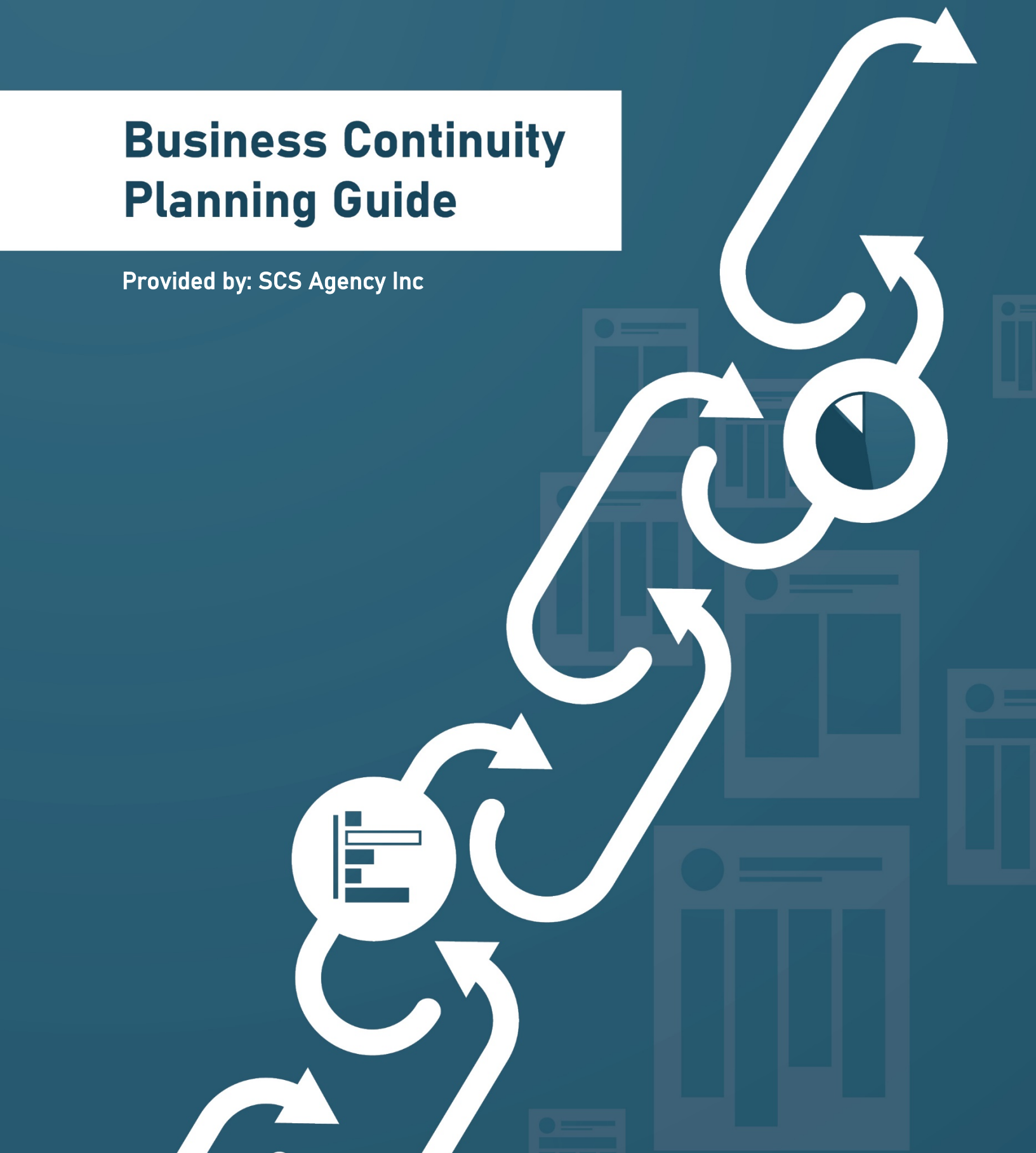
Business Continuity Planning Guide

Provided by: SCS Agency Inc



Contents

Introduction

Various unexpected disasters and emergencies can impact organizations, their stakeholders and their operations. In particular, events such as natural catastrophes, cyberattacks, public health crises and supply chain incidents can have serious consequences. These emergencies can damage commercial property and digital assets, disrupt critical business functions, cause prolonged operational downtime, and result in severe illnesses or injuries, lasting emotional harm and possible financial losses among employees, customers and suppliers.

Altogether, these disasters can be extremely costly for affected organizations and lead to severe reputational damage. Sometimes, such events may even force organizations to close their doors permanently.

