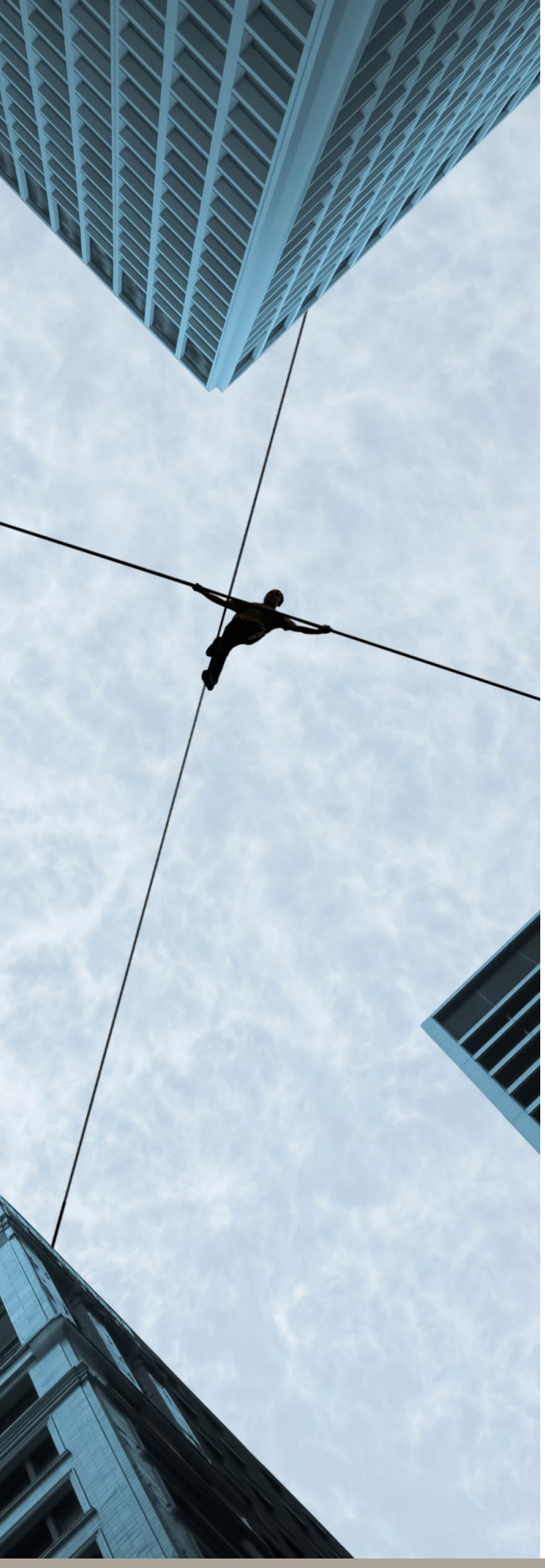
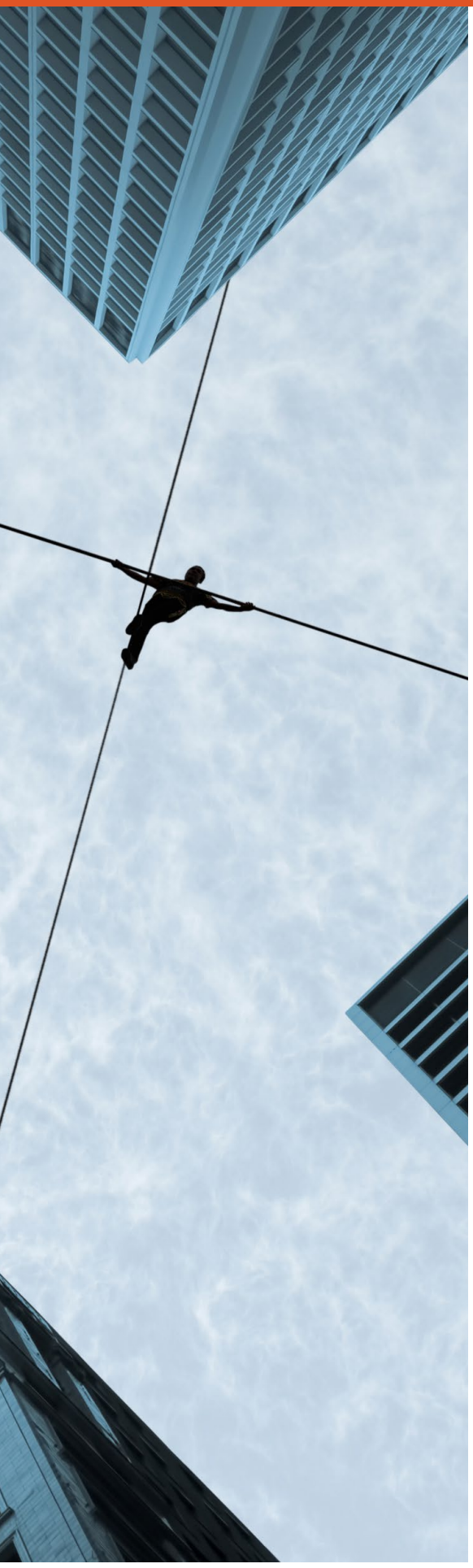


asae®
The Center for Association Leadership

In collaboration with ASIS INTERNATIONAL Advancing Security Worldwide® RIMS the risk management society

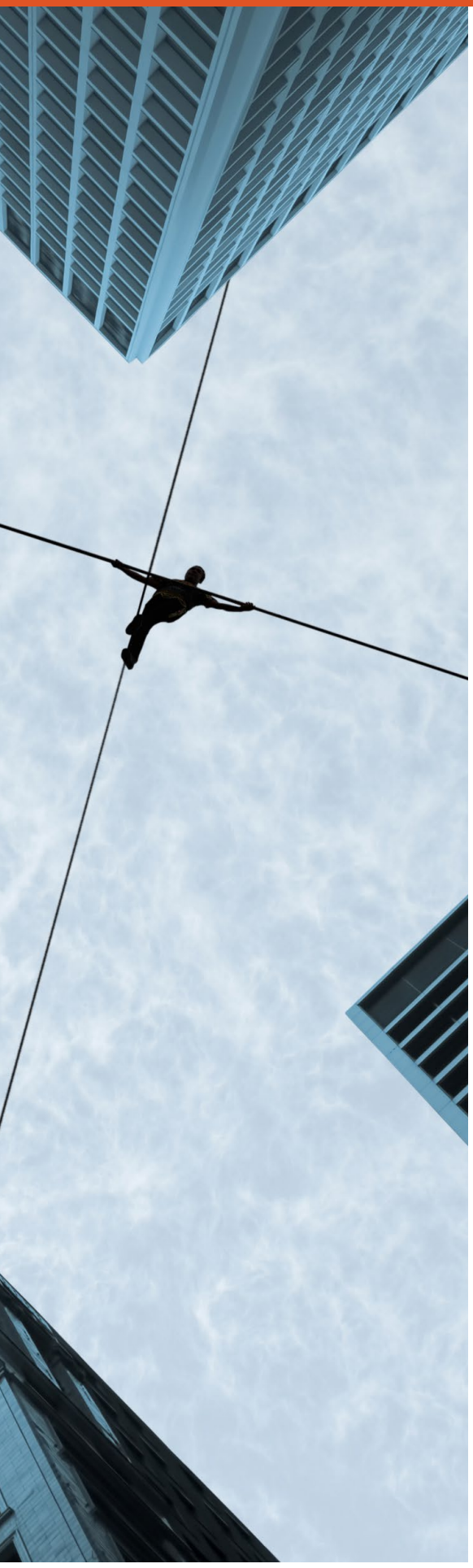
Associations' Guide to Risk and Crisis Management

Supported by AON



asae
The Center for Association Leadership

Contents



Welcome and Introduction

from ASAE's President and CEO

According to the World Economic Forum when introducing their Global Risks Report 2024, "risks are growing — but so is our capacity to respond." This is true for the association community as well. There is a lot of risk and uncertainty in the world, which is why we're introducing this risk, safety, and crisis management toolkit to help associations increase their knowledge and capacity to respond.

ASAE conducted a Risk Management and Safety survey in 2023 to help us better understand the risk and safety related concerns for associations. We found that associations rank cyber threats as their top risks, followed by crime/general safety at event cities/locations. Boards are being included in the risk and safety management conversation, with 85.4% of associations indicating they are discussing risks with their board of directors. This is a positive sign that associations recognize the importance of risk management at the highest levels of governance. However, we also found that more than half (58.10%) of associations do not have risk management, safety, and security integrated into their strategic plans.

This toolkit is designed to help associations:

1. Develop an understanding of where they are respective to their peers on their risk and safety journey;
2. Gain insights into the key terms and concepts of risk, emergency, and crisis management;
3. Attain a foundational understanding of how to get started with an enterprise approach to risk management and crisis management within the unique context of associations.

We are grateful to have worked with the leading associations on risk, RIMS, and security, ASIS International in the development of this toolkit. We thank them for their significant contributions and authorship on this resource. Their tools, frameworks, and models will help raise the standard of risk and crisis management for the association profession.

With meeting safety ranking as a top risk for associations, we take a deeper dive into meetings safety both through a case study provided by RIMS as well as insights from our association survey and collaboration with Destinations International, which had analyzed risk and crisis management at events from a destination perspective.

The association community is at its best when we're learning together and sharing with each other. This toolkit is a tangible example of that. As noted, many associations and industry experts have come together to create this resource for the benefit of the association community. We thank them for their expertise and commitment and truly hope this toolkit helps make associations, and the world, safer.

Michelle Mason, FASAE, CAE
ASAE President & CEO

A Call to Action

Associations are given a gift of immense value and power: The right to convene. The ability to call people together to learn, network and conduct business creates communities, builds identity, and provides the resources that associations need to thrive. Associations are trusted to use this gift to develop and deliver offerings and experiences that meet the needs of stakeholders and advance the organization's mission. In return for this trust, associations have a reciprocal duty to ensure the safety and security of event participants. The power to convene creates an obligation to care for the convened.

Associations convene thousands of conferences and conventions every year, and countless other, smaller events that are attended by millions. Most events are produced safely. Usually everything goes well. But sometimes it doesn't. Cybersecurity, physical safety, medical emergencies, and social unrest are among the event-related risks of most concern to association professionals. And associations face a wide array of other risks in every aspect of organizational life. Every association professional is a risk manager. Yet nearly 60% of associations do not address risk in their strategic plans and fewer have enterprise risk management programs.

That is why RIMS, *the risk management society*®, joined ASAE and ASIS in a strategic collaboration to strengthen the capacity of associations to manage risk, enhance the safety and security of association events, and plan for emergencies. Together, we bring to bear practical resources and valuable intelligence that associations can immediately apply to make people safer and more secure.

The world is riskier, and people are increasingly risk aware. Associations are trusted with the health and safety of millions of event participants every year. This Toolkit is dedicated to them and is given freely to the association community to employ on their behalf.

Gary A. LaBranche, FASAE, CAE
Chief Executive Officer
RIMS, *the risk management society*®

Safer Together

Disasters can strike anywhere—wars, famines, natural disasters, and civil and social unrest continue to proliferate around the globe. Combine these with the reputational risk in operating an association in these environments, and it becomes clear that managing such threats is a critical part of any business strategy. Comprising a global community of security practitioners, ASIS International exists to make the world a safer place in which to live, work, and play. ASIS members have a role in the protection of assets—people, property, and/or information—in virtually every industry in the public and private sectors, and organizations of all sizes. From entry-level managers to the C-suite, from security veterans to consultants and those transitioning from law enforcement or the military, the ASIS community is global and diverse.

Protecting organizations and their employees whether in an office, at a conference, or working anywhere in the world, is the daily mission of the professionals at ASIS International. The experts that form ASIS offer a range of education programs, publications, and events to help industry professionals thrive. These resources, developed in consultation with leading industry experts, represent the most reliable and cutting-edge information.

ASIS is pleased to include these resources in this toolkit, created in collaboration with ASAE and RIMS, which brings the crisis management, resilience, and site security expertise of these professionals to associations that may need guidance when forming their security plans.

Peter J. O'Neil, FASAE, CAE
CEO
ASIS International

A Letter from Aon

Aon Affinity Nonprofits is honored to sponsor this first-ever ASAE Crisis/ Risk Management Toolkit for nonprofit associations. The importance of risk management is a vital topic to address proactively to ensure your association's mission can continue to be fulfilled, your members needs served, and inherent organizational business risks are mitigated. For over 25 years, Aon Affinity Nonprofits has been a proud ASAE Business Solutions-endorsed partner underwriting and servicing a portfolio of insurance products designed to meet the unique needs of the trade and professional association community. Sitting squarely in the intersection of insurance and risk management, Aon Affinity Nonprofits has worked closely with associations and their local insurance agents and brokers for decades to find ways to mitigate association risk. Many interesting insights are included in the toolkit including the following regarding insurance coverage;

- **Insurance decision making** — association c-suite and finance roles are charged most frequently regarding insurance matters but many other roles such as human resources and legal are involved as well.
- **Insurance types** — the insurance landscape can be complex with a multitude of types of insurance associations should consider ranging from business insurance to cyber liability to directors & officers liability and beyond.
- **Top insurance concerns** — not surprisingly, cost containment is a top priority for associations and one that needs to be balanced with managing evolving organizational exposures.

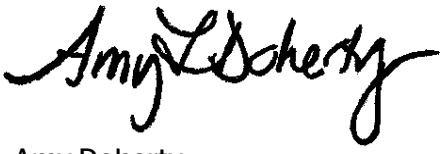
The current business environment brings its fair share of challenges to the nonprofit industry. To ensure associations position themselves for success and understand a complex and evolving risk management and insurance landscape, we have outlined some exposures to be aware of and the potential impact.

Antitrust:
Antitrust coverage for trade and professional associations, as many set standards as well as provide accreditation and certification, which can increase exposure to claims alleging violation of antitrust laws. A potential exposure may exist through the association's mission of promoting a specific industry or profession and the association being subject to accusations that a monopoly is being created reinforcing the importance of transparency and proper insurance protection.

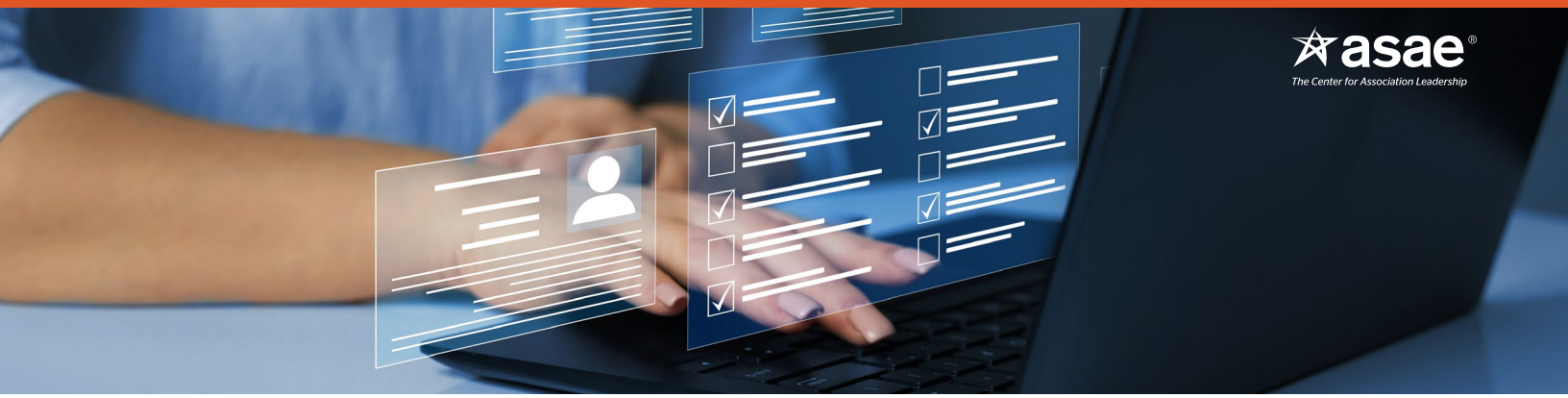
Social Inflation:
The term describes the rising costs of claims being above and beyond what can be explained by the overall inflation rate. There are several recent trends that have led to an increase in employment practices liability (EPL) claims such as growing awareness of the gender pay gap, COVID return to work issues and the #MeToo movement. Social media has amplified these issues in a way we've never seen before, mobilizing a global audience around an issue, and enabling them to connect directly with the individuals and organizations involved. Claimants are looking for hefty financial considerations to be made in lawsuits to help right the wrong, with sympathetic juries often in agreement, payouts for claims in the EPL arena are skyrocketing. Sometimes nonprofits can feel like they are immune to these types of issues, but they aren't. Nonprofits need to recognize the risk of social inflation and take proactive steps to mitigate its exposures through ensuring they have the correct coverage and limits of liability in place.

Weather volatility:
As climate risk continues to grow, the severity of weather continues to be of considerable concern for organizations with respect to owned property as well as exposure for events. The Wall Street Journal indicated that 2023 was a record-breaking year for convective storm damage, estimated at over 76 billion in North America and Europe. "The record global temperatures that spawned heavy rainfall, disastrous floods and raging wildfires in 2023 will likely continue in 2024, according to the European Union's Copernicus Climate Change Service. The service is the first analysis to declare — after months of speculation — that 2023 was the hottest year since record-keeping began in the mid-1800s." The other factor at play? Unpredictable weather patterns. While we're used to seeing hurricanes in the south and wildfires in the west — and, to some extent, had been able to plan around those peak seasons — extreme weather today seems to know no season or geographic boundary. In short, everyone's at risk. While exposure to a nonprofit's property has risen so to have associated insurance premiums for property, particularly areas of the U.S that are deemed vulnerable to catastrophic weather. In addition, many associations rely on revenue generated from their annual schedule of sponsored events. Traditionally, income generated through conventions, conferences and meetings can represent up to 30–40% of an association's expected annual revenue. For nonprofit organizations to not only continue to survive but also thrive, they need to take a "it can happen to us" mindset when they assess limits in place for property (including inflationary factors) as well as plan events with risks in mind, whether that's a weather event striking your meeting location or one impacting your attendees' ability to travel to your event.

As a firm, Aon is in the business to shape decisions for the better — to protect and enrich the lives of people around the world. Now more than ever, organizational resilience and growth are dependent on leaders in the nonprofit sector taking action to respond to their organization's challenges and opportunities. Our aim is to help nonprofits thrive while ensuring the communities and members they serve and the people they employ flourish.



Amy Doherty
Senior Vice President
Aon Affinity Nonprofits



Results of the 2024 Association Risk and Safety Survey

Key Insights

- **Top Security/Safety Concerns:** Cyber threats such as data security, IP privacy, and ransomware are the primary concern for organizations, followed by concerns about crime/general safety at event cities/locations, and medical emergencies.
- **Board Discussions on Risks:** A significant majority of organizations (85.4%) are discussing risks with their board of directors, indicating a recognition of the importance of risk management at the highest levels of governance.
- **Understanding of Risk by Business Leaders:** While a significant portion of respondents (78.8%) report that business area leaders have some degree of understanding of how risk impacts their overall strategy and operations, there is room for improvement in enhancing their understanding.
- **Budget Allocation:** While some organizations have seen an increase in their budget for managing security/safety over the past three years (30.30%), a significant portion report that their budget stayed the same (41.9%), and roughly one in five (21.7%) do not have a budget allocated for this purpose.
- **Emergency Communication/Response Plans:** Two-thirds of organizations (67.7%) believe their emergency communication/response plan would be at least moderately effective during a crisis.
- **Collaboration and Communication:** Many organizations foster cross-departmental collaboration to discuss the impact of risk (60.6%) and encourage managers to share potential impediments to achieving business objectives (62.6%).
- **Factors Influencing Destination Selection:** Crime and safety, destination weather/climate predictions, and health and safety measures are the top factors considered when selecting event destinations. Accessibility policies and initiatives ranked fourth. Factors like political climate, perception of social justice & equality, and active legislation around Human Rights generally ranked lower.

Methodology

The 2024 ASAE Risk & Safety Management Survey (RSMS) was sent to 4,739 respondents. Respondents consisted of leaders of associations/organizations within the ASAE membership (Directors and above). Of the 4,739 respondents, 198 completed the survey for a response rate of 4.2%. The survey was open from January 25 to February 9, 2024; five contacts were made during the fielding period.

Full Insights

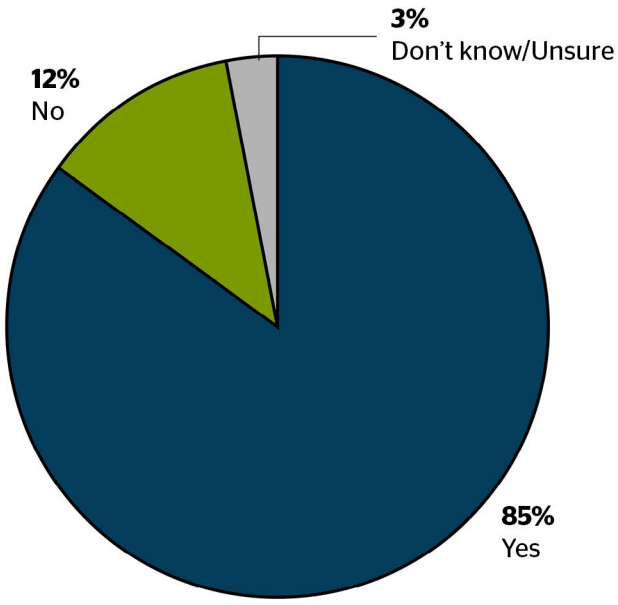
- **Top Security/Safety Concerns:** Cyber threats such as data security, IP privacy, and ransomware were ranked as the top security/safety concern followed by concerns about crime/general safety at event cities/locations, medical emergencies, and social unrest. Extreme weather, political uncertainty/war, embezzlement/fraud, and active shooter/assailant were the lowest ranked security/safety concerns.

Item	Overall Rank	Rank Distribution	Score	Number of Rankings
Cyber Threats (data security, IP privacy, ransonware)	1		1,338	190
Crime/General safety at event cities/locations	2		994	175
Medical Emergencies	3		804	171
Social Unrest (protests, riots, event disruption)	4		751	170
Extreme Weather	5		704	169
Political Uncertainty/War	6		625	170
Embezzlement/Fraud	7		600	165
Active Shooter/Assailant	8		580	165

Lowest Rank Highest Rank

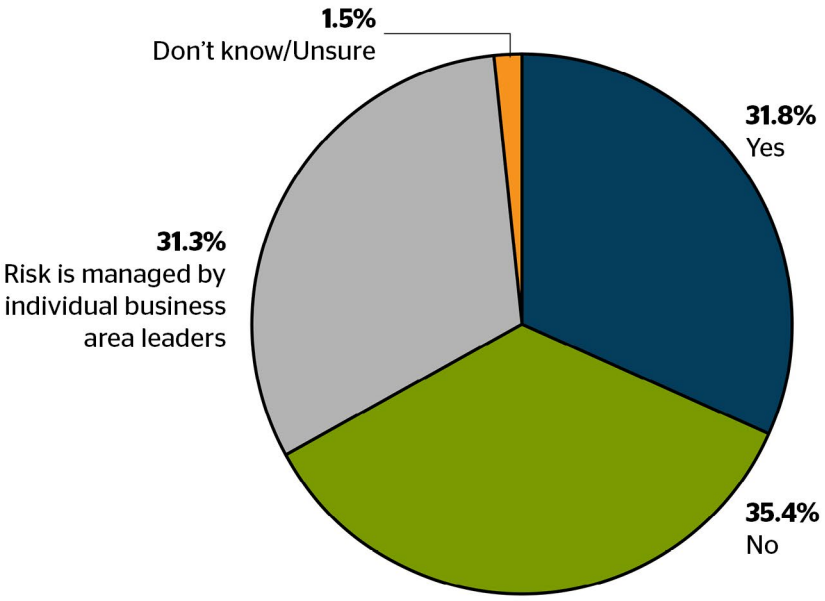
- **Board Discussions on Risks:** A significant majority of organizations (**85.40%**) are discussing risks with their board of directors, indicating a recognition of the strategic importance of risk management.

