to rank risks. Surveys can be sent to just the risk council and or the board or can be sent to an entire organization as well as third parties. See the Appendix for more guidance on surveys and a sample risk survey for an association.

Risk Register: Developing a risk register is a cost-effective method for associations to systematically capture and document identified risks, including their potential impact and likelihood. These registers can be maintained in Excel or within a dedicated GRC (Governance, Risk, and Compliance) system. A risk register serves as a dynamic, real-time record of the organization's risk landscape, facilitating continuous tracking of risk status and mitigation efforts. It provides a foundation for transparent reporting to senior management, the Board of Trustees, and other stakeholders. By keeping risks visible, the risk register promotes a culture of risk awareness and accountability throughout the organization.

The risk register often includes the following information:

Risk ID#	Category	Risk Name	Description	Owner	Likelihood	Impact	Risk Rating	Response Plan Link	Response Status	Date Updated	Next Update	Closed Reason

Common Risks Faced by Associations

It is important to understand your Associations context (Industry, Strategy, Culture, Structure, Processes, Systems, and People). Associations operate within unique environments that expose them to risks across all facets of their operations. Identifying and understanding your context and common risks specific to associations is crucial for board members to effectively mitigate and manage potential threats. Some of the prevalent risks encountered by associations are as follows:

Governance and Compliance Risks:

Governance and compliance risks center around the association's adherence to legal, regulatory, and ethical standards. Common risks in this category include:

- **Third-Party Compliance:** Risks related to third-party vendors, partners, or contractors failing to meet compliance standards, which could impact the association's operations as well as adherence to laws and regulations.

- **Non-Compliance:** Failure to comply with applicable laws, regulations, and industry standards, which may result in fines, legal liabilities, or loss of credibility.
- **Conflicts of Interest:** Instances where personal interests of board members or stakeholders conflict with the association's objectives, potentially leading to ethical dilemmas or legal implications.
- **Anti-Trust Violations:** Associations are not allowed to fix prices or discuss fixing prices in their industry. Thus, associations must be mindful of this when the board of directors has meetings and when members have meetings.
- **Inadequate Governance Structures:** Weak governance frameworks or ineffective oversight mechanisms that undermine decision-making processes and accountability.
- **Reputational Damage:** Negative publicity or public perception due to governance failures, compliance issues, or ethical lapses, impacting stakeholder trust and organizational credibility.
- **Whistleblower Protection:** Ensuring mechanisms are in place to protect those who report unethical behavior.
- **Document Management:** Risks related to poor handling and retention of important documents and records.

Financial Risks:

Financial risks encompass threats that could impair the association's financial stability and sustainability. Key financial risks include:

- **Insufficient Funding:** Inadequate revenue streams or funding sources needed to sustain operational needs, fund strategic initiatives, or support growth objectives.
- **Mismanagement of Resources:** Poor financial management practices, including budgetary oversights, inefficient resource allocation, or inadequate financial controls.
- **Budgetary Constraints:** Inability to effectively forecast and manage expenses, leading to budget deficits, cash flow issues, or financial strain.
- **Economic Volatility:** Fluctuations in economic conditions, market trends, or funding availability that impact the association's financial health and viability.
- **Level of Operating Reserves:** Associations should use the risk assessment process in ERM to determine the top risks, assign an estimated value to those risks, and then implement a reserves policy to target the level of reserves that addresses the top risks face by the association.
- **Investment Risks:** Risks associated with the association’s investment strategies.
- **Revenue Diversification:** Risks related to over-reliance on a single revenue source.

Membership and Stakeholder Risks:

Associations depend on their members and stakeholders for support, engagement, and advocacy. Risks in this category include:

- **Member Attrition:** Loss of members due to aging population, dissatisfaction with programs offered, changing needs, or competitive offerings, all of which reduce the association’s revenue and diminish its influence.

- **Declining Engagement:** Decreased participation or involvement of members in association activities, programs, or initiatives, affecting membership retention and organizational relevance.
- **Ineffective Communication:** Challenges in effectively communicating with members and stakeholders, leading to misunderstandings, disengagement, or missed opportunities.
- **Meeting Stakeholder Expectations:** Difficulty in meeting diverse stakeholder expectations, including member needs, industry standards, or community obligations, impacting overall organizational effectiveness.
- **Membership Growth Strategies:** Risks associated with ineffective strategies for attracting new members.
- **Stakeholder Engagement:** Risks related to not adequately engaging with key stakeholders.

Technology and Cyber Risks:

In an increasingly digital world, associations are vulnerable to technology-related threats that jeopardize data security, operational continuity, and member trust. Common technology and cyber risks include:

- **Data Breaches:** Unauthorized access or exposure of sensitive member information, leading to financial loss, legal liabilities, or reputational harm.
- **Cyberattacks:** Malicious activities such as phishing, ransomware, or denial-of-service attacks targeting association systems, disrupting operations, and compromising data integrity.
- **System Failures:** Technical failures or disruptions in IT infrastructure, applications, or online platforms that impair service delivery, member engagement, or operational efficiency.
- **Privacy Breaches:** Mishandling or misuse of member data, violating privacy regulations or contractual obligations, resulting in legal consequences and loss of member trust.
- **Technology Obsolescence:** Risks of outdated technology impacting operations.
- **Data Integrity:** Risks related to maintaining the accuracy and reliability of data.