Considering these concerns, it's imperative for organizations to have proper business continuity plans (BCPs) in place. These plans establish frameworks to help organizations limit possible damage and ensure crucial business functions can continue when disasters and emergencies strike. BCPs also outline protocols to minimize the risk of these events causing widespread destruction and disruptions in the first place. These plans are essential for organizations across industry lines and can make all the difference in fostering disaster resilience amid unforeseen circumstances. However, business continuity planning is a complex and multifaceted process. What's more, it's an ongoing effort; organizations need to consistently review, assess and update their BCPs to ensure they remain effective. That's where this guide can help.

The following document provides more information on business continuity planning, explains the main benefits of having BCPs in place, outlines key initiatives and goals of such plans, highlights common threats that BCPs can help address, and offers step-by-step guidance on creating, implementing and maintaining these plans. This guide also includes an appendix featuring additional business continuity content. By utilizing this guide, organizations can equip themselves with the knowledge and resources necessary to engage in successful business continuity planning and remain prepared for the unexpected, thus reducing the likelihood of disasters causing irreparable damage.

Keep in mind that this guide is not intended to be exhaustive, nor should any discussion or opinions be construed as legal advice. Organizations should contact legal counsel or an insurance professional for appropriate advice. Reach out to SCS Agency Inc today for further risk management guidance and insurance solutions.

Business Continuity Planning Explained

Business continuity planning refers to the development of organizational strategies, standards and policies that can promote the continuation of critical business operations and services amid various disasters and emergencies. In other words, BCPs include detailed measures to help organizations remain functional and safeguard their stakeholders and essential assets when unanticipated events take place. Although specific plans may vary based on the disaster at hand, a typical BCP outlines steps to assist an organization in upholding the following initiatives:

Continuing to deliver products and services to customers

Keeping employees and any other individuals on-site safe from harm

Minimizing potential property damage, data loss and infrastructure concerns

Maintaining access to all equipment, tools and technology necessary to perform crucial functions

Cultivating clear and open communication with all relevant parties (e.g., staff, customers, business partners, suppliers and emergency responders) to ensure everyone is well-informed on the current situation, its latest developments and any responsibilities they may have in addressing the matter

For BCPs to be successful, they should include detailed guidelines, provide defined levels of response that outline the most vital business functions and recovery objectives, offer flexibility in navigating different emergency scenarios, and allow for maximum collaboration and transparency among stakeholders to keep all parties on the same page. Above all, the protocols and procedures provided in BCPs should be centered around business resiliency, rapid recovery and thoughtful contingency planning.

Key Components of Business Continuity Planning

Some organizations may mistakenly confuse BCPs with other types of recovery or response plans. However, these plans are likely smaller components of BCPs; after all, business continuity planning involves a wide array of recovery and response processes. Here are the different plans that can generally be found in BCPs:

- **Disaster recovery plans (DRPs)**—This type of plan focuses on promoting business continuity within an organization's IT infrastructure. The main priorities of DRPs entail

limiting operational downtime caused by technology-related disruptions and reducing the likelihood of such disruptions destroying, corrupting or otherwise impacting essential data (e.g., private stakeholder information, financial records and confidential business files).

- **Crisis management plans (CMPs)**—This plan outlines criteria to help an organization determine whether a disaster has occurred. If an event meets these standards, then the organization can move forward with activating its BCP. CMPs also include a chain of command to consider amid emergencies, establish disaster reporting measures and offer customized best practices for crisis communication.
- **Emergency response plans (ERPs)**—This type of plan provides steps to assist an organization in mitigating the immediate impacts of a disaster. ERPs primarily focus on ensuring employee and customer safety, protecting critical business property and infrastructure, and fostering prompt restoration and remediation protocols.

As a whole, these plans (as well as other processes) form an organization's larger BCP, thus tackling the numerous elements involved in disaster resilience.

Debunking Common Misconceptions

Despite the importance of business continuity planning, certain myths have led some organizations to make false assumptions about BCPs, many of which undermine the depth and overall value of these plans. The most common misconceptions surrounding BCPs include the following:

- **BCPs are only essential for large corporations or those prone to natural catastrophes.** Some organizations may believe that BCPs only make sense for large businesses with more people and assets to protect. Nevertheless, these plans are imperative for organizations of all sizes, especially small businesses. Due to their limited capital, small organizations are more likely to encounter major financial challenges from a single disaster, potentially leaving them unable to recover.

Multiple studies found that between 40% and 60% of small businesses fail shortly after experiencing a crisis. For example, the U.S. Bureau of Labor and Statistics reported that more than 100,000 small organizations permanently closed their doors due to the fallout from the COVID-19 pandemic.

Some organizations may also assume that BCPs are only valuable for organizations located in areas more prone to natural catastrophes. While these catastrophes can certainly be devastating and require proper planning, they comprise only one of several types of emergencies that BCPs can help address. Organizations located in less catastrophe-prone regions could still be susceptible to cyberattacks, public health crises, supply chain incidents and other impactful events.

