



Architect's Guide to Business Continuity

Guidance for reducing firm disruption

- Business Continuity Planning is preparation—of people, premises, technology, information, supply chains, stakeholders, and reputation—for adverse events so the firm can continue to provide services, generate revenue, and reduce the negative consequences of business interruption.

Published 03/20
Interim release



**The American
Institute
of Architects**



Acknowledgements

The American Institute of Architects (AIA) recognizes that buildings and communities are subjected to destructive forces from natural and human-caused hazards. Architects and their businesses must also be resilient to disasters and disruption in order to protect themselves and service clients. The AIA would like to recognize the expertise and generosity of the following individuals that contributed to the creation of this Guide:

2019 and 2020 Resilience & Adaptation Advisory Group: Contributing authors

Allison Anderson, FAIA, 2019 Chair
Dr. Janice Barnes, AIA
Aaron Bowman, AIA
Louis Conway, Intl. Assoc. AIA
Jori Erdman, AIA
Jeffrey Gill, FAIA
Rosemarie G. Grant, AIA
Ann Kosmal, FAIA
Nancy McNabb, AIA
Gail Napell, AIA, 2020 Chair
Robert Phinney, AIA
Dr. Nicholas Rajkovich, AIA
Megan Recher, AIA
Robin Seidel, AIA

2019 and 2020 Disaster Assistance Committee: Contributing authors & peer reviewers

John Blumthal, FAIA
Ava Christie, AIA
Albert Comly Jr., AIA
J. Scott Eddy, AIA, 2019/2020 Chair
Kenneth J. Filarski, FAIA
Shawn Gillen, AIA
Janine Glaeser, AIA
Kathleen Gordon, Assoc. AIA

Christopher Kiefer, AIA
Lester Meu, AIA
Adrienne Montare, FAIA
William Robarge, AIA
Matthew Tierney, AIA
Meghan Walsh, AIA
Sandi Worthman

Peer contributors, reviewers, & advisors

Michael Bomba, Esq.
Glenn Birx, FAIA
Islay Burgess, AIA
Ann Casso, Hon. AIA
Behrooz Emam, AIA, PE, CFM
Harry Gaveras, AIA, AIA Small Firm Exchange 2019 Regional representative
James Germano, Esq.
Stacey Keller, AIA, AIA Center for Practice 2020 advisor
Jay A. Knetter, AIA, AIA Small Firm Exchange 2019 Regional representative
Scott Knudson, AIA, AIA Practice Management Knowledge Community advisor
Michael W. Lassel, AIA, AIA Small Firm Exchange 2019 Regional representative
Michael Lejong, AIA, AIA Small Firm Exchange 2019 Regional representative

Warren Lloyd, AIA, AIA Small Firm Exchange 2019 Regional representative
Kathleen McCormick, CAE
William Melby, AIA
Michael Mitchell, CFM
Jenifer Navard
Praveen Patel, PMP, CSPO, CSM
Bill Peck, AIA, AIA Small Firm Exchange 2019 Regional representative
Katherine N. Peele, FAIA, AIA Center for Practice 2020 advisor
Lara Presber, AIA, AIA Small Firm Exchange 2020 Regional representative
Jay Raskin, FAIA
Eva Read-Warden, AIA, AIA Small Firm Exchange 2020 Regional representative
David Richards, FAIA, AIA Center for Practice 2019 Advisory Group Chair
Mark Ripple, FAIA
Fredric W. Schultz, CPCU, ARM
Christopher A. Toddy, AIA, AIA Small Firm Exchange 2019 Chair

Editors

Lindsay Brugger, AIA, Sr. Manager, Resilient Communities
Rachel Minnery, FAIA, Sr. Director, Resilience, Adaptation, and Disaster Assistance

“The AIA supports policies, programs, and practices that promote adaptable and resilient buildings and communities. Buildings and communities are subjected to destructive forces from natural and human-caused hazards such as fire, earthquakes, flooding, sea level rise, tornadoes, tsunamis, severe weather, and even intentional attack. The forces affecting the built environment are evolving with climate change, environmental degradation, population growth, and migration; this alters long term conditions and demands design innovation. Architects design environments that reduce harm and property damage, adapt to evolving conditions, and more readily, effectively and efficiently recover from adverse events. Additionally, the AIA supports member training and active involvement in disaster assistance efforts, providing valuable insights and aid to communities before, during, and after a destructive event.”
–AIA Resilience and Adaptation Position Statement, approved December 2017

Legal notice

Copyright © 2020. The American Institute of Architects. All rights reserved. The information provided is for informational purposes only. You should consult your own specialized advisors and counsel for your specific set of circumstances.

Architect’s Guide to Business Continuity, Published 03/20
All rights reserved American Institute of Architects © 2020

Contents

5 Why business continuity matters

6 What is business continuity planning?

7 The business case for business continuity planning

9 How to use this Guide

- 9 Who to engage in the business continuity planning process

10 Part 1: Business impact assessment

- 10 Overview
- 11 Understanding hazards
- 13 Understanding disruptions

14 Step 1: Risk assessment

17 Step 2: Impact analysis

- 18 Category 1: Revenue loss
- 19 Category 2: Increased operational costs
- 20 Category 3: Insurance
- 21 Category 4: Credibility
- 22 Category 5: Technology
- 23 Category 6: Marketplace

24 Part 2: Developing a business continuity plan

24 Step 3: Plan

25 Step 4: Implement

- 26 Facilities management
- 29 Information technology
- 33 Project management
- 37 Office administration/human resources
- 43 Maintaining your plan

44 Step 5: Assess

44 Triage

45 In the event of a disaster

50 In the event of a cyberattack

52 In the event of a key team member vacancy

53 Definitions & concepts

54 Resources

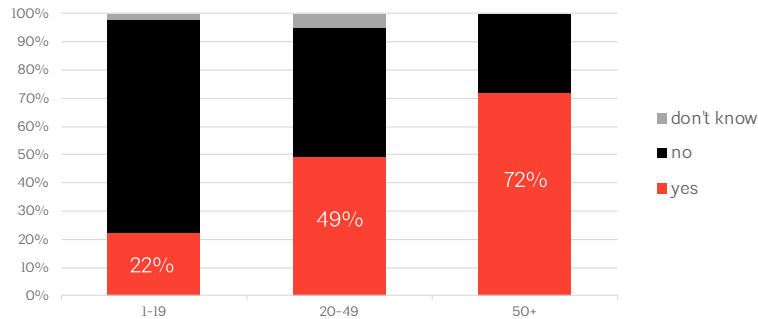
55 Appendix: Example business impact assessment

Why business continuity matters

Imagine your office is inundated with 4 feet of water or endures 80 seconds of seismic shaking, damaging interior conditions and crippling lifeline utilities. Or, imagine you open an email and suddenly your project, accounting, and contract files are held hostage and inaccessible. What would happen if your most integral team member or firm leader suddenly dies, and you lose irreplaceable institutional knowledge? What if a global pandemic requires all employees to self-isolate away from the office? Each of these is a type of disaster and each represents an actual event that a design firm previously experienced. The question is, could work continue?

AIA’s Center for Practice found that for too many firms, a plan was not in place to mitigate such disruption. In a 2018 AIA survey, only 22% of firms with 1-19 employees reported having a business continuity plan. This Guide incorporates lessons learned from previously impacted firms, builds on best practices, and integrates business aspects unique to the building industry profession to help firms remain open and profitable in the face of disruption, be aware of vulnerabilities in their business, and expand firm resilient design services.

43. Does your office currently have a business continuity plan?
Percent of firms by employees count



The practice of architecture exists in a complex, unpredictable, and inherently risky environment. To survive and thrive in this world, firms need to draw upon their foresight, strategic planning, and creativity to prepare, react, and quickly adapt to a wide range of disruptive, business-altering events.

Disruption takes a variety of forms: mental anguish, displacement, temporary accommodations, lost revenue, unexpected operational costs, and mountains of paperwork. And those are the effects for the lucky and the prepared. Many businesses never reopen following disasters, and sole practitioners and small firms may be disproportionately impacted.

Factors that impact the likelihood of business recovery, in addition to the cost of repairs, include revenue lost to closure, compromised operations, or clients in the impacted area who are unable to continue with their projects. The Federal Reserve studied the impact of 2017’s record-breaking disasters on 1,800 sole practitioners and small firms and found that 35% lost more than \$25,000 in revenues;¹ for a small business, this amount can make the difference between recovering or not.

Natural disasters are far from the only threat. Architecture firms are also at risk from everyday threats such as the sudden absence of a team member, or a cybersecurity breach. According to the National Cyber Security Alliance, 60% of hacked small and mid-sized businesses go out of business within six months² of the breach. So what is a firm to do? **Create a business continuity plan.**



What’s at stake

According to the Federal Emergency Management Agency and the US Small Business Association:

- 40% of small businesses fail to reopen after a disaster due to an inability to afford repairs or due to lost revenue. That failure rate increases when a business can’t reopen quickly.³
- Up to 90% of small business fail within one year if operations are impacted for five days or more.³

¹ Report on Disaster-Affected Small Firms Provides Critical Insight for Understanding Regional Economic Recovery, Federal Reserve Bank of San Francisco, 2018. <https://www.frbsf.org/our-district/press/news-releases/2018/small-business-credit-survey-report-on-disaster-small-firms/>
² Galvin, Joe. 60 Percent of Small Businesses Fold Within 6 Months of a Cyberattack. Here’s How to Protect Yourself, *Inc.*, 2018. <https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html>
³ Make Your Business Resilient, FEMA. https://www.fema.gov/media-library-data/1441212988001-1aa7fa978c5f999ed088dcaa815cb8cd/3a_BusinessInfographic-1.pdf

What is business continuity planning?

The primary purpose of business continuity planning is preparation—of people, premises, technology, information, supply chains, stakeholders, and reputation—for adverse events so the firm can continue to provide services, generate revenue, and reduce the negative consequences of business interruption.

Continuity planning provides a framework for organizational resilience in response to disruptive events such as natural and human-caused disasters, cyberattacks, and the sudden absence of a key team member. Regardless of size, every firm has the ability to think strategically, efficiently, and effectively to reduce the impact of potential disruptions.



Continuity planning provides a framework for organizational resilience in response to disruptive events such as natural and human-caused disasters, cyberattacks, or the sudden absence of a team member.

- **Public utility mishap:** The city was working on the street outside our office. They burst a water main, which flooded our office basement but did not flood our office. Job files, resource books, corporate files, tax filings, accounting records, software disks, backup tapes, and drawing archives were destroyed. –Firm owner
- **Sudden loss of key employee:** Our office and financial manager passed away unexpectedly. All aspects of our business were affected, from payroll to billing, HR, and day-to-day office activities. –Firm owner
- **The hurricane:** Twenty-eight feet of storm surge and Category 3 winds devastated the entire coast. Our house was five weeks old but was still standing. Office: gone. Books and computers: gone. We gutted the house, polished the floors, and moved back in seven weeks later, the day the power was restored. There was no space available to rent, so our office was in the dining room. Communication lines were still down, so we went to the library to pick up a Wi-Fi signal. –Firm owner
- **Cyberattack:** We had no idea the attack even happened until we came in the next day and found our entire system was locked. The cyberattack was so stealthy it took weeks to figure out what happened. We finally identified a virus embedded in an email file from our attorney. –AIA chapter executive director
- **Unexpected team member vacancy:** When my business partner announced he was moving and leaving the business, we had about 10–12 projects in the design phase and five in the construction phase, and we had three employees. My former partner had been managing probably half of those projects and was working closely with two employees. I began working closely with three employees and became the principal in charge of 15 projects. Three of the projects were vastly over budget. The experience was overwhelming in many ways, and I was completely unprepared for the scenario. –Firm owner
- **Embezzlement:** During an extended illness of our long-term bookkeeper/office manager, irregularities in accounting were discovered. After investigating these discrepancies, it was determined that the bookkeeper had been diverting a portion of incoming wire transfers into an account we didn't know we had and forging checks made out to themselves for "bonuses" and reimbursement. When I finally learned of this, our operating account didn't have enough money in it to cover payroll. It was a tough couple of months to cover operating expenses and get adequate cash flow back into the firm. –Firm owner
- **The disconnect:** The phone company and 200 of their subsidiaries unexpectedly went bankrupt. I lost nearly every contact number and email address. –Firm owner

The business case for business continuity planning

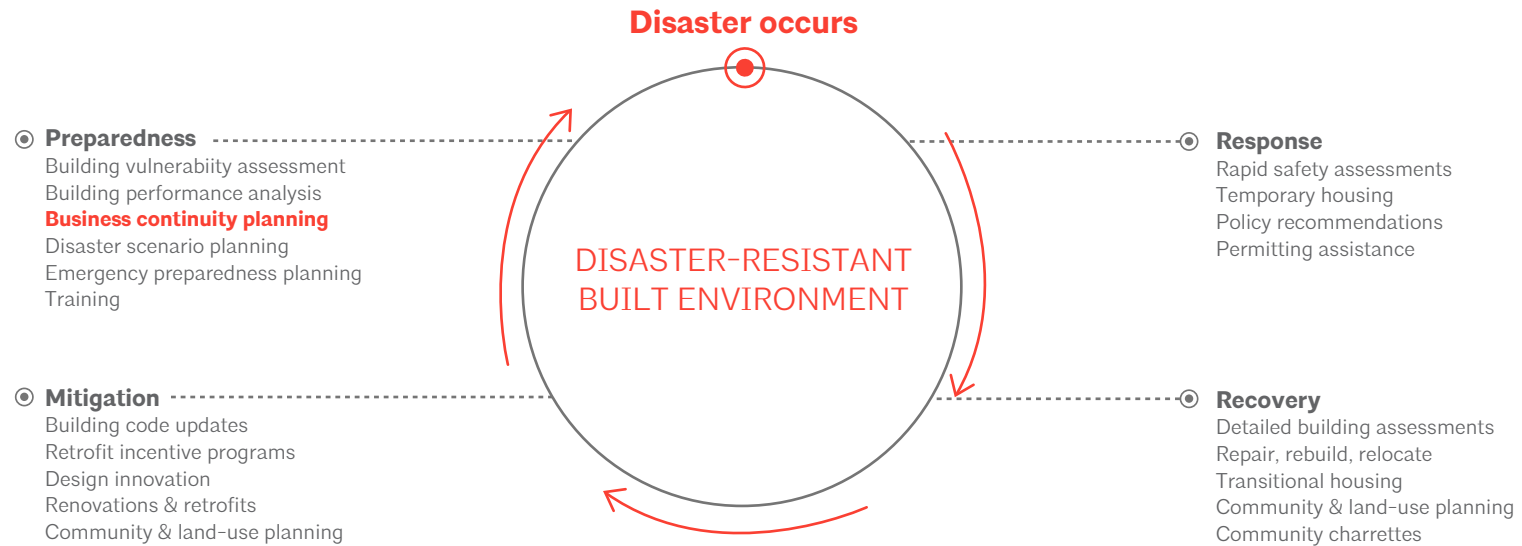
Business continuity planning and the financial safety net it provides isn't simply a nicety or a good idea; it's vital to your business.