In the last five years, have any of the risks mentioned above been discussed by your organization's Board of Directors?



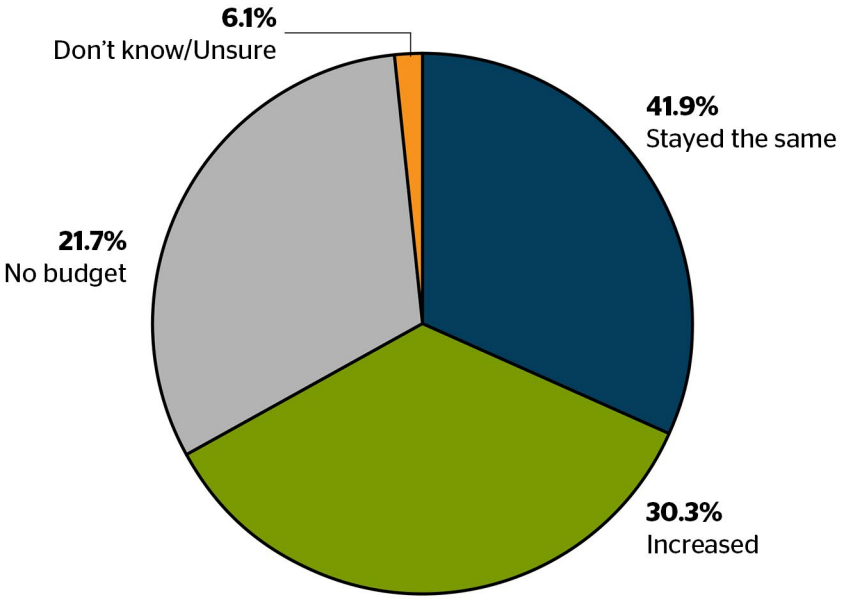
- **Diverse Risk Management Staffing Approaches:** Organizations vary in their approaches to staffing risk management, with **31.80%** having dedicated positions or teams, **35.40%** not having dedicated positions or teams, and **31.30%** reporting that risk is managed by individual business area leaders.

Does your organization have a team or position dedicated to managing risk for your association (including events)?



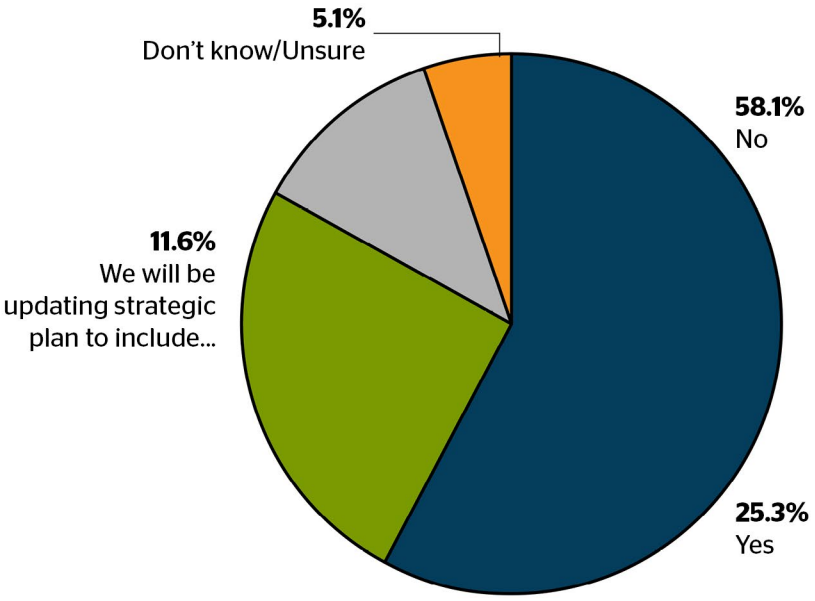
- **Budget Allocation:** While **30.30%** of organizations have seen an increase in their budget for managing security/safety over the past three years, a significant portion (**41.90%**) report that their budget stayed the same, and roughly one in five (**21.70%**) do not have a budget allocated for risk management.

Has the budget to manage security/safety at your organization's event increase, decreased or stayed the same over the past three years?



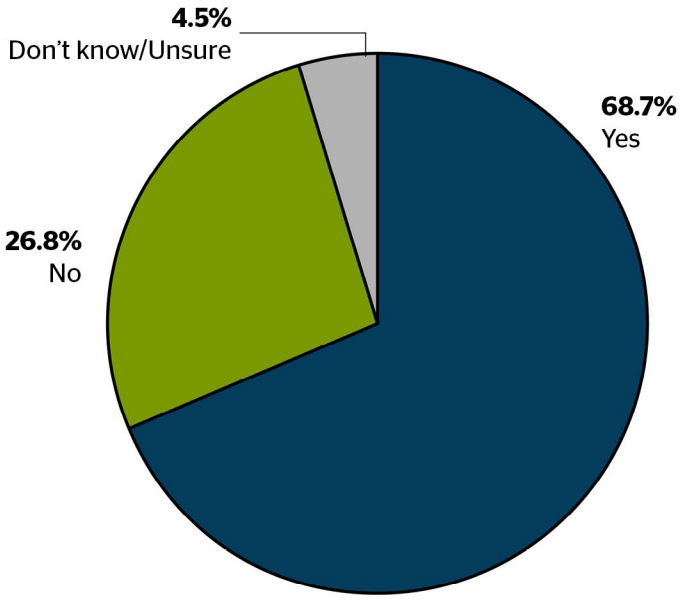
- **Incorporation into Strategic Plans:** While more than half (**58.10%**) of associations do not have risk management, safety and security integrated into their strategic plans, **25.30%** of organizations have incorporated safety and security into their strategic plans, with **11.60%** reporting plans to do so in the future.

Is risk management, safety and security incorporated into your organization's strategic plan?



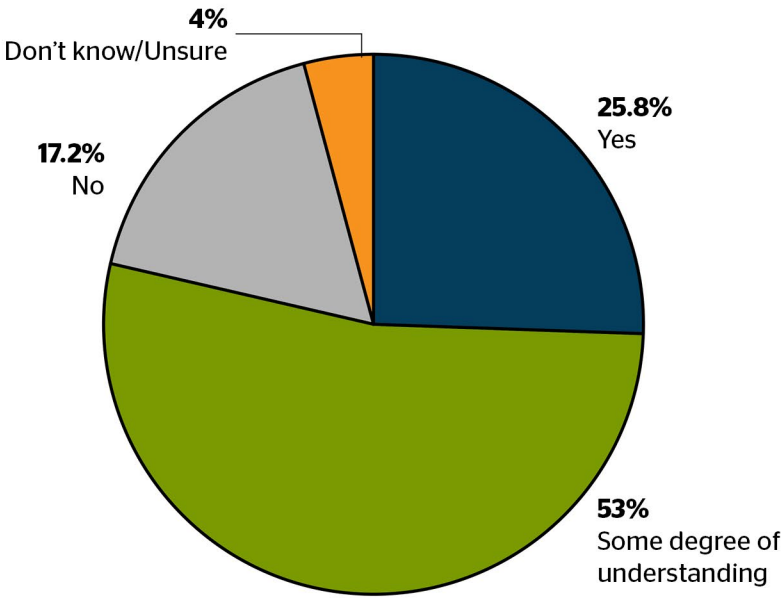
- **Conversations About Event Crisis Response:** More than two thirds (**68.70%**) of associations have had leadership conversations about how to respond to a crisis at an organizational event. Slightly over one quarter (**26.80%**) haven't yet had these discussions at the leadership level.

Has your organization's leadership had conversations about how to respond to a crisis at one of your events?



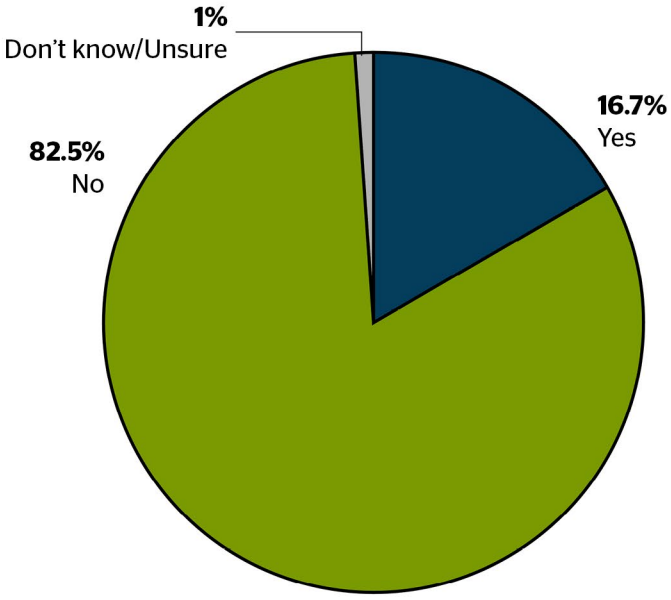
- **Understanding of Risk by Business Leaders:** While a significant portion of respondents (**78.80%**) report that business area leaders have at least some degree of understanding of how risk impacts their overall strategy and operations, there is room for improvement in enhancing their understanding.

In your opinion, do your business area leaders have a good understanding of how risk impacts the overall strategy and operations of the organization?



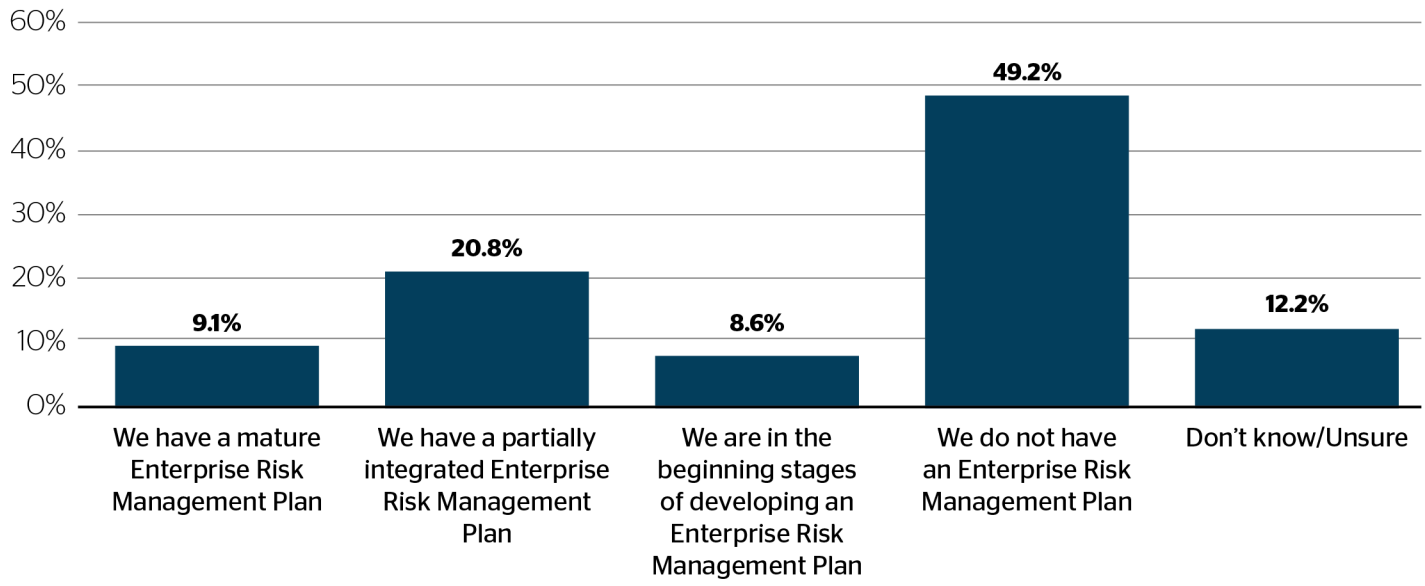
- **Experienced a Crisis:** While **82.50%** of respondents indicated that they have not experienced a crisis (excluding COVID-19), **16.70%** of respondents have experienced a crisis event in the past 12-18 months.

Not including the disruption caused by COVID-19 pandemic, has your organization experienced a crisis event in the past 12-18 months?



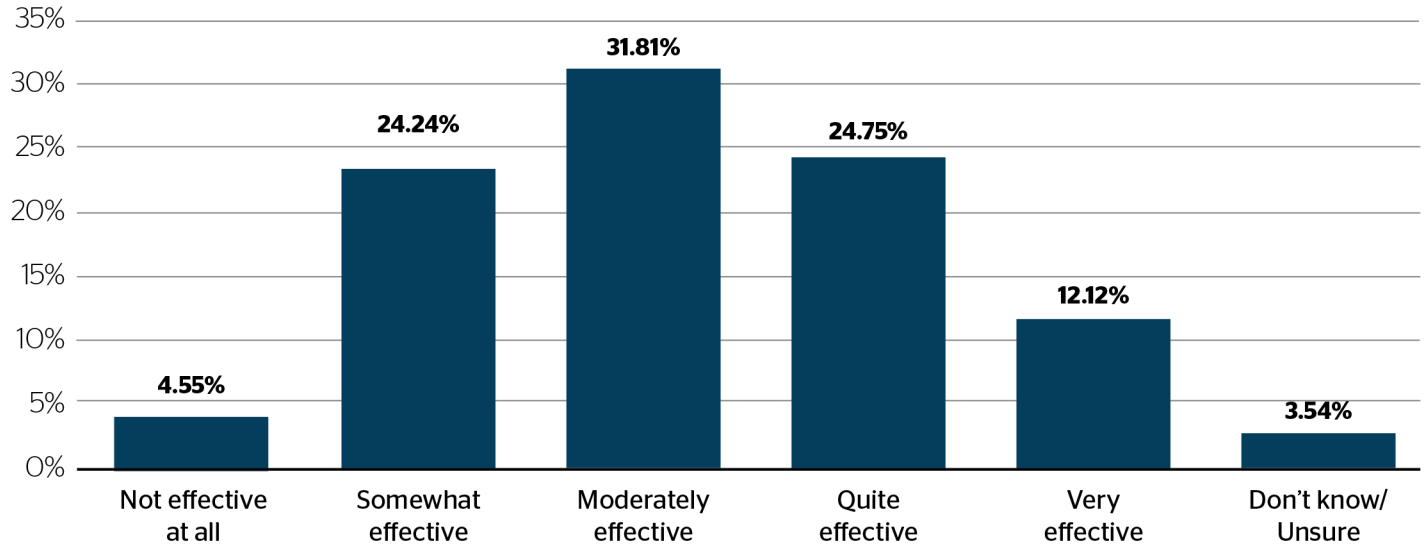
- **Enterprise Risk Management Plans:** Half of organizations (**49.20%**) do not have a formal Enterprise Risk Management plan, while others have either a mature or partially integrated plan (**29.90%**).

Does your organization have a formal Enterprise Risk Management Plan?



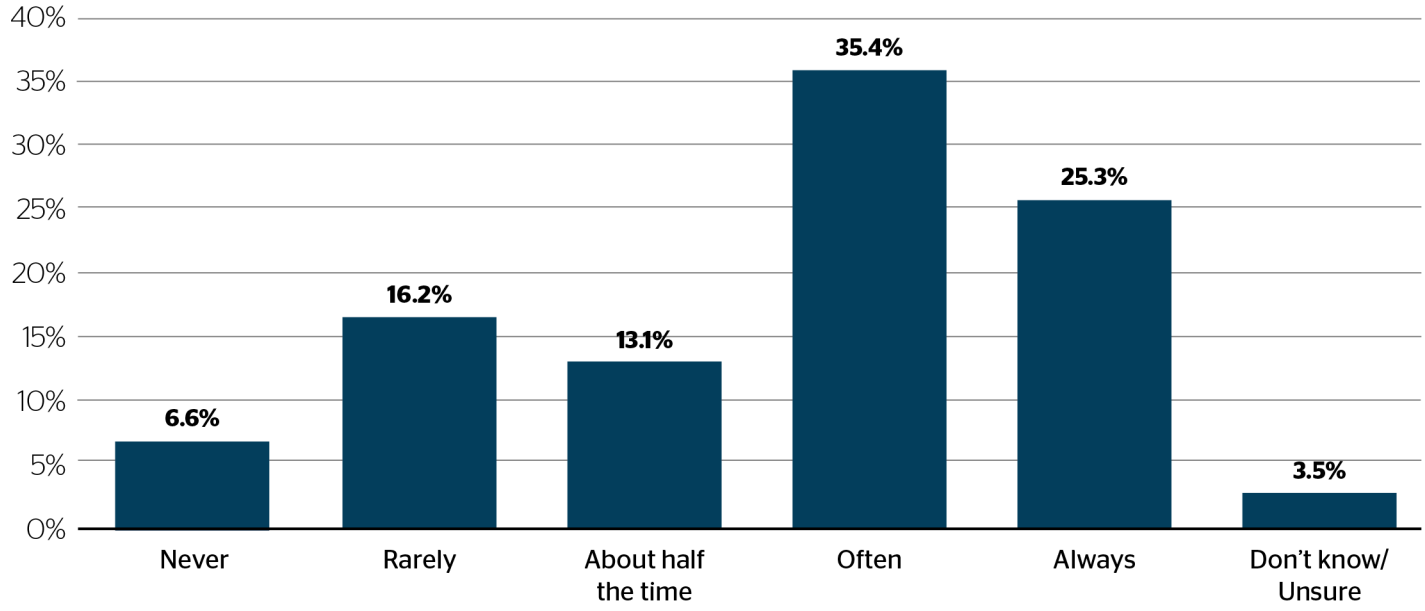
- **Emergency Response Effectiveness:** Slightly under one third of associations (**28.79%**) indicated they felt their association's emergency response was not at all or only somewhat effective. Over one third of respondents (**36.87%**) indicated they felt their plans would be quite or very effective. The remaining third (**30.81%**) indicated their plans may be moderately effective. Given the importance of response plans on safety and high impact events, there is room to move on these numbers.

In the event of an emergency, how effective would you say your organizations emergency communication/response plan would be?



- **Collaboration on the Impact of Risk:** Almost three quarters of associations (73.80%) indicated that they foster cross-departmental collaboration to discuss the impact of risk about half the time, often, or always, while 22.80% of respondents indicated they never or rarely foster this type of collaboration.

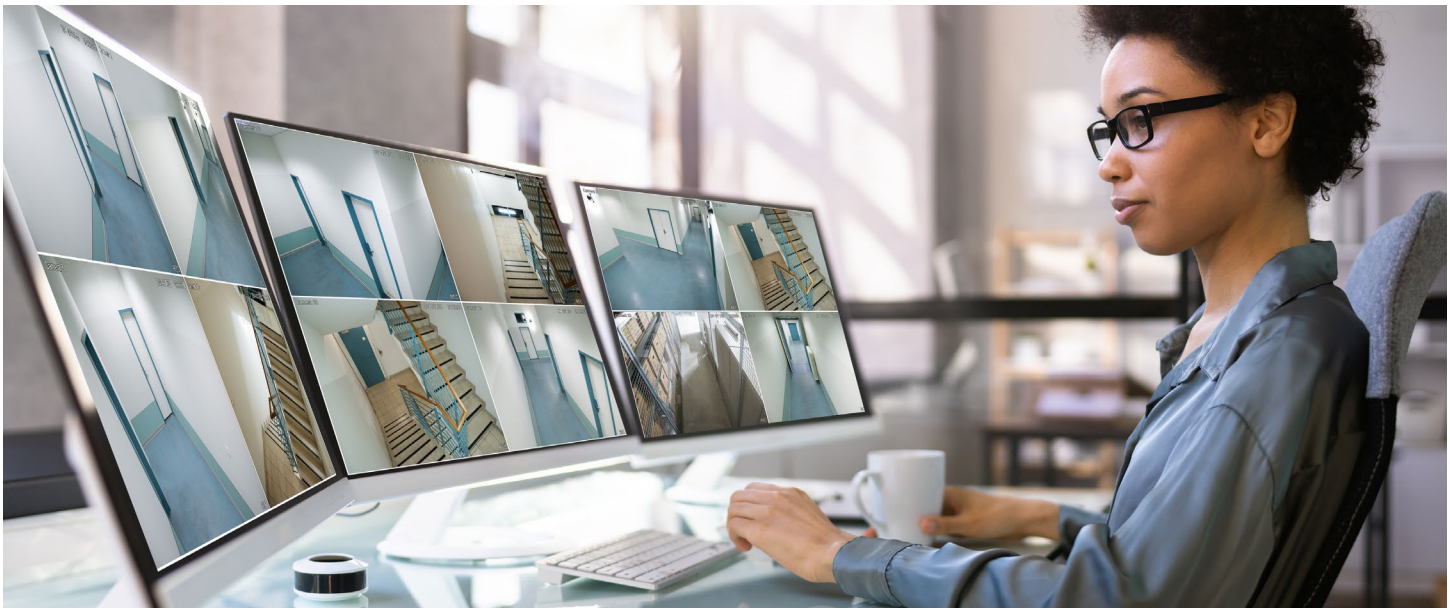
Does your organization foster cross-departmental collaboration to discuss the impact of risk (i.e., Event Team and IT discussing drawbacks/benefits of a new registration platform)?



