Building a strong business continuity plan
Protect your clients and firm with a well-planned business continuity plan

A solid business continuity plan (BCP) is about more than simply staying in compliance. It’s about building trust and doing what’s right—for your clients, employees, and firm. A BCP is your firm’s lifeline in the face of natural disaster, pandemic, cyber attack, terrorism, or other disruptive events.

A well-executed BCP could help you maintain your firm’s reputation with clients. When a disruptive event happens, your plan will help determine whether your business can continue to operate, maintain communication, and preserve your clients’ confidence.

Templatized BCPs may fail to take all the important pieces into consideration. By focusing on your clients’ needs and the people, systems, third-party providers, and technology in place to serve them, you can create a more functional BCP—one built uniquely for your business. Here’s where to start.

Before you begin

To many, disaster recovery (DR) and business continuity seem interchangeable. But DR is actually just one part of a complete BCP. DR is focused on technology; its goal is to keep data secure and quickly restore IT infrastructure and operations after a crisis. BCPs look at the continuity of the entire organization. To learn more about DR, read Five Keys to a More Secure Data Environment.
Building the plan

There is no one-size-fits-all BCP. Before you can create a BCP, you need to understand the idiosyncrasies of your business.

Identify impact scenarios

What we categorize as a disruptive event can run the gamut—from large-scale tragedies (e.g., the terrorist attacks of 9/11 and Hurricanes Katrina and Sandy) to smaller-scale disruptions (e.g., key staff resignations or a localized power outage). Take time to consider the risks most likely to affect your firm. It may be helpful to think of these as “failures of the nouns”: people, places, and things.

• People—“People”-related failure might include the loss of executive staff or a widespread illness that keeps employees at home. Make a list of key people that includes contact information, which business priorities they handle, and those who might step in for them if they become unreachable.

• Places—Failure of “places” means any event that damages your physical office. This could include earthquakes, storms, or other events. Consider your firm’s location when identifying potential scenarios: Is your office on a fault line? In an area prone to flooding?

• Things—Failure of “things” includes hardware damage. Massive hardware failure can happen anywhere, shut down systems, and put data at risk. Most of the threats in this category should be addressed by your DR plan.

Remember, these are just starting points. It’s impossible to know every scenario your firm might face, and it is not practical to try. Instead, focus on creating a plan with the flexibility to adapt.

Who are your critical providers?

Your key contacts likely include critical third-party providers. To identify which providers and contacts should be categorized as critical, consider working backward. Start by identifying your client experience and the services and systems in place to support it. Then, determine which of those services or systems are made possible through outside providers. If any one of these connections is lost during an emergency, your client experience will be disrupted. These are your critical providers.

Pinpoint key contacts—and how to reach them

Communication is vital—consider who your critical internal and external resources are, and know how you’ll stay in touch during an emergency. Be sure to identify multiple methods of contact for these resources, and for your clients. For example, make a plan for communicating over cell phones if landlines are down. Or, if cell phone service is not available, set up a contingency to use email. Make sure to keep your contact list current. The more thorough your contact information and critical resources are, the better.
Building the plan (cont.)

Assess downtime risk

In business continuity, lost time is lost revenue. The average cost of downtime ranges from $6,900 per hour for small businesses to $1.1 million per hour for large businesses. Whether your business is shut down for a day, a week, or longer, you need to understand the consequences and be prepared to implement alternative plans in your front and back offices. For example, how do you plan to service clients, deliver products and services, and perform daily operational functions such as invoicing? How will your sales team continue to function if their computers are offline? Determine what tools and equipment employees need in order to access critical systems and keep operations running in an emergency.

Document the plan, and keep it on hand

Ultimately, your BCP is a reference document. Once you have worked through the considerations of your plan, it’s important to put it all together and make it physically available. Remember that a digital file will not be effective if your computers are out of service and laptops are unavailable. Many firms use a simple three-ring binder to keep everything in one place. Whatever method you use, be sure to create more than one copy. Then, distribute them among your key staff and store extra copies in multiple secure, off-site locations. These could include safe deposit boxes or electronic storage in another state.
Testing the plan

Once you have a documented plan in place, regular testing can help ensure that your firm is prepared to carry it out. Think of testing like running a fire drill. Once everyone knows where the stairs are and what to do, you continue to improve with every run-through. Testing should include both scenario-based walk-throughs of your BCP and targeted testing. Just as third-party vendors’ services directly relate to your firm’s operations, so do their BCPs. It’s important to understand what types of tests your third-party vendors run on their BCPs and how often. A viable BCP on their side can mean success on yours.

**To conduct a scenario-based test:**

- Choose an event from your list of potential impact scenarios.
- Then, test each of the steps outlined in your BCP with the core team, up to the point of actually contacting clients.
- While you are making your way through the steps, take the opportunity to record any weaknesses you discover in the plan. The weaknesses you uncover will serve to strengthen your BCP as you go.

**DR testing**

Components of your data infrastructure should be tested at least annually. Any change made to your infrastructure—including updates or enhancements—adds to its potential to fail. It’s important to conduct additional testing before any new functionality goes live. In addition, it’s critical to understand how your key third-party vendors test their systems; if disaster strikes either your business or theirs, you’ll need to know that data will continue to flow. As a best practice, any DR test should be run in both your firm’s primary data site and its DR site to help verify that the DR site seamlessly replaces and fully functions as the primary site.

**Metrics of success**

Ultimately, the goal of testing is to make sure that during or after a disruptive event, you’ll still have working data connections and can meet your goals for recovery time objective (RTO) and recovery point objective (RPO).