Continuity planning may be a contractual requirement stipulated by certain companies or the government. A business continuity plan assures clients that their firm has analyzed their threats and capabilities and planned for the unexpected. Communities may also depend on a firm remaining open, particularly if the firm has critical knowledge regarding the design, construction, or commissioning of damaged structures or if the firm has post-disaster temporary housing or shelter solution experience.

Beyond reducing post-event hardships and ensuring contract compliance, business continuity planning can create savings and opportunities. A business

continuity plan may reduce a firm's business interruption insurance premium. And firms that remain open post-event have the capacity to provide post-disaster building assessments, repairs, and hazard mitigation retrofits for current or past clients. They can also provide volunteer assistance to overwhelmed building departments and community recovery activities.

Additionally, the process of developing a business continuity plan better positions architects to advise clients on business continuity needs and the associated design implications. These services may include site evaluation for building vulnerability assessments, facility feasibility studies, and design services for shelter in place and rapid recovery to promote business continuity goals.



Architects' role in the emergency management cycle

Within the Emergency Response Cycle of Preparedness, Mitigation, Response and Recovery, business continuity planning falls under Preparedness.
 Source: *AIA Disaster Assistance Handbook 3rd Ed.*



Making lemonade

How EskewDumezRipple survived—and thrived—in the face of disruption

THE EVENT

On Friday, August 26, 2005, the employees in our office were looking forward to the firm barbecue and pool party on Sunday. We were celebrating the end of summer and feeling satisfied that the firm was improving on both the design and financial side after struggling in 2002 with financial mishaps and work slowdown. We were keeping an eye on a hurricane in the Gulf named Katrina, but it was projected to hit east of New Orleans, and we would be on the less intense western side so weren't overly concerned.

By Saturday morning Katrina's path had shifted west and the storm was becoming more intense. The projections were looking scary and we began evacuation plans; our barbecue was canceled. By Monday morning, our city was flooded, more than half of our employees were homeless, and we realized we were in the middle of a major disaster.

ACTION

Cell phone communication was down, so our leadership team used personal email accounts to contact each other, setting up a conference call. There were more unknowns than knowns that week, but we moved forward with our best guess about what would happen. Assignments were handed out and we hit the ground running; within two weeks of Katrina we had completed the following tasks:

- **Workload:** Find out which projects were on hold and which were continuing.
- **New work:** Contact our network to let them know we were ready, willing, and ABLE to start working.
- **Infrastructure:** Find and set up temporary office space, set up a network of computers to load project and firm information (with an eventful and rather heroic journey into the still flooded city to our 31st floor offices to retrieve our server—yes it's quite difficult to carry an entire server down 31 flights in an unairconditioned stairwell with no light).

- **Employees:** Find out where everyone landed, who could work remotely, who needed a place to stay, and who was needed immediately to get us back to work.

- **Business:** Insurance claim initiated, SBA potential loan initiated, temporary line of credit initiated, collected outstanding receivable balances to support interim cash needs, and developed a plan to continue to pay employees and run the firm.

AFTERMATH

By late November, we were back in our office and had fully engaged all employees wanting to return, while temporarily employing staff from our peer firms for a large FEMA project we were engaged to complete. We had secured commissions to assist in recovery planning as well as several fast track projects to get clients back in buildings and working.

KEYS TO RESILIENCY

- **Infrastructure:** Nimble, insured, and flexible
- **Culture:** Empowered employees, sense of responsibility as a team
- **Lateral leadership:** Decisions can be made at all levels that will benefit the entire team
- **Transparency:** Entire team knows where we are going and how we plan to get there so we can all help when we need to move quickly

[Learn more](#)

How to use this Guide

The worksheets throughout this guide are designed to lead firms through the business continuity planning process. In *Part 1: Business impact assessment*, firm leaders will evaluate hazard **risk** and examine the associated direct and indirect impacts on the financial health, reputation, physical assets, and viability of a firm. Evaluating business impacts involves identifying critical functions, processes, infrastructure, systems, and applications, and establishing acceptable durations of interruption. For instance, an eight-hour power outage might be acceptable; a five-day interruption might be crippling. This is also the time to identify interdependencies across functions, processes, and applications and the potential for loss of information.

In *Part 2: Developing a business continuity plan*, firm leaders will be prompted by a series of action items that will better prepare the firm to weather disruptions of all kinds. Recommended action items are organized into a series of straightforward checklists spanning every facet of a firm. Only you, after identifying potential risks and business impacts, can determine which actions are most relevant to developing your own business continuity plan.

Once complete, it's important to **maintain your plan** through annual testing, learning, and updating. This is not a plan to sit on the shelf. A living document that reflects evolving risks will best position the firm for success.

When a disruption occurs, it's important to **assess** the experience and update your business continuity plan accordingly. Sometimes a hazard strikes before embarking on a business continuity plan or exceeds the anticipated impacts.

The *Triage* section of this guide recommends next steps after experiencing a disruption such as a natural disaster, cyberattack, or sudden absence of a key team member.

Who to engage in the business continuity planning process

Business continuity affects all facets of your firm, from human resources and information technology to facility management, office administration, and project management. To capture and catalog prospective impacts to every aspect of a firm, it's critical to build a diverse team to develop the firm's business continuity plan. For sole practitioners, the team might consist of the firm owner, an IT consultant, and your insurance agent. For small firms, the team might be the firm partners, office administrator, IT consultant, and a project architect. For others, the team might be much larger and include representatives from each office as well as employees and leaders representing IT, HR, administrative, general counsel, and project management.

Business continuity planning is like a resilient system that includes interdependencies. While it's important to have someone lead the business continuity planning process, it's equally important to include a wide range of stakeholders. Consider including input from not only firm leaders and employees, but also consultants, clients, and others who may further define the capabilities and demands on your firm.

Part 1: Business impact assessment

Step 1: Risk assessment (p. 14–16)

- Identify potential hazards
- Assess likelihood and severity of hazards
- Determine risk level posed by hazards

Step 2: Impact analysis (p. 17–23)

- Identify direct and indirect impacts
- Identify interdependencies
- Define duration threshold

Part 2: Developing a business continuity plan

Step 3: Plan (p. 24)

- Prepare for disruption

Step 4: Implement (p. 25–43)

- Conduct training for business continuity team
- Perform scenario exercises
- Conduct testing and regular plan maintenance

Step 5: Assess (p. 44)

- When a disruption occurs, reflect on the experience and update your business continuity plan accordingly

Part I: Business impact assessment

Overview

A **business impact assessment** is the first step to creating a business continuity plan and is comprised of two tasks: Step 1: Risk assessment and Step 2: Impact analysis. During Step 1: Risk assessment, firms look to local and regional insights on climate hazards as well as other types of hazards to identify the types of events that might impact the firm’s ability to conduct business. These hazard risks could include natural disasters, anthropogenic hazards, and the impacts of climate change. The analysis includes not just high-probability events, but also low-probability events with high-impact hazards. It’s important to consider a wide variety of hazards along with the likelihood (**probability**) and severity (**magnitude**) of each, which when calculated equates to **risk**.

A careful review of state and local hazard mitigation plans provides a good starting point for identifying hazards inherent to your practice location(s).⁴ These plans represent a consensus-based statement of risks and a commitment to address those risks. When analyzing these hazards, look for dependencies of community functions and the potential for your firm to be impacted by **secondary hazards** and unintended consequences.

Once hazards are identified, firm leaders will assess the potential business impacts associated with the hazard event(s) in Step 2: Impact analysis. Business impacts might include revenue loss, business interruption or relocation, damage to property and infrastructure, and supply line disruption.

For firms with multiple locations, a similar assessment will be conducted for each office as even offices located in the same region will face different hazard risks. The results of each assessment are synthesized into a threat matrix to prepare a full risk profile for the firm. This important step encourages a practice to determine the potential for compounding impacts and illuminates where redundant systems offer risk reduction.

⁴ Find your state, county, or city hazard mitigation plan by visiting your state emergency management agency’s website or your county/city website. Regional hazard mitigation plans may also be available.

Understanding hazards

Organizations and firms are primarily faced with three types of hazards: natural hazards, hazards instigated by individuals or groups (anthropogenic hazards), and hazards related to systemic failures. Today, natural hazards are often top of mind, given the growing prevalence of global weather events and the increasing impact of climate change. However, the awareness of anthropogenic, or human-influenced hazards, is often higher in firms that have experienced impactful events such as 9/11, cyberattacks hijacking firm data or impacting credit reporting, or the sudden absence of key team members. Systemic failures, though, are likely the most common and least considered category. These include threats to whole communities and infrastructure, particularly the inherent fragility of centralized power grids and internet services.

When identifying hazards, it's important to also consider hazards that might appear remote, as these may impact supply chains or the sequence of business operations. For example, on some projects, approximately one-third of the work could be the responsibility of consultants. A disruption in producing or receiving consultant work would significantly impact the firm's ability to deliver work to the client.

Additionally, keep in mind that many environmental hazards induce or trigger secondary hazards, or what is commonly referred to as cascading effects. These vary by location and are to be taken into consideration during planning efforts. Secondary hazards can range in scale from major hazard events themselves or nuisances that exacerbate damage—such as power outages caused by wind storms or wildfires preceding floods and mudslides.

Other examples of acute secondary hazards include fires caused by downed power lines or ruptured gas pipes because of an earthquake. The potable water supply system, either within the building or within the community, may also be damaged after an initial event. This has far-reaching consequences, from loss of the fire suppression system, to interior water damage, to the inability to use the sanitary system. Natural hazards often result in the release of hazardous materials from dislodged containers, excessive mold growth, garbage spills, debris, and displaced disease-carrying vermin. Power outages should be expected from even a minor disaster.

The sources of secondary hazards aren't always present at the building or property site; some are due to adjacent properties with collapse or fall potential. Secondary hazards could be an upstream contamination of a water supply, or the flooding that occurs due to a sudden heavy snow melt. An architect's ability to foresee and visualize the impacts of secondary hazards on building function and business continuity will enable them to hone in on the best areas to focus risk mitigation strategies.



Cascading effects

Secondary hazards vary by location. In this example, the initial event or primary hazard (far-left column) triggers secondary hazards shown as medium probability (light grey) or high probability (dark grey). Source: *Office of Emergency Management, City of Seattle*.

Secondary Hazard \ Primary Hazard	Earthquakes	Landslides	Volcano Hazards	Tsunami and Seiches	Disease Outbreaks	Civil Disorder	Terrorism	Mass Shootings	Transportation Incidents	Fires	HazMat Incidents	Infrastructure Failures	Power Outages	Excessive Heat Events	Flooding	Snow, Ice and Extreme Cold	Water Shortages	Windstorms	
Earthquakes																			
Landslides																			
Volcano Hazards																			
Tsunamis and Seiches																			
Disease Outbreaks																			
Civil Disorder																			
Terrorism																			
Mass Shootings																			
Transportation Incidents																			
Fires																			
HazMat Incidents																			
Infrastructure Failures																			
Power Outages																			
Excessive Heat Events																			
Flooding																			
Snow, Ice and Extreme Cold																			
Water Shortages																			
Windstorms																			



Types of hazards*

• Natural hazards

- High winds
- Tornado
- Drought
- Wildfire
- Extreme temperature
- Coastal erosion
- Landslide
- Earthquake
- Subsidence
- Liquefaction
- Volcanic eruption
- Heavy rainfall
- Storm surge
- Tsunami/seiche
- Hurricane
- Flood
- Sea level rise
- Ground saturation
- Hail storm
- Snow storm
- Ice storm
- Avalanche

• Anthropogenic hazards & systemic failures

- Cyberattacks
- Active shooter
- Hazardous materials/chemical spills
- Arson-caused fire
- Bomb or bioweapon threat or actual attack
- Infectious disease epidemic
- War
- Terrorism
- Infrastructure failure
- Environmental pollution
- Electromagnetic pulse (EMP) due to solar flares
- Permanent/temporary absence of key team member
- Civil unrest (local or global)
- Disruption in public transit/road closures
- Internet/cell service disruption
- Interruptions to site utilities: power, water, wastewater, communications
- Vendor or consultant supply chain disruption
- Recession
- Pandemic
- Electronic data loss
- Order of civil authority
- Unanticipated building dysfunction

*This list of examples is not exhaustive of all potential hazards.

Understanding disruptions

For each of the hazards identified, firms evaluate the degree to which the hazard poses a risk to business by analyzing the hazard’s capability for disruption to normal operations. **What is the impact of the hazard if realized?**

For each hazard risk, firms consider the range of impacts or possible disruptions and the degree to which they are able to be accommodated.

Hazards can be organized into short-term events that temporarily interrupt typical operations and higher-impact events that challenge the core business.

Operational disruptions reduce the practice’s ability to conduct its work. These range from common, limited-duration disruptions, such as a power or internet failure, to longer-duration disruptions, such as powerful storms that disable the power grid or the sudden absence of a key team member critical to winning or delivering work.

Core business disruptions⁵ fundamentally change the nature of the practice or disrupt critical business functions. These types of disruptions stem from more cataclysmic events such as Superstorm Sandy, California wildfires, St. Louis floods, the Joplin tornado, and Hurricane Katrina. In such events, businesses may be unable to continue operations without an alternative facility and activated business continuity plan.