- **Business continuity planning is solely an IT matter; backing up critical data is sufficient.** Organizations may mistakenly limit their BCPs to their IT operations, assuming that technology-related disruptions are the only costly or damaging type of emergency and that conducting frequent data backups will solve any issues. Even though technology may play a substantial role in performing critical business operations and services, other aspects are involved in remaining functional and reducing possible losses in times of disaster. What's more, data isn't the only asset that requires protection when these events occur. A successful BCP should aim to protect an organization's entire operational framework and infrastructure while safeguarding its people and property. Further, these plans can't be restricted to technology-related disruptions; they should address a range of disaster scenarios to ensure maximum preparedness.

- **BCPs aren't worth the time, money or labor required to implement them.** While organizations may believe that they can't afford to establish BCPs, the reality is that they can't afford not to. Although these plans require initial investments, they are well worth it to combat the cost of a large-scale disaster, as just one disruptive event could generate millions of dollars in losses. This means that investing time and money in business continuity planning now can prevent organizations from facing significant financial challenges in the future.

- **Business continuity planning isn't necessary; organizations can simply decide how to respond to disasters when they occur.** Some organizations may neglect to create BCPs under the assumption that they will be able to navigate emergencies on the spot. Yet, this approach could pose serious consequences. When a disaster strikes, time is of the essence; taking even a minor pause to determine response and recovery measures could leave the door open for additional damage and disruptions to occur, resulting in exacerbated losses. Not to mention that a lack of business continuity planning could add another layer of stress and confusion when unexpected events arise, causing extra chaos and increasing the likelihood of miscommunication during the restoration and remediation processes. Altogether, this approach could lead to prolonged operational downtime and considerable reputational damage. By developing detailed BCPs before disasters occur, organizations can equip themselves with the steps and resources necessary to ensure a swift and calm response amid these events, keeping associated losses to a minimum.

Benefits of Business Continuity Planning

Business continuity planning can provide several advantages, ultimately supporting organizations, their stakeholders and their operations through challenging circumstances. Specifically, organizations that implement BCPs may experience the following benefits:

- **Greater business resilience**—First and foremost, organizations with BCPs are far better equipped to handle unexpected disasters and emergencies than those without such plans, thus reducing the risk of major disruptions and damage when these events occur. This, in turn, can help organizations stay resilient and recover in a timely manner amid crisis situations, allowing them to minimize downtime and limit total losses.
- **Enhanced stakeholder confidence**—Organizations that create detailed BCPs can demonstrate to their customers, suppliers, business partners, investors and other key stakeholders that they are committed to disaster preparedness and ready to handle the most difficult scenarios. This can help organizations maintain trust among stakeholders, making these parties more confident that they will be protected during emergencies.
- **Increased competitive edge**—In addition to enhancing stakeholder confidence, organizations with BCPs can showcase their ability to manage crises effectively to prospective customers and the public. Especially as certain disasters (e.g., natural catastrophes and cyberattacks) become more frequent and costly, this can provide organizations with a much-needed competitive edge in their respective industries and help them foster ongoing financial and operational success.
- **Improved employee morale and decision-making processes**—Effective BCPs involve clear communication protocols with employees and empower them to be involved in making critical business decisions. By keeping their employees informed and encouraging them to play their part in executing disaster preparedness and recovery objectives, business continuity planning can help organizations cultivate a positive working environment.
- **Bolstered compliance**—While having a BCP is considered best practice for any organization, some industries have regulatory standards regarding such plans. For instance, organizations operating in the health care and financial sectors may be legally required to create well-documented BCPs. As a result, engaging in business continuity planning could help organizations comply with applicable legislation and avoid potential fines or penalties.
- **Reduced coverage costs and a better overall insurance experience**—BCPs may also improve insurance results because they can help organizations adopt more robust risk management strategies and enhance their remediation processes amid unanticipated disasters. That is, organizations with BCPs can reduce their total business income losses, making them less likely to exceed their policy limits when claims occur and allowing them to avoid out-of-pocket costs. As a result, underwriters may categorize organizations with BCPs as less risky to insure and deem them more optimal for selection. In that same vein, organizations with BCPs might also benefit from better coverage options, lower deductibles and expanded capacity.

Primary Objectives of Business Continuity Planning

When developing their BCPs, organizations need to have clear objectives in mind. This means that organizations should determine specific goals they seek to accomplish with these plans and identify key threats they want to address. Here's a breakdown of these objectives.

Determining Plan Goals

Establishing goals for their BCPs can help organizations better personalize these plans to manage their exposures and meet their unique needs. Valuable BCP goals may include the following:

1. **Operational stability**—This goal involves maintaining critical business functions and delivering products and services as usual throughout unexpected disasters. Upholding operational stability can make all the difference in limiting disruptions and reducing downtime when crises arise.

2. **Asset protection**—This objective refers to keeping an inventory of crucial business property (e.g., buildings, structures, equipment, supplies and data) and having measures in place to protect it amid emergencies. Without asset protection protocols, this property could be increasingly susceptible to widespread damage and loss.