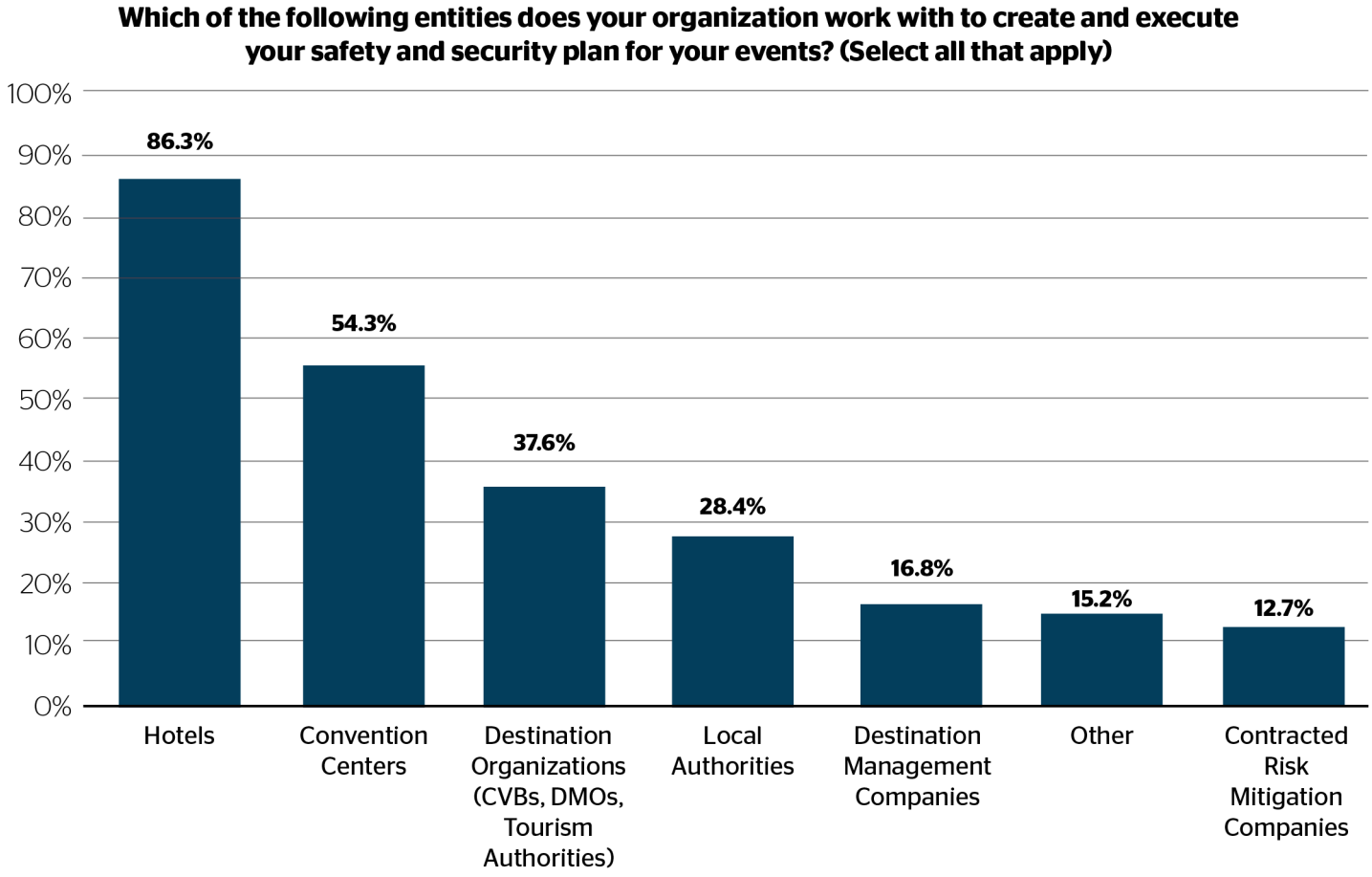
- **Factors Influencing Destination Selection:** Crime and safety, destination weather/climate predictions, and health and safety measures are the top factors considered when selecting event destinations. Accessibility policies and initiatives ranked fourth. Factors like political climate, perception of social justice & equality, and active legislation around Human Rights generally ranked lower.

Item	Overall Rank	Rank Distribution	Score	Number of Rankings
Crime and Safety	1		1,191	166
Destination Weather / Future climate predictions	2		1,154	161
Health and Safety measures	3		936	146
Accessibility policies and initiatives (beyond ADA requirements)	4		781	137
Politcal Climate	5		612	133
Other	6		610	120
Perception of Social Justice & Equality within the community	7		576	131
Active Legislation around Human Rights (Reproductive rights, LGBTQ+ rights, etc.)	8		522	132
Environmental policies and initiatives	9		472	128

Lowest Rank Highest Rank

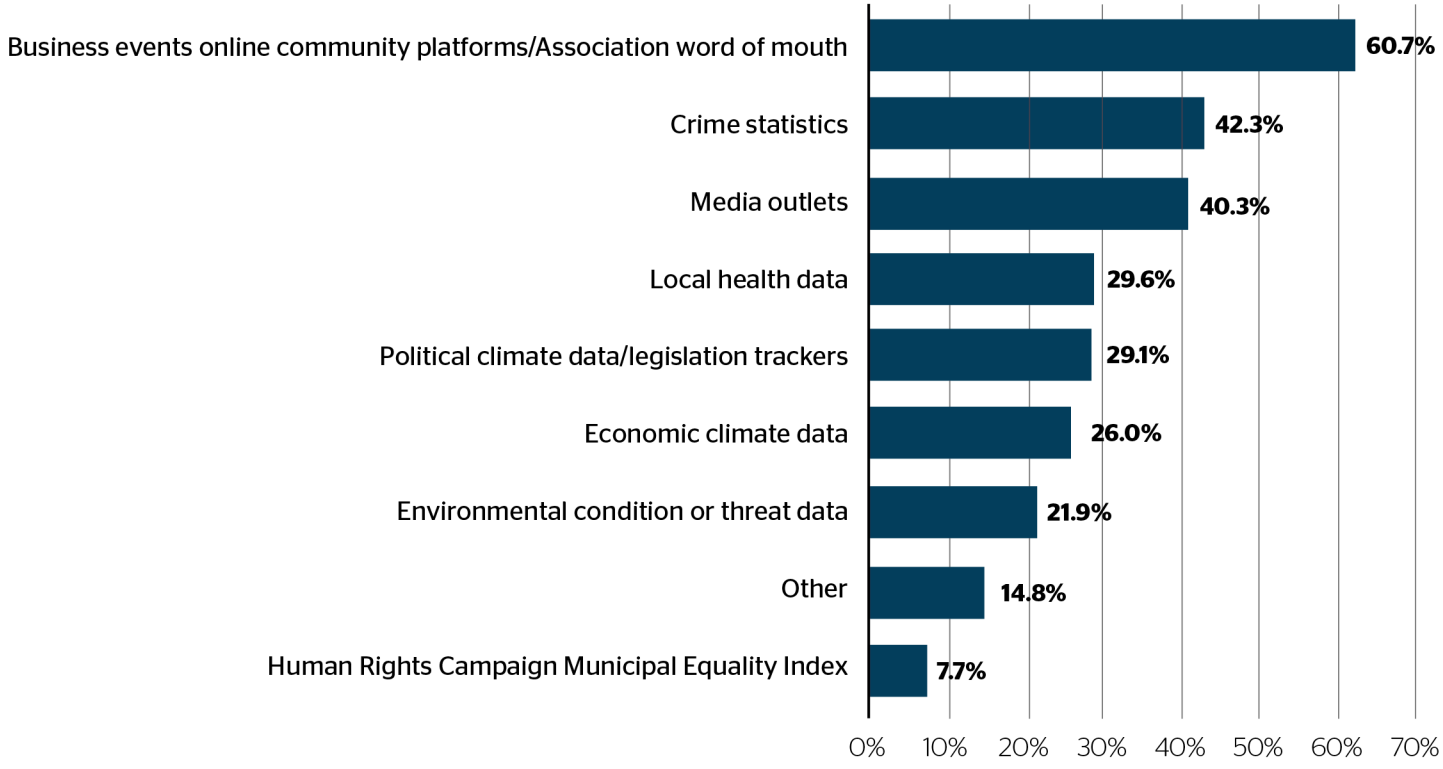


- **Partnerships for Safety and Security:** Organizations primarily work with hotels, convention centers, and destination organizations to create and execute safety and security plans for events. Local authorities ranked fourth.



- **Tools for Assessing Risk/Safety of Potential Event Locations:** More than half of associations rely on business events online community platforms/association word of mouth (**60.70%**) when assessing risk and safety of their potential event locations. Around 40% rely on crime statistics (**42.30%**) and media outlets (**40.30%**) whereas fewer rely on political climate data/legislation tracker (**29.10%**), economic climate data **(26.00%**), environmental condition or threat data (**26.00%**), other (**14.80%**), or Human Rights Campaign's Municipal Equality Index (**7.70%**).

What tool(s) is your organization using to assess the risk/safety of potential event locations? (Select all that apply)

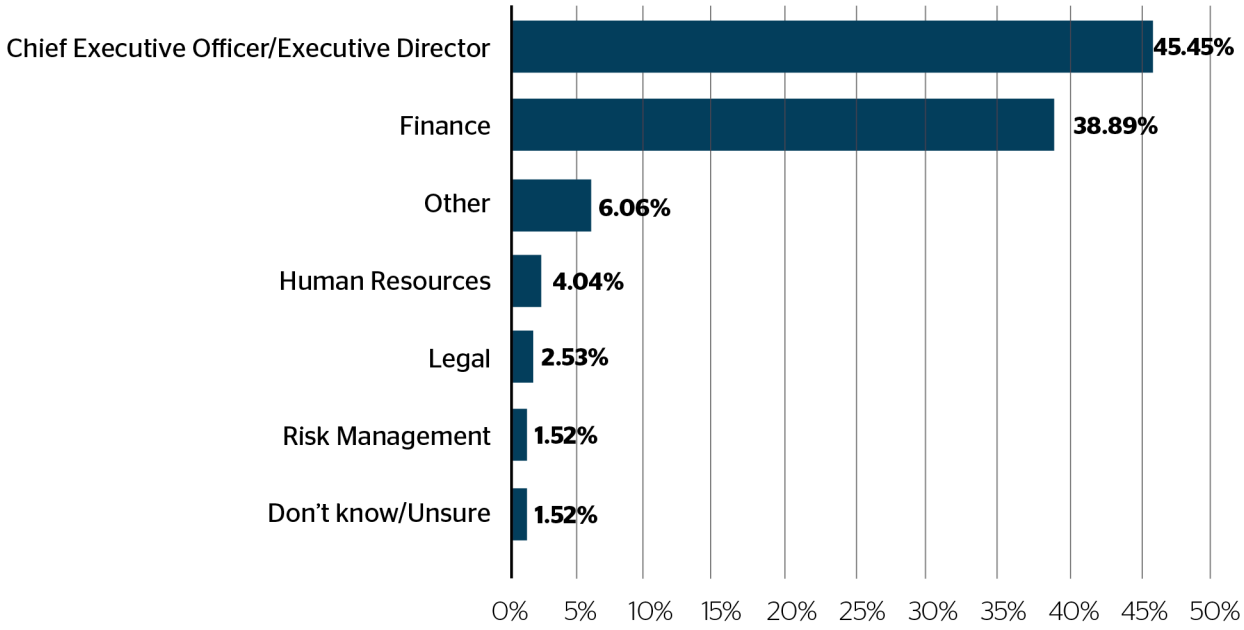


- **Types of Insurance:** Directors and Officers Liability (**85.86%**), Property/Casualty (**83.33%**) and Cyber Liability (**61.62%**) are the top three types of insurance associations reported purchasing.

Which types of insurance does your organization purchase?

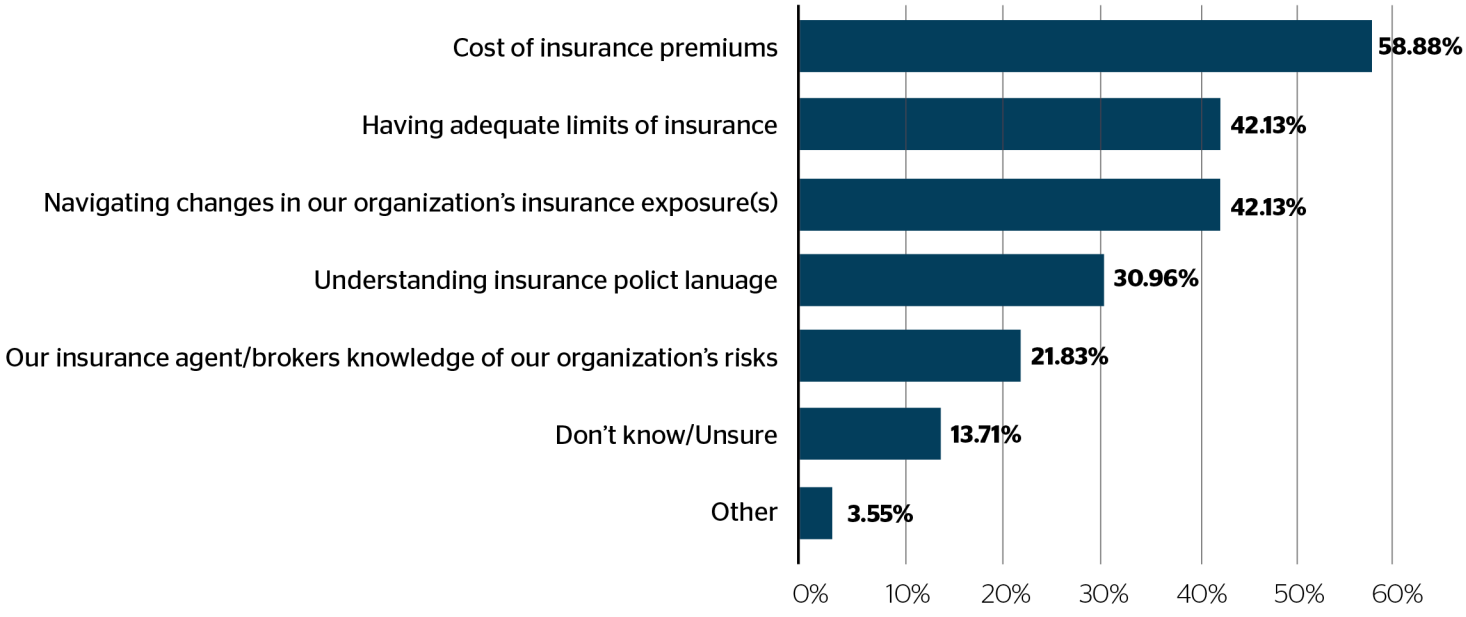
- **Who Purchases Insurance:** Responsibility for purchasing insurance primarily lies with the Chief Executive Officer/Executive Director (**45.45%**) or Finance department (**38.89%**).

Which types of insurance does your organization purchase?



- **Insurance Concerns:** The cost of insurance premiums is a significant concern for more than half (**58.88%**) of respondents.

What is the biggest concern with regard to your organization's procurement of insurance?



Glossary of Key Terms

- **Risk:** An uncertain future outcome that can either improve or worsen an organization's position; the effect of uncertainty on objectives (ISO 31000:2018[1]).
- **Dynamic risks:** Risks that are known to exist but may change over time.
- **Emerging risk:** A novel manifestation of risk or type that has not been experienced previously.
- **Strategic risks:** Internal or external uncertainties, whether event or trend driven, that impact an organization's strategies and/or the implementation of its strategies.
- **Risk appetite:** The total exposed amount that an organization wishes to undertake on the basis of risk-return trade-offs for one or more desired and expected outcomes.[2]
- **Risk management:** Coordinated activities to plan, direct, control and make decisions concerning the effects of uncertainty on objectives. (adapted from ISO Guide 31000:2018)
- **Strategic risk management (SRM):** A business discipline that drives deliberation and action regarding uncertainties and untapped opportunities that affect an organization's strategy and strategic execution.
- **Enterprise risk management (ERM):** A strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.
- **Risk tolerance:** The amount of uncertainty an organization is prepared to accept in total or more narrowly within a certain business unit, a particular risk category or for a specific initiative.[3]
- **Scenario planning:** A structured way for individuals or organizations to think about multiple plausible ways in which the future might unfold. The technique is used to inspire imagination and provoke "thinking the unthinkable," thereby increasing emerging risk sensing. Alternate definition from Art of the Long View, Peter Schwartz (1996): a tool for ordering one's perceptions about alternative future environments in which one's decisions might be played out.
- **Strategic risk assessment:** A systematic and continual process for assessing the strategic risks facing an organization.
- **Security:** The condition of being protected against hazards, threats, risks, or loss.

[1] https://www.iso.org/standard/65694.html
[2] Developing and Refining Risk Appetite and Tolerance (rims.org)
[3] Developing and Refining Risk Appetite and Tolerance (rims.org)
[4] https://instituteforpr.org/crisis-management-and-communications/

- **Crisis Management:** Holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience, with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities—as well as effectively restoring operational capabilities. NOTE: Crisis management also involves the management of preparedness, mitigation response, continuity, or recovery in the event of an incident—as well as management of the overall program through training, rehearsals, and reviews to ensure that preparedness, response, and continuity plans stay current and up to date.
- **Crisis:** The institute for public relations defines crisis as "a significant threat to operations that can have negative consequences if not handled properly."[4]
- **Emergency:** FEMA defines an emergency as "any incident, whether natural, technological, or human-caused, that requires responsive action to protect life or property."[5]

Crisis management also involves the management of preparedness, mitigation response, continuity, or recovery in the event of an incident.

- **Disaster:** FEMA defines a disaster as "an occurrence of a natural catastrophe, technological accident, or human-caused event that has resulted in severe property damage, deaths, and/or multiple injuries." [6]
- **Hazard:** FEMA defines a hazard as "something that is potentially dangerous or harmful, often the root cause of an unwanted outcome." [7]
- **Asset:** ASIS's Physical Asset Protection Standard published in 2021 defines an asset as "anything that has tangible or intangible value to an enterprise.
- **Business Continuity:** CISCO defines business continuity as: Business continuity is an organization's ability to maintain or quickly resume acceptable levels of product or service delivery following a short-term event that disrupts normal operations. Examples of disruptions range from natural disasters to power outages.[8]
- **Business Continuity Plan:** According to ISO 22301, business continuity plan is defined as "documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption."[9]

[5] https://training.fema.gov/programs/emischool/el361toolkit/glossary.htm
[6] https://training.fema.gov/programs/emischool/el361toolkit/glossary.htm
[7] https://training.fema.gov/programs/emischool/el361toolkit/glossary.htm
[8] https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-business-continuity.html
[9] https://www.iso.org/standard/75106.html

Business Continuity Planning

Provided by Bob Mellinger, CEO, Attainium Corp

A Business Continuity Plan (BCP) is a comprehensive strategy outlining how a business will continue operating during and after an unexpected disruption or disaster. Its primary goal is to ensure that essential business functions can continue with minimal interruption or be restored quickly in the event of a crisis.

A typical BCP includes:

1. **Risk Assessment:** Identify potential threats and assess their impact on business operations. This could include natural disasters, cyber-attacks, pandemics, supply chain disruptions, etc.
2. **Business Impact Analysis (BIA):** Evaluate the potential consequences of disruptions on critical business functions, such as financial loss, reputational damage, regulatory compliance issues, etc.
3. **Continuity Strategies:** Develop strategies and tactics to mitigate risks and maintain or restore operations. This may involve redundancy of critical systems, offsite data backups, alternative supply chain arrangements, remote work policies, etc.
4. **Emergency Response Procedures:** Establish protocols for responding to life safety and security emergencies, including communication plans, evacuation and shelter-in-place procedures, and coordination with emergency services.
5. **Crisis Management:** Designate a team responsible for implementing the BCP and managing crisis situations. This team typically includes senior leaders and key personnel from various departments trained to respond effectively to emergencies.
6. **Testing and Training:** The BCP should be regularly tested through drills, tabletop exercises, and simulations to ensure its effectiveness. Training employees on their roles and responsibilities during a crisis is crucial for successful implementation.
7. **Continuous Improvement:** Review and update the BCP periodically to reflect changes in the business environment, emerging threats, or lessons learned from past incidents.

By having a well-developed BCP in place, businesses can minimize the impact of disruptions and improve their ability to recover quickly, thereby safeguarding their reputation, revenue, and long-term viability.

BCP's primary goal is to ensure that essential business functions can continue with minimal interruption or be restored quickly in the event of a crisis.

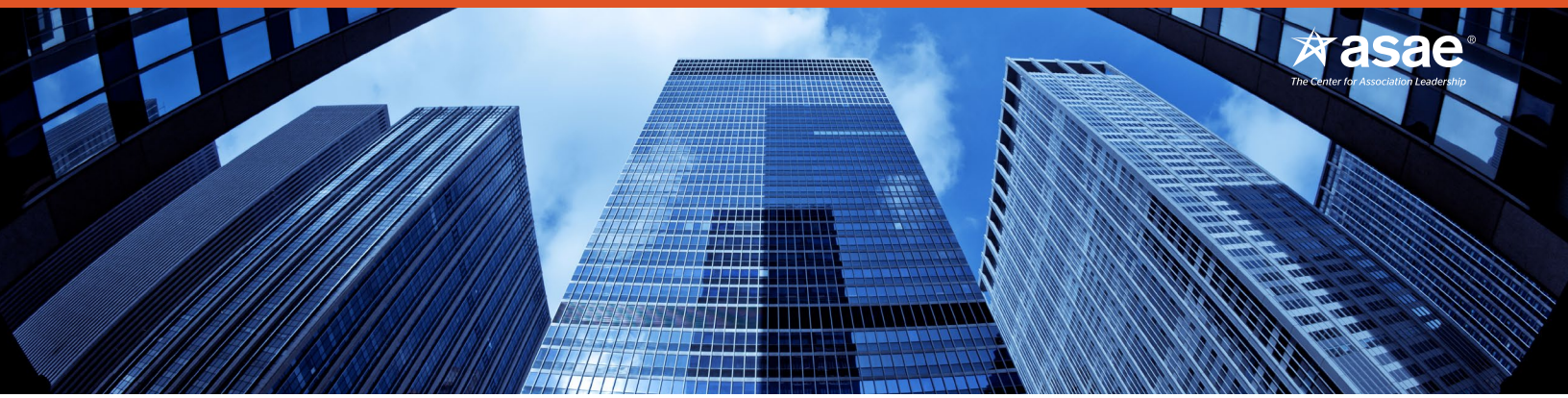
What Makes a Business Continuity Plan Successful

Provided by Bob Mellinger, CEO, Attainium Corp

Here are several factors that contribute to the effectiveness of a Business Continuity Plan (BCP):

1. **Comprehensive Risk Assessment:** An effective BCP begins with a thorough understanding of potential risks and threats that could disrupt business operations. This includes natural disasters, technological failures, cybersecurity breaches, supply chain interruptions, and other relevant hazards.
2. **Clear Objectives and Scope:** The BCP should have clearly defined objectives outlining what needs to be achieved during and after a disruption. Additionally, it should specify the scope of the plan, detailing which business functions, processes, and resources are covered.
3. **Involvement of Key Stakeholders:** Successful BCPs involve input and collaboration from key organizational stakeholders, including senior management, department heads, IT personnel, human resources, and other relevant parties. This ensures that all perspectives are considered and everyone understands their roles and responsibilities.
4. **Regular Testing and Training:** Testing the BCP through drills, simulations, or tabletop exercises is essential to identify weaknesses, improve response capabilities, and familiarize personnel with emergency procedures. Training employees on their roles and responsibilities during a crisis also enhances preparedness.
5. **Flexibility and Adaptability:** The BCP should be flexible and adaptable to accommodate changes in the business environment, emerging threats, and lessons learned from past incidents. Regular reviews and updates are necessary to ensure the plan remains relevant and effective.
6. **Effective Communication Protocols:** Clear communication is crucial during a crisis to coordinate response efforts, disseminate information, and keep stakeholders informed. The BCP should include communication protocols for internal and external stakeholders, specifying channels, procedures, and responsibilities.
7. **Backup and Redundancy:** Implementing backup systems, redundant resources, and alternative suppliers can help mitigate the impact of disruptions and ensure the continuity of critical business functions. This includes data backups, redundant IT infrastructure, secondary facilities, and diversified supply chains.
8. **Coordination with External Partners:** Collaboration with external partners, such as vendors, suppliers, customers, and emergency services, is essential for effective crisis management. Establishing relationships, sharing information, and coordinating response efforts can help minimize disruptions' impact on the broader ecosystem.
9. **Leadership and Decision-Making:** Strong leadership and clear decision-making processes are crucial during a crisis. Designating a crisis management team, empowering them to make timely decisions, and providing them with the necessary authority and resources can expedite response efforts and minimize downtime.
10. **Documentation and Documentation:** Documenting all aspects of the BCP, including risk assessments, procedures, contact information, and recovery strategies, ensures that information is readily available during a crisis. This facilitates a swift and coordinated response, reducing confusion and minimizing disruptions.