- **RTO**—This is how long it takes for data to be up and running at the DR site if the primary site is incapacitated. For example, if your primary site is located in California and is affected by an earthquake, the shortest amount of time it takes to get back online with your DR site in New York is your RTO.
- **RPO**—This refers to the amount of data at risk during an emergency event. For example, if your primary site goes down at 10 a.m., and the DR site makes data available again at 11 a.m., is the data from that hour lost, recoverable, or available? Losing as little data as possible is the goal.
Engaging an ongoing plan

A plan is only as good as its execution. And a successful execution is determined by how ready people are to make it happen. Once the core planning team has created the BCP, consider performing several run-throughs before introducing it to everyone at your firm. Then, training sessions with the full staff can help everyone understand their roles and feel empowered to act. Going forward, consider including employees who play a key role in the plan in an annual training to keep the BCP top of mind and ready to be deployed.

Keep the plan alive

In addition to being prepared and minimizing downtime during a disruptive event, educating employees about why business continuity is so important can help to reinforce a culture of client-first values. It’s equally important to understand that business continuity planning isn’t a one-time exercise. Many companies are not keeping their plans alive: 41% of respondents from a Ponemon Institute study reported having no set time for reviewing and updating their plans.²

Adapt to new threats

Your business is always evolving and growing, and the world doesn’t stand still, either. Every day, the news reveals the most recent events that could potentially affect your business—new weather patterns, new strains of influenza. Think of your BCP as a work in progress, which you can and should revisit and evolve over time as additional threats surface.

Who owns the plan?

As a compliance officer, you play a key role in creating and maintaining your firm’s BCP. But you’re not alone. It’s important to identify the right people in your firm who should be involved in the planning process and to bring them into the early conversations. Having your CEO involved gives you a head start on making your BCP successful. Only 29% of respondents in a recent study from Ponemon Institute said that C-level executives are involved in developing their BCP.² Depending on the size of your firm, your BCP team may also include other executives, such as the chief information officer, HR director, and IT personnel.
Questions to ask

Use this list of questions as a starting point for conversations.* Although the list of questions is not comprehensive, it does perform double duty by helping you navigate both your BCP and those of external providers that support your mission-critical systems. Since their services closely relate to yours, many of the questions you ask about your BCP should also apply to them.

Building the plan

Identify impact scenarios

☐ People: What are potential risks to your employees?
☐ Places: What are potential threats to your physical office?
☐ Things: If equipment is damaged, what parts of your business would be at risk?

Assess downtime risk

☐ How do you plan to service clients, deliver products and services, and perform daily operational functions such as invoicing?
☐ What communications will your clients need from your firm in a disaster?
☐ What applications are critical to your operations?
☐ What tools do employees need to have to continue working during an event?

Pinpoint key contacts and critical vendors

☐ Who are your key business contacts?
☐ How do you plan to keep your BCP and contact lists updated?
☐ What service providers are critical to keeping operations running?
☐ Which of your services are supported by third-party providers?

Document the plan

☐ Who owns your plan internally?
☐ Where do you keep copies of your BCP? Are they accessible in multiple formats and from different locations?
☐ Do key members of your staff have copies of the BCP?

Testing the plan

Scenario-based BCP testing

☐ Who are your key internal and external business contacts?
☐ Which potential impact scenario will you test?
☐ Where will you work?
☐ Do you have a third party to help oversee BCP management and testing? What BCP tests do your third-party vendors run?
☐ How often do you test your BCP?

DR testing

☐ Do you have a third party to help oversee DR management and testing?
☐ Do you run DR tests for every component of your infrastructure? How often?
☐ Where is your DR site located? Is it in a separate geographic location?
☐ Does your DR site have separate power sources?
☐ What is your strategy for maintaining redundant technology at other locations? How long can your redundant DR site generate power?
☐ What is your RTO?
☐ What is your RPO?

Engaging an ongoing plan

Training

☐ How often do you conduct BCP training with your staff?
☐ What type of training do you offer to help your staff understand their role in the plan?

Updating

☐ Has your firm invoked its BCP or DR plan within the last year? What were the incidence(s) and results?
☐ After testing your BCP, did you uncover any weaknesses that can inform improvements in your plan?
☐ How do you plan to update your BCP as new threats emerge?

*The above is not an extensive list of due diligence questions. Each situation will require different levels of due diligence.
Compliance Solutions

At Compliance Solutions, we take a comprehensive approach to business continuity. In the event of an emergency, we are ready to continue to provide the highest level of service to our clients. The highlights of our business continuity and DR planning include:

- **Third-party oversight**—Compliance Solutions works with a dedicated internal group from outside the immediate business line that oversees BCP and DR management and testing.

- **Rigorous testing**—We regularly test our BCP and DR plans.

- **Infrastructure monitoring**—As an extra layer of protection, we’ve enhanced the monitoring of our infrastructure and application components at both our primary and DR sites to safeguard the overall health of our systems.

- **Redundancy**—Redundancy throughout our technology infrastructure allows for transparent failover and recovery. We feature 100% server parity in our primary and DR sites, which means our DR site has the full capacity and functionality of our primary site.

Learn more
Interested in learning more about Compliance Solutions? Contact us today.

877-456-0777
schwab.com/compliancesolutions

About Compliance Solutions
Taking ownership of compliance means staying ahead of the regulatory landscape, seeing the big picture, and maintaining control. But it doesn’t mean doing it on your own. Compliance Solutions’ employee-monitoring offer includes Schwab Designated Brokerage Services, Schwab Compliance Technologies™ cloud-based employee-monitoring software, and a wide range of financial products and services for employees. These solutions can help you proactively manage compliance, promote a positive employee experience, build long-term value across your business, and instill trust in clients.