3. **Financial security**—This goal relies on ample risk management strategies and proactive loss mitigation measures to limit the financial fallout from unanticipated events. Maintaining financial security is key to avoiding long-term or even permanent closures when disruptions happen.

4. **Reputation preservation**—This objective pertains to maintaining organizational credibility and trustworthiness among stakeholders and other relevant parties through effective communication and crisis management procedures. Keeping a solid reputation when disasters strike can boost customer loyalty, employee retention and investor support.

Identifying Key Threats

The most effective BCPs can respond to several types of emergency scenarios. As such, organizations should identify possible threats their plans will address. Key threats to consider include:

Natural catastrophes—These catastrophes include various extreme weather and climate events, such as tornadoes, earthquakes, hurricanes, wildfires, droughts, hailstorms and snowstorms. Natural catastrophes can devastate impacted communities and organizations, causing substantial property damage, infrastructure breakdowns and loss of life.

Cyberattacks—Examples of such attacks include data breaches, phishing scams and ransomware incidents. Cyberattacks have surged in cost and frequency over the past few decades, resulting in major interruptions and leaving affected organizations and their stakeholders with considerable losses.

Public health crises—These crises include any emergencies (both natural and human-made) that pose a health risk to the public, such as infectious disease outbreaks (e.g., endemics and pandemics), chemical attacks, and the intentional or accidental release of hazardous materials. As evidenced by the COVID-19 pandemic, public health crises can arise quickly and without warning, leading to prolonged disruptions and endangering the well-being of entire communities and organizations.

Supply chain incidents—Such incidents include events that disrupt organizations' supply chains, usually resulting in substantial operational delays and making it challenging to continue delivering products and services. Because many organizations rely on third parties to perform critical business functions and often entrust these parties with private data and corporate assets, supply chain incidents can stem from multiple avenues (e.g., equipment breakdowns, transportation bottlenecks, cybersecurity vulnerabilities and property losses) and pose serious consequences.

Best Practices for Business Continuity Planning

Business continuity planning is an intricate process that requires careful consideration and ongoing updates. Here are best practices for organizations to keep in mind when creating, implementing and maintaining their BCPs:

- **Conduct a business impact analysis (BIA).** Conducting a BIA is an integral first step in the business continuity planning process. At a glance, a BIA examines the possible impacts that disasters and emergencies may have on an organization's critical business functions and collects the information necessary to determine short- and long-term response and recovery objectives. A BIA also includes an analysis of operational and financial losses that could stem from the disruption of key business functions.

  Potential impacts and losses for an organization to consider when conducting a BIA are lost or delayed sales, penalties related to not fulfilling contractual obligations, personnel concerns (e.g., the need for outsourcing or hiring overtime labor in response to employee injuries or compounded operational demands), diminished customer satisfaction and loyalty, obstructed future business plans and regulatory fines. Altogether, a BIA can help an organization identify its most crucial business functions and determine essential protocols, resources and dependencies to prioritize within its BCP.

- **Perform a risk assessment.** In addition to conducting a BIA, an organization must evaluate key hazards and threats that could affect its critical business functions. At a minimum, the risk assessment should include the previously mentioned threats, namely natural disasters, cyberattacks, public health crises and supply chain incidents. Depending on its unique operations, the risk assessment may also include threats such as power outages, equipment breakdowns and technology failures. Further, the size of an organization may determine additional threats; for example, smaller organizations are more likely than their larger counterparts to be significantly impacted by unexpected labor changes or major shifts in consumer demands.

  After identifying key threats in its risk assessment, an organization should determine the likelihood of them occurring and consider how such events could harm its people, property and reputation. Doing so can help the organization detect any vulnerabilities among its existing risk management measures and tailor its BCP to remedy these concerns. An organization's BIA and risk assessment should work together to provide the insight needed to move forward in the business continuity planning process. Specifically, these documents can help an organization calculate its recovery time objective (RTO) and recovery point objective (RPO). An RTO refers to an organization's targeted amount of time between a disaster occurring and the resumption of critical business functions, whereas an RPO indicates the maximum amount of data loss that the organization can handle. These objectives are fundamental in customizing an organization's disaster response and recovery strategies.

- **Develop response and recovery strategies.** The information collected from a BIA and risk assessment allows an organization to create detailed emergency response and recovery strategies. This entails outlining in-depth plans for maintaining each critical business function and service during several disaster scenarios and determining measures to safeguard the organization's stakeholders and vital assets when these events occur. Effective response and recovery strategies for an organization to consider include the following:

Follow guidance from authorities. An organization should rely on guidance from government agencies, local officials and public health experts regarding emergency evacuation requirements and related safety measures. Following this guidance can help ensure the safety of stakeholders during disasters.