Event and Crisis Planning Risks:

Associations often host events, conferences, and meetings that are critical to their operations and member engagement. Risks in this category include:

- **Event Disruptions**: Unexpected disruptions such as natural disasters, health emergencies, or logistical failures that lead to event cancellations, delays, or reduced attendance.
- **Crisis Management:** Inadequate planning or response to crises, including emergency situations, public relations issues, or member safety concerns, which can damage the association's reputation and operational continuity.
- **Liability Issues:** Legal liabilities arising from incidents or accidents during events, including personal injuries, slander or libel due to public speech by a leader of the association (board member or executive), property damage, or breaches of contract with vendors and participants.
- **Communication Failures:** Ineffective communication strategies during crises, leading to confusion, misinformation, or lack of timely updates for members and stakeholders.
- **Emergency Response Plans:** Risks associated with inadequate emergency response plans.
- **Vendor and Contractor Risks:** Risks related to vendors or contractors for event management.

Sustainability Considerations:

Associations are increasingly expected to operate in an environmentally and socially responsible manner. Risks in this category include:

- **Environmental Impact:** Negative environmental consequences of association activities, including events, operations, and resource usage, which can lead to regulatory penalties and reputational damage.
- **Social Responsibility:** Failure to address social issues such as diversity, equity, inclusion, and community impact, potentially resulting in stakeholder dissatisfaction and loss of member support.
- **Sustainable Practices:** Inability to implement and maintain sustainable practices, affecting the association's long-term viability and stakeholder trust.
- **Sustainable Supply Chain:** Risks related to not maintaining sustainable practices within the supply chain.
- **Climate Change Impact:** Risks related to the impact of climate change on operations.

Social and Political Divide Risks:

Associations have encountered situations in recent years stemming from the polarization of American political and social views, which may cause friction in board rooms, between members, and among employees.

- **Polarization Impact:** Risks related to how political and social polarization might affect organizational unity and operations.
- **Advocacy Risks:** Risks related to taking public stances on controversial issues.

Risk Assessment Methods and Tools

To rank and assess risk, we most often see associations take a qualitative risk assessment approach. This method involves evaluating risks based on subjective criteria, such as impact and likelihood or velocity ratings. Associations can use risk matrices, heat maps, or risk scoring systems to assess and categorize risks based on their qualitative attributes. It is essential to evaluate their potential impact and likelihood to effectively prioritize and allocate resources.

In the context of ERM, the board should focus on monitoring the risks that have the highest combined scores for "likelihood" and "impact." This approach ensures that the organization addresses the risks that truly impact its objectives, rather than those highlighted by individual stakeholders. Ultimately, ERM relies on the board and management's expectations regarding acceptable levels of risk, aligning with the organization's risk appetite or philosophy and strategic goals.

Once each risk is assessed for likelihood and impact, risks are plotted on a matrix to determine the overall risk rating. While the initial plot is determined by the likelihood and impact scores, a risk's location on the risk matrix requires judgment and may involve consideration of additional factors such as velocity (how quickly the risk could impact the association).

		Likelihood				
		Rare	Unlikely	Possible	Likely	Almost Certain
Impact	Catastrophic	Low	Moderate	High	Critical	Critical
	Major	Low	Moderate	High	High	Critical
	Moderate	Low	Low	Moderate	High	High
	Minor	Very low	Low	Low	Moderate	Moderate
	Insignificant	Very low	Very low	Low	Low	Low

Risk Prioritization: Prioritize risks based on their potential impact and likelihood, considering the association's risk appetite and tolerance levels. Focus on high-priority risks that have the greatest potential to negatively impact the achievement of objectives.

Risk Rating	Action Required	Minimum Review
Very Low	Risk is considered acceptable. No further action is required other than to ensure existing response activities are maintained.	Risk Owner reviews annually
Low	Ensure existing response activities are being followed. Additional actions are not high priority.	Risk Owner reviews every 6 months
Moderate	Response activities should be identified and implemented within a timeframe that is appropriate for the risk's speed of onset.	Risk Owner reviews quarterly; Risk Council reviews annually
High	Response activities should be identified and implemented urgently, and resources reallocated if necessary.	Risk Owner reviews monthly; Risk Council reviews quarterly; Board of Directors reviews biannually
Critical	Response activities must be implemented immediately. Consider suspending activities if the risk cannot be controlled by response activities.	Risk Owner reviews weekly; Risk Council reviews monthly; Board of Directors reviews quarterly

Understanding Risk Appetite and Risk Tolerance in ERM

Risk appetite and risk tolerance are key concepts in ERM. Those new to ERM should refrain from formalizing these elements until their ERM program is more established. Initially, associations can operate with general risk appetite guidelines as a foundation. As the ERM program matures, typically in years 3 to 5, they can develop formal risk appetite statements and provide comprehensive training across the organization.