The remainder of this resource takes a closer look at the risk and crisis management components of business continuity planning.



Risk Management for Associations

Provided by RIMS

Associations exist in a complex and unique environment. It is a people-centric business, engaging the time and talents of members, volunteers, staff, attendees, customers, students, and many others. While most things usually go well, bad things can and do happen. Risk is ever-present: at meetings and events, in the office, in the board room, in IT systems, in almost every aspect of association operations. Association professionals and association boards can address this reality by employing risk management strategies and tactics.

Association Risks

The following are major areas of risk that are common to associations. This list is not complete, nor does it provide legal advice. Association professionals and association boards should seek qualified legal advice, as well as advice from qualified risk management and insurance professionals.

Employees

- Many legal claims against associations are employee related and can range from discrimination, to unfair treatment, to wrongful termination, to improper handling of FLSA status, FMLA, or ADA accommodations.
- Conversely employees can also be a source of risk to the associations if they embezzle funds, show favoritism, and/or behave inappropriately toward colleagues or members.
- The need for physical safety and security is another consequence of having employees. This includes in the office, while traveling on association business, working from home and during conferences and other events.
- Associations that offer medical and other insurances for staff, or 401k programs and other benefits, are subject to the ERISA Act of 1974 and many other regulations.
- Succession and transition planning are other aspects of talent risk. Worker's compensation insurance, general liability and other insurance policies are important aspects of risk management mitigation.
- *Potential Solution:* An updated employment manual and regular training for supervisors and employees are important tools for mitigating these risks.

Members

- Member-related risks can include instances of discrimination and harassment during member-member or member-staff interactions.
- Associations need to mitigate their risk as it relates to possible antitrust violations.
- Member termination for anything other than not paying dues can also pose a risk to the association — this could be tied to a Code of Ethics violation or based on member behavior.

- *Potential Solution:* Clear bylaws are important for mitigating member-related risks as are accompanying policies and procedures with steps to assure due process.

Volunteers

- Volunteers can pose additional risks to an association since they can be perceived to be an actual or apparent authority as it relates to decision-making for the association.
- They can also pose a brand and reputational risk if they engage in inappropriate actions and/or behavior or speak publicly against association positions.
- Boards and other leaders are exposed to risk from decisions made, or decisions that are not made.
- *Potential Solution:* Due to the position of authority volunteers hold, providing regular training, having a Code of Conduct, and quickly addressing inappropriate actions are critical tools to minimizing risk. Additionally, Directors and Officers liability insurance should be obtained.

Advertisers, Exhibitors, Sponsors

- Associations need to communicate about and carefully choose advertising and exhibiting opportunities since there may be perception of endorsement of a company. Associations who actively engage in endorsement activities have to be doubly attentive to risk should one of the products/services they endorse prove to be dangerous, not meet published standards, or if a company is embroiled in controversy.
- Attention also needs to be paid to inclusion of advertisers to ensure none are excluded for reasons that could be perceived as anti-trust related or that is exclusionary to a demographic, culture or the like (for example excluding companies who compete with members from advertising in journals).
- Associations also need to be mindful of the risk related to taxes on unrelated business income.
- *Potential Solution:* Establishing objective standards for selection and promotion of advertisers and exhibitors and ensuring equity in access to opportunities can help mitigate risks in this area.

Meetings and Events

- In most large-scale events, medical emergencies tend to be most common and associations must be prepared to provide medical assistance onsite or direct attendees to locations to receive necessary care.
- Just as an organization would protect physical assets and property, association leaders have a responsibility to provide attendees with a secure meeting location.
- Inclement weather and natural disasters pose a significant threat to both indoor and outdoor meetings. Additionally, these threats can have a significant impact on transportation and housing arrangements.
- Cyber threats are a top concern for all organizations and are just as significant to the delivery of a successful meeting. Cyberattacks on registration data, speaker presentations, and other intellectual property in the form of ransomware attacks, as well as facility Wi-Fi or the theft of attendee lists are examples of this exposure.
- Attendees' misconduct is another threat that associations must consider. This could include threatening, abusive, or harassing language, assault and other actions that compromise safety and security.
- *Potential Solution:* Thorough planning is essential to help ensure the physical safety of event participants. Every conference, convention and event should have a detailed security plan, and a crisis management and communication plan. Engaging with local law enforcement and the safety officials from the meeting venue prior to the event is another measure associations can take, as well as increasing training on rapid response, communication and evacuation plans.

Intellectual Property

- Associations must be aware of and respectful of the intellectual property rights of individuals and companies – this includes copyright, trademarks, service marks, patents, etc.
- *Potential Solution:* Ensuring employees and volunteers understand IP protections and obtaining appropriate licenses are two critical methods for mitigating this risk.

Property and Casualty

- Loss of access or use of the space, damage or destruction of property, accidents or injury to people, environmental issues and contamination are just a few of the concerns.
- *Potential Solution:* Property and casualty insurance is typically an essential element in risk management programs.

Privacy

- Associations have an obligation to protect the personal information they receive from members and customers.
- Several laws, such as GDPR — the European Union's General Data Protection Regulation and many states such as the California Consumer Privacy Act — set forth the obligations of those who gather, pass or retain data.
- *Potential Solution:* Keeping informed of the various privacy laws and ensuring the association is in compliance wherever they are doing business is critical. This will require active management of vendors to ensure they are adhering to privacy laws if they are storing member data on behalf of the association.

Financial

- Disruptions that prevent the association from generating expected and new revenue vary from association to association.
- Depletion of reserves would have a significant impact on an association's ability to continue to innovate.
- Market fluctuation and inflation can also cause greater uncertainty.
- *Potential Solution:* Most associations engage independent outside auditors to assess financial controls, confirm financial reporting and evaluate the trust worthiness of financial systems. Additionally, central to financial risk management are budgeting, regular financial reporting, separation of duties, proper financial controls and independent auditing.

Chapter and Other Component Organizations

- Any activities or actions taken by formally affiliated or chartered components can pose a risk to the parent association.
- Many if not all the same risks that associations face are faced by components. However, since many components often rely on volunteers who change positions often, components can be the weakest link in an association's risk management program.

Potential Solution

- Regular training and monitoring is critical for mitigating risks within components.

Credentialling

- Violation of a Codes of Ethics can hinder the success of an association's credentialing endeavor.
- Failing to maintain an accreditation and meeting the standards of standard-setting agencies might result in both financial losses and reputational damage.
- *Potential Solution:* Objective standards, full disclosure, strict security, independent governance and due process are among the critical risk management aspects of such programs. Additionally, seeking the advice of qualified legal counsel is absolutely necessary to guide and operate these offerings.

Cybersecurity

- Like every person and every business, associations are vulnerable to cybersecurity breaches.
- Denial of Service attacks, ransomware, spear-phishing, trojan horse attacks, man-in-the-middle attacks, domain-name spoofing and a rapidly changing and evolving array of other schemes are among the cyber risks that associations face on a 24/7/365 basis.
- *Potential Solution:* Strong cybersecurity defenses, including network security, endpoint security, mobile security, strong firewalls, antivirus software, intrusion detection are just a few of the cyber risk mitigation tactics that associations employ. In addition, effective and ongoing user training is essential to protect data, member records, private information and financial information, among others.

Factors for Associations to Consider when Developing Risk Management Approaches

Provided by RIMS

Association professionals must be risk aware and proactive in developing risk mitigation and insurance programs. It is vital that association leaders, both staff and board, engage in open and honest dialogue about all aspects of the business, potential risks, and are aligned on a comprehensive plan for enterprise risk management. This process involves:

Outlining the risk environment and identifying risks	Deciding how risk will be managed, mitigated, or insured	Developing proactive measures to monitor risk	Evolving plans as needed

Specifically:

- Staff professionals and boards share the responsibility for risk management.
- Leaders must stay abreast of risks and the association's risk exposure.
- Associations may need to consider developing a formalized Enterprise Risk Management plan (ERM). That plan would help an association assess their risk exposure, determine their risk appetite, identify mitigation strategies, determine adequacy of insurance coverage, and establish processes, policies, and procedures that will help manage and respond to evolving risks..
- A careful, comprehensive, and transparent discussion about risk is essential. The board and staff must be aligned about the association's understanding of risk, its appetite for risk-taking and the proactive measures

that it will take to respond. Scenario planning exercises are one of the tools used to explore potential situations and responses, as well as challenging assumptions and expectations.

- Ultimately, association risk management ensures the continuity of the association's mission, its ability to serve members, support and protect employees, as well as ensure the safety, security, and sustainability of the organization.

Building a strategic approach to risk management within an association requires upfront planning and intentional focus and decision making. Associations should intentionally develop and consider:

Risk Appetite and Risk Tolerance

This section is adapted from RIMS' Developing and Refining Risk Appetite and Tolerance executive report*.

By definition, **risk appetite** is the total exposed amount that an organization wishes to undertake on the basis of risk-return trade-offs for one or more desired and expected outcomes. **Risk tolerance** is the amount of uncertainty an organization is prepared to accept in total or more narrowly within a certain business unit, a particular risk category or for a specific initiative.

In other words, risk appetite is the amount of risk your organization is willing to take to pursue its objectives. Risk tolerance sets an acceptable level of variation for that appetite around key risks or aggregation of risks, or around strategic initiatives.

By creating risk appetite and tolerance statements, an organization can develop an overall approach to how its policies, processes and controls are established, communicated, and monitored.

Sample risk appetite statements might include:

- A target of return on equity of X%
- Retention ratio equal to or better than our peers
- Less than X% chance of losing no more than X% of capital in a given year
- X% of asset loss in any given year
- Less than X% chance of reduction in net income of X%

In general, risk appetite and tolerance is a framework for strategic decisions because it links risk-taking to the organization's objectives. It promotes strategic alignment by providing clear articulation of the business activities employees should engage in and what levels of risk they should assume.

Risk appetite and tolerance also provides a structure for strategic decisions and a benchmark for discussing the implications of value-creation opportunities. It can help an organization understand the material risks it faces, both at an aggregate and a business unit level. Because it provides a tool for communication and monitoring, it can be used to engage the board in risk governance from a strategic point of view.

Clearly defined risk appetite and risk tolerance statements allow companies to better achieve targeted performance by helping management make risk-informed decisions, allocate resources, and understand risk/reward trade-offs.

* Developing and Refining Risk Appetite and Tolerance - https://www.rims.org/resources/risk-knowledge/white-paper/developing-and-refining-risk-appetite-and-tolerance

Risk Culture

In a paper on cultivating a "Risk Intelligent Culture," the global accounting and audit firm Deloitte, noted "Risk culture encompasses the general awareness, attitudes, and behaviors of an organization's employees toward risk and how risk is managed within the organization. Risk culture is a key indicator of how widely an organization's risk management policies and practices have been adopted."[10] Association leaders and boards should intentionally determine what their risk culture should be.

Who Manages Risk

Determining how consolidated risk management will be versus diffused across the organization is another intentional conversation associations may need to have. Even in a situation where the CEO, CFO, or a Chief Risk or Compliance Officer oversees the risk function, risk will continue to be part of everyone's job and organizations that develop strong risk management cultures will communicate and measure this. It's important that everyone in the organization understands their specific role relative to risk.

Identifying and Prioritizing Risks Within Your Association

Provided by RIMS

Risk Identification

How can an association identify its risks? Some organizations may benefit from scenario planning. Example scenario planning methods are included below from the RIMS' Managing Alternative Futures with Scenario Planning report[11]. Associations may benefit from surveying staff to help identify risks.

Scenario Planning Method	Use	Example	Considerations	Level of Effort, Engagement, and Resources
What If Scenarios	Considers the effects of variability of potential events on a project, strategy, assumption or timeline	Project planning, initiative decisions or product launch	Involves examining the outcomes if certain things take more or less time, require more or less funding, result in unintended consequences, or other unanticipated outcomes. In essence, a what-if scenario amounts to asking, "What if ...?" for each major decision or aspect associated with a developing plan. For example: • What if there is a budget shortfall? • What if the market shifts dramatically and we need to reorganize our teams? • What if a technological breakthrough makes half of our employees redundant? • What if the public reaction to our current social strategy is negative?	Minimal effort and resources. Can be conducted in 60-minute sessions each with a half dozen people with approximately 30–40-minute prep time

[10] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/center-for-corporate-governance/us-ccg-cultivating-a-risk-intelligent-culture-050212.pdf

[11] RIMS' Managing Alternate Futures with Scenario Planning report https://www.rims.org/resources/risk-knowledge/white-paper/managing-alternate-futures-with-scenario-planning

Scenario Planning Method	Use	Example	Considerations	Level of Effort, Engagement, and Resources
Key Risk Factor Scenarios	Determines the relevant uncertainties that are integral in the strategy or issue under consideration	Strategy, issue, challenge decisions	Involves developing story narratives for an array of key variables over a period of time. May be leveraged for identifying, focusing, analyzing, and tracking emerging risks. As scenarios are developed, action plans are likewise developed based on scenario possibilities that could be triggered if events similar to those covered in the scenarios begin to develop.	Minimal to moderate effort, engagement and resources depending on the complexity of the strategy or issue under consideration. Can be conducted in 60- to 90-minute sessions each with a dozen people with approximately 120-minute prep time.

Scenario Planning Method	Use	Example	Considerations	Level of Effort, Engagement, and Resources
PESTEL Scenarios	Reveals the impact of the external environment that could influence the success or failure of strategic decisions. This may also include key driving forces that are specific to an organization, such as customers, suppliers, competitors, etc.	Project or strategy decisions (e.g., major product launch)	Involves the evaluation of key external forces through the lenses of six categories: • **Political:** domestic and foreign policies (tax, fiscal, trade tariffs), elections, international relations, international trade, etc. • **Environmental:** business environmental analysis of factors such as natural resources, climate change, extreme weather, natural disasters, species migration, etc. • **Social:** population analysis including age, sex, birth rate, death rate, employment status, etc. Individuals, their ways of living, values and beliefs, consumption trends and decisions shaping the environment. • **Technological:** availability of and innovation in technological capabilities, automation, research and development advancements, etc. • **Economic:** leading and lagging macroeconomic trends such as inflation, interest rates, gross domestic product growth (GDP), foreign direct investment (FDI), foreign exchange, consumer purchasing power, stock market trends, etc. • **Legal:** current and upcoming legal and regulatory environment including relevant laws, regulations and standards.	Moderate to significant effort, engagement, resources and complexity. Can be conducted in multiple workshop sessions (2–3 hours) each with up to thirty people over several weeks with approximately 1–3 week prep time and 1–2 weeks for documentation and validation.

Risk Prioritization

Once the risks are identified, the organization needs to assess and prioritize them. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) of the Society of Corporate Compliance and Ethics & Health Care Compliance Association (SCCE & HCCA) developed the following key considerations for assessing risks:

- "Adopt a uniform scale/scoring system for measuring severity of compliance risks.
- Consider qualitative and quantitative measures.
- Establish criteria to assess impact and likelihood of compliance risk event occurrence.

- Assess severity of risk at different levels (organizational, regional, affiliate, etc.).
- Consider design and operation of internal controls intended to prevent or detect compliance risk events.
- Minimize bias and inadequate knowledge in assessing severity (e.g., minimize self-assessments, use multidisciplinary teams)."[12]

Associations could look at the potential **impact** to the organization if a risk materialized and the **likelihood** of the risk materializing and then plot risks on the likelihood and impact axes to obtain risks scores. They can then use these scores to identify which risks are the top risks and incorporate those into their dashboards and reports as well as into their mitigation planning.[13]

Communicating Risk to Boards

Assessing risk is a strategic function and communicating risks clearly to boards is important. When developing a plan to communicate risks to boards it is important to determine:

- **Who:** Deciding who will receive risk communications, such as an audit committee or the full board is a key step. Some associations may have a specific risk committee, however many will not. A risk report may also list the senior staff leads (CEO, CFO, CIO, or others in the organization who have those roles) responsible for specific risk areas. Another 'who' question is who will deliver the information to the board.
- **Cadence:** A study from North Carolina State University indicated that there isn't a consistent pattern of board reporting, however the report highlighted that "several respondents noted the scheduling of risk reporting coincided with the planning cycle of the organization."[14] Associations may need to determine, and then deliver on, the cadence for risk reporting to their boards.
- **Risk Prioritization:** Associations will need to determine which risks will be included in the risk reports. Some organizations may include the top 10 risks and others may include more but categorize them. Risk dashboards or heat maps can be used to highlight key risks.

The following additional elements that may be included in board communications comes from RIMS' Communication with the C-Suite and Board, Visualizing Enterprise Risk Management Information.[15]

- **Business context statement:** High-level snapshot of the coverage of the report, including part(s) of the organization, timeframes, perhaps brief restatement of top business priorities/key strategic objectives, summary of material business changes such as significant global/industry indicators, major mergers, acquisitions and divestitures activity, big wins or heavy losses, and top leadership changes as relevant to the organization. This focuses the audience and frames the enterprise risk information in a business context.
- **Risk appetite statement:** A clear, written risk appetite statement is essential to any ERM strategy. A responsibility of senior management and the board, this statement definitively states the organization's risk appetite in terms of acceptable and unacceptable risk to organizational strategy and objectives, especially with respect to outside stakeholders. A risk appetite statement should communicate the "tone from the top" and facilitate risk communication and understanding throughout the organization.

[12] https://www.coso.org/_files/ugd/3059fc_5f9c50e005034badb07f94e9712d9a56.pdf
[13] Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf
[14] https://us.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/erm-reporting-key-risk-2015.pdf
[15] Visualizing Enterprise Risk Management Information

- **Risk tolerance calculation:** The risk tolerance calculation is a determined or calculated amount of risk, expressed financially, that the organization is willing to take on in pursuit of business objectives. It should define both the amount of acceptable risk the organization wants to take on, as well as the upper limit of downside risk it can afford without material financial impact.
- **Emerging risk review:** Emerging risks may be one of the most difficult of information requirements — an understanding of technological disruption, the velocity of change in certain risks and global trends all need to be considered. The most discussed example in the boardroom of emerging risks is the threat posed by cybersecurity. Any relevant information that can be provided to the C-suite and board of directors should be considered for inclusion in reporting.

Small Staff Focus

Provided by RIMS

Dedicating resources, allocating employee time, as well as making financial investments can certainly accelerate and strengthen an association's risk and resiliency program. However, a risk management program can be tailored to an association's capacity and needs. The key is getting started, and then expanding incrementally over time.

For small-staffed associations — and perhaps those that have limited dispensable resources — there are cost-effective strategies that can enhance risk management capabilities, including:

1. **Tone at the Top.** For risk management to succeed it must have the support of leadership. Along with leadership's buy-in, there must be an effort to embed a risk-aware culture — the notion that "everyone is a risk manager" — across the organization. Only with leadership and managers on-board and managers embracing the power of risk management to help them reach their goals, can a risk management program effectively protect assets and support innovation.
2. **Identification.** Upon initiating the risk management journey, it is critical for the association to identify its most valuable assets. It must also conduct a financial analysis to better understand how revenue is generated today, and how (or opportunities for how) it will be generated in the future.
3. **Scenario Plan.** With an understanding of what is most valuable, association leaders should be proactive and start to plan. What happens if the organization is no longer able to deliver revenue-generating resources, services or products? What internal risks and external risks could cause the greatest disruption and delay the delivery of resources? And, what trends are impacting the organization's members or stakeholders and how is the industry or profession evolving? These challenging questions must be explored. Scenario planning can be conducted as a table-top exercise or brainstorming session and are an extremely effective way to engage the association's key decision-makers and uncover new, un-thought-of-before challenges.
4. **Lean on Vendors.** Associations can (and should) leverage the resources of the third-party vendors. Hotels, convention centers, housing partners, and even digital platform providers, could offer services or the expertise of their staff to help the association strengthen safety and security.
5. **Get an Expert.** Hiring a risk management professional would be ideal but, there are qualified and experienced risk management consultants available who specialize in guiding associations through the risk management process. Additionally, an organization's current insurance provider and/or insurance broker often provide risk management consultancy services.

Moving from Risk Management to Crisis Management

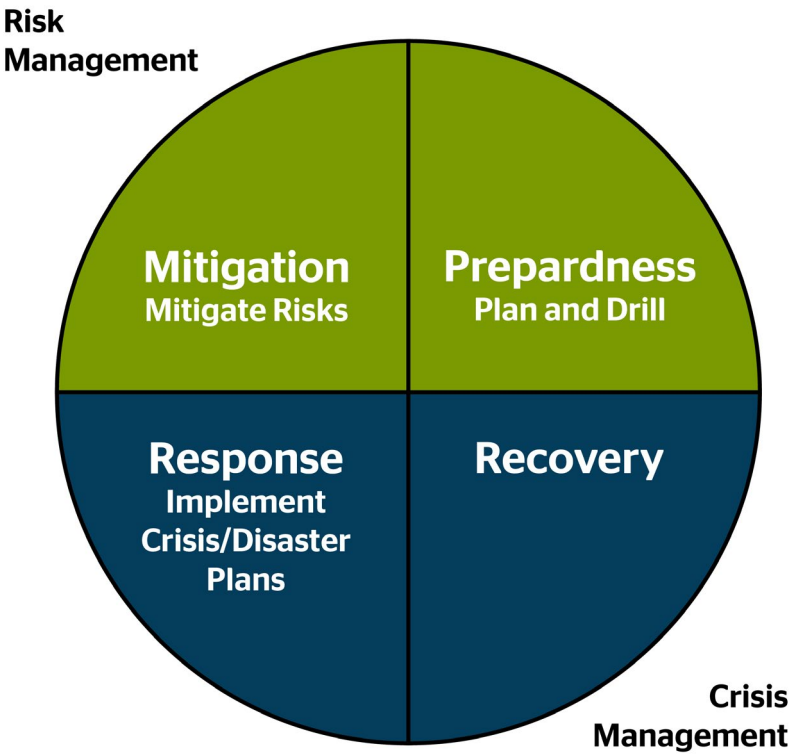
Emergency Management and Response

Managing risks is an essential function for an association, but so is the capacity to plan and manage emergencies and ensuring business continuity. ASIS defines emergency management/response as the planning and activity associated with detecting, containing, and dealing with the immediate impact of an event (such as putting out the fire in a fire event or locking down the network in a cyber breach).

The U.S. Federal Emergency Management Agency (FEMA) identified four components of emergency management and response. Those are mitigation, preparedness, response, and recovery.