Select an emergency operations center (EOC). By setting up an EOC, an organization can secure a temporary alternative location to perform critical business operations if its current facility is evacuated or shut down. This strategy allows for the continuity of product and service deliveries even in adverse conditions.

Foster supply chain resilience. An organization should maintain extra inventory on-site and consult with alternative suppliers to ensure the ongoing availability of essential materials during supply chain delays, disruptions or similar incidents.

Find backup equipment and technology. It's best for an organization to work with trusted third parties to secure access to backup equipment and technology in the event that its original assets become damaged or destroyed by disasters.

Maintain offline data storage. An organization should designate a safe location to store offline copies of critical data and confidential records to ensure data integrity and availability during emergencies, particularly those impacting its digital assets.

Implement strong cybersecurity measures. Creating and enforcing stringent cybersecurity measures (e.g., multifactor authentication protocols, access control policies, network segregation and segmentation, antivirus software, email authentication technology, and endpoint detection and response solutions) can help an organization prevent widespread disruptions and damage to its larger IT infrastructure during cyberattacks.

Purchase emergency generators. An organization should leverage emergency generators to maintain power in the event of outages or related technology failures and ensure critical business functions remain intact.

Establish an on-site shelter and supplies. Maintaining a shelter stocked with emergency supplies (e.g., first-aid kits, nonperishable food, water, radios, flashlights, batteries, phone chargers and blankets) can allow an organization to better protect its employees, customers and any other individuals on-site amid disasters that could threaten their safety (i.e., natural catastrophes).

Determine modified work arrangements. An organization should create modified work and service arrangements to follow during public health crises (e.g., telecommuting options and quarantining protocols for employees, virtual service offerings for customers, and on-site social distancing and sanitation requirements).

Prioritize open communication. Implementing solid public relations measures can help an organization ensure stakeholders and other relevant parties remain properly informed of disasters, their impacts and the organization's latest recovery updates.

- **Designate response and recovery teams.** Establishing disaster response and recovery teams can help an organization allocate its various BCP strategies across the workforce and ensure competent and qualified individuals oversee certain plan elements. These teams should be outlined in a documented roster, and everyone's key responsibilities should be explained. Specific BCP roles and expectations typically vary between senior leaders, continuity planning personnel and other employees. These responsibilities are as follows:
    - **Senior leaders**—Corporate executives and other members of the senior leadership team are generally in charge of evaluating emergencies as they occur and, if a situation warrants it, officially activating the BCP. Upon discovering or being notified of an ongoing disaster, senior leaders should carefully assess this threat and its impact on critical business functions. From there, such leaders should decide whether it's necessary to launch the BCP and, if so, promptly inform continuity planning personnel and other employees so that they can execute their roles. Together, these senior leaders form an organization's emergency management group (EMG), which gives them the authority to oversee the disaster response and recovery process, order a facility shutdown or evacuation, coordinate with stakeholders and the public as needed, and determine when a disaster has officially been resolved.
    - **Continuity planning personnel**—This personnel consists of department heads and on-site supervisors who may have specialized knowledge and experience regarding different BCP initiatives, such as IT professionals, legal counsel, HR leaders, property and supply chain managers, media and communication specialists, risk management and insurance experts, and financial administrators. Once the BCP has been activated, continuity planning personnel are in charge of maintaining critical business

functions by executing their assigned disaster response and recovery strategies in line with their specialties. Such personnel may also be responsible for leading the smaller plans within the BCP, including the DRP, CMP and ERP. Specifically, the head of the IT department would likely be best suited to manage the DRP, whereas on-site supervisors and risk management experts may be well-equipped to carry out the CMP and ERP. Among its EMG and continuity personnel, an organization should also select an incident commander. This individual is responsible for leading the EMG, establishing a chain of command and ensuring the successful deployment of the BCP as a whole.

  - **Other employees**—Continuity planning personnel will usually assign other employees within their departments, namely entry- and mid-level staff, to further assist them in performing their specified disaster recovery and response strategies. These employees should be properly informed of the actions they are in charge of deploying when emergencies strike, thus ensuring timely and successful remediation measures. Yet, such employees should also remain flexible and ready to adjust their actions based on the disaster at hand, its impact on critical business functions and current recovery developments.

- **Initiate communication protocols.** An organization must have effective communication protocols in place to prevent miscommunication or misinformation throughout the disaster response and recovery process. These protocols should define suitable methods for both internal (e.g., in-person meetings, phone calls, emails and corporate messaging applications) and external (e.g., social media, business website postings and press releases) communication during emergencies. They should also identify the key topics that necessitate such communication.

