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.