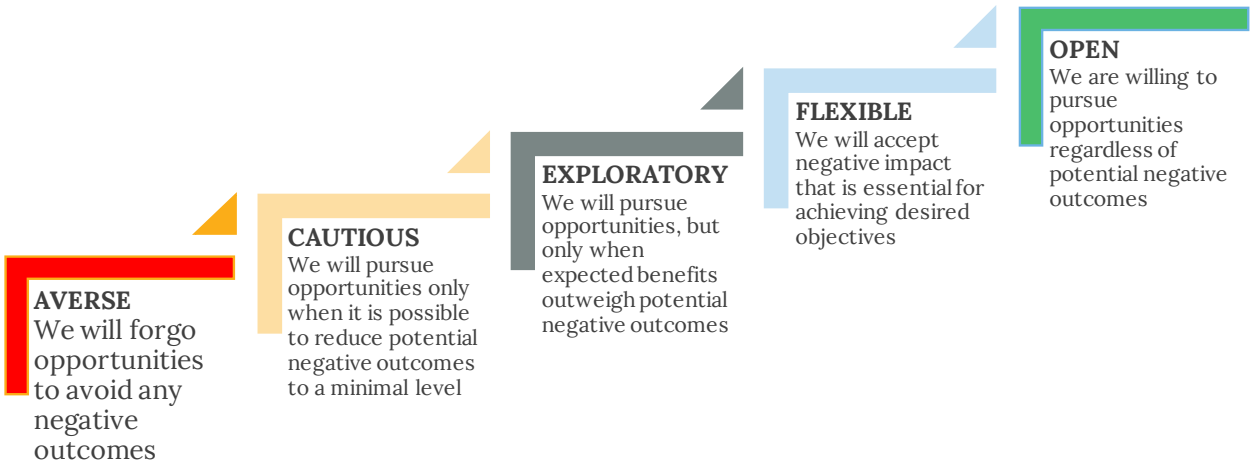
Risk Appetite Defined

Risk appetite refers to the amount and type of risk an association is willing to accept in pursuit of its objectives. It helps balance the potential benefits of risk-taking with the potential consequences of risk exposure. Taking on too much risk can lead to significant and potentially damaging consequences, while excessive caution may stifle innovation and growth, leading to missed opportunities and hindering the association's ability to achieve its goals.

A well-defined risk appetite ensures that the organization makes informed decisions that align with its strategic objectives, while maintaining a level of risk that is acceptable and manageable. It is often recommended that associations start with basic ERM practices and gradually introduce more formal risk appetite frameworks as their understanding and management of risks become more sophisticated.

To develop a risk appetite statement, an association begins by aligning the statement with its strategic objectives and understanding stakeholder expectations. The process involves identifying key risks and assessing the organization's tolerance for each risk category. By engaging leadership and key stakeholders, the association determines acceptable risk levels and defines parameters. The risk appetite statement is then documented, providing a clear articulation of the association's stance on risk-taking.

Once drafted, the statement is reviewed and approved by the executive team and board of directors. It is communicated internally to ensure all stakeholders understand its implications for decision-making. The risk appetite is embedded into the association's processes and is regularly monitored and updated to reflect any changes in strategy or risk environment. This ensures that the organization's approach to risk remains aligned with its goals and stakeholder expectations.



Topic 4:

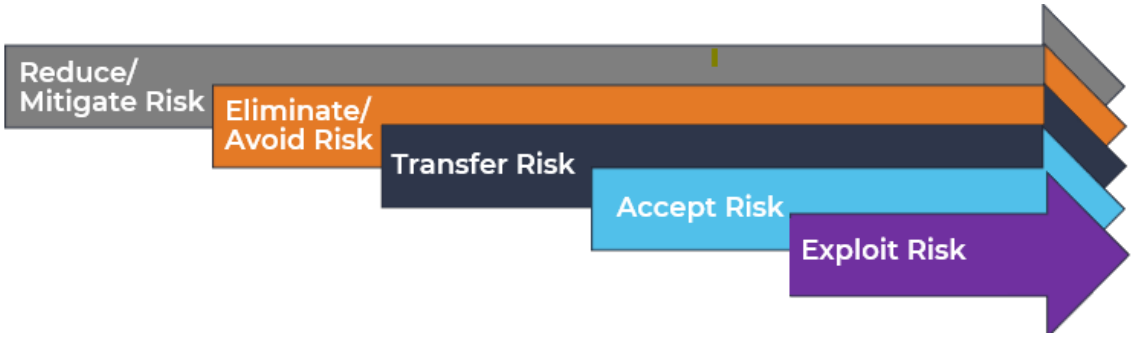
Risk Mitigation Strategies

Developing Risk Response / Handling Plans

Once risks are identified and assessed, the next critical step is to develop risk response plans for the top-ranked risks. Risk response involves taking actions to reduce the likelihood or impact of these risks. Best practice dictates assigning a single “risk owner” to each mitigation plan—this individual should be a member of the management-level risk committee or Risk Council, rather than the current ERM champion. The designated risk owner is responsible for reporting on the status of the risk response plan for the identified top risk. While tasks within the plan can be delegated, having one accountable owner ensures clarity and responsibility.

Risk Response Strategies: Determine appropriate risk response strategies for each identified risk. These strategies may include risk transfer, risk avoidance, risk reduction, or risk acceptance. Select the most suitable response strategy for each risk based on a careful evaluation of its feasibility, effectiveness, and cost-benefit considerations.

Additionally, associations should recognize that certain risks can present opportunities for growth, improvement, or competitive advantage. Develop strategies to exploit these opportunities to benefit the association.



Handling Plans: Develop detailed action plans for each risk response strategy selected. Clearly define the specific actions, responsibilities, timelines, and resources required to implement the handling plans. Assign accountability for monitoring progress and ensure that the handling plans align with the association's overall objectives and available resources.

Key considerations related to risk response strategies include:

Risk Transfer and Insurance

Risk transfer involves shifting the financial burden of a risk to a third party, such as an insurance company or a vendor via contractual agreement. Insurance is a common risk transfer mechanism that can provide financial protection in the event of an adverse occurrence.

- **Insurance Coverage Evaluation:** Assess the association's insurance needs by identifying key risks and evaluating the adequacy of existing insurance coverage. Engage insurance professionals to understand the specific insurance products available and ensure that the association's insurance policies align with its risk profile and requirements.
- **Contractual Risk Transfer:** Evaluate opportunities to transfer risks through contractual agreements with vendors, contractors, or partners. Carefully review contracts and agreements to ensure that risk allocation is clearly defined, and that appropriate indemnification and liability provisions are in place.
- **Captive Insurance:** Consider establishing a captive insurance company, which is a form of self-insurance where the association creates its own insurance entity to cover specific risks. Captive insurance can provide more control over coverage, risk management, and potential cost savings, but it requires careful evaluation and regulatory compliance.