Of course not all core business disruptions result from natural disasters. The 2020 coronavirus pandemic may prove to be a core business disruption. Other core business disruptors include shifts in industries that reduce or fundamentally alter the need for certain services. This type of core business disruption often follows a major industry shift in a region that may or may not be associated with a natural disaster. Core business disruptions may also result from anthropogenic hazards, such as a cyberattack.

The duration associated with disruptions and availability of resources to manage the disruption (capacity) equates to the length of recovery.



Business disruptions

To establish your business continuity goals, you’ll need to evaluate the anticipated duration of impact and the associated level of disruption for each identified hazard event. An extended duration may not correlate to an increased severity of disruption. Depending on the impacts of the hazard event, a 24-hour disruption could be significant.

● Disruption

- Temporary
- Minor
- Major
- Significant

● Duration

- Hours
- Days
- Weeks
- Months



Business impacts: Identifying disruptions

Most lease agreements give the landlord an extended period of time to make a decision on what to do and how to proceed to deal with damage resulting from a natural disaster or other hazard. This may include a waiting period until the insurance company has disbursed funds for the repair of the building. This period may take as long as 60 to 120 days, during which access to the building may be denied and as such create disastrous results for firms that rely on their leased space.

⁵ *Leadership in Times of Crisis: A Toolkit for Economic Recovery and Resiliency* (International Economic Development Council, 2015), 285-304.



Business impacts: The far reach of hazards

A major manufacturer located in the southeast of the United States had an interesting challenge in terms of business continuity planning. While its facilities were located well inland and away from coastal storm surges, its dependencies on systems that were in those high-risk flood zones were not. In lieu of looking at its local facilities and quickly surmising that they were relatively low risk, the manufacturer analyzed its supply chain to determine exposures throughout its business sequence.

By assessing supply chain risk in addition to facility risks, the manufacturer realized it was in fact terribly exposed to hurricanes given its shipping operations. As an international supplier with a dependency on bi-directional availability of materials, any interruption in the supply chain could stall local operations for days or weeks. Therefore, the hurricane risk to its shipping partners became its risk as well, although its actual facilities

were so far from the coast. Recognizing this hazard risk, in turn, made the manufacturer realize the potential exposure to an important impact: operational cost escalation. In response, the manufacturer had to assess its appetite for such vulnerability and determine whether to have a backup strategy, such as alternative shipping operations and/or additional on-site component storage, should that supply chain disruption occur.

As a design firm hired by the manufacturer, we were compelled to create the environment for a conversation about hazard risk and business impacts. This type of conversation is valuable for our projects as well as within our own offices.

-Firm leader

Step 1: Risk assessment

In this step you will look to local and regional insights on climate hazards as well as other types of hazards to identify the types of events that might impact the firm's ability to conduct business.

Instructions

Begin by gathering authoritative data and plans, including state and local hazard mitigation plans as well as resilience strategies such as a climate adaptation plans or disaster recovery plans. Such plans typically include a risk assessment that describes the hazards for the study area and may or may not reference future conditions such as climate change impacts. Plans typically list and rank hazards according to the risk, a function of the probability and magnitude of the hazard event. Not all cities and counties have these plans in place, but states do. Where available, local and county plans have more detailed local information. Plans are typically available online, most often through your state or local emergency management office.

Refer to these plans and in the following worksheet, select the applicable hazards and choose the probability, magnitude, warning, and duration for each hazard that most closely aligns. Remember to consider a wide range

of hazard types including social (i.e., active shooter), economic (i.e., market closure), and environmental (i.e., hurricane) hazards that may face your firm and your community.

In addition to hazards—or shocks—there may be stresses that could negatively impact your ability to conduct business. Consider both **shocks and stresses** when completing the worksheet below.

Remember, risk may be different depending on the hazards present where you work (office) versus the hazards present where your projects are. It is recommended to consider the hazards in your immediate (office) area as well as the region(s) in which you conduct business, particularly if the majority of your work lies in a vulnerable area that has a high probability of natural hazards.

This exercise is an important prompt for reflection. If done correctly, serious issues that we tend to be blind to often surface. An example of this exercise is included in the **appendix**.

Step 1: Risk assessment

List hazards:

Which hazards could affect your office or project locations?

Assess risk:

Which hazards pose the highest risk? Risk is based on the likelihood and severity of the hazard. High-probability, low-magnitude events may not be a high risk, though low-probability, high-magnitude events might be a medium or high risk.

Assess preparedness:

How much advanced notice of the hazard event will you have? How long could the hazard event affect your firm? These answers provide an indication of how prepared you might be to withstand the impacts of the hazard event.



Hazard potential source of danger	Risk = probability x magnitude			Warning time prior to hazard event	
	Probability likelihood of hazard event	Magnitude severity of hazard event		Duration time scale of disruption	
	High Medium Low	Highly likely Likely Possible Unlikely	Catastrophic Critical Limited Negligible	Minimum to none 6-12 hours 12-24 hours 24+ hours	Hours Days Weeks Months
	High Medium Low	Highly likely Likely Possible Unlikely	Catastrophic Critical Limited Negligible	Minimum to none 6-12 hours 12-24 hours 24+ hours	Hours Days Weeks Months
	High Medium Low	Highly likely Likely Possible Unlikely	Catastrophic Critical Limited Negligible	Minimum to none 6-12 hours 12-24 hours 24+ hours	Hours Days Weeks Months
	High Medium Low	Highly likely Likely Possible Unlikely	Catastrophic Critical Limited Negligible	Minimum to none 6-12 hours 12-24 hours 24+ hours	Hours Days Weeks Months
	High Medium Low	Highly likely Likely Possible Unlikely	Catastrophic Critical Limited Negligible	Minimum to none 6-12 hours 12-24 hours 24+ hours	Hours Days Weeks Months
	High Medium Low	Highly likely Likely Possible Unlikely	Catastrophic Critical Limited Negligible	Minimum to none 6-12 hours 12-24 hours 24+ hours	Hours Days Weeks Months
	High Medium Low	Highly likely Likely Possible Unlikely	Catastrophic Critical Limited Negligible	Minimum to none 6-12 hours 12-24 hours 24+ hours	Hours Days Weeks Months

Step 1: Risk assessment

Summarize your findings

Which hazards are high, medium, and low risk? Log your findings below.

Perform a gut check. Assuming the above risk assessment was based upon the risks conveyed in state or local plans, are all aspects of your business functions represented, such as location of employees, supply chain, or hazards that would have a more profound impact on your particular type of work?

When gut checking the risk level of identified hazards, it may be helpful to compare the relative potential impacts of identified hazards specifically for your firm. Are the anticipated firm impacts of extreme heat days equivalent

to the firm impacts of a disruption in communications? Similarly, is the loss of communications more critical than losing public transit? The goal is to gut check which hazards pose not only the highest risk, but the most significant impact to your firm. Ask yourself which hazards will truly impact your ability to provide services. The Risk Assessment Summary therefore will likely be close to, yet not identical to, your community's hazard mitigation plan because you've taken the time to correlate the hazard risks to your business functions.

Risk assessment summary

High risk hazards	Medium risk hazards	Low risk hazards


Step 2: Impact analysis

After you've identified your hazard risk, use this step to assess the potential business impacts associated with the identified hazard event(s).

Instructions

Begin by evaluating your firm's essential business functions. Which functions are critical to business continuity for your firm?

Next, look back on [Step 1: Risk Assessment](#). Which hazards pose the greatest risk? How do these risks impact your firm's ability to conduct business? For each of the hazards that concern you, complete the following six impact category worksheets (revenue loss, increased operational costs, insurance,



Tip When analyzing impacts, keep the warning and duration time scales from Step 1: Risk assessment in mind. How might the direct and indirect impacts change during a longer or shorter disruption?

credibility, technology, and marketplace) to determine the potential impact each hazard might have on your firm.

For example, if after conducting your risk assessment, you are concerned with extreme heat and flooding, examine each of the six categories for extreme heat as well as for flooding to determine the impact each hazard might have on your firm. An example of this exercise can be found in the [appendix](#).

Firm functions	What are the day-to-day responsibilities?	What tasks are essential to business continuity?
Accounting		
Contract Administration		
Facilities Management		
Human Resources		
Information Technology		
Marketing		
Office Administration		
Project Management		
Quality Control		
Design		
Legal/General Counsel		
Other:		
Other:		

Step 2: Impact analysis

Category I: Revenue loss

Consider: Loss of contracts, late payments, loss of work, loss of marketing or future pursuits

Hazards Referencing the Step 1: Risk Assessment, list risks starting with the highest hazards	Direct impacts To the firm's employees, building, server, hardware, etc. Consider: Does the office have to close for repairs or infrastructure work? Can your employees continue to work? Do they all have hardware/software to work remotely? Quantify impacts as: Per person per day, how much credit is available	Capacity Ability to respond What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?	Indirect impacts To clients and future work Consider: How will office repairs or relocation impact your ability to meet deadlines or acquire new work? Quantify impacts as: Per person per day, cost of contract penalty	Capacity Ability to respond What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?

Step 2: Impact analysis

Category 2: Increased operational costs

Consider: Temporary office, overhead payments, delay in earnings, line of credit, repair of damaged office (if applicable), permanent relocation, etc.

<p>Hazards</p> <p>Referencing the Step 1: Risk Assessment, list risks starting with the highest hazards</p>	<p>Direct impacts</p> <p>To the firm’s employees, building, server, hardware, etc.</p> <p>Consider: Can the office be repaired? How long will it take? Is temporary office space available? Will business interruption insurance cover the costs? If the office is significantly damaged, how will you establish new office space? If the office moves, do you run the risk of losing employees?</p> <p>Quantify impacts as: Per person per day, how much credit is available</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>	<p>Indirect impacts</p> <p>To clients and future work</p> <p>Consider: How will office repairs or relocation impact your ability to meet deadlines?</p> <p>Quantify impacts as: Per person per day</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>

Step 2: Impact analysis

Category 3: Insurance

Consider: Professional liability, property insurance, personal insurance

<p>Hazards</p> <p>Referencing the Step 1: Risk Assessment, list risks starting with the highest hazards</p>	<p>Direct impacts</p> <p>To the firm’s employees, building, server, hardware, etc.</p> <p>Consider: Will you be able to obtain insurance at current rates? How will increased insurance costs (or the inability to obtain coverage) affect your ability to retain, retrain, and/or recruit employees? How will you be affected by contractual insurance requirements?</p> <p>Quantify impacts as: Increased cost of coverage, fewer available carriers, increased deductibles or self-insurance</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>	<p>Indirect impacts</p> <p>To clients and future work</p> <p>Consider: How will increased insurance costs (or the inability to obtain coverage) affect your ability to be price competitive when seeking new work? How will you be affected by contractual insurance requirements?</p> <p>Quantify impacts as: Increased cost of coverage, fewer available carriers, increased deductibles or self-insurance</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>

Step 2: Impact analysis

Category 4: Credibility

Consider: Good reputation and client is confident in brand/firm or conversely a bad reputation and client is not confident in brand/firm

<p>Hazards</p> <p>Referencing the Step 1: Risk Assessment, list risks starting with the highest hazards</p>	<p>Direct impacts</p> <p>To the firm’s employees, building, server, hardware, etc.</p> <p>Consider: A good reputation will grow the firm. How might your inability to provide services affect your reputation?</p> <p>Quantify impacts as: Employee recruitment and retention (reputable firms attract high-quality employees)</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>	<p>Indirect impacts</p> <p>To clients and future work</p> <p>Consider: Will your client, city, and other contacts recommend you to others for future work? Are your employees engaged in the community and other leadership roles where they also raise the credibility of the firm?</p> <p>Quantify impacts as: How satisfied are your clients? What is the public perception of the firm?</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>

Step 2: Impact analysis

Category 5: Technology

Consider: Loss or lack of access to hardware (server, computers, printers), software, data, or VPN/cloud; power backup of critical equipment.

<p>Hazards</p> <p>Referencing the Step 1: Risk Assessment, list risks starting with the highest hazards</p>	<p>Direct impacts</p> <p>To the firm’s employees, building, server, hardware, etc.</p> <p>Consider: Ability to access files, systems, and applications</p> <p>Quantify impacts as: Cost to repair or purchase new equipment, time delay for fixing/replacing equipment, lost production time</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>	<p>Indirect impacts</p> <p>To clients and future work</p> <p>Consider: Ability to meet contractual obligations and regulatory compliance requirements</p> <p>Quantify impacts as: Time delay for fixing/replacing equipment, penalties for missed deadlines</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>

Step 2: Impact analysis

Category 6: Marketplace

Consider: The impact on various market sectors (health care, education, civic and corporate interiors, residential, etc.)

<p>Hazards</p> <p>Referencing the Step 1: Risk Assessment, list risks starting with the highest hazards</p>	<p>Direct impacts</p> <p>To the firm’s employees, building, server, hardware, etc.</p> <p>Consider: Can you demonstrate high performance for your primary market sector under distress? Does your firm work in one primary market sector? If so, what is the backup plan if the market sector slows down or demographic shifts occur?</p> <p>Quantify impacts as: Number of marketplaces currently served</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>	<p>Indirect impacts</p> <p>To clients and future work</p> <p>Consider: Can you evolve with your market sector as owners determine new ways of investing or divesting?</p> <p>Quantify impacts as: Marketplace health and interrelated-ness of skills offered</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>

Part 2: Developing a business continuity plan

Reflect on the essential functions of your firm previously identified and the direct and indirect impacts described in each of the six business impact areas in **Step 2: Impact Analysis**. How are the essential functions of your firm impacted? What actions will your firm undertake to reduce the vulnerability of these essential functions? Designate a department and responsible person(s) for implementing the identified action(s) and the collaborators. What is the

expected time frame to complete the action, and is there a critical path to consider? For example, is there one identified action that must occur before another? How does each action land in the budget for the firm? How can the identified action relate to—or enhance—ongoing or planned investments in firm technology, equipment, retrofits, or other upgrades?

Step 3: Plan

Use this information to help prioritize. Are there actions that can be rolled into an ongoing or planned investment? Which actions are most critical to the continuity of operations? If a critical action is just not in the budget, is there an alternative or band-aid approach that, while not ideal, might still reduce vulnerability? After all, when you’re bleeding, a band-aid is better than no band-aid at all!



