Prepare: Mitigating risk

An excerpt from:

Architect's Guide to Business Continuity

Interim release published March 2020
Update published June 2021

The 2021 update includes a refined Business Continuity Planning Process that includes a resource inventory, business impact analysis, recovery strategies and solutions, risk assessment, and risk treatment plan, updated worksheets, new interactive workbooks and case studies, and additional checklist items in the guide's section on preparing for and responding to a disruption.

We want to hear from you!

Take this survey and tell us about your experience using this guide.

"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

The information provided is for informational purposes only and not intended to provide professional advice of any kind, whatsoever. If the advice of a professional is needed, you should consult your own specialized advisors or counsel appropriate for your specific set of circumstances.

Recommended citation
The American Institute of Architects, (June 2021). *Architect's Guide to Business Continuity*. The American Institute of Architects. (aia.org/resources/6282340-architects-guide-to-business-continuity--:56)

Architect's Guide to Business Continuity, Published March 2020. Updated June 2021.

Prepare: Mitigating risk

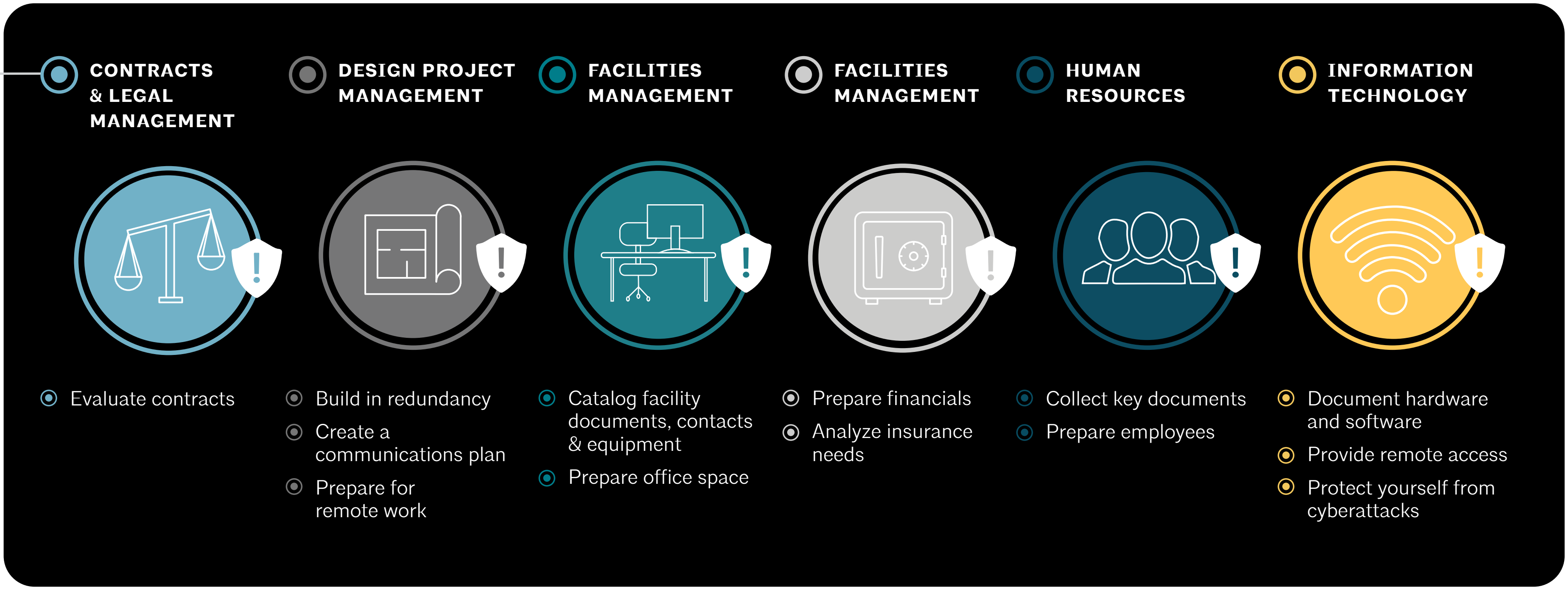
This section provides a series of non-exhaustive checklists organized by firm function:

- Contracts & legal management
- Design project management
- Facilities management
- Financial management
- Human resources
- Information technology

Each functional area includes checklists of recommended preparedness tasks. These checklists are designed to help firms prepare for disruption and are also available for reference when developing the risk treatment plan (see step 5 of the Business Continuity Planning Process). Remember to design in redundancy. It's important for all firm systems, staff roles, and technology to have backup measures or cross training.