Risk Avoidance and Reduction

Risk avoidance and reduction strategies focus on minimizing the likelihood or impact of identified risks including:

- **Process and Control Enhancements:** Review existing processes and controls to identify areas for improvement. Implement measures to strengthen internal controls, streamline workflows, and reduce vulnerabilities. This may include implementing segregation of duties, enhancing cybersecurity measures, or improving operational procedures.
- **Training and Education:** Invest in training and education programs to enhance staff and board members' risk awareness and skills. This helps build a risk-aware culture, equipping individuals with the knowledge and tools necessary to identify and address risks effectively.
- **Diversification and Redundancy:** Reduce the impact of specific risks by diversifying resources, dependencies, or supply chains. Explore redundancy options to ensure alternative sources or backup plans are in place to mitigate the impact of potential disruptions.

Risk Acceptance and Retention

In some cases, it may be appropriate to accept or retain certain risks based on the association's risk appetite and risk management strategy. Risk acceptance involves acknowledging the existence of a risk and its potential impact without taking specific actions to mitigate it.

- **Risk Monitoring and Review:** Establish monitoring mechanisms to regularly review and assess accepted risks. This allows for ongoing evaluation of risk levels, reassessment of risk tolerances, and prompt action if risks escalate, or circumstances change.
- **Contingency Planning:** Develop contingency plans and response strategies for accepted risks. Contingency plans outline specific actions to be taken if a risk materializes, minimizing its impact and facilitating a swift recovery.
- **Risk Communication and Disclosure:** Ensure transparent communication of accepted risks to stakeholders, including members, employees, and other relevant parties. This promotes informed decision-making and fosters trust and confidence in the association's risk management practices.

Exploiting Risks for Opportunities

Recognize that certain risks can present opportunities for growth, improvement, or competitive advantage. Develop strategies to exploit these opportunities to benefit the association. Key considerations include:

- **Enhancing Capabilities**: Leverage risks to improve the association's skills, processes, or technologies, leading to increased efficiency or new capabilities.
- **Market Advantages:** Identify and capitalize on market opportunities that arise from risk scenarios, such as entering new markets, expanding services, or gaining a competitive edge.
- **Improving Services:** Use risk situations to innovate and enhance the quality or scope of services provided to members, thereby increasing value and satisfaction.
- **Strategic Partnerships:** Form alliances or partnerships that can help mitigate risks while also opening new avenues for collaboration and resource sharing.

- **Financial Gains:** Turn potential financial risks into opportunities for cost savings or revenue generation through strategic investments or cost management initiatives.

Risk response plans detail the steps the association is taking to prevent risks from occurring and mitigate the impact of risks should they occur. When appropriate, similar risks may be grouped together and addressed in a single risk response plan. The risk owner monitors the risk, ensures that necessary actions are being taken, and serves as the communication link between the Risk Council and staff implementing the plan.

Topic 5:

Monitoring and Reporting

Establishing Key Risk Indicators (KRIs)

Establishing Key Risk Indicators (KRIs) is essential for effectively managing risks. KRIs are specific metrics or indicators that provide early warning signs or signals of potential risk events.

The process of establishing KRIs includes the following elements:

- **Identifying Risk Drivers:** Identify the key factors that contribute to the occurrence or amplification of risks within the association. These drivers may include financial metrics, operational performance indicators, compliance metrics, or other relevant factors specific to the association's objectives and risk profile.
- **Defining Risk Thresholds:** Determine the threshold levels for each KRI that indicate a deviation from acceptable risk levels. These thresholds serve as triggers for further investigation or action, providing an early indication of potential risk exposure.
- **Selecting Appropriate KRIs:** Choose KRIs that are relevant, measurable, and actionable. Ensure that the selected KRIs align with the association's risk appetite, objectives, and strategic priorities. Consider the availability and reliability of data needed to monitor the KRIs effectively.

Example KRIs

Membership Growth Rate:

"The association tracks the Membership Growth Rate as a key risk indicator, monitoring the percentage increase or decrease in new memberships quarterly. A declining growth rate may indicate a need to reassess member engagement strategies and program offerings."

System Downtime:

"System Downtime is measured as a key risk indicator to assess the reliability of the association's IT infrastructure. The association aims to maintain system availability at 99.5%, with any downtime exceeding 0.5% prompting an immediate review of IT support and backup processes."

Risk Monitoring Techniques

Risk monitoring involves continuously tracking and assessing risks to ensure that mitigation measures are effective and timely. There are various risk monitoring techniques that can be employed by association board members, including:

- **Regular Risk Reviews:** Conduct regular reviews of identified risks, mitigation plans, and progress towards risk mitigation goals. This may involve periodic risk assessments, control self-assessments, or internal or external audits to validate the effectiveness of risk management efforts.
- **Incident Reporting and Analysis:** Establish a system for reporting and analyzing incidents related to identified risks. Encourage employees and stakeholders to report incidents, near misses, or potential risk events promptly. Analyze these incidents to identify trends, root causes, and opportunities for further risk mitigation.
- **Ongoing Communication:** Foster open and transparent communication channels to encourage the sharing of risk-related information. Regularly engage with key stakeholders, management, and board members to discuss risk status, emerging risks, and the effectiveness of risk mitigation strategies.