Action plan:

Use the below matrix to identify and prioritize business continuity actions based on the “capacity” reflections logged in Step 2: Impact analysis.

Action	Responsible party	External collaborators	Implementation time frame	Budget implications	Relationship to ongoing/planned investments	Priority level

Step 4: Implement

Business continuity planning checklists

While action items will be unique to each firm, [Part 2: Developing a business continuity plan](#) provides a series of checklists organized by firm departmental area:

- facilities management
- IT
- project management
- office administration/
human resources

This organization provides the opportunity to assign department tasks to a department head or consultant if firm leadership chooses to do so. Each departmental area includes a checklist of recommended actions and description. Remember to design in redundancy. It's important for all firm systems, staff roles, and technology to have backup measures or cross training.



Firm departmental area checklists:

Click the title of each checklist to jump to recommended actions.

FACILITIES MANAGEMENT



- Catalog facility documents, contacts, and equipment
- Prepare office space

INFORMATION TECHNOLOGY



- Document hardware and software
- Provide remote access
- Protect yourself from cyberattacks

PROJECT MANAGEMENT



- Build in redundancy
- Evaluate contracts
- Create a communications plan
- Prepare for remote work

OFFICE ADMINISTRATION HUMAN RESOURCES



- Collect key documents
- Prepare financials
- Analyze insurance needs
- Prepare employees



🕒 Catalog facility documents, contacts, & equipment

Having important documents and contacts at your fingertips will make navigating a potential disruption easier and more efficient.

Collect facility documents 🕒

This includes the premises deed, mortgage, or lease. It is recommended to store this information in multiple locations: the cloud, server, on USB, paper copy at the office and/or at a key employee's home.

Collect facility contacts 🕒

This may include contact information for the building, security, power utility, water utility, internet utility, fire, police, and/or municipal emergency department. It is recommended to store this information in multiple locations: the cloud, server, on USB, paper copy at the office and/or at a key employee's home.

Establish expectations with emergency providers and service vendors 🕒

Touch base with your emergency providers and service vendors for items such as HVAC, electrical, fire, and plumbing to ensure they understand what is expected of them in a disaster type situation.

Photograph spaces and equipment, catalog, send to insurance company, and upload to the cloud 🕒🕒

Photograph office/equipment for potential insurance claims and update photos annually or after a remodel or significant purchase. Include date and time stamp. Send photos to insurance company, upload to cloud-based secure storage, and keep a hard copy in a safe place.

Enable remote access to critical documents 🕒🕒

Be prepared for an event where the engineering/facilities team may not be able to have access to engineering and facility documents such as operation manuals, blueprints and schematics—convert these into a digital format that is remotely accessible. This includes provisions for master keys, alarm codes, etc.



Prepare office space

We spend more than one-third of our time at work. Designing or retrofitting—and maintaining—your physical office space with these tips in mind can enhance your business continuity during a disaster, an attack, a pandemic, or other hazard event.

Preparations if you own or lease your facility ①

If you own—prepare a list of service and repair providers to contact in case of disaster. If you lease—prepare a contact list (landlord or management company) of who to reach out to that will take care of services and repairs in case of disaster. If your firm depends on leased space, then reviewing the lease terms related to the aftermath of a disaster is extremely important. Most lease agreements give the landlord an extended period of time to make a decision on what to do and how to proceed to deal with the damage. This may include a waiting period until the insurance company has disbursed funds for the repair of the building. This period may take as long as 60 to 120 days, during which access to the building may be denied and as such create disastrous results for firms that rely on their leased space. These terms can be renegotiated to provide immediate access at the firm's own risk and expense in order to get equipment, files, or other vital information out of the building or, if conditions are right, to make repairs and then negotiate the payments at a later date after insurance determination has been made. Whether your office is owned or leased, learn what insurance you should carry and get a policy.

Appropriately address issues identified in the building vulnerability assessment ① Varies

Does the design and organization of your physical office space support business continuity? How can the design or retrofit of your office space reduce your vulnerability? Understand your building's anticipated performance level by conducting a building vulnerability assessment.

[Learn more with AIAU.](#)

Locate office in a building near public transit, amenities, and emergency service facilities, or know where these are in an existing building ①

Where are the nearest public transit stations? Where are secondary locations? What will employees do if there is NO public transit available within reasonable walking distance after a crisis?

Know the intended performance level of your facility ①

What is the performance level of your building (type, age, and capacity of mechanical, electrical, fire protection, and plumbing systems)? Is there redundancy of mechanical, electrical, fire protection, and plumbing systems? Upgrade systems to achieve desired performance capacity.

Clearly emphasize safe exit routes ①①

Does the design and organization of your physical office space support business continuity and safety? Straightforward design and/or clear signage as well as employee training and testing support swift and safe escape.

Require landlord documentation that all systems are regularly tested and any deficiencies are promptly addressed ①

Include this requirement in your lease if you lease or have an authorized memorandum from the landlord showing compliance.

Plan for shelter in place ①①①

Document location, amount, and expiration date of emergency supplies. FEMA recommends enough non-perishable food, blankets, communication equipment (such as flashlights, radios, and batteries), alternate power sources, first-aid supplies, necessary medications, and durable medical equipment (e.g., hearing aid batteries, catheters) to allow self-sustainment in that location for a minimum of 72 hours. For a detailed list, see Ready.gov. Keep in mind, not all facilities will be suitable for shelter in place. If shelter in place is not appropriate, it is recommended to have a comprehensive evacuation plan in place.

Provide fire extinguishers, AEDs, first-aid kits, evac chairs, or stretchers, and communicate storage location to staff ①

The safety/protection of human life is a critical component to business continuity planning. Test, plan, and do drills regularly.



① Prepare office space (cont.)

Perform routine environmental cleaning ①

Routinely clean all frequently touched surfaces in the workplace, such as workstations, countertops, and doorknobs, and provide disposable wipes so that commonly used surfaces (such as keyboards, remote controls, desks) can be wiped down by employees before each use.

Know how an event such as a biological or contagion incident impacts your HVAC equipment and the office environment ①

HVAC systems that require a large quantity of fresh air are vulnerable to these types of events. Understanding how to shut down or circumvent an HVAC system that needs a delivery of fresh air is important.

Understand the run times for generators ①

Have plans in place for refuels and service. Periodically check automatic transfer switches for backup generators prior to an event.

Understand the minimum your property would need to keep running and how that impacts your manpower ①

For example, do you need more than one person to check boiler operations?



Document hardware & software

Documenting IT equipment, software, and processes can make insurance claims easier and provides a record should a key team member absence occur.

Photograph/document IT hardware for potential insurance claims ⌚⌚

Photograph IT equipment for potential insurance claims and update photos annually or after a significant purchase. Include date and time stamp. Send photos to insurance company, upload to cloud-based secure storage, and keep a hard copy in a safe place.

Review the technology rider in your insurance coverage ⌚

Catalogue major software licenses ⌚

Have a checklist (printed or stored off-site) of each application. Include in-case-of-emergency phone numbers and points of contact as well as customer-specific information such as the vendor customer number, license keys, and administrative user IDs.

Create a list of passwords ⌚

Leverage a password management system, preferably hosted on a system not dependent on internal IT resources. During disaster recovery, passwords and access keys will be critical for service restoration.



Provide remote access

If schools are temporarily closed, for instance, can your employees work remotely? Do your employees rely on public transportation to get to the office? What if the power is out at the office? Providing remote access enables projects to continue in the face of many disruptions.

Establish a redundant off-site location to host office data to allow employees to work remotely at home, a common space, or other community offices ⌚⌚⌚

To ensure minimal dependency on the server room within a specific office, leverage systems to replicate office data to an off-site location (alternate office, data center, or cloud) with sufficient infrastructure to support remote work.

Provide for portability of key equipment ⌚⌚

Laptop computers with docking stations, for example, provide more mobility than desktop computers.

Institute multi-factor authentication ⌚

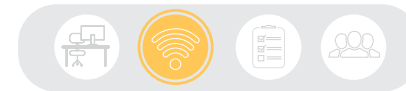
Where possible, leverage an identity provider for IT systems, which adds a second component to employee log-ons to remote systems, cloud-hosted resources, and internal sensitive systems. A second factor can be a mobile app, a hardware USB key, or a text message, which helps validate the user access as authentic and reduce the impact of password theft.

Define service level agreements ⌚

Determine with firm leadership what type and length of outages are acceptable and how much data loss is acceptable. Then design systems, redundancy, and protections around those requirements while taking into consideration systems costs related to reduced downtime.

Review vendor service level agreements ⌚⌚

Do vendor service level agreements match firm expectations and tolerance for outages? Ensure service level agreements are defined in contractual agreements.



Protect yourself from cyberattacks

Defending against cyberattacks and data loss begins long before a potential attack.

Conduct periodic IT/cyber security training

Set up backup servers

Backing up critical data is the best defense against cyberattacks. Ensure data backups are conducted on an appropriate schedule/frequency and retained for a sufficient period. If backup servers are located on-site, who will be responsible for evacuating this equipment should the need arise? Or better yet, obtain secure cloud storage for backups.

Set up cloud-based backup

Replicate backup data to an off-site location such as a cloud provider. Most importantly, know what you are backing up. Verify that important data is saved and can be restored to a new server in an acceptable amount of time.

Educate staff on cyber security risks, including malware, hacking, and passwords

Malware commonly occurs when downloading free software packages, sharing internet files, utilizing removable media, clicking on suspicious email links, and when an internet security software program is not in place. To minimize attacks, educate employees on what is unacceptable use and have them sign a document of acceptance. Hacking typically occurs through sharing of credentials and passwords and can be facilitated through too-good-to-be-true email offers. Always verify the sender via phone call or separate email. Educating why and placing restrictions on sharing will help to minimize hacking. Simple passwords that are easy to remember and don't change are targets for intruders. Put in place passwords that are multi-factor, and periodically change them to help minimize risk.

Implement cyber security backup measures

Cloud-based services are becoming more prevalent as a way to minimize a cyberattack. Research companies before signing an agreement to understand what security measures they take to protect data. Additionally, implement a strong spam filter to minimize many types of cyber risks.

Implement a process to change passwords and delete accounts upon an employee's termination

Are passwords changed once employees leave? If not, the firm is open to outside risk. Firms can also monitor internet use to help minimize attacks.

Institute privileged access management

Isolate privileged IT tasks within the firm to dedicated privileged accounts. Do not grant administrative privileges to "everyday" accounts used to check e-mail and browse the internet. Incorporate two-part passwords for sensitive accounts where each half is maintained by a pair of employees who each only has one-half of the password, and both persons (or a pair from column A and column B of a pre-established list of approved employees) must come together to access the highly privileged account. As with all accounts, change administrative account passwords regularly, and always after an employee leaves.

Engage an IT specialist before an attack

IT is more than fixing a computer. IT specialists can help educate the firm on how best to protect data internally and externally to minimize cyber risk. Initiate strong spam filters, monitor risk, and assist with cloud services that best fit the firm's needs. If the expertise is not on staff, IT consultants offer these services.

Perform routine security audits and testing

Hire a third-party security vendor to scan public internet-facing systems as well as internal systems for weaknesses and known vulnerabilities on a routine basis, and take the necessary steps to remediate the threat.

Perform system updates

Ensure all systems, both internal and public, receive regular security and functionality updates and all systems in use are supported by its vendor. Subscribe to vendor email lists to receive notifications when vulnerabilities are discovered and patch; follow vendor update release cadences.



○ Protect yourself from cyberattacks (cont.)

Develop an incident management plan ⌚⌚⌚

Develop plans for cyber security incidents, data loss incidents, and disaster and recovery incidents. The plan defines common risk scenarios and provides guidance on mitigation opportunities and procedures to follow; including which systems to verify for health and data availability and notification procedures. Once developed, test recovery procedures. It is also recommended to conduct annual incident response tabletop exercises to evaluate the firm's preparedness in handling the incident and to inform required participants of their roles in the response.

Consider continuous security monitoring ⌚⌚

Implement email security software to reduce suspicious email. Where possible, deploy a security monitoring system (audit logging as well as an intrusion detection system) and retain dedicated employees to observe for anomalous user activity, unexpected network activity, and system events.



Build in redundancy

Your team members—both within and outside the firm—are valuable assets and critical to the smooth execution of projects. What would happen if a key team member was suddenly absent? Protect your firm and your projects by building in redundancy.

Reduce single point of contact ①①

To the extent possible, it's recommended to have at least two principals involved in each project. One as a backup to the principal in charge in case the prime contact is unavailable. Ensure the backup principal knows the contract agreement (or where the contract is located), the owner's representative, the consultants on the project and the general contractor. Should something suddenly happen to the principal in charge, the project would be able to continue.

Cross-train employees to perform more than one task ①①

Cross-train personnel to perform essential functions so that the workplace is able to operate even if key staff members are absent.

Establish business continuity expectations with consultants and clients ①①

Discuss how work will continue should a hazard event occur.

Develop a succession and transition plan ①①①

While this type of plan isn't designed for the sudden absence of a key team member, developing a succession plan may help ease such an occurrence (in addition to helping the firm maintain a strong footing during planned leadership transitions). A succession plan identifies your target retirement date or the date you'd want to shift roles, who (first, second, third) would ideally replace you, and how each individual currently ranks in their ability to do so and what needs to be done to get them ready to actually do so. The transition plan details how to get from today to that succession with key milestones to achieve. [Learn more about succession planning.](#)

Have a collaborative firm ready to recommend ①

Should your firm suddenly be unable to meet your contractual obligations, it may be helpful to have a trusted, collaborative firm ready to recommend.



Learning from disruption

Unexpected team member vacancy:

I have now prepared myself a little bit better for the possibility of another team member loss by maintaining close relationships with some key consultants and independent contractors who I could rely on if I needed to outsource work. Sometimes this means hiring them to do work that I could do in the office, but it is worth it to continue building a relationship. -Firm owner



● Evaluate contracts

Contracts govern a firm’s work. Do your contracts adequately anticipate risks and provide for new business opportunities?