Mitigation	Preparedness	Response	Recovery
Definition: This phase includes any activities that prevent an emergency, reduce the likelihood of occurrence, or reduce the damaging effects of unavoidable hazards. Mitigation activities should be considered long before an emergency. **Example(s):** Purchasing insurance	**Definition:** This phase includes actions taken to prevent or reduce the cause, impact, and consequences of disasters. **Example(s):** • Developing disaster preparedness plans for what to do, where to go, or who to call for help in a disaster • Exercising plans through drills, tabletop exercises, and full-scale exercises	**Definition:** The response phase occurs in the immediate aftermath of a disaster. During the response phase, business and other operations do not function normally. Personal safety and wellbeing in an emergency and the duration of the response phase depend on the level of preparedness. **Example(s):** Implementing disaster response plans	**Definition:** During the recovery period, restoration efforts occur concurrently with regular operations and activities. The recovery period from a disaster can be prolonged. **Example(s):** • Preventing or reducing stress-related illnesses and excessive financial burdens • Rebuilding damaged structures based on advanced knowledge obtained from the preceding disaster • Reducing vulnerability to future disasters

When overlaying the framework of mitigation, preparedness, response, and recovery to risk and crisis management, the first two areas, mitigation and preparedness, more closely align to risk management. Response and recovery align with crisis management. That said, the concepts overlap and have a lifecycle approach. Its objective is to avoid crisis and recover from any active emergency with as minimal disruption as possible.



Organization-Wide Crisis Management

Provided by ASIS

When a crisis or emergency strikes, many decisions must be made while the event is still unfolding, and the true dimensions of the situation are unknown. While some decisions may affect the health of the organization for many years, others will have an immediate effect on its ability to survive at all. An emergency or crisis can overwhelm those who have done no planning or preparation. The logical beginning of all aspects of responding to an emergency or a crisis is the development of a plan that does the following (ASIS BCM 2021):

- Defines the term and scope of a crisis or emergency in terms relevant to the organization;
- Establishes a group or team to perform specific tasks before, during, and after a disruptive event;
- Establishes a method for using available resources and for obtaining additional resources at the time of an event;
- Provides a means for moving normal operations into and back out of the crisis mode of operations;
- Provides a plan and framework to continually test and maintain the plan and response capabilities.

This section is taken with permission from ASIS International's Protection of Assets, Crisis Management publication.

The ASIS International Business Continuity Management Guideline describes crisis management as:

[A] holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience, with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities—as well as effectively restoring operational capabilities.

The ultimate goal of crisis management is to protect core assets of the organization (e.g., reputation, brand, financial wellbeing, trust, physical and intellectual property, and key relationships) from as much harm as possible caused by a business-interrupting event. Crisis management must take into account how to best keep the enterprise fulfilling its mission while also recovering from the impact of the event once the continuity and recovery phase is entered.

Team Position	**Name**		
Crisis Management Team Leader	Named Per Event		
Department Representation	**Name**	**Contact Information**	**Tole on Team**
Corporate Security			• Management of all law enforcement and emergency management relationships, and the flow of information to and from, Local, State, and Federal agencies • Governance over all Business Continuity, Disaster Recovery, and Crisis Management programs for the enterprise
Customer Facing Security			
Crisis Management			
Information Security			• Responsible for the direct management of and technology impact of the event to include analysis and resolution
Legal			• Provide legal council from beginning to end of event • Monitor for PII Other privacy issues • Communicate privacy issues to executies
Public Affairs/Corporate Communication			• Internal/external communication to all stakeholders
Humane Resources			• All aspects of employee welfare and impact assessment
Facilities			• Manages impact of any critical event on the event facility, in particular providing support to incident commanders at facilities

(ASIS International's Protection of Assets – Crisis Management)

A healthy crisis management program ensures that all functions in the organization are prepared to support all levels of the organization that are affected. It also ensures that the crisis management program is not dominated by one functional area.

Crisis Management Plan

Provided by ASIS

The crisis plan will need to be tailored to the specific needs of the organization and its mission. However, some typical aspects of crisis management plans include:

- Crisis management team;
- Crisis management activation and escalation;
- Crisis command and management succession;
- Crisis recovery logistics and resources; and
- Crisis communications.

Organizational Crisis Management Teams

Provided by ASIS

The crisis management team (CMT) is perhaps the most critical piece of crisis management. Naming the critical personnel who will deal with any business disrupting or impacting event is the first step to having an overarching crisis management program in place.

The crisis team should have members from:

- Executives
- Human resources
- Public affairs/communications
- Safety/security
- IT
- Legal
- Finance or other shared service
- Critical operational departments

In large organizations it is common for the senior leadership team to be separate from the CMT. This allows the senior leadership team to focus on strategic decisions that affect the organization's strategic goals. The senior leadership team then drives those decisions down to CMT for implementation. The necessary CMT members will be different for different organizations and should reflect the most critical groups responsible for ongoing business operations. However, effective crisis planning includes all areas within the organization that can be activated if necessary. CMT members should be identified by position (primary and alternates). This ensures that if the person with that title is not available, another team member is prepared to step in to complete the task.

Crisis Communications

Provided by ASIS

Like crisis management, crisis communications is strategic, not tactical. It is focused on not only communicating messages regarding a disruptive event but also on broader issues that support organizational resilience, and future strategic business plans. For example, if an organization is experiencing a disruptive event, it must not only deal with the acute event but it must make decisions and communicate those decisions to key external audiences that may be affected by its decisions.

Communications tactics are those tools used to carry messages to specific audiences such as news releases, social media, use of a company's website, town halls, etc. They should not be confused with strategic communications.

A good working definition of crisis communications is:

1. Effective communications using public relations standards.
2. Carefully worded messages to specific audiences. There is no such thing as the "general public" in a crisis. Crises affect specific audiences (members, volunteers, employees, vendors, customers, etc.), each of whom have unique concerns requiring messages tailored to those concerns.
3. Focuses on critical issues, disruptive events, and crises.
4. Is executed in a compressed time frame.

Crisis communications is an essential part of the overall crisis management process and crisis lifecycle. It is not a standalone function and is integrated into the crisis management infrastructure, including the senior leadership team, and the crisis management team.

Crisis Communications Plan

Provided by ASIS

The crisis communications plan (CCP) can either be a standalone document or be integrated into the overall crisis management plan. In either case, the CCP should have notification and activation procedures identical to the crisis management plan. The CCP will list the members of the CCT and their roles. The most important part of the CCP is the actual communications section. Using information from the risk assessment and other sources, the CCT will document the following for each disruptive scenario:

1. Identify affected or key audiences.
2. Identify audience concerns.
3. Develop messages specific to audience concerns.
4. Determine a spokesperson/messenger for each audience.
5. Select tactics to deliver each message.

All Hazards

Provided by ASIS

When planning to migrate, prepare, respond, and recover from a crisis event, it's important to determine if the approach will be threat specific or a more global all hazards approach. The following is from ASIS' Protection of Assets. The specific emergency planning format used by an organization depends on the nature of the organization and the organization's policy. For many organizations that are exposed to a variety of different potential types of threats and hazards, an all-hazards approach is the best course of action for planning. This approach provides for a basic emergency operations plan (EOP), with sections that apply to multiple emergency situations (i.e. contact lists), and hazard specific checklists for event types (i.e. hurricane checklists in coastal areas or flood sections in geographies prone to flooding). The all-hazards approach works well in many situations because quite often planning requirements are similar regardless of whether an incident is a natural threat, a human threat, or an accident. For example, an evacuation plan is essentially the same for fi res, bomb incidents, utility shutdowns, or HAZMAT spills.

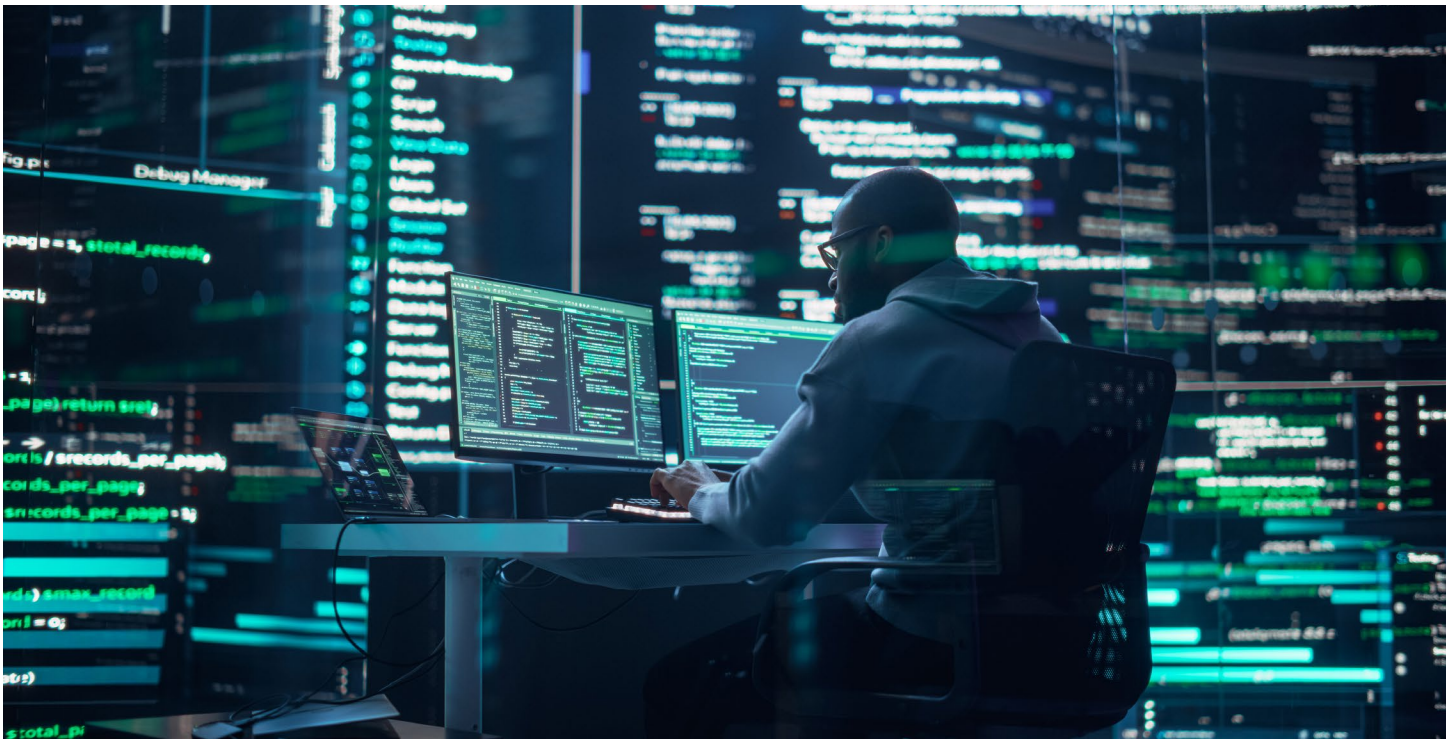
Cyber Security Actions

Cyber security merits it's own resource, however since cyber risks ranked as the number one concern is the risk survey, below are some helpful resources for associations grappling with their cyber security planning.

AON

Eight Actions Your Organization Can Take Today To Reinforce Its Cyber Security Strategy

1. **Review business continuity and disaster recovery (BCDR) plans** to ensure they take account of, and regularly test for, cyber threats.
2. **Assess vulnerabilities.** This allows organizations to strategically budget and address critical areas.
3. **Review governance, controls, roles, and responsibilities** and develop protective safeguards to prevent ransomware attacks.
4. **Quantify the financial loss** associated with an incident, breach, or disruption.
5. **Engage in breach simulations** and tabletop exercises to test incident preparedness.
6. **Check contractual protections** and have all insurance policies reviewed to ensure the organization is covered for financial loss from a breach.
7. **Proactively utilize threat intelligence** to monitor for the tactics, techniques, and procedures (TTPs) of cyber attackers.
8. **Never stop cycling** through The Cyber Loop.



Cyber Security Checklist

GREAT AMERICAN INSURANCE GROUP

While the overall organization's approach to crisis and risk may be an all-hazards approach, there are cyber risks that are worth considering specifically. Great American Insurance Group developed a Cyber Security Checklist. This checklist is designed to provide security tips to assist business managers in assessing and improving their cyber security plans and procedures.

	Yes	No	N/A
Management. The key to effectively managing cyber security is to demonstrate top-level executive support. Some key management activities that should be addressed include:			
Have you created security policies to match the size and culture of your business?	☐	☐	☐
Are security policies written, enforced, and kept updated?	☐	☐	☐
Have you established a computer software and hardware asset inventory list?	☐	☐	☐
Have you classified data by its usage and sensitivity?	☐	☐	☐
Have you established ownership of all data?	☐	☐	☐
Information Technical Staff. They are on the front line when it comes to cyber security and are responsible for some key activities. Examples of activities to be addressed include:			
Are you maintaining configuration management through security policy implementation and systems hardening?	☐	☐	☐
Are you maintaining software patch management on all systems by following a regular schedule for applying patches for operating systems, specific software, and anti-virus updates?	☐	☐	☐
Do you subscribe to security mailing lists?	☐	☐	☐
Are you maintaining operational management through the reviewing of all log files, ensuring system backups with periodic data restores (data restores shouldn't be done unless a problem corrupted the live data), and reporting any known issues or risks?	☐	☐	☐
Are you performing security testing through security audits and penetration scanning?	☐	☐	☐
Are you ensuring physical security of systems and facilities?	☐	☐	☐
Do you ensure users have anti-virus software loaded and active on systems?	☐	☐	☐

	Yes	No	N/A
End Users. Some of the key activities that end users should address include:			
Do you have anti-virus software loaded and active on your computer?	☐	☐	☐
Do you delete, without opening, e-mails from unknown sources?	☐	☐	☐
Do you back up data on a regular basis?	☐	☐	☐
Do you utilize strong, hard-to-guess passwords?	☐	☐	☐
Do you use personal firewalls?	☐	☐	☐
Do you download and apply security patches?	☐	☐	☐
Do you disconnect your computer from the Internet when not in use?	☐	☐	☐
Do you restrict access to systems to authorized users only?	☐	☐	☐
Business Continuity. In order to ensure continuity of business, proactive security measures must be taken and be part of daily operations. Routine security testing, and regularly-scheduled risk assessments and third-party security audits, should be performed. These are continuity measures that should be addressed:			
Do you have an emergency response plan?	☐	☐	☐
Have you systematically evaluated all of the potential sources of disruption to your business?	☐	☐	☐
Do you have an active program to reduce the likelihood of a disruption?	☐	☐	☐
If you could not re-enter the workplace because of an emergency, do you have a pre-determined location to meet to coordinate recovery operations?	☐	☐	☐
Do you maintain a current list of employees, customers, and suppliers at an off-site location?	☐	☐	☐
Have you met with local emergency response groups to discuss their role in maintaining the business?	☐	☐	☐
If you lost a critical system, do you have a pre-determined plan to restore the system?	☐	☐	☐
Do you have an established business resumption team?	☐	☐	☐
Is your business resumption plan securely stored in a remote location?	☐	☐	☐
Do you periodically test your business resumption plan along with your site emergency response plan?	☐	☐	☐

(Source: Great American Insurance Group)

The loss prevention information and advice presented in this brochure are intended to advise our insureds and their managers of a variety of methods and strategies based on generally accepted safe practices, for controlling potentially loss producing situations commonly occurring in business premises and/or operations. They are not intended to warrant that all potential hazards or conditions have been evaluated or can be controlled. They are not intended as an offer to write insurance coverage for such conditions or exposures, or to imply that Great American Insurance Company will write such coverage.

asae
The Center for Association Leadership

Deep Dive: Conference and Event

Conference and Event Crisis Framework

Planning for risk and crisis management around association events requires a deliberate and tailored approach. Kristin Richeimer, CAE, DES recommends the following steps for event crisis management:[16]

Recognizing Crisis Scenarios

The input highlights a wide range of potential crisis situations that event organizers should be prepared for, including medical emergencies, security threats, natural disasters, technology failures, and misconduct incidents. It emphasizes the importance of identifying these scenarios and developing tailored response plans accordingly.

Establishing a Crisis Communications Team

A dedicated crisis communications team with clearly defined roles and responsibilities is crucial for effective crisis management. Key roles include an incident leader, media contact, event logistics coordinator, registration contact, travel coordinator, speaker liaison, technology expert, and exhibitor representative.

Determining Crisis Communication Strategy

Developing a comprehensive crisis communication strategy is essential, involving identifying the level of crisis, considering venue and destination plans, establishing communication flows and timing, and updating leadership and stakeholders. Different response levels are outlined, from contained incidents to hazardous situations requiring public statements or event postponement.

Ideas for Providing Attendees with Critical Emergency Procedures

What?

- How to report an emergency
- First aid location and telephone number
- Basic emergency procedures for fire, suspicious package, evacuation
- Traveler safety tips (links)
- Hospital, urgent care, and pharmacy

How?

- Create page on event website
- Link on mobile app
- Page on conference program
- Print on back of the badge
- Walk-in-slides

[16] AI synthesis and summary of Kristin Richeimer, CAE, DES's original content created for ASAE's Master Event Crisis Management online course

Understanding Legal Obligations

Event organizers must be aware of legal obligations related to crisis management, such as the accuracy and timing of statements, attendee rights to information, liabilities, and elements of negligence cases. Conducting due diligence, ensuring safety protocols, and adhering to policies are crucial to mitigate legal risks.

Building a Crisis Management Plan

A well-structured crisis management plan is vital, incorporating venue-specific information, evacuation protocols, first aid procedures, cancellation policies, and clear communication flows. Regular updates and scenario testing through backtesting and root cause analysis are recommended.

Staff Training and Communication

Ongoing staff training, including crisis response simulations, CPR training, and establishing communication channels, is essential for effective crisis management. Clear communication with attendees regarding emergency procedures and contact information is also highlighted as a critical aspect.

Virtual Event Considerations

For virtual or hybrid events, due diligence should extend to the digital domain, encompassing platform security, redundancy measures, vendor coordination, privacy policies, and measures against cyber threats like hacking or spamming.

Importance of Accuracy and Speed

During a crisis, maintaining accurate and timely communication is paramount. Event organizers must balance the need for swift response with the responsibility of disseminating factual information to ensure attendee safety and protect the organization's reputation.

Root Cause Analysis

Conducting root cause analysis after a crisis event is crucial for identifying underlying issues, preventing recurrence, and continuously improving crisis management strategies. This proactive approach aims to address problems at their source rather than merely reacting to emergencies.

Event and Destination Risk and Crisis Management Framework

Destinations International developed the following framework for associations and destinations to collaboratively consider when evaluating and planning for conference and event conference risks.

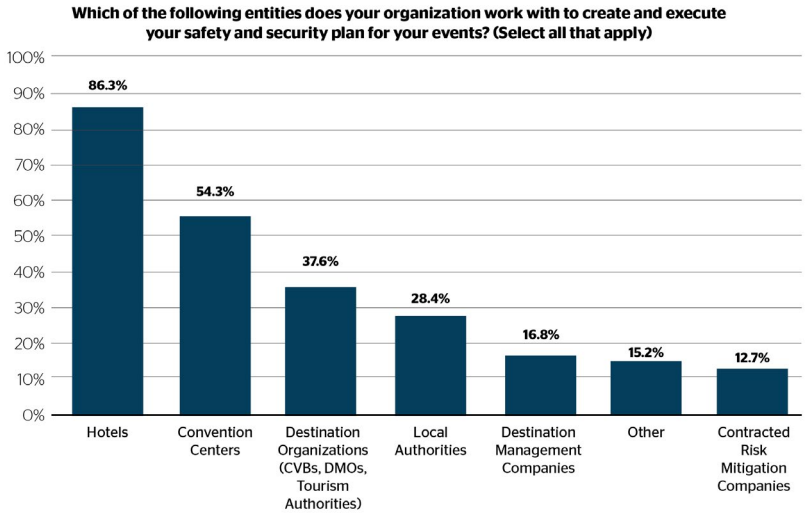
Destinations International also provided the following context on the destination and meeting related survey questions from the beginning of this document.

Item	Overall Rank	Rank Distribution	Score	Number of Rankings
Crime and Safety	1		1,191	166
Destination Weather / Future climate predictions	2		1,154	161
Health and Safety measures	3		936	146
Accessibility policies and initiatives (beyond ADA requirements)	4		781	137
Politcal Climate	5		612	133
Other	6		610	120
Perception of Social Justice & Equality within the community	7		576	131
Active Legislation around Human Rights (Reproductive rights, LGBTQ+ rights, etc.)	8		522	132
Environmental policies and initiatives	9		472	128

The impact of Risk Mitigation on destination selection can be complex with variations that must be considered across associations, time of year, board and leadership shifts, booking timelines and rotational patterns, attendee variables, and the destinations where the events are hosted. The considerations can fluctuate annually pending the aforementioned factors. Examples of factors impacting rankings may include:

- **Subjective interpretations of categories by respondents and stakeholders:** In the example of Crime and Safety, some respondents have a broad definition inclusive of panhandling perceived as aggressive, whereas others may be narrower with specific definitions around criminality ranging from violent to petty crime or active shooter.
- **Booking patterns affecting perceptions of risks:** The ranking of risk-associated issues can be pending the timeline of the booking or the patterns in rotation, influenced by the number of destinations that are viable due to the booking restrictions. For example, business events scheduled during natural disaster-prone periods are likely to prioritize weather-related concerns and longer booking cycles also necessitate climate impact consideration for associations planning city-wide events 5-10+ years in advance.
- **Discrepancies between media portrayal and actual statistical safety data, especially in convention districts:** The influence of media can create a bias in perception not only around the destination itself but around the importance of specific risk factors outlined, increasing the perceived importance pending the destinations that are actively being considered.

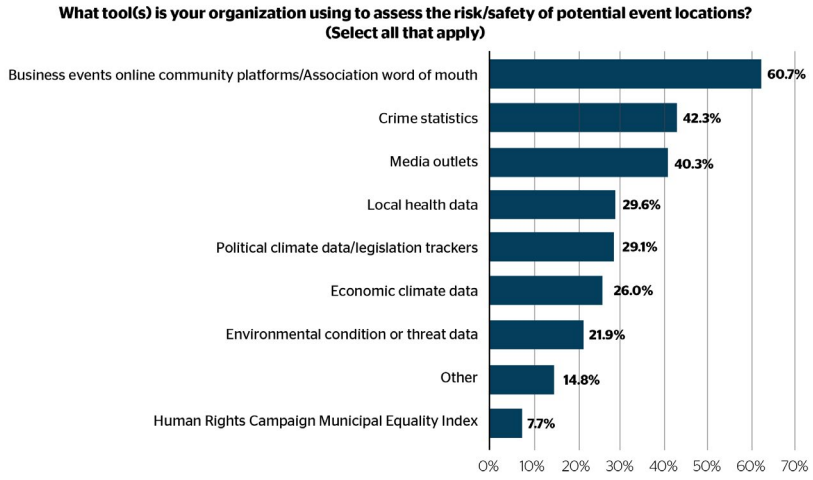
Associations work with an assortment of partners to ensure the safety and security of their business event(s) and the delegates who attend. Understanding the role that each partner plays in the extension of the planning team is vital to success.