Reporting Mechanisms for Board Members

Board members require timely and relevant information to fulfill their risk oversight responsibilities and these communications can take several forms such as:

- **Regular Risk Reporting:** Establish a risk reporting governance cadence to provide periodic updates on the association's risk landscape. These reports should include information on identified risks, mitigation efforts, key risk trends, and the effectiveness of risk controls. Reports should be concise, focused, and tailored to the board's needs but include enough information that board members can comfortable the risk is being managed to an appropriate level.
- **Executive Summaries:** Develop executive summaries that highlight the key risk-related findings, trends, and implications. These summaries should provide a high-level overview of the association's risk exposure, progress in risk mitigation, and notable developments.
- **Ad Hoc Reporting:** In addition to regular reporting, establish mechanisms for ad hoc reporting in response to significant risk events or emerging risks. This ensures that board members receive timely information about critical risks that require immediate attention or decision-making.

Board-Level Reporting Templates and Dashboards

Board-level reporting templates and dashboards provide a structured format for presenting risk-related information to board members. Management should develop a visual dashboard that presents key risk

indicators, risk heat maps, and other relevant risk information in a concise and intuitive format. This allows board members to quickly grasp the association's risk profile and trends at a glance. In addition, it is very helpful to establish standardized reporting templates that capture essential trends and other information over time related to risks, including risk descriptions, risk owners, mitigation plans, and status updates. These templates promote consistency and streamline the reporting process, making it easier for board members to review and compare risk information across different periods.

Keep in mind that board risk reporting should be focused on the critical risks driving strategy (e.g., the top eight to ten risks), not the entire risk register. This type of approach provides focus and allows the board to connect the dots between strategy and risk, which is key to strategic decision making in the board room.

Ensure that reporting templates and dashboards can be customized to align with the board's specific needs and preferences. Flexibility in the reporting format allows for the inclusion of additional information or specific risk areas of interest to the board.

By establishing key risk indicators (KRIs), implementing effective risk monitoring techniques, establishing appropriate reporting mechanisms, and utilizing board-level reporting templates and dashboards, board members can stay well-informed about the association's risk landscape and make informed decisions to effectively oversee risk management efforts. These monitoring and reporting practices enable the board to maintain a proactive and comprehensive approach to risk oversight.

Topic 6:

ERM Best Practices Checklist for Association Boards

ERM Best Practices for Association Boards

Boards should actively engage in risk oversight, providing leadership and setting the tone for risk management within the association. Board members must prioritize risk discussions, participate in training and education, and demonstrate commitment to risk management practices. Below is a checklist to help you on your ERM Journey:

1. Establish a Risk Management Framework

- ✓ **Define Risk Appetite and Tolerance:** Set clear boundaries for risk-taking that align with the association's mission, vision, and strategic goals.
- ✓ **Develop an ERM Playbook:** Create a formal policy that outlines the principles, responsibilities, and processes for risk management.

2. Engage in Continuous Risk Identification and Assessment

- ✓ **Conduct Regular Risk Assessments:** Regularly identify and assess risks, including strategic, operational, financial, compliance, and reputational risks.
- ✓ **Use a Risk Register:** Maintain a comprehensive list of identified risks, including their potential impact, likelihood, and mitigation strategies.

3. Integrate Risk Management into Strategic Planning

- ✓ **Align Risk Management with Strategic Objectives:** Ensure that risk management activities support the achievement of the association's strategic goals.
- ✓ **Consider Risk in Decision-Making:** Evaluate potential risks and opportunities when making key decisions.

4. Develop Risk Mitigation Strategies

- ✓ **Implement Risk Mitigation Plans**: Develop and implement plans to reduce, transfer, accept, or avoid risks.
- ✓ **Monitor and Review Risk Mitigation Efforts:** Regularly review the effectiveness of risk mitigation strategies and adjust as necessary.

5. Foster a Risk-Aware Culture

- ✓ **Promote Risk Awareness:** Encourage board members, staff, and stakeholders to recognize and communicate potential risks.
- ✓ **Provide Training and Education:** Offer ongoing training and resources on risk management practices and trends.

6. Establish Clear Roles and Responsibilities

- ✓ **Define Board and Management Roles:** Clearly delineate the roles and responsibilities of the board, management, ERM champion and other stakeholders in the risk management process.
- ✓ **Create Risk Committee(s):** Consider establishing both board level and management level risk committees to oversee the ERM process and report to the board.

7. Leverage Technology and Data Analytics

- ✓ **Leverage Technology:** Consider using technology to streamline risk management processes, track risks, and generate reports.
- ✓ **Analyze Data for Risk Insights:** Leverage data analytics to identify trends, predict potential risks, and make informed decisions.

8. Maintain Transparency and Communication

- ✓ **Communicate Risk Information:** Share relevant risk information with stakeholders, including members, donors, and partners, as appropriate.
- ✓ **Report on Risk Management Activities:** Provide regular updates to the board and stakeholders on risk management efforts and outcomes.

9. Prepare for Crisis and Business Continuity

- ✓ **Develop Crisis Management Plans:** Create plans to respond to potential crises, such as natural disasters, cybersecurity incidents, or reputational crises.
- ✓ **Ensure Business Continuity:** Implement strategies to ensure the association can continue operations during and after a crisis.

10. Evaluate and Improve the ERM Process

- ✓ **Regularly Review and Update the ERM Framework:** Periodically assess and refine the ERM framework to ensure it remains relevant and effective.
- ✓ **Conduct Independent Audits:** Consider engaging external auditors or outside consultants to review the ERM program and provide recommendations for improvement. The results and opportunities for improvement should be shared with the board.

Conclusion

This ERM Association Handbook for Board Members provides valuable insights and practical guidance on implementing effective risk management practices within associations. By embracing the principles and practices outlined in this handbook, association board members can foster a risk-aware culture, strengthen governance practices, and enhance the association's ability to navigate uncertainties, seize opportunities, and achieve its objectives.