Ensure the contract has a fair and equitable means of terminating the project in case the project is cancelled post-disaster ⌚

In the AIA B101 Contract, the owner has the right to terminate the agreement at any time. In that situation, the architect would be paid for services provided and costs incurred up to that point and, if they negotiated for one, they could receive a termination fee. See B101 Sections 9.5 through 9.7. This owner right is specific to the AIA documents. Termination for Convenience by the Owner is a common contractual right in construction contracts, but it’s not universal. Another possibility in B101 is that the architect could terminate the agreement if the owner suspends the project for 90 cumulative days. It’s not an automatic termination, but the architect would have that option. If the architect chose not to terminate, the architect’s fees and time to perform would be equitably adjusted to account for the suspension. See B101 Sections 9.2 and 9.3.

Know your legal liabilities post-disaster ⌚

If the owner intends to resume the project at a later date (after the event has passed and things are back on track) but does not want to (or cannot) retain the original architect, the owner has rights to the architect’s instruments of service (IOS). The standard AIA documents allow the owner to continue using the architect’s IOS for the project under a termination for convenience situation, but it must release the architect from claims and indemnify the architect from any claims by third parties that arise from the owner’s use of the IOS. See B101 Section 7.3.1.

Anticipate the possible need for additional services for projects under construction that might be damaged by a disaster but continue ⌚

For a significant hazard event that adds additional scope to the original project, the parties are likely best served by amending the agreement to address the change. This would give the parties the ability to clearly define the scope of the new work, how the architect will be compensated for it, and how it will affect the schedule for the overall project.

Prepare for post-disaster building assessments of projects ⌚

Will you provide damage assessments for past projects? Remember: If you are providing emergency services, even if you are not accepting a fee, it is important to get some kind of agreement in writing. Did you address damage assessments as an additional service in contract language?

Be aware of contract clauses related to both design schedule and construction schedule delays ⌚

Most contracts contain strict requirements related to schedules. If a disaster impacts a schedule, communicate with the owner early and often, and proposes a plan about how to recover. Most owners will be reasonable if you do this with their project in mind. Also be aware of “force majeure” clauses in your contract, which may allow for a contractual forgiveness for certain disasters outside of the architect’s control.

Review identified force majeure events carefully ⌚

Many contracts will have a force majeure clause that will allow for an extension of time to perform or maybe even allow a party to end the agreement after specific hazard events. In a contract, the clause will usually list hazard events considered to be a force majeure event. If the hazard event experienced is listed, then it’s covered. If not listed, it’s questionable as to whether the hazard event would be considered a force majeure event under the contract provision.



● Create a communications plan

Communicating—to employees, to clients, and to the public—is a critical component of managing any disruption. Developing template messaging beforehand can reduce time and stress during an event.

Create a post-disaster communications plan ⌚⌚

Firm leadership is the primary point of contact to coordinate all communications within the firm and externally to key clients, consultants, contractors, and other contacts. Who is responsible for maintaining an up-to-date employee contact list? Who is responsible for maintaining the client, user, consultant, contractor, critical vendor, and stakeholder database for each project? How is the directory accessible from multiple access points (Dropbox, hard copy, USB, server, etc.)? Who is responsible for communicating with the client for each project?

Create a template for communicating short-term and long-term interruptions to employees ⌚⌚

How will the team communicate, particularly if the team is dispersed?

Create a template for communicating short-term and long-term interruptions to clients/the public ⌚⌚

A template for notifying clients, consultants, contractors, and other contacts in the case of disruption may be prepared in advance, so that the firm can communicate quickly. Be sure multiple individuals are able to access and update your firm's website and social media to provide pre-disaster and post-disaster information.

Develop a script for out-of-office voicemail and out-of-office email messages during a disruption ⌚



○ Prepare for remote work

Working remotely involves more than the information technology infrastructure to do so. Ensure tools, resources, and policies align for optimum remote productivity.

Educate employees on how to work remotely ⌚⌚

Host regular training sessions and share procedures for accessing “work remotely” systems and ensure employees can connect. During a remote work event, if employees are unfamiliar with the procedure or have not completed prerequisites, it is highly likely they will be unable to work. Consider alignment of tools, policies, training, practice, and performance reviews to effectively integrate remote work.

Identify a “sister-firm” and/or “sister-office” for large firms ⌚

A “sister-firm” or “sister-office” is a firm/office of similar size and practice type that can temporarily provide assistance (space, printers, etc.) to your firm to enable continuity of services until you can return to your place of business. Document the sister-firm/office name, primary and alternative point of contact and contact info (phone/email), and location. Share the relevant sister-firm information with key employees. Depending on your firm size, you may need to plan for employees to be placed within a network of collaborators as your sister-office(s) may not have room to absorb a complete practice.

Establish work-at-home policies and logistics as part of your normal work procedures ⌚

The more employees at all levels that have established work-at-home routines, the more seamless the transition will be. Consider the use of cloud file storage and laptops instead of desktops as standard practice to facilitate mobility and adaptability

Understand the legal regulations of remote practice ⌚⌚

Nearly every practicing architect engages in some form of “virtual practice” because the pace and practicalities of life demand it—employees travel or relocate, must limit work time for family responsibilities, or want to take on other enterprises as consultants. The virtual architectural practice model is far more flexible than traditional practice—and may be all but recession-proof since it can grow and shrink with market fluctuations. While the benefits of virtual practice are many, there are important regulations that must be followed. [Learn more with AIA Trust.](#)



Collect key documents

Compiling—and ensuring easy access to—key documents can help facilitate efficient communication across the team and filing of insurance claims should disruption occur.

Collect business license(s) 1

Many jurisdictions require these be placed on a wall. But what happens if your office is damaged? Having a secured file with a copy of your license on a cloud-based platform allows access from any location. In some states, you may also be able to re-print your license through their online system.

Store client and consultant contracts 1 1 1

Because contracts are signed in ink, quite often they are placed into a paper file. But how are they accessed if your office is damaged or inaccessible? Scan and save them to a secure cloud-based platform to allow additional access to contracts. It is recommended to include cyber security within client contracts to protect the firm. Make sure consultants follow the same cyber security rules prior to signing contracts. Remember to add more than one individual with permission to access the cloud-based files. This is necessary in case someone is unable to perform due to injuries or is non-responsive to requests.

Collect contact lists for employees, vendors, consultants, insurance, etc. 1 1

On a regular basis, update a master list of employees, vendors, consultants, insurance reps, and others that you may need to correspond with should a disruption occur. Keep up-to-date employee rosters by periodically requesting staff for revisions. Addresses, secondary contact info, and cell phone numbers are common items that require updates. Keep a copy on a cloud-based platform with security access to protect employee information. Even a sole proprietor working from home needs to consider how they access information if their home is inaccessible. It is still acceptable to have paper files and office servers, but off-site and cloud-based storage can also be used to better protect important documents. Restrict and protect paper copies for security purposes.

Compile Insurance documents 1 1

See checklist of insurance coverage considerations.



🕒 Prepare financials

Whether riding out an economic downturn or ensuring access to capital during a disruption, preparing your financials is a critical component to business continuity.

Protect your assets 🕒

In addition to employing best accounting practices, it is recommended to have a regular audit done of the firm's finances. Depending on the firm and work volume, this may be an annual or bi-annual undertaking.

Make a plan for financial continuity 🕒

Whether writing checks or through a payroll company, consider alternate access to capital. Have backup checks available off-site and designate secondary signature in case first signature is incapacitated. Consider establishing a line of credit. Similarly, evaluate if your financial institution has the redundancy needed.

Know your financial obligations and create a plan to meet them 🕒

We trust our financial institutions to store our documents, but are you in compliance with state corporate laws and the IRS on the length of time for storing your own financial files? Check state and bank policy to maintain compliance.

Get paid without getting sued 🕒🕒

Without payment for services, design firms will suffer, starve, and even die. Importantly, payment issues are also often the single greatest warning sign of a project in trouble. [Learn how to implement billing controls to minimize the professional risk that comes with trying to collect on an unpaid invoice with the AIA Trust.](#)

Seek projects in new geographies 🕒🕒🕒

Even global downturns usually affect regions at different times. Consequently, when one market is down, others are likely to be recovering (or not yet affected). Firms large and small have diversified their portfolios by exploring new markets at home and abroad.

Create client diversity 🕒🕒🕒

Just as economic downturns rarely affect all regions at once, so too are there industries or market sectors that thrive while others are down. During the Great Recession, firms of all sizes survived (and sometimes grew) with institutional and public clients that were on a different spending cycle than private industry.

Consider contract innovations 🕒🕒

Traditional contractual arrangements have been challenged by evolving delivery methods and the assignment of delivery roles. Whereas firms may once have supplemented their design fees with construction administration, today an owner's representative may perform those services. Rather than cede those responsibilities entirely, some firms are creating opportunities to manage or supervise parts of the construction process that align with their technical specialties. For example, one firm with a strong practice in designing sustainable facades is regularly hired to supervise the construction of only the building envelope on its projects. In this way the firm can ensure that its design work truly delivers the benefits and cost savings that it promises clients.

Consider service diversity 🕒🕒🕒

During the Great Recession even the largest and most prestigious firms suffered. One such firm fought back by building up a property management practice. Despite its seeming lack of creativity, property management allowed the firm to not only survive, but also ensure its buildings were operated to optimize performance.



Analyze insurance needs

Insurance is a risk transfer mechanism that can soften the blow of a disruption. Insurance needs vary based on the risks identified by each firm. It is recommended to quantify coverage needs as informed by the Business Impact Assessment (Part 1) compared to current coverage.

Evaluate necessary coverage and compile key documents for business interruption (BI) insurance

BI insurance covers insured businesses for losses of income stemming from unavoidable disruptions to their regular operations as a result of damage to property. In addition to coverage resulting from damage to the policyholder's own property, BI coverage also may be triggered by circumstances including utility service interruption, a government evacuation order, or a substantial impairment in access to a business's premises if those result from a covered property loss. When buying BI insurance, it is important to understand how long the firm may be shut down and what workarounds are covered. Policy endorsements are available to extend BI insurance if the firm suspects a prolonged interruption is possible. Learn more with the [AIA Trust](#).

Evaluate necessary coverage, learn what documentation is required for a claim, and compile key documents for extra expense coverage

Extra expense coverage applies to additional costs incurred by the policyholder as a result of damage to its property, and to costs incurred to mitigate economic losses. Extra expense is written as an endorsement to a business owner's package policy. It is triggered by a covered property loss and covers items such as the additional cost to rent other space due to a fire or other additional expenses necessary to keep your business running. Cyber insurance also generally has an extra expense component. Learn more with the [AIA Trust](#).

Evaluate necessary coverage and compile key documents for business overhead disability insurance

Business overhead disability insurance provides a monthly benefit to cover most business expenses associated with keeping a firm operating if the owner is unable to work due to disability. This can cover employee salaries and benefits, rent, business loans, utilities, professional membership fees, insurance premiums, and other monthly business bills. This plan is especially important for sole practitioners and single-professional firms. This type of plan can also be beneficial for those firms set up in a partnership given that one's portion of ongoing expenses continue whether or not one is working. Learn more with the [AIA Trust](#).

Evaluate necessary coverage and compile key documents for key person/essential employee insurance

Key person insurance is life insurance coverage usually owned by the business on the key individuals within that business. In a small business, this individual is normally the owner/co-founder of the business, managing partner, and/or person responsible for the majority of profits. The aim of key person insurance is to compensate the business with a specific monetary amount for the losses incurred when a key income generator is lost, in order to continue the business. The business purchases life insurance coverage on this key person, pays the premiums, and is named the owner and beneficiary of the coverage. In the event of the key person's death, the firm receives the death benefit, which can be used to help keep the business afloat. Learn more with the [AIA Trust](#).

Evaluate necessary coverage and compile key insurance documents for facility-related insurance policies

Property coverage protects you against loss of or damage to essential pieces of your business such as valuable documents, laptops, or your place of business—because it only takes one disaster to wipe them out. Casualty coverage protects your business from personal injury and property damage claims that could seriously and detrimentally impact your firm or component office. Every claim can cost you money, either in paying the legitimate ones or defending yourself against fraudulent ones. General liability coverage protects you from these lawsuits and provides you the peace of mind to be effective. Learn more about [business owners insurance](#) and [flood insurance](#) with the AIA Trust.



🕒 Analyze insurance needs (cont.)

Evaluate necessary coverage and compile key insurance documents for cyber liability insurance 🕒🕒

The unique exposures and liabilities associated with privacy breaches and cyberattacks are not properly addressed in traditional general liability and professional liability coverages. To help transfer the cyber risks identified above, evaluate the cyber liability policy options to limit your exposure to both first-party and third-party cyber risks. Understanding scope of coverage and insurer services is vital. There is no standardized policy form, but many insurers offer a checklist of coverage items to compare against their competitors. Learn more with [AIA Trust](#).

Evaluate necessary coverage and compile key documents for professional liability insurance 🕒🕒

A professional liability insurance policy (sometimes called errors-and-omissions or E&O insurance) agrees to pay on behalf of the architect for claims related to an error or negligence in the performance of professional duties, in exchange for the premiums paid to the insurance company. There are many reasons why an architect might consider the purchase of professional liability insurance:

1. Business survival – Be aware of the potential liability of possible delays due to disasters beyond the control of the architect.
2. Contract requirements – Many projects include a requirement for professional liability insurance subject to a certain predetermined limit. Certain projects require separate project professional liability insurance for the project work alone, independent of any other work done by the architect.

It is important to note that even with professional liability coverage, a firm continues to retain some risk such as expenses within their deductible, any self-insurance retention, costs exceeding their policy limits, or costs for claims that are excluded from the scope of coverage. Learn more with the [AIA Trust](#).



🕒 Prepare employees

Employees can be an asset during a variety of disruptions. Adequate training and communication will help enhance safety and response during a disaster, attack, pandemic, or other hazard event.

Institute safety captains 🕒

Depending on the size of the firm, designate a safety captain for the firm or safety captains for each floor or department. Typically, a safety captain will take attendance during fire drills and assist with emergency preparedness tasks. A firm-wide safety captain may lead preparedness efforts and direct implementation of the firm's emergency preparedness plan. It is recommended to have a backup/assistant "marshal" if only one safety captain is designated for the firm in case the captain is absent.

Identify or train first-aid and mental health first-aid employees 🕒🕒

Collect name, phone number, and training type/specialty. Test, plan, and do drills regularly.