The size and scale of an event directly influence the selection of involved entities. Smaller events, often confined to a single hotel property, require less local public engagement compared to larger, city-wide events spanning multiple properties and venues. Given the prevalence of small events compared to citywide ones, hotels naturally play a prominent role in the execution of risk mitigation plans.

When reviewing the survey findings, the factor of integration between the entities must also be considered. Though convention centers, Destination organizations, local authorities, and DMCs are listed individually, many hosting organizations utilize a blend of these to achieve risk mitigation goals. Convention center teams may lead venue-specific risk mitigation efforts, collaborating with destination organizations to facilitate meetings among the venue, local authorities, and hotels.

Business event organizations employ a diverse set of criteria for destination selection, spanning accessibility, safety, and destination appeal. The primary determinant often revolves around stakeholders' perceptions, emphasizing the importance of acquiring accurate contextual information. Survey findings highlight a mix of objective and subjective factors driving the selection process.



Assessing the sources included in the destination selection process are also inclusive of additional data context:

- **Isolated experiences vs consistent data:** The information provided is determined to be based on isolated incidents or reflects consistent patterns over time.
- **Validity of the source:** The credibility and reliability of the sources providing the information. Reliable sources ensure that the data used for decision-making is accurate and unbiased, reducing the risk of misinformation.
- **Statistical boundaries:** The scope and limitations of the data, particularly regarding the severity of incidents and the geographic area they represent. Understanding these boundaries helps contextualize the data accurately, preventing misinterpretation or overgeneralization.

Small Staff Focus: Convention Safety & Security

Provided by RIMS

Tips for Small-Staffed Associations and Events Under 1,000 Attendees

Pre-Event Activity

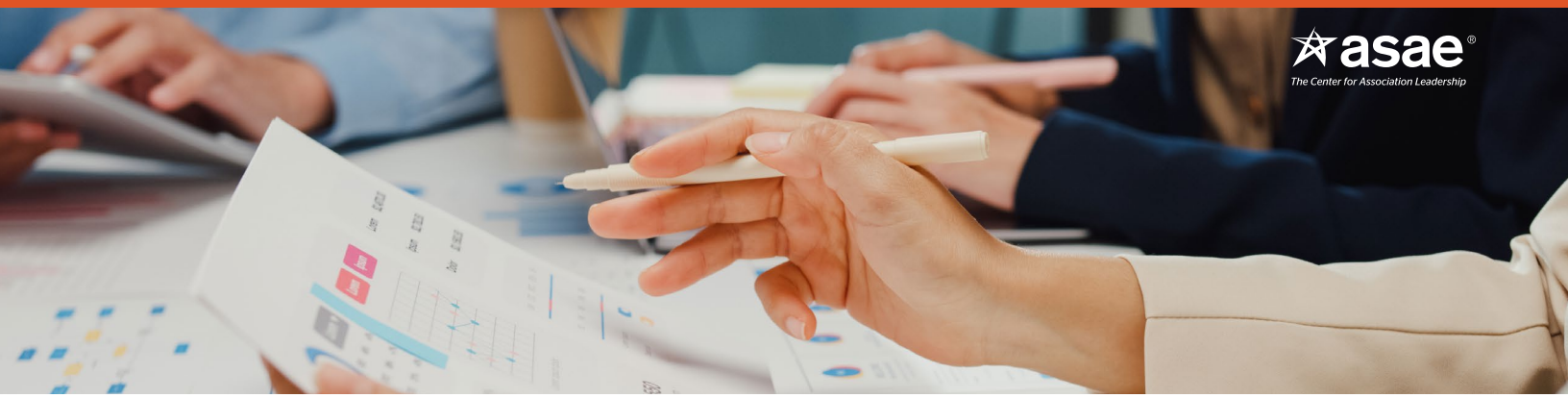
- **Control the Access.** In the event of an emergency it is important that the event organizer knows who is in the building and how to communicate with them. Consequently, every attendee must be registered and badged.
- **Require Contact Information.** To ensure the ability to rapidly reach every attendee in the event of an emergency, attendees must provide their cell phone numbers during the registration process. Use a simple SMS mass-text program.
- **Provide Pre-Event Safety & Security Messages.** Distribute a "Safety & Security Know-Before-You-Go" communication to all registrants prior to the event. In addition, post it on the event website, and include it in the event mobile app. If possible, produce a short safety and security video and deliver it by email about a week or so before the event.
- **Identify Emergency Responders.** Create a Communication Ownership Map that lists at least two staff members responsible for each communication channel. Also, identify the staff member responsible for coordinating with key vendors (i.e. housing/hotel, shuttle bus, etc.). Make sure that those listed are informed of their onsite emergency communication responsibility prior to the event. They should also be trained and drilled in the mechanics of issuing messages.
- **Develop Pre-Recorded Messages.** Pre-record (or write out) emergency communications prior to the event. The communications should be developed for delivery via at least four channels: audible public announcement in the center/hotel, visual signage boards in the Convention Center, social media, and the Mobile App push notifications.
- **Train the Team.** Expand security and safety training to include key vendors, partners and volunteers. Ask them to be the "eyes and ears" of the event and train on them how to report an incident or suspicious situation. Conduct an extensive walk-through of the venue and orient them to various emergency response tools, exits, security stations and the like.

Onsite Safety & Security Activity:

- **Secure the Perimeter.** To maintain better control and to prevent unauthorized/unregistered individuals from entering the facility, secure and patrol all doors to the venue, leaving just one point of access to get into event. (However, ensure that all the doors could be used to exit the building).
- **Enhance Planning for Under 21 Attendees.** If students or others under 21 years of age attend the event, take special care to orient them. Make sure that they understand which, if any, events are 21+ to enter, and note that they should not expect to be served alcohol at receptions, etc. Attendees under 21 should receive a distinctive event badge. Pre-conference messaging and a webinar should emphasize what events were 21+ and what behavior was expected.
- **Add Security Personnel.** Additional security personnel should be deployed throughout the venue to monitor and respond to potential security threats and to ensure all access points are closed upon an individual's exit.
- **Enhance Communication.** Equip some or all staff, as well as key vendors and key venue personnel, with radios. This expands surveillance, sharpens situational awareness and enables a rapid, coordinated response. In addition, pre-populate an SMS text chain with key personnel.

- **Provide On-Site Safety & Security Messages.** Run the Event Safety and Security messages and video on the screens prior to each keynote presentation. The messaging should provide safety tips, information about local medical facilities, and other onsite security measures at the event. Coordinate with hotel partners and arrange for registrants to receive a safety and security letter upon check-in, customized for each hotel.
- **Coordinate with Unions.** Meet with the leaders of the Unions at the event venue and discuss the planned safety and security measures. Invite the Union leaders to share their ideas and ask them to participate in security meetings. Ask if the Union leaders would carry an event radio to communicate in an emergency.
- **Heighten Visual Deterrence.** Deliberately heighten presence of armed and uniformed police personnel in and around the venue. If possible, engage K-9 units and prominently place them near the entrance and other high-trafficked areas.
- **Publicize Prohibited Items.** Publicize a list of restricted items, such as handguns, banners, spray paint, etc. Include the list in pre-event communications and prominently post it at the entrance.
- **Post Zero Tolerance Message.** Post a strong, clear notice in several places detailing that event has a zero-tolerance policy regarding harassing language, hate speech, threats, sexual harassment, etc., and noting that event organizer retains the right to cancel credentials and deny access to the venue to anyone who breached that policy.
- **Strengthen Cybersecurity.** Trained IT staff should monitor the venue's WiFi system, as well as social media and the internet (look for related hashtags and postings) and deploy a robust suite of cybersecurity software to protect the Event registration and exhibit management systems and servers.

The following Toolkit, develop by RIMS, with the advice of global security firm Merrill Herzog Group, is provided as a template for your use.



Event/Conference Crisis Case Study: RIMS After Action Report

Annually, associations produce thousands of in-person events around the world. Those events, which can draw hundreds of people or hundreds of thousands provide valuable connections and learning. However, as the world becomes more volatile and unpredictable, a new risk for association leaders has emerged: violence.

According to the Gun Violence Archive, there were 656 mass shootings in the U.S. in 2023.[17] Active shooter incidents show no signs of slowing down.

While there is no quick solution for completely preventing such incidents from occurring at an association event, there are steps that leaders can proactively take to elevate the safety and security of events.

RIMS, *the* risk management society®, experienced an active shooter incident less than three miles from its annual conference, RISKWORLD®. The shooting, which did not involve anyone from RISKWORLD, resulted in a temporary shelter-in-place order, and the cancellation of all events on the last afternoon and evening of the conference. RIMS, an association dedicated to serving the world's risk management and insurance community, took significant precautions prior to RISKWORLD, but still recognizes opportunities to improve upon such measures to better protect and serve the 10,000+ risk management professionals who attend the event each year.

RIMS has developed an After-Action Report recounting the timeline of events that transpired at RISKWORLD® 2023 following the active shooter incident. The report documents the association's response, lessons-learned, and outlines next steps the association will take to ensure its community can continue to meet safely in-person.

RIMS and ASAE invite you to learn from this experience.

[17] https://www.gunviolencearchive.org/

ATLANTA 2023

RISKWORLD®

APRIL 30–MAY 3

After Action Review:

RISKWORLD 2023

Atlanta Active Shooter Incident

RIMS the risk management society®

Summary
RISKWORLD® 2023 was held in Atlanta, Georgia's Georgia World Congress Center (GWCC) from April 30th to May 3rd. The conference drew nearly 9,000 risk management professionals from around the world, 300 exhibitors and delivered over 150 educational sessions. In addition to the education sessions, for the first time, RISKWORLD featured four keynote presentations that included: Opening Session Keynote Johnny C. Taylor, Jr. (SHRM CEO), Awards & Leadership Keynote Josh Linkner (Jazz musician, author, entrepreneur), State of the Industry Keynote Evan Greenberg (CHUBB CEO), and Closing Finale Keynote Danica Patrick (former NASCAR driver).

To accommodate RISKWORLD 2023 guests, 32 hotels were contracted to provide housing for attendees. Additionally, shuttle bus service was provided to and from the GWCC to non-walking distance hotels. RISKWORLD 2023 had eight different shuttle routes serving 27 of the 32 hotels.

On May 3, 2023 (the last day of RISKWORLD) just after 12:00 p.m., an armed assailant opened fire at the Northside Medical Midtown facility located at 1110 West Peachtree Street, NW, approximately two-and-a-half miles from the GWCC. The incident resulted in one fatality and four others receiving medical treatment for gunshot wounds.

Atlanta's response to the attack resulted in a shelter-in-place in midtown Atlanta, road closures, activation of numerous city-wide video surveillance systems, air support, as well as investigations for numerous false reports of "shots fired." Atlanta Police Department (APD) had video footage of the suspect stealing a car and heading toward Cobb County, approximately 20 miles from the GWCC. The eight-hour manhunt culminated in a housing complex in Cobb County at approximately 8:00 p.m.

RIMS multi-faceted response to the active shooter incident in Atlanta comprised key action items derived from the Society's comprehensive crisis plan, collaboration with local authorities and GWCC staff, strategic communications tactics, as well as leveraging available resources and intuitive and spontaneous action.

This After Action Review aims to provide a timeline of RIMS response to the May 3rd active shooter incident, as well as key lessons learned from the experience and steps to enhance and guide RIMS onsite crisis plan moving forward.

Incident Timeline

TIME (EDT)	LIAISON	COMMUNICATION	COMMUNICATION DELIVERY
12:37	Atlanta Police Department (APD)	APD: Investigating Active Shooter.	LOCAL AUTHORITIES
12:38	GWCC	Chief of Police informed the GWCC.	LOCAL AUTHORITIES
12:42	APD	Confirmed Active Shooter. No suspect in custody.	LOCAL AUTHORITIES
12:46	GWCC	GWCC informed RIMS Chief Events & Sales Officer Stuart Ruff-Lyon of active shooter but no immediate danger to those in the Convention Center.	PHONE
12:52	RIMS	Stuart Ruff-Lyon reaches out to RIMS CEO Gary LaBranche and RIMS Communications Director Josh Salter	TEXT/PHONE
12:58	RIMS	Gary LaBranche informed.	IN-PERSON
13:00	Security	Impromptu Briefing by Dupree Security Outside of Ballroom.	IN-PERSON
13:05	GWCC	GWCC Staff Member Kim Allison met Gary LaBranche at Ballroom to escort him to the Response Center.	IN-PERSON
13:10	GWCC	All parties arrive at Response Center (GWCC Administrative Office).	IN-PERSON
13:10	BOD	A board member delivered initial notification via text of the shooting in Midtown Atlanta.	BOARD OF DIRECTORS (BOD) TEXT
13:10 - 13:30	APD/GWCC	Conflicting reports, all of which proved false: additional shots fired; suspect is on MARTA; suspected is "cornered."	LOCAL AUTHORITIES
13:18	BOD	A board member shared report via a text that the suspect is moving away from GWCC.	BOD TEXT
13:26	RIMS	Gary LaBranche informs RIMS COO Annette Homan.	PHONE
13:26	BOD	A board member notified all that RIMS is preparing a statement, gives basic details of the incident and that additional information is forthcoming.	BOD TEXT
13:26	BOD	A board member shared a false report that suspect was in custody.	BOD TEXT
13:32	RIMS	Gary LaBranche informs RIMS President Jennifer Santiago.	PHONE
13:32	RIMS	First Urgent Alert Message drafted by Josh Salter and sent for Mobile App Distribution.	EMAIL
13:34	RIMS Message Delivered	URGENT ALERT: RIMS is aware of the incident in midtown Atlanta and is working with local police, law enforcement agencies and the convention center to deliver you with more information. The incident took place in 1100 Block of West Peachtree (more than 2 miles from the Convention Center). RIMS urges all attendees to avoid that area until further notice. RIMS will continue to provide information as it becomes available.	MOBILE APP
13:35	RIMS	Gary LaBranche and Stuart Ruff-Lyon request housing list of attendees in impacked hotels.	PHONE
13:37	RIMS Message Delivered	All Staff, Please respond to this message to confirm your well-being and that you are safe at this time. Additional information to follow shortly.	TEXT TO ALL STAFF

Incident Timeline

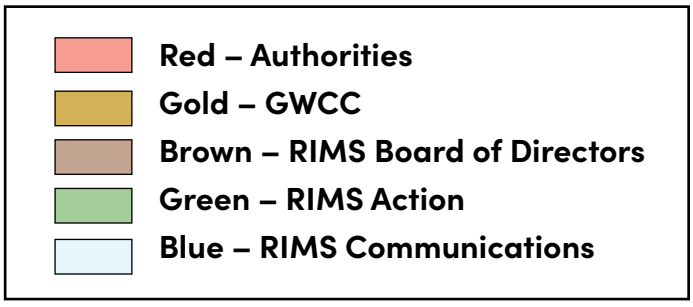
TIME (EDT)	LIAISON	COMMUNICATION	COMMUNICATION DELIVERY
13:40	BOD	A board member notified all that the RIMS Crisis Plan has been activated and only official communications from RIMS should be shared.	BOD TEXT
13:45	RIMS	TEXT to staff drafted by Josh Salter and sent to RIMS CIO Mike Peters for distribution.	EMAIL
13:48	RIMS Message Delivered	Attention staff. We are aware of the situation in midtown Atlanta. The incident took place approximately two-plus miles from the Convention Center. Please stay in the Convention Center. If you're in your hotel, please stay in your room. Avoid the mid-town area. RIMS is working with local authorities and will provide more information as it becomes available. Communications will be sent by text message.	TEXT TO ALL STAFF
13:49	RIMS Message Delivered	Email to Board with first URGENT ALERT message and TEXT to Staff.	EMAIL
13:51	RIMS	Gary LaBranche discusses the status of the Closing Finale with Jennifer Santiago.	PHONE
13:55	BOD	A board member shared that the suspect seems to be moving away from the GWCC. A decision regarding the cancellation of the Conference Finale would be made at approximately 14:15.	BOD TEXT
14:05	RIMS Message Delivered	Gary LaBranche provided incident updates to RIMS Board Directors.	EMAIL
14:07	RIMS/Connection Housing	List of guests in impacted hotels received.	TEXT/EMAIL
14:07	CNTV/RIMS	Gary LaBranche records video message with CNTV.	IN-PERSON
14:11	RIMS Message Delivered	Message created for Mid-Town Hotel Guests: URGENT ALERT FROM RIMS Please be advised that there has been an emergency incident in mid-town Atlanta. The safety of RISKWORLD attendees is our top priority. RIMS urges all attendees to avoid the West Peachtree area. If you are staying in the mid-town area, please consider staying in your hotel room until your hotel provides you with clearance. If you are in the convention center, RIMS recommends that you stay there. RIMS is working with local law enforcement agencies and is providing additional information to attendees via the RISKWORLD mobile app as it becomes available.	EMAIL
14:15	RIMS	Decision to cancel Closing Finale made.	DECISION
14:15	RIMS	RIMS notified Danica Patrick that the Closing Finale was cancelled.	IN-PERSON
14:22	BOD	A board member shared that the Closing Finale is cancelled.	BOD TEXT
14:25	BOD	A board member notified the group that GWCC signage is being updated with emergency messaging.	BOD TEXT
14:29	RIMS Message Delivered	URGENT ALERT -- In an abundance of caution, the RISKWORLD Closing Finale has been cancelled. RIMS will provide more information as it becomes available.	MOBILE APP

Incident Timeline

TIME (EDT)	LIAISON	COMMUNICATION	COMMUNICATION DELIVERY
14:30	RIMS Message Delivered	Email to Board notifying them that the Closing Finale was cancelled.	EMAIL
14:30	RIMS/Sedgwick	RIMS Director of Sales Kris Wolcott reaches Sedgwick to discuss closing party.	PHONE
14:33	GWCC	GWCC began preparation to change digital signage.	GWCC SIGNAGE
14:39	BOD	A board member confirmed that transportation (unimpacted shuttle and taxi service) was operating as normal.	BOD TEXT
14:35	RIMS Message Delivered	Gary LaBranche and Stuart Ruff-Lyon address attendees in the GWCC Thomas Murphy Ballroom. Announcement included the cancellation of the Closing Finale and shelter in place in Midtown Atlanta.	ONSTAGE ANNOUNCEMENT
14:44	RIMS Message Delivered	Confirmation that all signage displayed: In an abundance of caution, the RISKWORLD Closing Finale has been cancelled. RIMS will provide more information as it becomes available.	GWCC SIGNAGE
14:46	GWCC via APD	Suspect identified. Still at-large.	LOCAL AUTHORITIES
14:47	RIMS Message Delivered	Today's closing finale is cancelled. Please head to the Ballroom to check-in with staff.	TEXT TO ALL STAFF
14:47	RIMS	RIMS staff mobilized to provide attendees approaching the Thomas Murphy Ballroom with direction and information.	ACTION
15:06	GWCC via APD	Shelter in place lifted in Midtown Atlanta.	LOCAL AUTHORITIES
15:15	RIMS Message Delivered	Message delivered to RIMS Board: Shelter in Place order was lifted by the Atlanta Police.	EMAIL
15:19	RIMS Message Delivered	The Atlanta Police Department has lifted the shelter in place in Midtown Atlanta	TEXT TO STAFF
15:20	RIMS Message Delivered	Gary LaBranche and Stuart Ruff-Lyon deliver updates onstage in the GWCC Thomas Murphy ballroom, states that Shelter in Place order has been lifted; shuttle routes will be up soon but for now two shuttle routes serving the 4 hotels remain impacted due to traffic issues, gridlock.	ONSTAGE ANNOUNCEMENT
15:36	RIMS Message Delivered	URGENT ALERT - UPDATE – Atlanta Police Department has lifted the shelter in place in midtown Atlanta.	MOBILE APP
16:07	RIMS Message Delivered	The RIMS staff appreciation event this evening has been cancelled. Additionally, the RIMS-Sedgwick official closing party has also been cancelled.	TEXT TO ALL STAFF
16:08	GWCC via APD	Gunman no longer in midtown. Police focus on Cobb County.	LOCAL AUTHORITIES
16:28	RIMS/Sedgwick	Confirmation from Sedgwick on language to cancel closing party.	EMAIL

Incident Timeline

TIME (EDT)	LIAISON	COMMUNICATION	COMMUNICATION DELIVERY
16:39	RIMS Message Delivered	CANCELLED: RIMS-Sedgwick Official Closing Party Due to the unfortunate event that occurred in midtown Atlanta today, the RIMS-Sedgwick Official Closing Party (scheduled for May 3, at 7pm) has been cancelled out of respect to the families impacted and the safety of RISKWORLD attendees. Your well-being is a top priority shared by both RIMS and Sedgwick.	MOBILE APP
16:40	GWCC	All signage switched back.	GWCC SIGNAGE
16:50	RIMS / CNTV	Gary LaBranche video message received and posted to RISKWORLD website.	VIDEO
17:13	RIMS Message Delivered	A Message from RIMS CEO Gary A. LaBranche.	MOBILE APP
17:32	RIMS Message Delivered	CANCELLED: RIMS-Sedgwick Official Closing Party Due to the unfortunate event that occurred in midtown Atlanta today, the RIMS-Sedgwick Official Closing Party (scheduled for May 3, at 7pm) has been cancelled out of respect to the families impacted and the safety of RISKWORLD attendees. Your well-being is a top priority shared by both RIMS and Sedgwick.	EMAIL
20:07	APD	Suspect in custody.	LOCAL AUTHORITIES



Notable Action & Key Takeaways

Pre-Event Preparation is Critical

As an association dedicated to the advancement of risk management, RIMS has always placed a high-priority on preparing for adversity and uncertainty. RIMS has a comprehensive 72-page crisis plan for addressing an incident during RISKWORLD that includes: Activation and Deactivation plans, key locations and resources, communication and coordination, as well as guidelines for shelter-in-place and evacuation scenarios.

Additionally, the RIMS Events Team presents components of the Crisis Plan during an All-Staff call preceding the conference. RIMS also arranged for all staff who desire to become CPR certified, adding yet another layer of safety to the event.

RIMS engaged a private security consultant to advise on safety and security matters. This team provided a comprehensive range of services, including the use of EOD canines, monitoring of social media feeds and interfacing with local law enforcement.

In addition, additional language about safety and security was prominently added to the RISKWORLD website and in other places, and additional messaging was displayed during general sessions and throughout the convention center.

In advance of RISKWORLD, RIMS conducted a safety walk-thru of the facility. Another safety walk-thru was held at the convention center the day prior to the event. RISKWORLD 2023 extended an invitation to attendees to join the safety walk-thru to further educate them about the facility's amenities, egresses and safety features.

- ***Key Takeaway:*** *A 72-page crisis plan developed for staff, while comprehensive, is too long to memorize and too big to carry.*
- ***Key Takeaway:*** *While thorough, the existing Crisis Plan mainly focuses on emergency incidents in or near the convention center as opposed to emergencies in the city.*
- ***Key Takeaway:*** *Some aspects of the Crisis Plan were outdated – for example: storing the crisis plan on a "thumb drive," and carrying a hard copy of contact lists.*
- ***Key Takeaway:*** *Safety walk-thrus provided an important and helpful orientation.*

Support from Local Authorities

With several incidents of civil unrest and the coinciding Taylor Swift concert that would take place during RISKWORLD, RIMS held several advance meetings with local law enforcement and GWCC staff. The meetings allowed RIMS to address looming housing issues, potential traffic interruptions and structure events held outside of the convention center more effectively. In addition to providing critical intel regarding potential issues, the meetings promoted familiarity and helped to identify roles, responsibilities and capabilities.