Remember, ERM is more art than science and is a journey that requires dedication, collaboration, and continuous improvement. By actively engaging in risk management practices and sharing knowledge with other associations, board members can contribute to the success and sustainability of their associations in an ever-changing landscape. Thank you for embarking on this important journey to strengthen risk governance and drive the success of your association through effective ERM.

Appendix

Key Terms and Definitions

To aid your understanding of ERM concepts, here are key terms and their definitions:

Enterprise Risk Management (ERM)	A comprehensive and integrated approach to managing risks across an organization. ERM involves identifying, assessing, prioritizing, and mitigating risks to achieve objectives effectively.
Risk	The potential for events or circumstances to have an adverse impact on objectives. Risks can be threats or opportunities that arise from internal or external factors.
Risk Mitigation	Actions taken to reduce the likelihood or impact of identified risks. Mitigation strategies may include risk transfer, risk avoidance, risk reduction, or risk acceptance.
Key Risk Indicators (KRIs)	Specific metrics or indicators that provide early warning signs of potential risk events. Monitoring KRIs helps assess the status of risks and the effectiveness of risk mitigation efforts.
Risk Assessment	The process of evaluating risks by considering their potential impact and likelihood. Risk assessments aid in prioritizing risks and allocating resources effectively.
Risk Appetite	The level of risk an organization is willing to accept in pursuit of its objectives. It reflects the organization's willingness to take risks to achieve its strategic goals.
Risk Tolerance	The acceptable level of variation an organization is willing to tolerate in the achievement of its objectives. It helps define the boundaries within which risks are considered acceptable.
Risk Transfer	Shifting the financial burden of a risk to a third party through mechanisms such as insurance or contractual agreements.
Risk Avoidance	Eliminating activities or exposures that could give rise to risks. This strategy aims to completely eliminate the potential for a risk event to occur.
Risk Reduction	Implementing measures to reduce the likelihood or impact of identified risks. Risk reduction strategies focus on minimizing the adverse consequences of a risk event.

[Association Name] Risk Committee Charter

I. Purpose

The Risk Committee (the "Committee") is established by the Board of Directors (the "Board") of [Association Name] to oversee the association's Enterprise Risk Management (ERM) framework. The Committee's purpose is to ensure that significant risks are identified, evaluated, and managed in alignment with the association's strategic objectives, mission, and values.

II. Responsibilities

ERM Framework Oversight

- *Review and approve the association's ERM framework, including risk policies, procedures, and risk management strategies.*
- *Monitor the effectiveness of the ERM framework in identifying, assessing, and mitigating risks.*

Risk Assessment

- *Ensure that a comprehensive risk assessment is conducted periodically to identify and evaluate significant risks facing the association.*
- *Review risk assessment reports and ensure appropriate actions are taken to address identified risks.*

Risk Mitigation

- *Oversee the development and implementation of risk mitigation strategies and action plans.*
- *Evaluate the effectiveness of risk mitigation efforts and recommend adjustments as necessary.*

Risk Reporting

- *Review and approve risk reports prepared by management, including risk profiles, risk dashboards, and significant risk incidents.*
- *Ensure that the Board receives timely and accurate information on significant risks and risk management activities.*

Compliance and Internal Controls

- *Oversee the association's compliance with relevant laws, regulations, and industry standards related to risk management.*
- *Ensure that internal controls are effective in managing and mitigating risks.*

Crisis Management and Contingency Planning

- *Review and approve crisis management and contingency plans to ensure preparedness for significant risk events.*

- *Monitor the association's response to crises and major risk incidents.*

Communication and Reporting

- *Communicate the Committee's activities and recommendations to the Board.*
- *Ensure that there is an effective process for reporting risk-related issues to the Board.*

Review and Evaluation

- *Periodically review the Committee's charter and performance to ensure its effectiveness.*
- *Recommend changes to the charter as necessary.*

III. Composition

Membership

- *The Committee shall consist of at least [number] members of the Board, with a majority being independent directors.*
- *Members shall possess relevant experience and expertise in risk management, finance, or related fields.*

Chairperson

- *The Committee shall appoint a Chairperson from among its members.*
- *The Chairperson shall be responsible for setting the agenda, leading meetings, and acting as a liaison between the Committee and the Board.*

IV. Meetings

Frequency

- *The Committee shall meet at least [frequency, e.g., quarterly] and as needed to fulfill its responsibilities.*

Agenda and Minutes

- *The Chairperson shall set the agenda for each meeting and ensure that minutes are taken and approved.*

V. Authority

Access to Resources

- *The Committee has the authority to access necessary resources, including internal and external advisors, to fulfill its responsibilities.*

Decision-Making

- *The Committee may make recommendations to the Board regarding risk management strategies and policies, but final decisions rest with the Board.*

VI. Approval

This charter was approved by the Board of Directors of [Association Name] on [Date].

Chairperson:

[Name]

Date:

[Date]

Example Association Risk Survey

Creating an association risk survey can help identify and assess the various risks an organization may face. Here's an example list of questions that could be included in such a survey, categorized by risk type:

Strategic Risks

- What are the top three strategic risks facing our association?
- How well do we understand our competitive landscape and potential market changes?
- Are there any emerging trends or changes in regulations that could impact our strategic goals?
- How confident are you in the association's long-term strategic planning?

Operational Risks

- What operational challenges does our association currently face?
- How effective are our current processes in achieving operational efficiency?
- Are there any critical dependencies (e.g., suppliers, technology) that pose a risk to our operations?
- How well do we manage project timelines and budgets?