Train personnel on emergency preparedness procedures, such as when and who to call for help, how to operate fire protection, power/water shut-off, and emergency devices such as AEDs 🕒🕒

Document frequency of training, names of trained individuals, phone numbers of trained individuals, and the training type/specialty completed. You might also recommend employees complete their local [CERT training](#).

Encourage employees to complete AIA Safety Assessment Program (SAP) training 🕒🕒

SAP training provides architects, engineers, building officials, and inspectors with the knowledge and protocol to evaluate homes, buildings, and infrastructure in the aftermath of a disaster. This knowledge can be used to evaluate your own office facility in case of disaster. Learn more with [AIA's Disaster Assistance Program](#).

Have an emergency preparedness plan 🕒🕒

An emergency preparedness plan seeks to maintain safety during an emergency, while the goal of a business continuity plan is to minimize disruption to business functions. An emergency preparedness plan contributes significantly to the success of a business continuity plan. Learn more about emergency preparedness planning at [ready.gov](#).

Host an info session to advise employees on safest places to be/go during each disaster type 🕒🕒

Document the **best available refuge area (BARA)** for each hazard type and include in office policy or employee manuals. When sheltering in place, BARA should be located in areas away from exterior walls, in rooms with solid walls on all sides and adequate ceiling coverage, and with a direct egress route. Schedule regular sessions to refresh employees and test the plan. It is recommended to host a session once a month for new employees and anytime there are changes to the plan. It is recommended to send employees reminders every six months.

Have a lock-down procedure 🕒

Domestic violence, upset clients, or other situations may result in workplace violence. Remember, safety is top priority in these situations. Creating a plan, training employees, and testing the plan for such a situation is recommended. Learn more at [Ready.gov/active-shooter](#).

Familiarize employees with the lock-down procedure 🕒🕒

Schedule regular sessions to refresh employees and test the plan. It is recommended to host a session once a month for new employees and any time there are changes to the plan. It is recommended to send reminders to all employees every six months.

Train personnel on exits and a primary and secondary safe zone meeting point for an evacuation 🕒🕒

Create graphic depicting emergency exits and associated meeting points for intranet/break room(s) 🕒🕒

Infographics like these provide an on-site 24/7 reminder of recommended procedures.



① Prepare employees (cont.)

Encourage sick employees to stay home ①

Ensure that your sick leave policies are flexible and consistent with public health guidance and that employees are aware of these policies. By minimizing the spread of colds and viruses, you can enhance the health of your firm and your community.

Encourage healthy habits ①

Instruct employees to clean their hands often with an alcohol-based hand sanitizer that contains at least 60–95% alcohol, or wash their hands with soap and water for at least 20 seconds. Soap and water is recommended if hands are visibly dirty.

Travel smart ①

Limit non-essential travel when the risk of contracting and spreading disease is high. Advise employees before traveling to take certain steps:

Check the CDC's Traveler's Health Notices for the latest guidance and recommendations for each country to which they will travel.

Advise employees to check themselves for symptoms of illness before starting travel and notify their supervisor and stay home if they are sick.

Ensure employees who become sick while traveling or on temporary assignment understand that they should notify their supervisor and should promptly call a health care provider for advice if needed.

If outside the US, sick employees should follow your firm's policy for obtaining medical care or contact a health care provider or overseas medical assistance company to assist them with finding an appropriate health care provider in that country. A US consular officer can help locate health care services. However, US embassies, consulates, and military facilities do not have the legal authority, capability, and resources to evacuate or give medicines, vaccines, or medical care to private US citizens overseas.

Step 4: Implement

Maintaining your plan

While your initial efforts at business continuity planning may be a focused project, business continuity planning is an ongoing cycle of testing, exercising, evaluating, and updating your plan.⁶ After all, risk is not static. Future events may reveal new vulnerabilities or opportunities to enhance business continuity. Most experts recommend an annual review of your business continuity plan. Outside of the annual review, additional circumstances that warrant a plan review may include⁷:

- newly identified hazards
- changes to hazard vulnerability
- weaknesses identified by tests, drills, or exercises
- issues identified by post-incident critiques
- new office acquired, integrated, or divested
- significant changes to critical suppliers or supply chain
- significant increase in on-site workforce population
- significant changes to site, buildings, or layouts
- changes to surrounding infrastructure

It is critical to review the plan with all firm employees on a regular basis and to solicit feedback when the plan is practiced and improved.



Business Continuity Planning (BCP) Life Cycle

Training, testing, and maintaining the firm's business continuity plan is an important part of the business continuity planning life cycle.

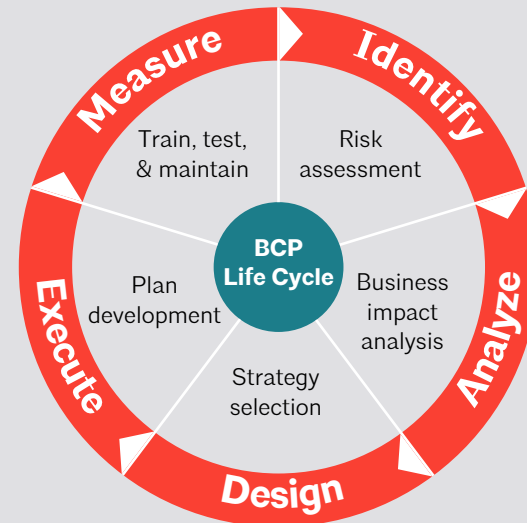


Image courtesy of Raymond-Cox Consulting, LLC

⁶ Skolnik, Aaron. *Business Continuity Training Part Three – What is the Business Continuity Planning Process?*, FEMA, 2012, [fema.gov/media-library/assets/videos/80240](https://www.fema.gov/media-library/assets/videos/80240)

⁷ *Program Reviews*, Ready.gov, [ready.gov/business/program/reviews](https://www.ready.gov/business/program/reviews)

Step 5: Assess

When a disruption occurs, it's important to reflect on the experience and update your business continuity plan accordingly. Reflecting on your experience and understanding what to do (or not do) when a disruption occurs can help the firm navigate the unexpected as well as better understand and plan for future events.




Triage: If you experience a disaster, cyberattack, or key team member vacancy

Sometimes a disruption occurs before embarking on a business continuity plan or the event exceeds the anticipated impacts. When unexpected disruptions occur, the shock can be paralyzing. If you've experienced a disaster, cyberattack, or sudden absence of a team member, the checklists linked within the "In the event of" graphic can help guide the firm through recovery. Informed by firms that have experienced such disruptions, these checklists are intended to ease the burden of unforeseen impacts and get the firm back up and running as soon as possible.

In the event of:

Business continuity planning means preparing for disruption. Here's what to do if a disaster, cyberattack, or key personnel vacancy happens to you.

Click the title of each checklist to jump to recommended actions.

-  **DISASTER**
-  **CYBERATTACK**
-  **KEY TEAM MEMBER VACANCY**



In the event of: Disaster

Disasters can keep a firm from re-opening their office doors, delay projects, and turn your personal life upside down. Below are a few recommendations to help you should disaster strike. Keep in mind, when disasters occur, your firm, as well as your broader community, may be affected. If employees have lost their home or had family members hurt due to an event, they may not be available to assist the firm.



If a hazard event is forecasted

Monitor emergency operations center's notices and evacuation status.

Communicate with internal team: Team assignments may change to focus on preparing for a forecasted event. Confirm with employees as to whom they will report to during evacuation. Additionally, employees will need to know if or when the office will close in order to plan for their own preparations and safe evacuation.

Ensure physical facilities are secured to the extent possible: Preparations will vary based on the event forecasted. Ensure recent photographs of the office/equipment are available for potential insurance claims.

Create a go box for each project: Archive projects in the design phase in a common, accessible location and, of course, make all information available on the server and accessible for remote work. Employees can assist with preparing a go box for each project, including critical information for remote work and project continuity: drawings, project manuals, contracts, notebooks, etc. Assemble these materials in a banker's box or weatherproof box, and remove the box from the threat area should evacuation be required.

Ensure files and contacts are backed up and current login info to the remote server is available.

Ensure engineering/facilities employees are scheduled in a manner that provides maximum coverage: Consider staggering work schedules and having on-call employees available.

Photograph projects under construction: If there is time, it is good practice to photograph projects under construction with a date stamp, including completed sections and materials stored on the job site—if there is a loss, the architect may be part of the claim team for the builder's risk insurance.

Obtain flash drives, banker's boxes, chargers, and other supplies for potential evacuation: Depending on the event forecasted and your office setup, this may include removal of the server computer, original software files, cameras, projector, license stamps, laptops, rolodexes, password log, checkbooks, tax files, bank records, insurance records, etc.

Conduct external outreach: Prior to a forecasted event, when feasible, send email communications to clients, consultants, contractors, and other contacts describing the office status. Project managers can share any updated contact information as the primary person in charge of a project and identify an alternate contact if they are unavailable.

Set out-of-office messages: Electronic messages with alternative contact information can be posted to regular communication channels including phone, email, and shared information-sites and indicate a potential delay for replies. Prepare social media posts for interruption and recovery procedures.

Support past clients: When an event approaches or a reminder of hazard risk occurs, past clients may scramble for information; as time permits, you may remind them about owners & maintenance information previously provided for operation systems, warranties, and other potentially useful features. Remind your current clients of emergency notices from authorities. Never promise that a building will withstand a threat; maintenance and construction defects may result in performance that is less than the designed condition.



During disaster

Emphasize life safety: Prioritize human life and safety over property in all actions during an event (i.e., leave the building rather than stay to fight a fire or collect valuables; break a window or door to get out if necessary).

Communicate the type of event underway and action(s) to be taken: For example, lock-down procedures, exits that are no longer viable, etc.

Activate shelter in place procedures as necessary and reasonable: If a prolonged stay is necessary (i.e., overnight because no transit is accessible), rearrange common areas if necessary and assign employees who are there to coordinate food and sleeping areas.

Allow individuals to work remotely if circumstances permit.

Ensure everyone at the site is safe: Take roll of all employees in the office and triage for physical or emotional injuries. If safe to do so, encourage employees to stay at home or return home. If shelter is needed and the office is stable, welcome employees to shelter in place.

Determine if employees not present at the office are safe after the event: Contact employees and follow up if there is no response.



Business is operational

Re-evaluate project schedules: For projects in design, identify the schedule impacts from the closure and advise the client. One or more projects may have to be put on hold if employees are unable to work, the contractor cannot access the site, or a number of other challenges are encountered. Contact the authority having jurisdiction to determine emergency procedures or ordinances available for obtaining permits and resuming work. Coordinate with the clients, contractors, and other parties to determine an acceptable solution; it may require teaming up with an unaffected colleague or alternate contractor. If the client terminates a project due to the changed conditions, work with them to identify an alternative lot, size, scope, schedule, or delivery method if possible. If there is no opportunity for a modified contract, AIA contracts provide for termination expenses to be paid to the architect. Government and other client's contracts often include force majeure clauses allowing for contract termination in case of extended force majeure events.

Examine/evaluate projects under construction: If projects under construction experience damage, use the situation to learn more and share across the firm.

Examine/document damaged projects and determine the cause of failures: Architects need to continually educate themselves about the causes of building failures in order to prevent them from happening in the future.

Be a resource: If a client or essential consultant is displaced, consider the availability of space in your office to provide temporary workspace for them. Consider allowing colleagues or community groups to use your office conference space for community meetings—this is an opportunity to become a hub for information and idea-sharing. If sharing office space is disrupting operations or too costly, an alternative is to utilize a less-used location that could host supportive events long term, particularly for long-term recovery. Also contact your local AIA component. They can help you provide resources to your peers.

Conduct outreach to clients, community groups or government agencies, and design partners to determine new project opportunities (repairs, retrofits): Make your skills available to former clients for technical assistance. Become an active part of the recovery efforts. Help the community analyze reconstruction principles and priorities by joining committees, providing assistance in visioning, writing grants, and fundraising.

Assess and update plan: Reflect on the experience. What went wrong? What went right? How can you use these findings to enhance your business continuity?



Learning from disruption

The hurricane: Few people had the resources to rebuild immediately, so we organized community meetings about rebuilding, participated in the charrettes, and volunteered where we could to help with disaster assessments and planning for future improvements. –Firm owner



Business is disrupted

Update office website with status information: If the scope of the event warrants a change in the office re-opening date, update the office website with new information.

Determine ability to access the site following a disaster: Confirm with the authority having jurisdiction (AHJ) that it is safe to enter the facility. If you have AIA SAP-trained employees, this determination can be made by those trained staff members. The evaluation conducted only informs your own actions and is not a means of tagging the building, which is the responsibility of the AHJ.

When it is safe to do so, designate firm leaders or employees to enter the disaster area and review the status of the building and/or projects under construction: If the damage is significant or access to the building is otherwise restricted, coordination with local authorities will be needed.

Retrieve key documents: Collect copies of all key documents and meet with building/fire officials, landlord, and insurance agent to advise status of building; schedule next steps/actions needed.

Contact insurance agent(s) about coverage and claims.

Check on impact to employees and provide office status update: Within a certain time frame, the primary contact should reach out to the team. If the designated time frame is reached without communication from the primary contact, the secondary contact needs to reach out to employees. Employees will provide a status update, location, and availability. If they have been affected by the event, they should contact a designated person to find out how to receive assistance during the recovery period. Communicate if the office is safe for re-occupation and any alternate provisions. If the scope of the event warrants a change in the office re-opening date, communicate this to your team as soon as possible so they can plan ahead. Communicate any pay impacts that may occur.

Determine who can return to work: Coordinate with employees to determine who is able to return to work in person and who needs to work remotely. Adjust project assignments as necessary.

Confirm which staff have access to safe remote work options: If employees cannot return immediately to work or need personal time off, try to be as flexible as possible.

Restore office space: Contact the insurance claim adjuster to schedule the insurance assessment. Alternatively, photograph (with date and time stamp) the office “as is” and share documentation to advise status. If damage is sustained beyond the ability of employees to clean up/repair, schedule cleanup/repair. If it is not possible to use the office again ever, arrange for lease of a new location. If seeking a temporary or permanent new location, consider the availability of housing in the area, access challenges, and the mental health impacts of returning to a place that has been devastated.

Triage

Contact your local AIA component: After an event, state and local components may be reached via email, phone, or social media depending on the impacts. Reach out when you are able; they can be a resource to you.