- ***Key Takeaway:*** *Having an understanding of the convention center's safety capabilities, as well as what authorities will be onsite during an emergency was helpful.*
- ***Key Takeaway:*** *Having a map of geographic areas in the city where RIMS has exposures would help RIMS identify crisis (and those impacted) quicker.*

Meeting Point

Upon learning of the incident, RIMS Staff was instructed to (a) meet in the ballroom if they were in the convention center; (b) remain in their room if they were in their hotel, until further notice.

- ***Key Takeaway:*** *RIMS staff presence at the entrance to the Thomas Murphy Ballroom allowed RIMS to effectively deliver direction and new information.*
- ***Key Takeaway:*** *Identifying a safe place for staff to convene in the event of an emergency not only helped to ensure the safety of employees, but also provided yet another opportunity for RIMS to account for its employees.*

Housing and Shuttle Service

At the height of the active shooter incident, it became apparent that four of RISKWORLD's 32 hotels were in the impacted area – midtown Atlanta. Working with RIMS vendor Housing Connections, a list of attendees staying in the effected hotels was provided to RIMS leadership. Subsequently, an email alert was then able to be sent to those on the list.

Additionally, RIMS collaborated with its shuttle bus vendor TCS Transportation Services. Two shuttle routes were impacted by the incident in midtown.

- ***Key Takeaway:*** *Housing Connections possesses the ability to build a list of RISKWORLD attendees by the hotel they are staying in.*
- ***Key Takeaway:*** *RIMS did not receive any communications from its hotel partners.*
- ***Key Takeaway:*** *Shuttle bus service was disrupted during the incident.*

Notable Action & Key Takeaways

Internal Communication

As noted in the RIMS Crisis Plan, in the event of an emergency, RIMS will initiate its "Telephone Tree" to notify staff of an incident. At RISKWORLD, the telephone tree was initiated.

RIMS employs a service that enables the Society to deliver text message notifications to staff. That service was employed during the incident. RIMS text messaging service is managed by RIMS Chief Information Officer.

RIMS CEO Gary LaBranche and RIMS President Jennifer Santiago were in contact via phone. Emails were also sent to RIMS Board of Directors by RIMS Director of Communications.

- ***Key Takeaway:*** *A "telephone tree" can be an effective model to account for employees, but it is cumbersome and time-consuming.*
- ***Key Takeaway:*** *Text messages are useful to notify employees of danger, however, RIMS existing system does not identify if the individual has read the message, nor does it identify the staff member that replies to the text alert.*
- ***Key Takeaway:*** *The time between the initial text requesting a response of "safe" was way too long.*
- ***Key Takeaway:*** *RIMS Board Directors Text Message Group was an effective vehicle for RIMS President and leadership to provide updates and stay informed.*

External Communications

RIMS leveraged several tools to alert conference attendees of danger, to provide updates about both the incident and its impact on RISKWORLD. During the response, the RIMS team adapted to communication channels that were not in the original crisis plan.

RIMS Mobile App was used to deliver push notifications to all conference attendees who downloaded the mobile app and who also had "push notifications" enabled. Mobile App push notifications are managed by RIMS Business Events Manager. Note: attendees can choose to disable "push notifications." About 50% of attendees had downloaded the Mobile App.

Email was another tool used by RIMS to deliver pertinent information to conference registrants. Email distribution is a manual process and had to be done in batches to avoid being "black-listed." Realizing this, the RIMS team pivoted to use an "automated marketing software" to issue the emails in bulk, a process managed by the RIMS Director of Marketing.

RIMS also pivoted during the incident to issue notifications to attendees via the digital signage within the convention center. This was not in the original plan, but was a very effective adaptation, which was managed by the GWCC staff. RIMS also went outside of the written plan to collaborate with CNTV, RISKWORLD's show production vendor, to record a message from RIMS CEO Gary LaBranche. The recorded message was shared via the Mobile App, email and posted on the RISKWORLD website. Additions to the RISKWORLD website are managed by RIMS Chief Information Officer.

- ***Key Takeaway:*** *RIMS must improve instant attendee communication.*
- ***Key Takeaway:*** *RIMS Mobile App was an effective mode of communication, however, only half of RISKWORLD attendees download the mobile app.*
- ***Key Takeaway:*** *RIMS Mobile App also allows users to turn off push notifications.*
- ***Key Takeaway:*** *Changing digital signage throughout the convention center was effective, as was RIMS ability to quickly leverage CNTV to create a video message from RIMS CEO.*
- ***Key Takeaway:*** *RIMS adapted on-site during the incident and developed responses that were not contemplated in the original crisis plan.*
- ***Key Takeaway:*** *Most of the communication vehicles leveraged by RIMS are managed by different business owners.*

Enhancing RIMS Crisis Response

RIMS Crisis Plan & Planning

1. RIMS will leverage the services of an outside vendor (potentially a current RISKWORLD exhibitor) that specializes in developing crisis plans to update, modernize and improve the RIMS Crisis Plan.
2. The updated plan will address incidents that happen within the convention center, as well as those that impact the surrounding city.
3. An abbreviated (one-pager) version of the Crisis Plan will be distributed to RIMS staff and modified for RISKWORLD attendees.
4. Prior to each RISKWORLD, a designated meeting spot for RIMS staff will be noted in the plan.
5. Develop a map that identifies areas within the city where RIMS has exposures (i.e., events, hotels, shuttle routes)
6. Develop a checklist that would include evacuation plans, rally points and communications strategies.
7. Implement scenario planning with desktop drills, on-site training, and other exercises to assess effectiveness of the crisis and communications strategies.
8. Build a cloud-based, internal Resource Center to house communications templates, plans, lists, etc.
9. Evaluate RIMS insurance coverage vis a vis different scenarios.

Registration & Communications

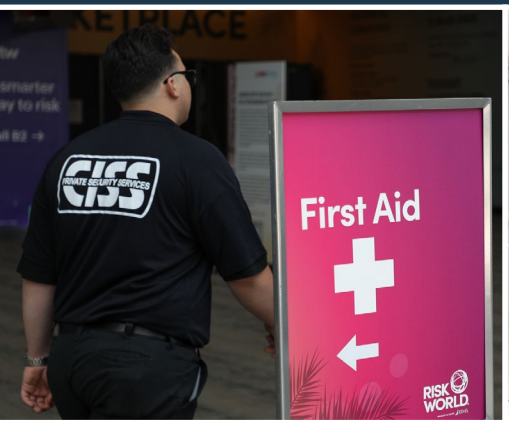
1. To improve RIMS ability to effectively communicate to all attendees in the convention center, RIMS must make it a requirement that any person entering the convention center be registered for RISKWORLD.
2. RIMS will mandate that cell phone numbers for all RISKWORLD attendees are a required part of the registration process.
3. Explore and employ an emergency text messaging service to notify all attendees of an emergency. RIMS would agree to only use cell phone information in the event of an emergency.
4. Explore and employ a more sophisticated text messaging service to notify RIMS staff of an emergency. Throughout the year, RIMS would conduct a series of practice "drills" to ensure all staff members are receiving the messages and that they are prepared to respond quickly.
5. Key RIMS business owners who manage critical emergency communications vehicles will be identified and prepped prior to RISKWORLD. Examples of critical emergency communications vehicles include: text messaging, email messaging, mobile app alerts, digital signage, hotel outreach, shuttle bus updates and others.
6. Leverage communications channels such as general sessions and the Show Daily to communicate safety procedures.

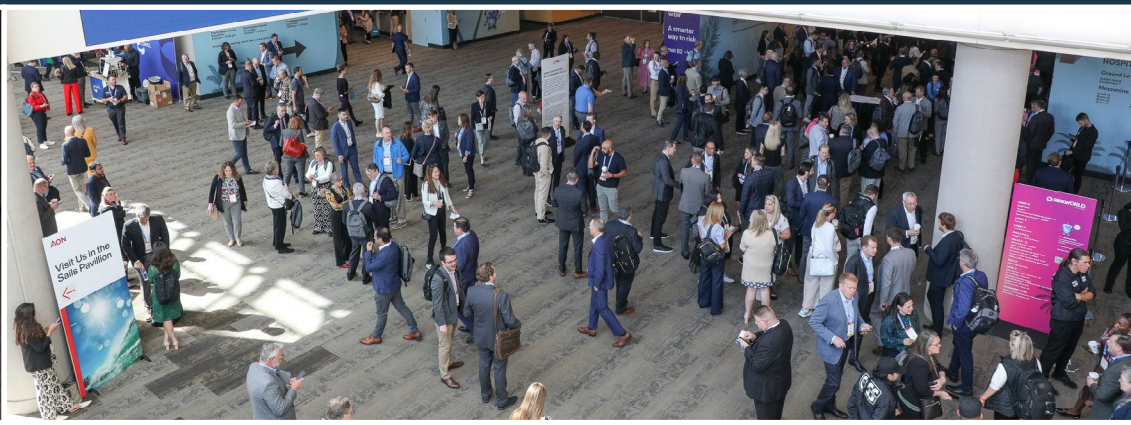
Local Authorities, Convention Centers and Future Convention Centers

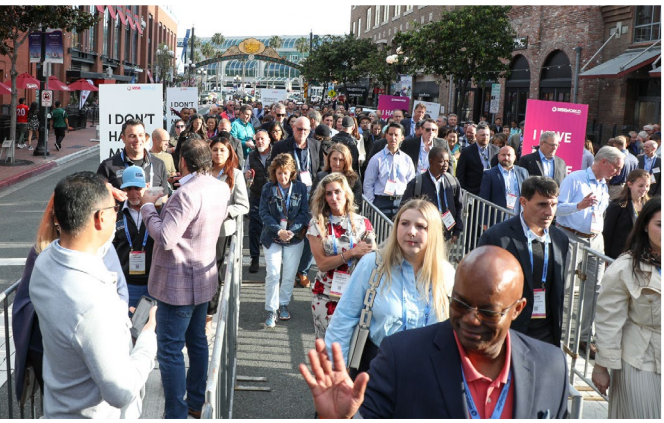
1. Establish relationships with the San Diego Convention Center's safety personnel, as well as city law enforcement prior to RISKWORLD 2024.
2. Define San Diego Convention Center's safety capabilities and coordinate walk-thrus leading up to the conference, as well as right before it begins.
3. Prior to RISKWORLD 2024, understand the venue's digital signage and public announcement system capabilities and the process for their implementation in an emergency.
4. Explore opportunities with the RISKWORLD audio/visual partner (FREEMAN) to assess capabilities to deliver messages in education session rooms.
5. Consider convention center safety capabilities in future site selection.

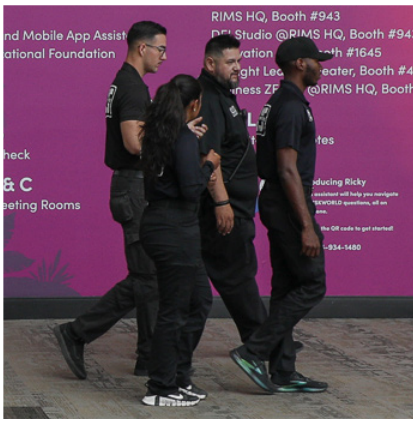
Housing and Shuttle Partners

1. Collaborate with housing partner to develop lists of attendees, organized by hotel, prior to RISKWORLD.
2. Request that each hotel within the RISKWORLD housing block provide a direct, emergency contact person.
3. Ensure that RIMS private security team is connected with the shuttle service vendor to ensure RIMS leadership is informed of any issues impacting the city.









RISKWORLD Safety & Security: One Year Later

Safety and Security Enhancements Implemented at RISKWORLD 2024

RIMS
the risk management society

The active shooter incident in Atlanta during RISKWORLD 2023 provided RIMS with an invaluable opportunity to assess existing event safety and security measures and make impactful enhancements for the future.

From more in-depth pre-event planning and added security personnel, to the integration of cutting-edge security technology, the following highlights some of the new safety and security enhancements implemented one year later at RISKWORLD 2024.

Pre-RISKWORLD 2024 Activity

> **Engaged Expert Services.** Recognizing the importance of safety and security at RISKWORLD and future events, RIMS employed world-leading security firm Merrill Herzog Group (MHG). In addition to managing onsite safety and security during the event, the MHG team conducted a 360-degree assessment of RISKWORLD, led pre-event crisis preparedness meetings with the emergency response team, and developed a customized Crisis Plan for RISKWORLD 2024.

> **Controlled Access.** In the past, unregistered attendees were allowed to enter the Convention Center to attend business meetings but were restricted from education sessions, keynote presentations and the exhibit hall. In 2024, RIMS eliminated that access. RIMS created a new, lower-priced registration category to accommodate these individuals but to also ensure RIMS possessed emergency contact information for everyone in the building.

> **Required Contact Information.** To ensure the ability to rapidly reach every attendee in the event of an emergency, RIMS required attendees to provide their cell phone numbers during the registration process.

> **Provided Pre-Event Safety & Security Messages.** RIMS developed a "Safety & Security Know-Before-You-Go" communication that was emailed to all registrants, posted on the RISKWORLD website, and included in the RISKWORLD Mobile App. In addition to a written message, a safety and security video was also delivered by email.

> **Identified Emergency Responders.** A RISKWORLD Communication Ownership Map was created that listed at least two RIMS staff members responsible for each communication channel. The map also identified the staff member responsible for coordinating with key vendors (i.e. housing, shuttle bus, etc.). Those who were listed were informed of their onsite emergency communication responsibility prior to RISKWORLD. They were also trained and drilled in the mechanics of issuing messages.

> **Developed Pre-Recorded Messages.** Pre-recorded emergency communications were developed prior to the event. The communications were developed for delivery via four channels: audible public announcement in the center, visual signage boards in the center, social media, and RISKWORLD Mobile App push notifications.

> **Enhanced Training.** While security training was a part of the pre-event planning in prior years, in 2024 RIMS expanded security and safety training to include key vendors, partners and volunteers. More than 70 people participated in an extensive walk-through of the convention center during which they were oriented to various emergency response tools, exits, security stations and the like. They were asked to be the "eyes and ears" of the conference and trained on how to report an incident or suspicious situation.

Onsite Safety & Security Activity

> **Secured the Perimeter.** To maintain better control and to prevent unauthorized/unregistered individuals from entering the Convention Center, all the doors to the convention center were secured and patrolled, leaving just one point of access to get into RISWORLD. (All the doors could be used to exit the building).

> **Enhanced Planning for Under 21 Attendees.** More than 250 university students attended RISKWORLD. Not all are over 21, which was required for some events. Attendees under 21 received a distinctive RISKWORLD badge. Pre-conference messaging and a webinar emphasized what events were 21+ and what behavior was expected.

> **Added Security Personnel.** Additional security personnel were deployed throughout the venue to monitor and respond to potential security threats and to ensure all access points were closed upon an individual's exit.

> **Enhanced Communication.** RIMS staff, key vendors and convention center personnel were equipped with 80 radios, enabling surveillance, situational awareness and rapid, coordinated response. In addition, an SMS text chain was pre-populated with key personnel.

> **Provided On-Site Safety & Security Messages.** Safety and security messages and a video were played prior to each keynote presentation. Both the written and video communications provided safety tips, information about local medical facilities, and other onsite security measures at RISKWORLD. In addition, RIMS coordinated with its hotel partners and arranged for registrants to receive a safety and security letter upon check-in, customized for each hotel.

> **Coordinated with Unions.** RIMS met with the leaders of the Unions at the Convention Center and briefed them about safety and security measures being undertaken for RISKWORLD. RIMS invited the Union leaders to share their ideas and they participated in RIMS security meetings. Union leaders were given RIMS radios to communicate in the event of an emergency.

> **Heightened Visual Deterrence.** In collaboration with local law enforcement agencies, RISKWORLD 2024 had a heightened presence of armed and uniformed police personnel in and around the venue. In addition, K-9 units were used and were prominently placed at the entrance and other high-trafficked areas. Two marked police cars were parked along the front of the Convention Center.

> **Publicized Prohibited Items.** A list of restricted items, such as handguns, banners, spray paint, etc., were included in the pre-meeting communications and prominently posted at the entrance.

> **Required Scanning.** All attendees were subject to metal detection screening upon entering the venue. The screening gates, designed for high traffic throughput, were staffed by trained and experienced security personnel who conducted bag searches as necessary.

> **Posted Zero Tolerance Message.** A strong, clear notice was posted in several places detailing that RIMS had a zero-tolerance policy regarding harassing language, hate speech, threats, sexual harassment, etc., and noting that RIMS retained the right to cancel credentials and deny access to the convention center to anyone who breached that policy.

> **Strengthen Cybersecurity.** RIMS IT staff monitored the convention center WiFi system, as well as social media and the internet, and deployed a robust suite of cybersecurity software to protect RISKWORLD registration and exhibit management systems and servers. RIMS IT staff also visits the center several times prior to a RISKWORLD to assess the strength of each center's cybersecurity.

> **Created Unified Command Center.** A Unified Command Center (UCC) was established at the Convention Center. The UCC was staffed by RIMS IT personnel along with security professionals throughout the entirety of the conference. The UCC had access to the Convention Center's Closed Circuit Television System, monitored traffic on the 80 radios, tied into the Gabriel Security System and had direct links to local law enforcement, fire safety and others, enabling RIMS to respond to emergencies faster.

> **Deployed Gabriel.** RIMS was the first conference in North America to employ the Gabriel Security System. This state-of-the-art technology featured a series of devices prominently placed throughout the Convention Center. In the event of an emergency, any attendee could activate Gabriel. When activated, the system would initiate instant audio and video communication between the individual who activated the system and the Unified Command Center (UCC). The UCC would deploy the proper response and notify security and local authorities. CCTV cameras would be positioned to best view the scene. Additionally, Gabriel capabilities included a virtual command center that would allow authorized users access to security camera footage via a mobile app or desktop computer.

A documentary video highlighting safety and security measures taken at RISKWORLD 2024 is available at **www.RIMS.org/activeshooter**. The RIMS "*After Action Review*" report, "*RISKWORLD Safety & Security: One-Year Later*" report, and other relevant resources are also available at **www.RIMS.org/activeshooter**.

Tools and Resources

[Take These Steps to Mitigate Operational Risks]

[How Cyber Risk Touches Nearly all Aspects of Business Risk]

[Copenhagen Risk Assessment 2023]

asae BUSINESS SOLUTIONS

insurance source

Association Risks Covered

Governance Checklist for Associations and Nonprofit Organization Boards

Brought to you by AON

The Importance of Evaluating Your Nonprofit Board's Governance Practices

ASSESSING YOUR BOARD OF DIRECTORS POTENTIAL RISKS

The Checklist consists of lists of questions about nonprofit organization policies, programs or procedures that could carry legal liability risks. The Checklist can be used by a nonprofit organization as a self-evaluation document to help understand and evaluate the potential risks they might face.

Subjects addressed in the Checklist were identified through studies of areas in which claims against nonprofit organizations covered by Directors & Officers Liability Insurance have most often been brought.

YOU CAN'T PASS OR FAIL

The Checklist is not an objective criterion document, but instead a subjective evaluation document. It is not a test that a nonprofit organization can "pass" or "fail."

Although the questions are designed to be answered either "yes" or "no," there are no right or wrong answers for all nonprofit organizations in all circumstances.

- In most cases the answer "yes" suggests a lower risk for the nonprofit organization.
- The answer "no" suggests that consideration should be given to whether a risk exists and whether it is acceptable to the nonprofit organization.

Your answers will not necessarily identify the nonprofit organization as one that is, or is not, "liable."

- Legal liability for a nonprofit organization can only be assessed with respect to its specific factual situation under applicable legal authority.
- Only a court can determine if a nonprofit organization is "liable" when the nonprofit organization is challenged.
- Whether the nonprofit organization is likely to be able to secure insurance indemnification depends upon underwriting guidelines, available underwriting authority and other internal insurance company factors when the association applies for insurance.

YOU CAN REDUCE YOUR RISK

The exercise of attempting to answer the Checklist can be valuable, because the questions relate closely to liability and potential claims made against directors and officers.

- Use of the Checklist may lead a nonprofit organization to more knowledgeable planning to eliminate or reduce unnecessary liability risks.
- Even if the nonprofit organization has no insurance and is "self-insured," this exercise may help make it a better risk.

YOUR NONPROFIT BOARD'S GOVERNANCE PRACTICES CHECKLIST

FOR GENERAL GOOD GOVERNANCE.

GENERAL	YES	NO
1. Is the leadership of the nonprofit organization routinely advised, through oral or written communications, regarding avoidance of potential legal liability?	☐	☐
2. Is the nonprofit organization managed by one or more experienced and knowledgeable professional nonprofit organization executives?	☐	☐
3. Has the executive attended educational programming on legal liability of nonprofit organizations?	☐	☐
4. Does the executive receive and review books, periodicals or other literature covering nonprofit organization law?	☐	☐
5. Is qualified legal counsel available either "inside" (on staff) or "outside" (on a retained basis) to consult regarding potential legal liability situations?	☐	☐
6. Is legal counsel especially knowledgeable and experienced in nonprofit organization law because of professional memberships, educational seminars, legal publications, or representation of other nonprofit organizations?	☐	☐
7. Does consultation with legal counsel typically occur when potential liability situations are first identified rather than later when a claim or challenge is received?	☐	☐
8. Does legal counsel attend meetings of the governing board of the nonprofit organization?	☐	☐
9. Does legal counsel regularly receive and review minutes, communications and publications of the nonprofit organization?	☐	☐
10. Does the nonprofit organization have governing documents--a corporate charter, bylaws, and a compilation of policies and procedures--that clearly specify the rights and obligations of members, directors, officers and staff?	☐	☐
11. Are the governing documents periodically reviewed to make them current and consistent with present interpretation of nonprofit organization law?	☐	☐
12. Is the purpose of the nonprofit organization stated clearly in its governing documents with no implication of illegality?	☐	☐
13. Are volunteers or staff indemnified through the governing documents or otherwise?	☐	☐
14. Is there an established policy as to who among the volunteers and staff is specifically authorized to communicate outside the nonprofit organization its views, comments and positions?	☐	☐
15. Are volunteers and staff periodically advised regarding authority to communicate on behalf of the nonprofit organization?	☐	☐
16. Are volunteers prohibited from using nonprofit organization letterhead except when authorized for a specific task, project or purpose?	☐	☐
17. Has the nonprofit organization previously carried any form of "errors and omissions," "directors" and officers" or "nonprofit organization professional liability insurance"?	☐	☐
18. Were there no claims made under that insurance?	☐	☐
19. Has that insurance been terminated?	☐	☐

YOUR NONPROFIT BOARD'S GOVERNANCE PRACTICES CHECKLIST

FOR BEST PRACTICES RELATED TO BOARD MEETINGS.