Prepare

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



CONTRACTS & LEGAL MANAGEMENT

- Evaluate contracts

DESIGN PROJECT MANAGEMENT

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

FACILITIES MANAGEMENT

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

FACILITIES MANAGEMENT

- Prepare financials
- Analyze insurance needs

HUMAN RESOURCES

- Collect key documents
- Prepare employees

INFORMATION TECHNOLOGY

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

◉ 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 canceled 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 hazard 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.** ◷
Past and current clients may be reaching out to your firm to assess damage to their buildings, to determine a scope of work for repairs, retrofits or rebuilding, or to advise on navigating the complex landscape of federal and state disaster recovery grants, loans and policies. Refer to the AIA Safety Assessment Program for information on training and policies for volunteer assessments. Once you've trained your employees, consider offering these valuable skills as part of a contract retainer with your clients.

□ **Be aware of contract clauses related to both design schedule and construction schedule delays** ◷
Most contracts contain strict requirements related to schedules. If a disruption impacts a schedule, communicate with the owner early and often, and propose 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 events 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.

◷ = low time commitment; ◷◷◷ = high time commitment

◉ 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** 🕓🕓
To the extent possible, it's recommended to have at least two client-facing staff members involved in each project. One as a backup to the principal in charge in case the prime contact is unavailable. Ensure the backup staff member 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.

□ **Mitigate risk** 🕓
Consider whether or not key team members should be permitted to travel together. Staggering travel will reduce the chance that an accident could devastate the entire firm leadership.

□ **Cross-train employees to perform more than one duty** 🕓🕓
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** 🕓🕓
Discuss how work will continue should a hazard event occur.

□ **Develop a succession and transition plan** 🕓🕓🕓
While this type of plan isn't specifically designed for the sudden loss 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, 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 an alternative firm ready to recommend** 🕓
Should your firm suddenly be unable to meet your contractual obligations, it may be helpful to have a trusted, collaborative firm ready to recommend.

Redundancy is resiliency

Firm strategies: Minimizing disruption due to key 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 whom 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

◉ We prioritize mentoring and work to engage employees in all aspects of the firm: from construction administration to marketing and business development. We even include younger staff members in client presentations—after practicing ahead of time, of course. We want our staff to be prepared to jump in to more advanced roles should circumstances require it.
–Principal

◉ I have a hit-by-a-bus policy: Whenever possible, two people are included in client meetings. This not only provides for continuity but ensures salient details are heard and understood.
–Senior Architect

◉ When our sole licensed architect suddenly retired, we had to scramble to hire a licensed architect. Now, we maintain a minimum of two licensed architects on staff and proactively support our emerging professionals on their path to licensure.
–Principal

🕓 = low time commitment; 🕓🕓🕓 = high time commitment

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 a hazard event.

□ **Create a post-disaster communications plan** 🕒🕒
Who 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 other 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 disruptions to employees** 🕒🕒
Who is responsible and how will communications be disseminated, particularly if the employees are dispersed?

□ **Create a template for communicating short-term and long-term disruptions to clients/the public** 🕒🕒
So that a firm can communicate quickly, develop messaging in advance of a disruption for notifying clients, consultants, contractors, and other contacts of any operational changes. Be sure multiple employees are able to access this communication template and to also 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** 🕒

Learning from disruption

● **Unexpected team member vacancy:** Staff turnover is inevitable. Whether sudden or planned, how staff changes are communicated is key. Work to get buy-in from the client—as well as the user group, if applicable—when transitioning staff. This process will be smoother if the initial project procurement is centered on the capabilities of the firm rather than the reputation of a team member. A firm's marketing strategy needs to go beyond a single individual's talent.
–Senior Architect

◉ 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.

□ **Coordinate remote work arrangements with each employee** 🕒🕒
Host regular network and software training sessions, share procedures for accessing "work remotely" systems, and ensure employees can connect. Remote work is most successful when employees are familiar with virtual communication and collaboration tools, and have the space, broadband internet connection, and equipment to support them. Consider alignment of policies, tools, 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, contract labor, 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 all staff members.

□ **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, have flexible schedules 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.

🕒= low time commitment; 🕒🕒🕒 = high time commitment

◉ 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. Listing this information in step 1 of the Business Continuity Planning Process is one method of collection.

□ **Establish expectations with providers and service vendors** 🕒
Touch base with your providers and service vendors for items such as HVAC, electrical, fire, and plumbing to ensure they understand what is expected of them during a hazard event.