Assess: Reflect on the experience. What went wrong? What went right? How can you use these findings to enhance your business continuity?



In the event of: Cyberattack

- Cyber security and digital information loss are growing concerns across all industries. Should your firm be held hostage by ransomware or experience the loss of sensitive data, below are recommended next steps.



During event:

Contact cyber insurance carrier: Many policies offer assistance to help mitigate the risk during the attack.

Identify incident type: Contact IT upon initial suspicion of an attack or abnormality to minimize continued risk. Is it a single computer or firm-wide? Is the event data loss limited to a single office, a building environmental issue impacting office technology, a natural disaster impacting the office and employees, a broader IT incident affecting a large part of the firm, or a cyber security incident? Quickly analyzing the problem can assist in reduced spread and damage. Follow the incident management plan to identify and address the incident as planned (where possible) and adapt as the situation warrants.

Identify cyber security breach type: Understand the attack. Is it easily resolved, or does it involve significant damage and/or piracy? Piracy, which is a worldwide threat, can attack individuals and firms. Piracy has a specific process to regain data. This can include tutorials on where to pay the ransom, how to process payment, and how to regain data. Piracy may also have time frames for payment that increase with delays. Analyzing the loss and its impact will help determine if the information lost or pirated is worth recovering. Backup systems when correctly designed, deployed, and appropriately isolated, can nullify piracy events as damaged data can simply be recovered. In certain situations, if internal IT expertise is not available, contacting a security incident management company as soon as possible may be the best approach to understanding the scale and scope of the incident.

Mitigate or nullify attack when possible: If the source of malicious/unwanted activity can be located through IT forensics, disable accounts, change passwords, shut down internet connectivity, isolate office network, or take other appropriate actions.

Analyze data loss and recovery methods: Firms are technology-based. Analyzing loss needs to quickly happen once an attack occurs to understand what is impacted by an attack, and to minimize additional attacks. An IT specialist can analyze and discuss recovery.

Prioritize restoration: Identify each application criticality as a basis for prioritizing the recovery process. For example, CAD or BIM systems and associated files may be more critical than office productivity software. The ease with which an application can be restored as well as the business cycle will impact criticality. For example, a down payroll system the day before payday will have a higher criticality than the day after payday.



After event:

Engage internal team leaders on extent of loss if documents are unrecoverable: Cyberattacks impact the entire firm and can quickly spiral out of control. Make everyone aware of the attack, what is impacted, how it is resolved, and how they should proceed in notifying outside sources.

Notify clients, consultants, and other deadline-related sources of the breach: Cyberattacks can occur without an employee even knowing they have allowed access. They can be passed on from reliable sources, such as consultants, accountants, professionals, or what appear to be secure websites (banks, government). It is important to notify a project team so they understand the reason for possible delays and so they understand how it is being resolved.

Review documentation and interview stakeholders: Review documentation recorded during the event and interview stakeholders to understand their perspectives and insights. Discern where the incident response plan was insufficient, and make corrections and additions based on lessons learned. Update the incident response plan as needed.

Implement more robust backup, disaster recovery, and monitoring systems: Depending on the incident source, impact, and perceived future risk, implement improved backup systems to reduce impact and time-to-recovery during a future data loss or cyber security attack.

Educate employees on cyber risks/vulnerabilities: Understand why the attack occurred and educate employees on how to minimize future risk. Was it from a source deemed reliable? Asking the source through a separate process before responding or opening links often will greatly diminish attacks.

Implement changes based on broader lessons learned: Execute changes to routine testing, drills, procedural reviews, and user training to mitigate future risks. Ensure lessons learned are embodied to prevent future reoccurrence.

Assess: Reflect on the experience. What went wrong? What went right? How can you use these findings to enhance your business continuity?



In the event of: Key team member vacancy

Whether unexpected death, sudden departure, or temporary inability to work, a key team member vacancy can be detrimental to the daily needs of a firm. Below are a few tips should this happen to you.

After event:

Assess team impact: Determine the essential activities of the key team member and find the right team member to fill the gaps. Recognize that tasks may need to be prioritized. Even in a large firm, it may not be reasonable for remaining team members to take on substantial new responsibilities on top of existing assignments.

Communicate employee changes to the entire staff with transparency: Anticipate when temporary circumstances will resolve or change and communicate both unknowns and expectations.

Notify clients: Communicate the succession plan to clients with care, individually, and with clear assignment of new team members. Recognize that some clients will be disappointed—take steps to address their concerns.

Revise website and marketing materials as needed: Remove the individual from firm literature, website, social media, etc. to avoid clients/vendors asking for a team member who is no longer available.

Provide training and mentorship for team members with new responsibilities: Reassess other work expectations and reprioritize. Employees experiencing new duties may feel quickly overwhelmed. Try to provide time and flexibility to accommodate onboarding to new duties and projects.

Communicate the ongoing strength of the firm through the media, community partners, service, etc.

If a death is experienced, celebrate the life of the team member (as appropriate) and allow the office time to grieve: This will be unique to the situation. Examples of celebrating the life of the team member include establishing a scholarship to recognize the loss and contributions of the team member, hosting a memorial with a firm-wide and external message (particularly when the individual has an industry-level presence), providing an internally focused message, and offering a very local office message with clear support for the remaining family. Where appropriate, the office may also consider offering support to the team member's family.

Assess: Reflect on the experience. What went wrong? What went right? How can you use these findings to enhance your business continuity?

Definitions & concepts

Adaptation: The adjustment in natural or human systems in response to actual or expected climatic stimuli or their effects, which moderates harm or exploits beneficial opportunities.⁸

Best available area of refuge (BARA): A location within a facility best suited for sheltering in place, which provides some protection against building damage. Usually, an interior space with solid walls without windows and a solid lid or ceiling, and with adequate egress route.

Business continuity: The capability of the organization to continue delivery of products or services at acceptable, pre-defined levels following a disruptive incident.⁹ An ongoing process to ensure that the necessary steps are taken to identify the impacts of potential losses and maintain viable recovery strategies, recovery plan, and community services.¹⁰

Business continuity impact analysis: Identifies the effects resulting from disruption of business functions and processes.¹¹

Building performance objectives¹²: How much damage is acceptable?

- Immediate occupancy (IO): Following a significant natural hazard event, buildings maintain occupancy and functionality with minimal repairs.¹³ The ability to safely re-occupy a building after the event, in order to take shelter or begin making repairs.
- Life safety (LS): Structure is damaged but retains a margin against the onset of collapse.
- Collapse prevention (CP): Structure is damaged and maintains gravity support but retains no margin against collapse.

Direct impact: Impacts that are specific to the firm's ability to operate, such as employees, building, server, hardware, etc.

Disaster: A serious disruption of the functioning of a community or a society causing widespread human, material, economic, or environmental losses that exceed the ability of the affected community or society to cope using its own resources.¹⁴

Disruption: The consequences of a hazard event that results in loss of services or functions in a community.¹⁵

Functional recovery: Post-event structural and nonstructural capacity are maintained or can be restored to support the basic intended functions of the building's pre-event use and occupancy within a maximum acceptable time, which might differ for various uses or occupancies.

Hazard: A potential source of danger caused by a naturally occurring or human-induced process or event with the potential to create loss.¹⁶

Hazard event: The occurrence of a hazard.¹⁷

Indirect impact: Impacts specific to a firm's clients and future work.

Magnitude: A measure of the severity of a hazard event.

Probability: A measure of the likelihood that the undesirable event will occur.

Risk: The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.¹⁸

Secondary hazard: A threat that its potential would be realized as the result of a triggering event that in itself would constitute an emergency. For example, dam failure might be a secondary hazard associated with earthquakes

Shelter in place: Safely remaining in a building (e.g., a residence) during or after a hazard event.¹⁹

Vulnerability: The degree to which a system is susceptible to, and unable to cope with, adverse effects.²⁰

- 8 *Glossary of Terms*, IPCC, 2012. https://archive.ipcc.ch/pdf/special-reports/srex/SREX-Annex_Glossary.pdf
- 9 *Standard on Continuity, Emergency, and Crisis Management NFPA 1600*, National Fire Protection Association, 2013.
- 10 *Business continuity ISO 22300*, International Organization for Standardization, 2019.
- 11 *Business Continuity Plan*, Ready website, Department of Homeland Security. ready.gov/business-continuity-plan
- 12 *FEMA P-2006 Example Application Guide for ASCE/SEI 41-13 Seismic Evaluation and Retrofit of Existing Buildings with Additional Commentary for ASCE/SEI 41-17*, FEMA, 2018. [fema.gov/media-library-data/1532488318586-01acca43f245b646e127791792afe278/FEMA_p2006_June2018_508.pdf](https://www.fema.gov/media-library-data/1532488318586-01acca43f245b646e127791792afe278/FEMA_p2006_June2018_508.pdf)
- 13 *Research Needs to Support Immediate Occupancy Building Performance Objective Following Natural Hazard Events*, NIST, 2018. nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1224.pdf
- 14 National Science and Technology Council, 2005.
- 15 *NIST Special Publication 1190: Community Resilience planning Guide for Buildings and Infrastructure Systems - Volume 1*, NIST, 2015.
- 16 *AIA Resilience and Adaptation online series glossary*. AIA, 2018. <https://aiaa.aia.org/aia-resilience-and-adaptation-online-certificate-program>
- 17 *NIST Special Publication 1190: Community Resilience planning Guide for Buildings and Infrastructure Systems - Volume 1*, NIST, 2015.
- 18 *AIA Resilience and Adaptation online series glossary*. AIA, 2018. <https://aiaa.aia.org/aia-resilience-and-adaptation-online-certificate-program>
- 19 *NIST Special Publication 1190: Community Resilience planning Guide for Buildings and Infrastructure Systems - Volume 1*, NIST, 2015.
- 20 *Glossary of Terms*, IPCC, 2012. https://archive.ipcc.ch/pdf/special-reports/srex/SREX-Annex_Glossary.pdf

Resources

IBHS Open for Business (2013). Customizable worksheets for documenting employee, consultant, client, and vendor contact information as well as IT equipment.

Ready.gov/business. Recommendations for business continuity development, implementation, and training.

Leadership in Times of Crisis: A toolkit for economic recovery and resiliency (2015). Resources Appendix, Resource 2: Critical Business Functions, pages 287-288, assists in the identification of core business functions.

National Fire Protection Association (NFPA) 1600: Standard on disaster/emergency management and business continuity programs. Covers cyberthreats, terrorist attacks, and natural disasters. Details process of risk assessment, business impact analysis, and planning.

International Standards Organization (ISO) 22301: This publication covers security and resilience, business continuity management systems, and requirements. Specifies “requirements to plan,

establish, implement, operate, monitor, review, maintain and continually improve a system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.”


Supply Chain Climate Risk Management Framework: This tool from the US General Services Administration can help firms evaluate the products or services they rely on and the impact disruption of those supply chains may have on their business. The Self Assessment Questionnaire and Companion Workbook are especially recommended.

AIA Trust: Insurance products and information.

Risk Management: Free practice resources for AIA members.

Appendix: Example business impact assessment*

The below worksheets provide an example business impact assessment for a small firm located in Dallas, Texas. The below fields were completed after consulting the Dallas County Hazard Mitigation Plan, the City of Dallas Local Mitigation Action Plan, the Resilient Dallas Strategy, and local, historical events.

 Hazard potential source of danger	Risk = probability x magnitude	Probability likelihood of hazard event	Magnitude severity of hazard event	Warning time prior to hazard event	Duration time scale of disruption
EXTREME HEAT	<input checked="" type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	<input checked="" type="checkbox"/> Highly likely <input type="checkbox"/> Likely <input type="checkbox"/> Possible <input type="checkbox"/> Unlikely	<input type="checkbox"/> Catastrophic <input checked="" type="checkbox"/> Critical <input type="checkbox"/> Limited <input type="checkbox"/> Negligible	<input type="checkbox"/> Minimum to none <input type="checkbox"/> 6-12 hours <input type="checkbox"/> 12-24 hours <input checked="" type="checkbox"/> 24+ hours	<input type="checkbox"/> Hours <input checked="" type="checkbox"/> Days <input type="checkbox"/> Weeks <input type="checkbox"/> Months
TAP WATER CONTAMINATION	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Low	<input type="checkbox"/> Highly likely <input type="checkbox"/> Likely <input checked="" type="checkbox"/> Possible <input type="checkbox"/> Unlikely	<input type="checkbox"/> Catastrophic <input type="checkbox"/> Critical <input checked="" type="checkbox"/> Limited <input type="checkbox"/> Negligible	<input checked="" type="checkbox"/> Minimum to none <input type="checkbox"/> 6-12 hours <input type="checkbox"/> 12-24 hours <input type="checkbox"/> 24+ hours	<input type="checkbox"/> Hours <input checked="" type="checkbox"/> Days <input type="checkbox"/> Weeks <input type="checkbox"/> Months
DISRUPTION OF TELECOMMUNICATIONS AND BROADBAND	<input checked="" type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	<input checked="" type="checkbox"/> Highly likely <input type="checkbox"/> Likely <input type="checkbox"/> Possible <input type="checkbox"/> Unlikely	<input type="checkbox"/> Catastrophic <input checked="" type="checkbox"/> Critical <input type="checkbox"/> Limited <input type="checkbox"/> Negligible	<input checked="" type="checkbox"/> Minimum to none <input type="checkbox"/> 6-12 hours <input type="checkbox"/> 12-24 hours <input type="checkbox"/> 24+ hours	<input type="checkbox"/> Hours <input checked="" type="checkbox"/> Days <input type="checkbox"/> Weeks <input type="checkbox"/> Months
CLOSURE OF AFFORDABLE DAYCARE	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Low	<input checked="" type="checkbox"/> Highly likely <input type="checkbox"/> Likely <input type="checkbox"/> Possible <input type="checkbox"/> Unlikely	<input type="checkbox"/> Catastrophic <input type="checkbox"/> Critical <input checked="" type="checkbox"/> Limited <input type="checkbox"/> Negligible	<input type="checkbox"/> Minimum to none <input type="checkbox"/> 6-12 hours <input type="checkbox"/> 12-24 hours <input checked="" type="checkbox"/> 24+ hours	<input type="checkbox"/> Hours <input type="checkbox"/> Days <input type="checkbox"/> Weeks <input checked="" type="checkbox"/> Months
DISRUPTION TO THE LIGHT RAIL/PUBLIC TRANSPORTATION	<input type="checkbox"/> High <input checked="" type="checkbox"/> Medium <input type="checkbox"/> Low	<input type="checkbox"/> Highly likely <input type="checkbox"/> Likely <input checked="" type="checkbox"/> Possible <input type="checkbox"/> Unlikely	<input type="checkbox"/> Catastrophic <input checked="" type="checkbox"/> Critical <input type="checkbox"/> Limited <input type="checkbox"/> Negligible	<input checked="" type="checkbox"/> Minimum to none <input type="checkbox"/> 6-12 hours <input type="checkbox"/> 12-24 hours <input type="checkbox"/> 24+ hours	<input type="checkbox"/> Hours <input checked="" type="checkbox"/> Days <input type="checkbox"/> Weeks <input type="checkbox"/> Months
FLOODING	<input checked="" type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	<input checked="" type="checkbox"/> Highly likely <input type="checkbox"/> Likely <input type="checkbox"/> Possible <input type="checkbox"/> Unlikely	<input type="checkbox"/> Catastrophic <input checked="" type="checkbox"/> Critical <input type="checkbox"/> Limited <input type="checkbox"/> Negligible	<input type="checkbox"/> Minimum to none <input checked="" type="checkbox"/> 6-12 hours <input type="checkbox"/> 12-24 hours <input type="checkbox"/> 24+ hours	<input type="checkbox"/> Hours <input type="checkbox"/> Days <input checked="" type="checkbox"/> Weeks <input type="checkbox"/> Months

*This example is not a comprehensive business impact assessment and is provided only to help users navigate the supplied worksheets.