  When it comes to internal communication, an organization should leverage the proper channels to keep its employees updated on the details of the disaster, their evolving business continuity responsibilities during the event and any notable recovery progress. An organization should also implement internal communication protocols that clearly outline how employees can promptly report disasters and related disruptions as they arise and introduce a tiered alert system that helps indicate the overall severity of an emergency. For instance, a “code red” alert may represent the most serious types of crises that involve the loss of several critical business functions and pose significant safety hazards, while a “code yellow” alert may pertain to a less disruptive situation and a “code green” alert may signify that the organization continues to operate or has resumed operating in its normal capacity.

  In the realm of external communication, an organization should rely on the proper channels to inform stakeholders and other relevant parties of the emergency, how it could affect these individuals and the steps the organization is taking to resolve the situation. These individuals should also receive timely updates as recovery progress occurs. Depending on the nature of the situation, an organization should also consider

whether it needs to inform the public of the disaster or comply with applicable incident notification requirements, particularly any local, federal or international data breach reporting laws. Further, an organization's external communication protocols should involve keeping updated contact information for trusted third parties (e.g., the owner of the EOC, alternate suppliers, equipment operators, emergency responders, local officials, public health experts and government agencies) that could help remedy different disasters and stipulate when and how these parties need to be contacted. Regardless of the type or channel of communication, an organization needs to confirm that any information it shares during an emergency is swift, accurate and consistent.

- **Engage in proper resource management.** An organization should include a list of key resources within its BCP, including equipment, technology, and essential work materials and supplies. Creating this list can better assist the organization in determining which resources could be impacted by unexpected disasters and identifying alternative suppliers and trusted third parties to help secure backup resources amid these events. As an organization's operations shift over time, its key resources will likely follow suit, so the list should be reviewed routinely and updated as needed. This may entail eliminating resources that are no longer vital or adding new items due to workplace advancements. Upon making these updates, the organization should also review its alternative suppliers and third parties to ensure their backup services remain suitable. Depending on the amount and type of changes to its resource list, the organization may need to search for new or additional suppliers and third parties to meet its evolving needs.
- **Offer training and run tests.** To make sure its EMG, continuity personnel, other employees and any additional parties (e.g., business partners and primary and alternative suppliers) are well-versed on the BCP and their particular roles and responsibilities, an organization must conduct regular training on the subject. This training should not only highlight key elements of the BCP but also provide individuals with guidance on protecting their own families and personal assets during communitywide disasters, namely natural catastrophes and public health crises. An organization should also run frequent tests that evaluate the effectiveness of its BCP against various threats. Tests to consider include the following:
    - **Tabletop exercises**—A tabletop exercise is an activity that allows an organization and its EMG to simulate a realistic disaster scenario (e.g., a tornado, supply chain delay or infectious disease outbreak) to test its BCP's efficiency. In other words, this exercise serves as a business continuity drill, giving participants (typically continuity personnel and other employees) the opportunity to practice responding to an emergency. Conducting tabletop exercises is a valuable way for an organization to assess the overall reliability of its BCP and ensure that this plan will run successfully during an actual disaster.

  - **Penetration testing**—While tabletop exercises can help assess an organization's response to most disaster scenarios (i.e., natural catastrophes, supply chain incidents and public health crises), penetration testing is solely centered around evaluating an organization's ability to remain functional during a cyberattack. Such testing consists of an IT professional mimicking the actions of a cybercriminal to determine whether an organization's workplace technology possesses any vulnerabilities and is able to withstand attack efforts. This type of testing usually targets a specific type of technology and may leverage multiple attack vectors. Conducting penetration tests can help an organization review the effectiveness of the cybersecurity measures within its BCP, identify the most likely avenues for cyberattacks and discover potential weaknesses.

- **Prioritize continuous improvement.** A successful BCP requires frequent updates and changes, thus equipping an organization with the response and recovery strategies necessary to address operational shifts, emerging threats and new hazards. Several instances may prompt an organization to update and improve upon its BCP. For example, based on the results of its tabletop exercises and penetration testing, an organization should make the necessary changes to address any vulnerabilities or weaknesses found in its plan. Additionally, an organization should regularly review its BIA, risk assessment and resource list for any new developments, such as a change in critical business functions, potential threats, safety concerns or important assets. In most cases, any of these shifts would warrant BCP updates. When making changes to its plan, an organization should be sure to properly document these alterations and clearly communicate the updates with all relevant parties. Changes should also be reflected in BCP training and tests.
- **Consult external resources and insurance professionals.** An organization doesn't need to navigate the business continuity planning process alone. Instead, it's best to consult a variety of external resources for assistance in creating a BCP, including the in-depth guidance and templates provided by the Federal Emergency Management Agency and the U.S. Department of Homeland Security. Furthermore, it's imperative to consider possible coverage solutions for unexpected disasters that may result in widespread damage and disruptions. Collaborating with insurance professionals, including brokers and carriers, to ensure coverage strategies align with the BCP is often necessary. This process can help an organization identify coverage gaps and tailor its policies to address specific risks. By transferring some financial risks with insurance, an organization can mitigate the impact of disruptive events on its operations and assets.