□ **Photograph spaces and equipment, catalog, send to insurance company, and upload to the cloud, server, and/or USB** 🕒🕒
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 your insurance company, upload to cloud-based secure storage, and keep at least one hard copy in a safe place.

□ **Enable remote access to critical documents** 🕒🕒
Be prepared for a hazard event where the engineering/facilities team may not be able to have access to their file cabinet for operation manuals, blueprints, and schematics—convert these into a digital format that is remotely accessible. This includes provisions for master keys, alarm codes, etc.

🕒= low time commitment; 🕒🕒🕒 = high time commitment

Prepare office space

The average worker spends more than one-third of their time at work. Designing or retrofitting—and maintaining—your physical office space with these tips in mind can enhance your business continuity during extreme weather, an attack, a pandemic, or other hazard event.

□ **Preparations if you own or lease your facility** ◷
If you own, prepare a list of service and repair providers to contact in case of a hazard event. 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. 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** ◷ **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** ◷
Where are the nearest hospitals/clinics and public transit stations? Where are secondary locations? What will employees do if there is no public transit available within reasonable walking distance after a hazard event?

□ **Know the intended performance level of your facility** ◷
What is the performance level of your building (construction type, age and building code edition, and capacity of mechanical, electrical, fire protection, and plumbing systems)? Is there system redundancy? Upgrade systems to achieve desired performance and service levels, and consider future conditions when making investments.

□ **Clearly label safe exit routes** ◷◷
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 evacuation.

□ **Require landlord documentation of systems testing and performance** ◷
Include this requirement in your lease to ensure systems are running properly and deficiencies are addressed.

□ **Plan for shelter in place** ◷◷◷
Document location, amount, and expiration date of emergency supplies. FEMA recommends enough non-perishable food, utensils, 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. Identify staff member(s) responsible for monitoring severe weather. Severe winter weather and hurricanes can sometimes be forecast days in advance and a work-from-home order can be initiated. Severe thunderstorms, earthquakes, volcanic eruptions, flooding, or hazardous material release may necessitate sheltering in place.

◷ = low time commitment; ◷◷◷ = high time commitment

● Prepare office space (cont.)

□ **Provide fire and medical equipment and communicate storage location to staff** 🕒
The safety/protection of human life is a critical component to business continuity planning. Provide fire extinguishers and first-aid kits as needed to accommodate the size of your office and if feasible evacuation chairs and stretchers. Test, plan, and perform drills regularly.

□ **Perform routine environmental cleaning** 🕒
Routinely clean all frequently touched surfaces in the workplace, such as workstations, countertops, and doorknobs, and provide disinfection supplies so that commonly used surfaces (such as keyboards, remote controls, desks) can be wiped down by employees before each use.

□ **Know how a biological or contagion event impacts your HVAC equipment and the office environment** 🕒
HVAC systems that require a large quantity of fresh air are vulnerable to these types of hazard 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** 🕒
Have plans in place for refuels and service. If generators do not self-test, periodically check automatic transfer switches for backup generators prior to a hazard event.

□ **Understand the minimum your property would need to keep running and how that impacts your manpower** 🕒
What services are essential to the function of your building and what resources are needed to ensure those essential services continue? For example, do you need more than one person to check boiler operations?

🕒 = low time commitment; 🕒🕒🕒 = high time commitment

Prepare financials

Whether riding out an economic downturn or ensuring access to capital during a disruption, financial management 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 biannual undertaking.

□ **Make a plan for financial continuity** 🕓
Whether writing checks or through a payroll company, consider alternate access to capital; including virtual banking, electronic transfers, and manual backups. 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, stall and may not survive. 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** 🕓🕓🕓
A wide range of services can protect a firm during times of economic uncertainty.

Learning from disruption

Economic downturn: During the Great Recession even the largest and most prestigious firms suffered. One firm fought back by building up a property management business. Property management allowed the firm to not only survive, but also encouraged the development of new skillsets that lead to the design and operation of higher performing buildings.

🕓= low time commitment; 🕓🕓🕓 = high time commitment

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 Analysis (see step 2 of the Business Continuity Planning Process) compared to current coverage.

□ **Business interruption (BI) insurance: Evaluate coverage and compile documents** 🕓🕓

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.

□ **Extra expense coverage: Evaluate coverage and compile key documents** 🕓🕓

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 added expenses necessary to keep your business running. Cyber liability insurance also generally has an extra expense component. Learn more with the AIA Trust.