Summarize your findings

Which hazards are high, medium, and low risk? Log your findings below.

Perform a gut check. Assuming the above risk assessment was based upon the risks conveyed in state or local plans, are all aspects of your business functions represented, such as location of employees, supply chain, or hazards that would have a more profound impact on your particular type of work?

When gut checking the risk level of identified hazards, it may be helpful to compare the relative potential impacts of identified hazards specifically for your firm. Are the anticipated firm impacts of extreme heat days equivalent

to the firm impacts of a disruption in communications? Similarly, is the loss of communications more critical than losing public transit? The goal is to gut check which hazards pose not only the highest risk, but the most significant impact to your firm. Ask yourself which hazards will truly impact your ability to provide services. The Risk Assessment Summary therefore will likely be close to, yet not identical to, your community's hazard mitigation plan because you've taken the time to correlate the hazard risks to your business functions.

Risk assessment summary

High risk hazards	Medium risk hazards	Low risk hazards
<i>EXTREME HEAT</i>	<i>TAP WATER CONTAMINATION</i>	
<i>DISRUPTION OF TELECOMMUNICATIONS AND BROADBAND</i>	<i>CLOSURE OF AFFORDABLE DAYCARE</i>	
	<i>DISRUPTION TO THE LIGHT RAIL / PUBLIC TRANSPORTATION</i>	

Example

Category I: Revenue loss

Consider: Loss of contracts, late payments, loss of work, loss of marketing or future pursuits

<p>Hazards</p> <p>Referencing the Step 1: Risk Assessment, list risks starting with the highest hazards</p>	<p>Direct impacts</p> <p>To the firm’s employees, building, server, hardware, etc.</p> <p>Consider: Does the office have to close for repairs or infrastructure work? Can your employees continue to work? Do they all have hardware/software to work remotely?</p> <p>Quantify impacts as: Per person per day, how much credit is available</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>	<p>Indirect impacts</p> <p>To clients and future work</p> <p>Consider: How will office repairs or relocation impact your ability to meet deadlines or acquire new work?</p> <p>Quantify impacts as: Per person per day, cost of contract penalty</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>
<p>EXTREME HEAT</p>	<p><i>Office cooling equipment could break, necessitating an office closure and lost work time.</i></p> <p><i>Energy demand for cooling may strain power grid and can result in brownouts or blackouts.</i></p> <p><i>Planned site visits may need to be rescheduled impacting milestone completion and billing cycles.</i></p> <p><i>Design strategies for adapting to extreme heat may need to improve given the escalation projected.</i></p> <p><i>Clients in recently designed structures that are not heat ready may express dissatisfaction with firm performance due to poor building performance and/ or escalating costs of managing cooling environment.</i></p>	<p><i>Develop alternative work arrangements to allow employees to work elsewhere when office power is off.</i></p> <p><i>Invest in server backup locations on alternative grids.</i></p> <p><i>Train design teams to better understand extreme heat adaptive strategies for projects.</i></p> <p><i>Consider how retrofit strategies may improve previously completed facilities, and approach clients with this opportunity.</i></p> <p><i>Consider market position/ brand if recognized as a leader in this adaptive space. Or conversely, recognize weakness if projects perform poorly.</i></p>	<p><i>Consider impacts to employees who need to work elsewhere or who are hourly and are thus financially impacted by office closures.</i></p> <p><i>Construction teams may not be able to work or may have reduced hours.</i></p> <p><i>Duration of construction will most likely lengthen, meaning increase in construction costs.</i></p>	<p><i>Work with employees to develop alternative support strategies to reduce personal financial burdens.</i></p> <p><i>Develop project scheduling to reflect extreme heat days and avoid escalation.</i></p>

Category 2: Increased operational costs

Consider: Temporary office, overhead payments, delay in earnings, line of credit, repair of damaged office (if applicable), permanent relocation, etc.

<p>Hazards</p> <p>Referencing the Step 1: Risk Assessment, list risks starting with the highest hazards</p>	<p>Direct impacts</p> <p>To the firm’s employees, building, server, hardware, etc.</p> <p>Consider: Can the office be repaired? How long will it take? Is temporary office space available? Will business interruption insurance cover the costs? If the office is significantly damaged, how will you establish new office space? If the office moves, do you run the risk of losing employees?</p> <p>Quantify impacts as: Per person per day, how much credit is available</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>	<p>Indirect impacts</p> <p>To clients and future work</p> <p>Consider: How will office repairs or relocation impact your ability to meet deadlines?</p> <p>Quantify impacts as: Per person per day</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>
<p>EXTREME HEAT</p>	<p><i>Additional stress on mechanical systems may raise utility bills and/ or lower the life of the system. Brownouts may reduce work output.</i></p> <p><i>Increased energy costs.</i></p>	<p><i>Budget for increased energy costs.</i></p> <p><i>Consider ways to reduce heat stress in work environment, whether owned or leased.</i></p>	<p><i>Deadlines may be missed if brownouts reduce capacity to produce work. A tight deadline could increase employee overtime costs. An extended timeline could come with contract penalties.</i></p>	<p><i>Develop project scheduling to reflect extreme heat days and likelihood of impact on production. Provide alternative strategies, such as work from home, to moderate impacts.</i></p> <p><i>Determine degree of off-grid efficiency.</i></p>

Category 3: Insurance

Consider: Professional liability, property insurance, personal insurance

<p>Hazards</p> <p>Referencing the Step 1: Risk Assessment, list risks starting with the highest hazards</p>	<p>Direct impacts</p> <p>To the firm’s employees, building, server, hardware, etc.</p> <p>Consider: Will you be able to obtain insurance at current rates? How will increased insurance costs (or the inability to obtain coverage) affect your ability to retain, retrain, and/or recruit employees? How will you be affected by contractual insurance requirements?</p> <p>Quantify impacts as: Increased cost of coverage, fewer available carriers, increased deductibles or self-insurance</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>	<p>Indirect impacts</p> <p>To clients and future work</p> <p>Consider: How will increased insurance costs (or the inability to obtain coverage) affect your ability to be price competitive when seeking new work? How will you be affected by contractual insurance requirements?</p> <p>Quantify impacts as: Increased cost of coverage, fewer available carriers, increased deductibles or self-insurance</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>
<p>EXTREME HEAT</p>	<p><i>Potential increased health insurance claims from employees.</i></p> <p><i>Potential lawsuits from under-performing buildings.</i></p> <p><i>Potential increase in professional liability insurance if firm is working in areas of high risk.</i></p> <p><i>Potential increase in property insurance for workplace as claims rise due to extreme heat stress.</i></p>	<p><i>Work with employees to raise awareness of heat stress and personal safety .</i></p> <p><i>Evaluate exposure in portfolio due to historic ability to address extreme heat solutions in designs.</i></p> <p><i>Work with insurers to understand trending in the marketplace as regions defined as extreme risk face insurance retreat.</i></p> <p><i>Consider your property exposure to extreme heat and the readiness to respond to extended heat.</i></p>	<p><i>The cost of construction insurance and/or personal insurance may rise with increased claims.</i></p> <p><i>Owner expectations on design strategies to moderate extreme heat may force a new level of competitiveness into the marketplace. Performance targets may introduce greater exposures on professional liability.</i></p> <p><i>Similarly, upgrades in codes and energy reduction targets combined with increases in energy costs may require new trainings for teams to be able to respond. Team members who are not ready introduce greater exposure to the delivery of work.</i></p> <p><i>Upgrades in codes and energy reduction targets combined with increases in energy costs may require new training to ensure teams are able to respond, thereby reducing firm exposure.</i></p>	<p><i>Training to understand and reduce extreme heat in projects.</i></p> <p><i>Dialogue with clients regarding performance targets and reasonable measures.</i></p> <p><i>Working with local code and energy target policies to align with transformation cycle.</i></p>

Category 4: Credibility

Consider: Good reputation and client is confident in brand/firm or conversely a bad reputation and client is not confident in brand/firm

<p>Hazards</p> <p>Referencing the Step 1: Risk Assessment, list risks starting with the highest hazards</p>	<p>Direct impacts</p> <p>To the firm’s employees, building, server, hardware, etc.</p> <p>Consider: A good reputation will grow the firm. How might your inability to provide services affect your reputation?</p> <p>Quantify impacts as: Employee recruitment and retention (reputable firms attract high-quality employees)</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>	<p>Indirect impacts</p> <p>To clients and future work</p> <p>Consider: Will your client, city, and other contacts recommend you to others for future work? Are your employees engaged in the community and other leadership roles where they also raise the credibility of the firm?</p> <p>Quantify impacts as: How satisfied are your clients? What is the public perception of the firm?</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>
<p>EXTREME HEAT</p>	<p><i>Extreme heat may cause major construction holdups or delays due to increased temperatures. This could cost client a lot if they can’t meet their start dates.</i></p> <p><i>Recognize that increased awareness of risks comes with increased expectation of positive environmental performance.</i></p>	<p><i>Critique where your firm stands within the spectrum of performance readiness. Develop approaches to train existing staff and collaborate with other experts to improve overall performance. Monitor and measure and report on said performance for greater transparency and improvement of firm credibility.</i></p>	<p><i>Clients may not recommend you if you’ve missed deadlines or are late on start dates.</i></p> <p><i>Clients may not recommend you if your design does not perform with evolving climate conditions.</i></p>	<p><i>Directly address expected climate changes and how current performance may evolve as climate shifts over the service life of the facility and require adjustments to facility systems.</i></p>

Category 5: Technology

Consider: Loss or lack of access to hardware (server, computers, printers), software, data, or VPN/cloud; power backup of critical equipment.

<p>Hazards</p> <p>Referencing the Step 1: Risk Assessment, list risks starting with the highest hazards</p>	<p>Direct impacts</p> <p>To the firm’s employees, building, server, hardware, etc.</p> <p>Consider: Ability to access files, systems, and applications</p> <p>Quantify impacts as: Cost to repair or purchase new equipment, time delay for fixing/replacing equipment, lost production time</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>	<p>Indirect impacts</p> <p>To clients and future work</p> <p>Consider: Ability to meet contractual obligations and regulatory compliance requirements</p> <p>Quantify impacts as: Time delay for fixing/replacing equipment, penalties for missed deadlines</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>
<p><i>EXTREME HEAT</i></p>	<p><i>Extreme heat taxes power grid resulting in either planned or unplanned brownouts/blackouts. Dependency of cloud-based software/systems for business transactions may be interrupted.</i></p>	<p><i>Determine degree of off-grid efficiency.</i></p>	<p><i>Extreme heat may cause grid failure at project sites and slow or stall progress.</i></p>	<p><i>Determine degree of off-grid efficiency.</i></p>

Category 6: Marketplace

Consider: The impact on various market sectors (health care, education, civic and corporate interiors, residential, etc.)

<p>Hazards</p> <p>Referencing the Step 1: Risk Assessment, list risks starting with the highest hazards</p>	<p>Direct impacts</p> <p>To the firm’s employees, building, server, hardware, etc.</p> <p>Consider: Can you demonstrate high performance for your primary market sector under distress? Does your firm work in one primary market sector? If so, what is the backup plan if the market sector slows down or demographic shifts occur?</p> <p>Quantify impacts as: Number of marketplaces currently served</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>	<p>Indirect impacts</p> <p>To clients and future work</p> <p>Consider: Can you evolve with your market sector as owners determine new ways of investing or divesting?</p> <p>Quantify impacts as: Marketplace health and interrelated-ness of skills offered</p>	<p>Capacity</p> <p>Ability to respond</p> <p>What is your capacity to manage the impacts? Which impacts can you resolve, cope with, or otherwise accommodate?</p>
<p>EXTREME HEAT</p>	<p><i>Extreme heat may require typical approaches to design to radically refigure site and building planning approaches. Preparing projects to sustain extreme heat waves and preparing for passive survivability or alternative support in cases of grid failure changes the nature of the approach to the marketplace.</i></p>	<p><i>Determine your team’s readiness to evaluate, understand the implications of, and act on projected extreme heat for your work regions.</i></p> <p><i>Directly engage your clients in this discussion and determine, or co-create, approaches to enable the timely shifts necessary to design.</i></p>	<p><i>Extreme heat introduces expectations of design strategies for heat management. These necessarily extend beyond mechanical means. Facilities that are not designed with this in mind may be considered anachronistic, and firms that lack the ability to converse about these issues as design problems may offer less competitive advantage.</i></p>	<p><i>Train design teams to better understand extreme heat impacts and adaptive strategies for projects.</i></p>