Financial Risks

- What financial risks could impact our association's stability?
- How well do we manage our cash flow and reserves?
- Are there any concerns about our funding sources or revenue streams?
- How effective are our financial controls and reporting mechanisms?

Compliance Risks

- How well do we adhere to relevant laws, regulations, and industry standards?
- Are there any areas where we might be exposed to legal or regulatory risks?
- How effectively do we manage compliance-related policies and procedures?
- Have there been any recent changes in regulations that we need to address?

Reputational Risks

- What potential events or issues could harm our association's reputation?
- How well do we manage communication with stakeholders, including members, donors, and the public?
- Are there any past incidents that could resurface and affect our reputation?
- How prepared are we to handle public relations crises?

Technology Risks

- What technology-related risks does our association face?
- How secure are our IT systems and data?
- Are there any concerns about our technology infrastructure or software?
- How effectively do we manage and protect member and stakeholder data?

Human Resources Risks

- What are the key human resources risks in our association?
- How well do we manage employee recruitment, retention, and development?
- Are there any concerns about employee morale or workplace culture?
- How effective are our succession planning and leadership development efforts?

Event and Crisis Management Risks

- How prepared are we to handle emergencies or crises?
- Do we have adequate plans for business continuity and disaster recovery?
- How well do we manage risks related to hosting events or public gatherings?
- Are there any vulnerabilities in our crisis communication plans?

ESG (Environmental, Social, Governance) Risks

- How well do we manage environmental impacts and sustainability initiatives?
- What social responsibility risks might affect our association?
- How strong are our governance practices and board oversight?
- Are there any risks related to diversity, equity, and inclusion in our organization?

General and Other Risks

- Are there any other risks not covered in this survey that we should consider?
- How well do we integrate risk management into our day-to-day decision-making?
- What additional support or resources would help us improve our risk management efforts?

This list can be tailored to the specific needs and context of the association. It's important to provide respondents with the opportunity to elaborate on their responses and suggest additional risks or mitigation strategies.

Recipients of Risk Surveys

- **Board Members:** To gain insights into strategic risks and governance issues. To understand the Board's risk perception and ensure alignment with management.
- **Senior Management:** To assess operational, financial, and compliance risks from a leadership perspective.
- **Department Heads and Managers:** To gather information on specific operational and departmental risks.
- **Staff Members:** Depending on the context, it may be valuable to include a broader group of employees to identify risks related to day-to-day operations and workplace culture.
- **Key Stakeholders:** Such as members, donors, volunteers, or partners, to understand external risks and perceptions.

Frequency of Risk Surveys

- **Annual Surveys:** Conducting a comprehensive risk survey annually can help identify emerging risks and review the effectiveness of existing risk management strategies.
- **Quarterly Surveys:** For dynamic environments or high-risk areas, quarterly surveys can provide more frequent updates on specific risk categories.
- **Event-Driven Surveys:** Following significant events (e.g., major projects, organizational changes, crises), surveys can assess the impact and identify new risks.
- **Periodic Check-ins:** Shorter, targeted surveys can be conducted periodically to monitor specific areas of concern or high-priority risks.

Best Practices for Conducting Surveys

- **Anonymous Responses:** Offering anonymity can encourage more honest and open feedback, especially when assessing sensitive areas like workplace culture or compliance.
- **Clear Communication:** Clearly communicate the purpose of the survey, how the data will be used, and the importance of participant contributions.
- **Actionable Feedback:** Ensure that the survey results lead to actionable insights and that there is a process in place to address identified risks.
- **Follow-Up:** Communicate the results and any subsequent actions taken to participants to demonstrate that their input is valued and impactful.

By tailoring the frequency and recipients of risk surveys to the organization's specific needs, associations can effectively monitor and manage risks, ensuring a proactive approach to risk management.

Example Risk Response Plan

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					

Additional Resources

To further enhance your knowledge and implementation of ERM practices, consider exploring the following additional resources:

Why Associations are getting Started with ERM

- ASAE Website: https://www.asaecenter.org/resources/articles/an_plus/2019/october/why-associations-are-implementing-enterprise-risk-management
- Brief article discussing the benefits of ERM for Associations

Gettering Started with Enterprise Risk Management – A guide for Nonprofits

- Website: https://www.grfcpa.com/enterprise-risk-management-resources/
- Detailed guidebook including templates and resources by GRF CPAs & Advisors & NC State's ERM initiative.

NC State ERM Initiative

- Website: https://erm.ncsu.edu/
- Leading-edge insights and education in ERM

COSO (Committee of Sponsoring Organizations of the Treadway Commission)

- Website: https://www.coso.org/Pages/erm-integratedframework.aspx
- COSO provides a comprehensive framework for enterprise risk management that is widely recognized and used globally.

ISO (International Organization for Standardization)

- Website: https://www.iso.org/iso-31000-risk-management.html
- ISO 31000 is the international standard for risk management, providing principles and guidelines for effective risk management.

RIMS (Risk and Insurance Management Society)

- Website: https://www.rims.org/resources/risk-knowledge
- RIMS offers various resources, tools, and guides on enterprise risk management, including RIMS Risk Maturity Model (RMM).

The Institute of Internal Auditors (IIA)

- Website: https://www.theiia.org/en/resources/
- IIA provides resources and guidance on integrating ERM with internal auditing practices.

These resources should provide a strong foundation for understanding and implementing effective ERM practices. By leveraging these additional resources and utilizing the sample templates and ERM framework examples provided in the appendix, you can further strengthen your association's risk management practices and enhance its overall resilience.