□ **Business overhead disability insurance: evaluate coverage and compile documents** 🕓🕓

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.

□ **Key person/essential employee insurance: Evaluate coverage and compile documents** 🕓🕓

Key person insurance is life insurance coverage usually owned by the business on the key individuals within that business. In a small firm, 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 firm with a specific monetary amount for the losses incurred when a key income generator is lost, in order to continue the business. The firm 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.

□ **Facility-related insurance policies: evaluate coverage and compile documents** 🕓🕓

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.

□ **Cyber liability insurance: evaluate coverage and compile documents** 🕓🕓

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 the AIA Trust.

◉ Analyze insurance needs (cont.)

□ **Professional liability insurance: evaluate coverage and compile documents 🕓🕓**
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 hazard events 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.

◉ 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)** 🕒
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. Backup copies could also be stored on the server or on a USB. In some states, you may also be able to reprint your license through their online system.

□ **Store client and consultant contracts** 🕒🕒🕒
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. Backup copies could also be stored on the server or on a USB. It is recommended to include cybersecurity within client contracts to protect the firm. Make sure consultants follow the same cybersecurity 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 nonresponsive to requests.

□ **Collect contact lists for employees, vendors, consultants, insurance, etc.** 🕒🕒
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. Backup copies could also be stored on the server or on a USB. Restrict and protect paper copies for security purposes. Listing this information in step 1 of the Business Continuity Planning Process is one method of collection.

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. Ensure supplies are assessed and restocked regularly.

□ **Train personnel on immediate steps to take in an emergency** ◷◷
Train employees on communication procedures (who to call for help), operation of fire suppression and medical equipment, and where to find and shut off gas, electricity and water. 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 (Community Emergency Response Team) training.

□ **Encourage employees to complete AIA Post-Disaster Safety Assessment Program (SAP) training** ◷◷
SAP training provides architects, engineers, building officials, and inspectors with the knowledge and protocol to evaluate 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.

□ **Maintain an emergency response plan** ◷◷
An emergency 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 response plan contributes significantly to the success of a business continuity plan. Additionally, encourage employees to create their own personal preparedness and response emergency plans for the health and safety of their own families and to be able to return to work more quickly. Learn more about emergency 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 reminders to all employees every six months.

□ **Have a lockdown procedure** ◷
Domestic violence, upset clients, or similar hazard events may result in workplace violence. Creating a plan, training employees, and testing the plan for such a hazard event is recommended. Learn more at Ready.gov/active-shooter.

□ **Familiarize employees with the lockdown procedure** ◷◷
Schedule regular sessions to refresh employees awareness of appropriate procedures 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.

● Prepare employees (cont.)

□ **Train employees on exiting procedures** 🕒🕒
Train personnel on exits and a primary and secondary safe zone meeting point for an evacuation.

□ **Create graphics 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.

□ **Encourage sick employees to stay home** 🕒
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** 🕒
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** 🕒
Prohibit firm leaders or key employees from traveling together. Limit nonessential 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 U.S., 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 U.S. consular officer can help locate health care services. However, U.S. 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 U.S. citizens overseas.

🕒= low time commitment; 🕒🕒🕒 = high time commitment

Document hardware & software

Documenting IT equipment, software, and processes can make insurance claims easier and provides a record should a key team member loss 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, server, USB, and keep a hard copy in a safe place. If possible include identifying information such as make, model, and serial numbers, and link images to a sales receipt or invoice.

□ **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. Listing this information in step 1 of the Business Continuity Planning Process is one method of collection.

□ **Maintain a secure 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 multifactor 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 reduces 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/cybersecurity 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 cybersecurity 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. Placing restrictions on sharing will help to minimize hacking. Simple passwords that are easy to remember and are updated infrequently are targets for intruders. Put in place passwords that are multifactor, and periodically change them to help minimize risk.

□ **Implement cybersecurity 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 cyberattacks.

□ **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 email 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 a cyberattack** 🕒🕒🕒
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.

🕒= low time commitment; 🕒🕒🕒 = high time commitment

◉ Protect yourself from cyberattacks (cont.)

□ **Develop a technology recovery plan** 🕒🕒🕒
Develop plans for technology failure including data loss, telecommunications outage, cyberattacks, and security 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, it is recommended to conduct annual exercises to evaluate the firm's preparedness in handling technology outages 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.

□ **Consider need for cyber liability insurance.** 🕒🕒
See "Analyze Insurance Needs" section for more information on cyber liability insurance.

🕒 = low time commitment; 🕒🕒🕒 = high time commitment