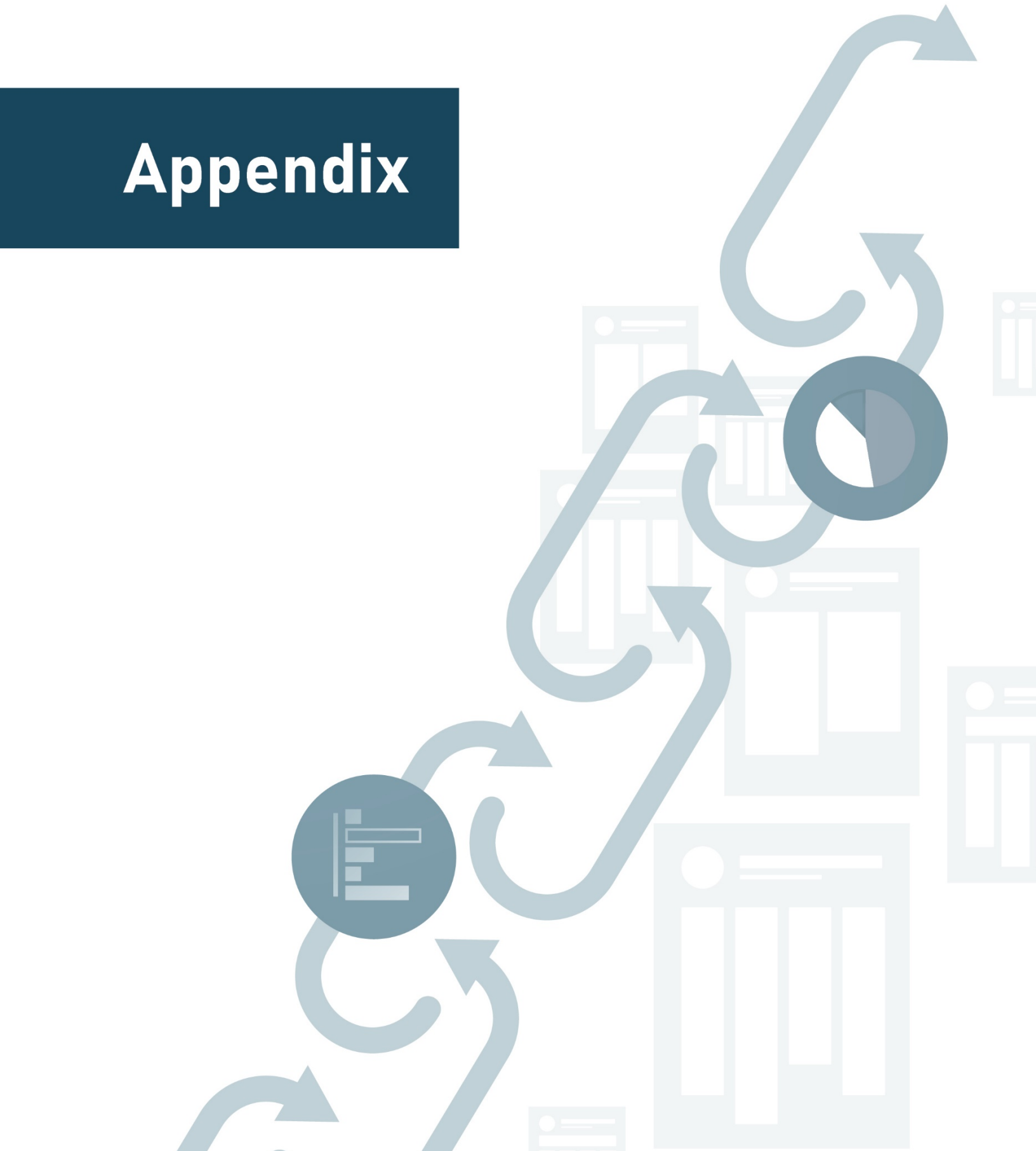
Conclusion

Disasters and crises can happen at any time, wreaking major havoc on affected communities and organizations. It's vital for organizations to be prepared for these events and have effective protocols in place to help them respond and recover. By creating, implementing and maintaining effective BCPs, organizations can equip themselves with the information and strategies needed to handle a wide range of emergency scenarios, therefore mitigating associated damage and disruptions.

Further, engaging in business continuity planning can help organizations better protect their people and property when disasters strike. This can allow them to maintain a solid reputation, avoid possible compliance issues, and foster financial and operational success for years to come. Altogether, BCPs are an essential business tool, as they may serve as the deciding factor between organizations staying resilient amid emergencies or having to close their doors for good.

Contact us today for more risk management guidance and insurance solutions.