Remember, the implementation of ERM is a continuous process that requires commitment, adaptability, and ongoing learning. Stay informed about new developments and emerging risks to ensure that your association remains proactive in managing risks effectively.

About the Authors

Melissa Musser, CPA, CIA, CITP, CISA

Partner and Director, Risk & Advisory Services

301-951-9090

mmusser@grfcpa.com

Ms. Musser is a recognized authority in the field of risk management. She leads GRF's dynamic risk advisory department, ensuring clients receive strategic guidance and tailored solutions to effectively identify opportunities and manage risks. Her expertise encompasses establishing and maintaining Internal Audit Departments, optimizing internal controls, strategic planning, compliance, Enterprise Risk Management (ERM), and cybersecurity programs.

Ms. Musser is a highly sought-after public speaker, sharing her insights and knowledge on enterprise risk management, internal audit, cybersecurity, and governance at various industry conferences and events. Her engaging presentations and ability to simplify complex concepts have made her a trusted resource for professionals seeking guidance on risk-related matters.

She received the prestigious 2018 AICPA Information Management and Technology Assurance (IMTA) Standing Ovation award and was honored with the Excellence in Innovation award in Consulting® Magazine's 2022 Women Leaders in Technology awards. She recently served as president of the Washington, DC Chapter of the Institute of Internal Auditors. Additionally, Melissa is the founding partner of the NC State ERM Initiative's Annual Events focused on Enterprise Risk Management for Nonprofit Organizations.

Susan Colladay, CPA

Partner, Audit

301-951-9090

scolladay@grfcpa.com

A partner in the audit services department at GRF, Ms. Colladay has served as the lead partner on the audits of trade associations, professional membership societies, arts and humanities nonprofits, advocacy organizations, and grant-making foundations. With 30 years working in the nonprofit industry and 25 years in public accounting, her depth of nonprofit experience includes audits of federal award programs and employee benefit plans, integrated audits of internal control and financial statements, and agreed-upon procedures engagements. During her career, Ms. Colladay has led a team that provided outsourced internal audit services to nonprofits and applied her knowledge of tax-exempt organizations to various consulting engagements such as finance and accounting process reviews and enterprise risk management.

Prior to working in public accounting, Ms. Colladay worked in the accounting department at the American Society of Travel Agents (ASTA) where she had the opportunity to travel to Bangkok, Thailand, and Lisbon, Portugal for ASTA's international meetings. A member of the American Institute of Certified Public Accountants (AICPA), the American Society of Association Executives (ASAE), and the Greater Washington Association of Certified Public Accountants (GWSCPA), Ms. Colladay was recognized by GWSCPA as a Woman to Watch in the Experienced Leader category in 2015. She is also a charter member of the Maryland Delta Chapter of Pi Mu Epsilon, the National Mathematics Honor Society, and currently serves on the board of directors of Mindful Memorial Foundation as a member of the Finance Committee.

Joseph M. Pugh, CCEP, CFE, RIMS-CRMP, CRMA, CDPSE

Senior Director, ERM & Compliance, AARP

Joe is a strategic risk management professional with experience maturing Enterprise Risk Management (ERM) and Ethics and Compliance programs within for-profit and not-for-profit organizations. Joe has a passion for building strategic ERM programs from the ground up.
Joe is currently the Senior Director, ERM & Compliance at AARP, the nation's largest nonprofit, nonpartisan organization dedicated to empowering people 50 and older to choose how they live as they age. Joe leads the ERM program at AARP, where he built, matured, and focused on creating an ERM framework that is strategic-centric and an ERM governance cadence that provides risk-informed information to executives, the Board of Directors, and key decision makers at all levels of the organization. Under Joe's leadership, the organization has become more risk savvy and able to understand the enterprise risks "to" and "of" strategic priorities, as well as the capability to act quickly when risk exposures change.

In addition to his ERM role, Joe works closely with the Chief Ethics and Compliance Officer in developing and executing various strategies designed to promote a strong ethical culture and ensure compliance with applicable laws and regulations. Joe played a key role in AARP being named one of the World's Most Ethical Companies for three consecutive years.

Joe is a frequent speaker on ERM. He co-authored with AARP's COO the publication "AARP's Innovative Past Inspires Transformation Today," via the Wall Street Journal – Risk & Compliance, 2019, and co-authored the publication "Where to Start: Risk Management 101" in the Compliance & Ethics Professional (CEP) magazine, July 2023.

Please note: I am contributing to the handbook on my behalf and the ideas and information shared do not represent those of my employer.

Trade and Professional Associations

Trade and professional associations play an important role in our economy by uniting businesses in the same industry or people in the same profession to advance their common interests. While there are many advantages to their members in terms of education and networking opportunities, associations themselves face a number of challenges in the current business climate. Those that are thriving are embracing private sector business practices and innovative technologies, identifying and leveraging additional sources of revenue, and proactively addressing regulatory and industry issues like privacy.

Dedicated Association Expertise

GRF provides trade and professional associations with the support they need to tackle these economic and technological shifts. Our experts provide accounting, tax and advisory services with a focus on industry best practices and innovation from the business world. As a result of GRF's work with clients around the world, international membership organizations can draw upon our firm's extensive global experience.

Services to Trade and Professional Associations

Our approach is to work with you, side-by-side to tackle the special business challenges that trade and professional associations face. We bring a wealth of knowledge of accounting, tax, and advisory services from all sectors of the economy. Together we can deploy the best business practices in the industry, innovative technologies, and our deep understanding of legal and regulatory issues to foster your success.

Contact

GRF CPAs & Advisors | 301-951-9090 | www.grfcpa.com