MEETINGS	YES	NO
1. Is each nonprofit organization meeting held according to a notice and agenda distributed in advance to attendees?	☐	☐
2. Are those who preside at nonprofit organization meetings made aware by staff or legal counsel of subjects that must not be discussed because of potentially adverse legal ramifications?	☐	☐
3. Are attendees at nonprofit organization meetings admonished against discussion of subjects with potentially adverse legal ramifications?	☐	☐
4. Are minutes taken of nonprofit organization meeting proceedings?	☐	☐
5. Do the minutes record all or most comments, views, criticisms, considerations or discussions of each subject rather than merely reports, communications and resolutions?	☐	☐
6. Are minutes prepared by staff rather than by volunteers?	☐	☐
7. Are draft versions of minutes removed from the nonprofit organization's records once the final version is approved?	☐	☐
8. Are minutes reviewed by legal counsel before distribution?	☐	☐
9. If audio recordings are maintained of nonprofit organization meeting proceedings, are they destroyed after use in preparing written minutes?	☐	☐
10. Are "rump," "secret" or "off-the-record" meetings by the nonprofit organization or among its leadership or members prohibited and avoided?	☐	☐

asae BUSINESS SOLUTIONS insurance source

Association Risks Covered

Discover Where Associations Turn to for Business Insurance

Selecting an insurance provider who understands your operations, unique risks and budgetary concerns is essential to running a successful organization and your peace of mind. If you or your local insurance agent are looking for a partner that specializes in providing insurance to professional and trade associations, ASAE Business Solutions has done the legwork for you by selecting ASAE-endorsed insurance providers. Aon Affinity Nonprofits is a vetted provider that can assess your risks and provide customized solutions at competitive premiums.

Take the next step in protecting your organization. Learn more at www.asae-aon.com.

---

www.asaebusinesssolutions.org

202.626.2880

businesssolutions@asaecenter.org

Sample: Event Crisis Management Team Roles

Name: _____

Date trained: _____

In an actual emergency or crisis, the Crisis Management Team will serve in the following roles:

Incident Commander (Meeting Logistics Lead; Back-up: Meetings Coordinator): Acts as the Crisis Management Team chair and is in charge until or unless this person relinquishes their role to another member of the team. This duty might also be held by the Chief Staff Officer.

Media Contact (Communications, Marketing & Sales Leads; Back-up: Director, Meeting Logistics): Accountable for ensuring no individuals make inappropriate or unauthorized statements to the media. Monitors news and communicates with the team. Provides continuous communication to staff members on site and at headquarters office to keep them apprised of the emergency. Manages on-site press and distributes press releases. Prepares a position statement and identifies individuals who are willing to be interviewed on behalf of the organization. Responsible for updating content on the organization's website.

Event Logistics Contact (Meetings Lead; Back-up: Events Manager): Liaison to all hotels, vendors, convention center, and city to keep them apprised of the crisis or emergency.

Registration Contact (Member Services or Registration Lead): Communicates and sets up an emergency help desk to provide information to all individuals on site to keep them apprised of the emergency.

Travel Services Contact (Events Team Member; Back-up: Event Team Supporting Staff): Communicates with travel agencies and sets up emergency travel services help desk to provide information to all individuals on site about airports, hotels, car rentals, trains, buses, and ride-sharing.

Speaker/Moderator Contact (Program Manager; Back -up: Education Coordinator): Communicates with speakers and moderators to keep them apprised of the crisis or emergency.

Technology Contact (IT Lead; Back-up: Director of Member Services): Employs cybersecurity tools to protect registration and exhibit management systems, as well as systems used by third-party providers such as housing.Proactively gathers threat intelligence by monitoring social media, the internet and the dark web. Manage cyberattacks, publish information on the organization's website, and disseminate mass emergency communications to attendees as needed.

Exhibitor Contact (Senior Director of Exhibitions or Exhibit Manager): Informs all exhibitors to keep them apprised of the emergency.

Sample: Your Crisis Management Team Worksheet

INCIDENT COMMANDER
Primary: Director, Meeting Logistics
Name:
Date trained:

Back-up: Meetings Coordinator
Name:
Date trained:

MEDIA CONTACT
Primary: Senior Director of Communications, Logistics Marketing & Sales Leader
Name:
Date trained:

Back-up: Director, Meeting
Name:
Date trained:

EVENT LOGISTICS CONTACT
Primary: Meetings Coordinator
Name:
Date trained:

Back-up: Program Manager
Name:
Date trained:

REGISTRATION CONTACT
Director of Member Services or Registration
Name:
Date trained:

TRAVEL SERVICES CONTACT
Primary: Assistant Director of Education
Name:
Date trained:

Back-up: Education Coordinator
Name:
Date trained:

SPEAKER/MODERATOR CONTACT
Primary: Program Manager
Name:
Date trained:

Back-up: Education Coordinator
Name:
Date trained:

TECHNOLOGY CONTACT
Primary: Director of IT
Name:
Date trained:

Back-up: Director of Member Services
Name:
Date trained:

EXHIBITOR CONTACT
Senior Director of Exhibitions or Exhibit Manager

<Company logo or Conference banner>

<Company Name>

Crisis Response and Event Emergency Plan

<Date Last Updated>

Table of Contents

1. Objective

<Company Name> provides this document to ensure the safety of Staff, Volunteers and Conference Attendees as they address issues and options being faced by travel during crisis or critical incidents. The development of effective and efficient crisis response and crisis management procedures is predicated upon preparedness, pre-planning, recognizing options, training and a vigilant perception of the world in which we live. This document is updated each year, with current facility and destination specific information.

2. Purpose

In the event of an emergency, <Company Name> will act to protect lives and property and to avoid liability. The purpose of this document is to develop and maintain standard procedures for Staff, Volunteers and Attendees to prepare for and respond to emergency situations.

The Crisis Response Plan is a working document and will be continually reviewed, revised and rewritten as necessary. Potential crisis situations, which have not been addressed in the plan at this point, may need to be added at a later date.

3. Internal Communications

<Company Name> employees on-site will be advised of a meeting point in the event of emergency. Staff members have received the following instructions for internal communications in the event of an emergency:

<insert your companies specific instructions for staff communication to include the chain of command and roles and responsibilities>

4. Public Communications

To ensure a consistent message, it is important that all communications are directed to the assigned <Company Name> Crisis Management team. The Media Contact will manage all communication with the press and general public.

When discussing a particular crisis situation, all staff members should be cognizant of their surroundings and who may be within listening distance. Radios/walkie talkies should not be used to communicate the details of an emergency.

If a concerned volunteer, attendee or exhibitor approaches a staff member, our response should be conservative. If the situation becomes critical – staff must relax, be calm, and explain to the person(s) that a member of <Company Name> will be making an official statement in the near future.

Crisis Management Team Members will manage the crisis response in the event that Team Members on-site are unable to participate.

5. Crisis Level Definition

Different crises require different responses. Specific scenarios listed in this document should be labeled Level 1 and Level 2.

Level 1 – Situations that can be contained and resolved by <Company Name> staff, facility personnel and contract security, without widespread action, public statement, risk or event disruption. Examples include: injury or illness limited in scope, routine theft, and limited disruptive behavior. Level 1 situations are likely to be reported to <Company Name> staff, facility and vendor personnel who are advised to report any situations to the nearest Show Management Office. The lead meeting planner at each facility, in conjunction with facility and vendor personnel will take appropriate action. Level 1 situations do not require the activation of the Crisis Management Team, however, the Team will be notified of a Level 1 event as these events may move from Level 1 to Level 2 at any time.

Level 2 – Situations that require higher level decision-making, event postponement, public statement, or have the potential to cause panic, injury, or controversy. Examples include hurricane, terrorist activities, or transportation disruption. Level 2 situations are likely to be learned about from external sources such as the media, Internet, volunteers and attendees. Staff members will notify the nearest Staff Management Office immediately of a potential Level 2 situation. Show Management Office personnel, facility lead or any member of the Crisis Management Team will arrange to convene the Team in person and/or by remote communication. Staff will be advised that the situation is being reviewed and instructions are forthcoming.

6. Crisis Response Personnel & Contacts

<Company Name> Crisis Management Team

The Crisis Management Team is comprised of <Company Name> staff members representing critical functions. The Crisis Management Team is responsible for reviewing and maintaining this document, monitoring threats and hazards and serving as the response team onsite in the event of an actual crisis or emergency.

Name	Responsibility	Work Phone	Cell Phone
	Incident Commander		
	Media Contact		
	Event Logistics Contact		
	Registration Contact		
	Exhibitions Contact		
	Travel Services Contact		
	Speaker Contact		
	Technology Contact		

Show Management Office Contacts

Name	Cell Phone

Key Staff

Name	Responsibility	Work Phone	Cell Phone

CPR/AED Certified Staff

Name	Cell Phone

Local Security & Emergency Contacts

Name	Location	Phone
Hotel or Convention Center		
Security		
First Aid		
Lost Prevention		
Urgent Care		
Hospital		
Local Pharmacy		
Local Police Department		
Local Fire Department		

Additional Resources

Crisis Text Line
crisistextline.org
FREE 24/7 SUPPORT
Crisis text line serves anyone, in any type of crisis, providing access to free, 24/7 counseling support and information via the medium people already use and trust: Text. Here's how it works:

1. Text 741-741 from anywhere in the USA, anytime, for any crisis.
2. A live, trained Crisis Counselor receives the text and responds quickly.

RAINN (Rape, Abuse & Incest National Network)
rainn.org
National Sexual Assault Hotline
800-656-HOPE (4673)

Directory of State Sexual Assault Hotlines
feminist.org/911
Directory of crisis center hotlines in the USA.

FEMA and Department of Homeland Security
fema.gov and dhs.gov
Multiple resources available such as storms, earthquake, fire, cybersecurity, terrorism, active shooter, transportation etc.

7. Crisis Management Team Members Responsibilities

In case of an actual emergency or crisis, the Crisis Management Team will serve in the following roles:

Incident Commander (Director, Meeting Logistics; Back Up: Meetings Coordinator): Act as the Crisis Management Team chair and is in charge until or unless this person relinquishes his or her role to another member of the team. Liaison to the Executive Director and the Chief Operating Officer and the rest of Crisis Management Team and will be the main medical emergency contact.

Media Contact (Senior Director of Communications; Marketing & Sales, Back Up: Director, Meeting Logistics): Accountable for ensuring no individuals make inappropriate or unauthorized statements to the media. Monitors news and communicates with the team. Provides continuous communication to staff members onsite and at the headquarter office to keep them apprised of the crisis or emergency. Manages onsite press and distributes press releases. Prepares a position statement and identifies individuals who are willing to be interviewed on behalf of <Company Name>. Responsible for news content on the <Company Name> website and emergency voicemail updates on the main <Company Name> phone line. Ensures telephone systems and televisions are set up and operational throughout the facility.

Event Logistics Contact (Meetings Coordinator; Back Up: Scientific Program Manager): Liaison to all hotels, vendors, convention center, and city to keep them apprised of the crisis or emergency.

Registration Contact (Director of Member Services or Registration): Communicates and sets up an emergency help desk to provide information to all individuals onsite to keep them apprised of the crisis or emergency.

Travel Services Contact (Assistant Director of Education ; Back Up: Education Coordinator): Communicates with <Company Name> travel agencies and sets up emergency travel services help desk to provide information to all individuals onsite about airports, hotels, car rentals, trains, buses, and ride-sharing.

Speaker & Moderator Contact (Program Manager; Back Up: Education Coordinator): Communicates with speakers and moderators by phone, email and in person to keep them apprised of the crisis or emergency.

Technology Contact (Director of IT; Back Up: Director of Member Services): On standby to be available to help in case of a technology emergency.

Exhibitor Contact (Senior Director of Exhibitions or Exhibit Manager): Communicates with all exhibitors by phone, email, and in person to keep them apprised of the crisis or emergency.

All Staff Members: Assist with the above communications and procedures where needed and assigned.

8. Destination & Facility Plan

a. Evacuation Plans

In the event of a serious emergency, it may find it necessary to evacuate the building. Should that become necessary, you will receive instructions about what to do and where to go by the Crisis Management Team and/or the Public Address System.

If evacuation is needed, use the closest marked "EXIT" or follow directions from building personnel. The evacuation or rally points can differ depending on where in the building the emergency is taking place. <Provide staff meeting places and point of contact for each property if applicable>. Staff roll call will be taken. If for some reason that location is inaccessible to you please go to the nearest safe location and text/call your supervisor with your location and status.

Incidents that may require evacuating the building include:

- Fire
- Bomb threat/suspicious package/suspicious mail
- Explosion
- Weather related emergency (with advanced notice)
- Chemical or Biological Incident

<insert information provided by the venue regarding evacuation plans, assembly areas, and the chain of command for determining an emergency>

The key to a successful evacuation is to remain calm and follow directions.

b. Shelter in Place Plan

Incidents that may require shelter in place include:

- Weather related emergency

- Civil Disturbance
- Suspicious package/suspicious mail
- Chemical or Biological Incident
- Hazardous material

<insert information provided by the venue regarding shelter in place>

c. ADA Compliance

The Americans with Disabilities Act (ADA), requires the both the venue and <Company Name> provide accessible accommodations to disabled persons.

<insert venues plan for assisting guests with disabilities>

d. Onsite First Aid Locations & Hours

<insert information provided by the venue or from contracted medical provider >

Location	Phone	Hours

e. Automated External Defibrillators (AED) Locations

An automated external defibrillator (AED) is a portable device that checks the heart rhythm and can send an electric shock to the heart to try to restore a normal rhythm. AEDs are used to treat sudden cardiac arrest (SCA). SCA is a condition in which the heart suddenly and unexpectedly stops beating.

Anyone who has minimal CPR and AED training can use an AED to help save a life. Refer to Section 6. Crisis Response Personnel & Contacts to see who on staff is AED certified.

<insert the locations of AED devices within the venue>

9. Cancellation Plans

In the event of a crisis or emergency warranting cancellation of the Meeting, all staff members and other key personnel will report to the Show Management office. If the venue is evacuated, report to <insert location>.

a. If the Meeting needs to be canceled prior to the start of move-in:

- All key personnel, will meet in the Show Management office to review implementation of cancellation plans or by conference call prior to arriving onsite
- Incident Commander enacts Emergency Phone Tree to inform all staff members of the cancellation and provide further instructions
- Media Contact to create a formal statement outlining the decision for cancellation and further actions, if necessary

    - Staff members and key personnel should use script provided to answer questions from individuals
    - Staff members and key personnel should state "no comment" for any questions asked by the media or press and inform them to contact the Media Contact.
- Media team will handle communications that should go out immediately to all individuals planning to attend the Meeting
    - A message announcing the cancellation will be posted on the <Company Name> website, main phone line, and an e-blast will be sent
    - To the extent possible, personal phone calls will be made to individuals attending the Meeting
- All staff members will update their voicemail at the office and their hotel room telephones with the same statement
- Facility personnel and staff members assigned will be at entrances to the convention center to let individuals know, who may not have received the message, that the Meeting has been canceled
- Media Contact will post cancellation information in key locations in facility
- Registration Contact and Exhibitor Contact will put into place policies for refunds of exhibitor and registration fees
- Incident Commander will contact the facilities, legal counsel, and the insurance company to alert them of the cancellation
- Event Logistics Contact will provide written notice by email of the cancellation to all facilities impacted by this decision (i.e. hotels, restaurants, CVB, etc.)
- Meetings with all staff members and key personnel will continue on a frequent basis as long as necessary to keep them updated on the situation

b. If the Meeting needs to be canceled during move-in:

- All key personnel, will meet in the Show Management office to review implementation of cancellation plans
- Incident Commander enacts Emergency Phone Tree to inform all staff members of the cancellation and provide further instructions
- Media Contact to create a formal statement outlining the decision for cancellation and further actions, if necessary
    - Staff members and key personnel should use script provided to answer questions from individuals
    - Staff members and key personnel should state "no comment" for any questions asked by the media or press and inform them to contact the Media Contact.
- Media Contact will handle communications that should go out immediately to all individuals planning to attend the Meeting
    - A message announcing the cancellation will be posted on the <Company Name> website, main phone line, and an e-blast will be sent
    - To the extent possible, personal phone calls will be made to individuals attending the Meeting
- All staff members will update their voicemail at the office and their hotel room telephones with the same statement
- Event Logistics Contact will provide information of the situation to all hotels impacted
    - Hotels will be asked to extend the convention rate as long as necessary

- Exhibitor Contact will contact exhibitors through a call to their home office as well as inform them verbally and in writing via email of the cancellation
- Facility personnel and staff members assigned will be at entrances to the convention center to let individuals know, who may not have received the message, that the Meeting has been canceled
- Media Contact will post cancellation information in key locations in facility
- Registration Contact and Exhibitor Contact will put into place policies for refunds of exhibitor and registration fees
- Incident Commander will contact the facilities, legal counsel, and the insurance company to alert them of the cancellation
- Event Logistics Contact will contact the shuttle bus company to set up transportation to hotels and/or airports for staff members.
    - To the extent possible, buses can be used to arrange transportation for individuals attending or providing service to the Meeting, that will be done
- Event Logistics Contact will provide written notice by email of the cancellation to all facilities impacted by this decision (i.e. hotels, restaurants, CVB, etc.)
- Meetings with all staff members and key personnel will continue on a frequent basis as long as necessary to keep them updated on the situation

c. If it is determined that the Meeting should progress until conclusion, but transportation home is limited:

- All key personnel, will meet in the Show Management office to confirm a plan of action
- Incident Commander enacts Emergency Phone Tree to inform all staff members of the situation and provide further instructions
- Media Contact to create a formal statement outlining the decision and further actions, if necessary
    - Staff members and key personnel should use script provided to answer questions from individuals
    - Staff members and key personnel should state “no comment” for any questions asked by the media or press and inform them to contact the Media Contact.
- Incident Commander or venue will make announcements on the public address system throughout the facility of the decision to continue the Meeting until conclusion
- Media Contact will handle communications that should go out immediately to all individuals attending the Meeting
    - A message announcing the decision of continuing the Meeting will be posted on the <Company Name> website, main phone line, and an e-blast will be sent
    - To the extent possible, personal phone calls will be made to individuals attending the Meeting
- All staff members will update their voicemail at the office and their hotel room telephones with the same statement
- Event Logistics Contact will provide information of the situation to all hotels impacted
    - Hotels will be asked to extend the convention rate as long as necessary
- Travel Services Contact will set up desk and include hotel policies as well as information on transportation options
- Media Contact will post cancellation information in key locations in facility

- Exhibitor Contact will communicate with the exhibitors and speakers about the importance of staying the course
- Continued communications sent out by the Media Contact will assure all individuals that the scheduled events will be held as planned
- Televisions, set up by the Media Contact, will be in key places to provide individuals with access to the News so that they can see what is going on and not feel the need to go to their hotels
- Building evacuation plans, provided by the facility contact, will be on hand should that become necessary
- Event Logistics Contact will contact the shuttle bus company to set up transportation to hotels and/or airports for staff members.
    - To the extent possible, buses can be used to arrange transportation for individuals attending or providing service to the Meeting, that will be done
- Incident Commander will contact the facilities, legal counsel, and the insurance company to alert them of the situation
- Event Logistics Contact will provide written notice by email of the situation to all facilities impacted by this decision (i.e. hotels, restaurants, CVB, etc.)
- Meetings with all staff members and key personnel will continue on a frequent basis as long as necessary to keep them updated on the situation

d. If the Meeting needs to be canceled once the meeting has begun, and if transportation is curtailed:

- All key personnel, will meet in the Show Management office at the convention center to review implementation of cancellation plans
- Incident Commander enacts Emergency Phone Tree to inform all staff members of the cancellation and provide further instructions
- Media Contact to create a formal statement outlining the decision for cancellation and further actions, if necessary
    - Staff members and key personnel should use script provided to answer questions from individuals
    - Staff members and key personnel should state “no comment” for any questions asked by the media or press and inform them to contact the Media Contact.
- Media Contact will handle communications that should go out immediately to all individuals attending the Meeting
    - A message announcing the cancellation will be posted on the <Company Name> website, main phone line and an e-blast will be sent
    - To the extent possible, personal phone calls will be made to individuals attending the Meeting
- Incident Commander or venue will make announcements on the public address system in the facility
    - All individuals will be assured that we are providing them with the most accurate information possible in order to help them make their decisions
- Event Logistics Contact will provide information of the situation to all hotels impacted
- Hotels will be asked to extend the convention rate as long as necessary
- Travel Services Contact will set up desk and include hotel policies as well as information on transportation options

- All staff members will update their voicemail at the office and their hotel room telephones with the same statement
- Cell phones most likely will not work. Media Contact will request telephones banks to be set up in order for individuals to contact their homes and offices
- Facility personnel and assigned staff members will be at entrances to the convention center to let individuals know, who may not have received the message, that the Meeting has been canceled
- Media Contact will post cancellation information in key locations in the facility
- Registration Contact and Exhibitor Contact will put into place policies for refunds of exhibitor and registration fees
- Televisions, set up by the Media Contact, will be in key places to provide individuals with access to the News so that they can see what is going on and not feel the need to go to their hotels
- Event Logistics Contact will contact the shuttle bus company will be contacted to set up transportation to hotels for staff members
    - To the extent possible that those buses can be used to arrange transportation for members, that will be done
- Event Logistics Contact will contact the facility catering department contact to see if unused food can be donated or converted to box lunches for individuals and staff members
- Incident Commander will contact the facilities, legal counsel, and the insurance company to alert them of the cancellation
- Event Logistics Contact will provide written notice by email of the cancellation to all facilities impacted by this decision (i.e. hotels, restaurants, CVB, etc.)
- Meetings with all staff members and key personnel will continue on a frequent basis as long as necessary to keep them updated on the situation

11. **Crisis Analysis Summary & Financial Impact**

Complete a full crisis analysis after an emergency has taken place. <Company Name> and all staff members must evaluate how well the situation was handled and investigate additional steps needed to better handle a similar situation in the future.

Acknowledgments

RIMS

Gary A. LaBranche, FASAE, CAE
Chief Executive Officer

Stuart Ruff-Lyon, CMP, DES
Chief Events & Sales Officer
Events & Exhibition

Joshua Salter, RIMS-CRMP, ARM
Director of Communications
External Affairs

RIMS Strategic and Enterprise Risk Management Council Members
https://rims.connectedcommunity.org/rims/communities/committeehome?CommunityKey=416a411a-f50f-4a58-b9a0-4e5191e5cba6

ASIS

Peter J. O'Neil, FASAE, CAE
Chief Executive Officer

Teresa Anderson, CAE
Vice President, Content

Katie Robert
Manager, Publishing and Commerce

ASAE

Michelle Mason, FASAE, CAE
President & CEO

Amy Hissrich, CAE
Vice President, International Affairs Global Operations

Timothy Sanders
Director, Research

Jim Myers
Creative Services Director

Destinations International

Don Welsh
President and CEO

Gretchen Hall
Chief Operating Officer

Emily Scheiderer
Senior Director of Education, Sales & Services

Association Community Experts

Bob Mellinger
Founder & CEO
Attainium

Kristin Richeimer, CAE
Executive Director
Council of Colleges of Acupuncture & Herbal Medicine

The Center for Association Leadership

1575 I Street, NW | Washington, DC 20005-1103 | 202-626-2763 | asaecenter.org