Appendix



CHECKLIST | BUSINESS RECOVERY

Presented by: SCS Agency Inc

When you have finished developing your business continuity plan (BCP), utilize this checklist to apply business controls to the BCP, if needed, or to assess the overall readiness and maintenance of your BCP documentation.

Upon completion of the checklist, review your answers. Any question with a "no" response is a challenge you'll need to address. Determine action items for each "no" response for correcting each and reassess your BCP. You should feel confident that all "yes" answers indicate that you have planned well; however, that does not necessarily guarantee a successful recovery.

Date: Review conducted by:

EXECUTIVE AWARENESS/AUTHORITY	YES	NO	N/A
Has a BCP been developed?	☐	☐	☐
Has a BCP been documented and maintained?	☐	☐	☐
Has the BCP been updated within the past year?	☐	☐	☐

PLAN DEVELOPMENT AND DOCUMENTATION	YES	NO	N/A
Has a classification (i.e., critical, important or marginal) been assigned to the business process/function/component that this facility/function supports?	☐	☐	☐
Does the BCP include sections dedicated to threat identification, incident management, restoration, plan exercise and maintenance, response and recovery teams, and contact information?	☐	☐	☐
Does the BCP identify hardware and software critical to recovering the business and functions?	☐	☐	☐
Does the BCP identify necessary support equipment (e.g., forms, spare parts and office equipment) to recover the business and functions?	☐	☐	☐
Does the BCP require an emergency operations center (EOC) or alternate site for recovery?	☐	☐	☐
Are all critical or important data required to support the business backed up? Are they stored in a protected location (off-site)?	☐	☐	☐
Do you conduct a walk-through exercise of your BCP at least annually? This should include a full walk-through as well as key elements of your plan (e.g., accounts payable, shipping and receiving).	☐	☐	☐
Do the walk-through element exercises have a plan that includes a description, scope and objective?	☐	☐	☐

Is a current copy of the BCP maintained off-site?	☐	☐	☐
Do all users of the BCP have ready access to a current copy at all times?	☐	☐	☐
Is there an audit trail of the changes made to the BCP?	☐	☐	☐
Do all employees responsible for the execution of the BCP receive ongoing training in disaster recovery and emergency management?	☐	☐	☐

MANAGEMENT AND RECOVERY TEAM ASSESSMENT	YES	NO	N/A
Have the incident commander, emergency management group (EMG) and other applicable continuity personnel approved the BCP?	☐	☐	☐
Do the incident commander and EMG maintain a copy and audit trail of changes made to the BCP?	☐	☐	☐
Do all aspects of physical and logical security at the EOC conform with your current workplace procedures?	☐	☐	☐
Are all employees and their alternates responsible for executing a manual work-around for a mechanized process identified in the BCP, and are they properly trained?	☐	☐	☐
Has an independent observer documented the simulation exercise(s), noting all results, discrepancies, exposures, action items and individuals responsible?	☐	☐	☐
Was a debriefing held within a reasonable period of time (typically two weeks) after the simulation exercise(s) to ensure all activities were accurately recorded?	☐	☐	☐
Did the exercise coordinator publish a simulation exercise(s) report within a reasonable period of time (typically three weeks) after the completion of the simulation exercise(s)?	☐	☐	☐
Did the exercise report include what worked properly, as well as any deficiencies and recommendations for improvement? Did the exercise report also include responsibilities and due dates for the development of the corrective action plan?	☐	☐	☐
Did the incident commander and EMG develop a corrective action plan to address any deficiencies identified by the exercise?	☐	☐	☐
Is there a retention plan for the exercise plans and corrective action plans (minimum retention of three years)?	☐	☐	☐
Is a walk-through element exercise performed at least quarterly?	☐	☐	☐
Did each walk-through element exercise have a plan that includes a description, scope and objective?	☐	☐	☐

When there is a change in hardware, software or a process that might impact the BCP, is it reviewed and updated within 30 days of the changes?	☐	☐	☐
Based on the joint assessment, have the incident commander and EMG determined that the BCP is effective?	☐	☐	☐
Has the entire BCP simulation exercise been performed at least annually?	☐	☐	☐
Did the BCP simulation exercise have a plan that includes a description, scope and objective?	☐	☐	☐
Did the BCP simulation exercise meet the acceptable recovery time objective (RTO) and recovery point objective (RPO) set by the incident commander and EMG?	☐	☐	☐
Based on the joint assessment, has the team determined that the BCP and exercises meet all requirements to provide reasonable assurance that the plan will work in the event of a disaster?	☐	☐	☐
Does the BCP specify the maximum acceptable RTO and RPO?	☐	☐	☐
Does the BCP specify the level of service (which the incident commander and EMG have agreed to be acceptable) to be provided while in recovery mode?	☐	☐	☐
Have all changes relating to RTO and RPO in the BCP been approved by the incident commander and EMG?	☐	☐	☐

For more risk management guidance, contact us today.