# To The Point
## Business Continuity Planning for Financial Institutions

Disasters come in many forms. Some are imposed by acts of nature such as hurricanes, floods, and earthquakes, while others occur through civil unrest, cyber attacks, and power failures. Financial institutions are uniquely susceptible to loss due to sensitive business operations and critical infrastructure.

### Requirements

The Financial Industry Regulatory Authority (FINRA) Rule 4370, Business Continuity Plans and Emergency Contact Information, requires financial institutions to create and maintain a written Business Continuity Plan (BCP) with procedures designed to enable firms to meet their obligations to customers, counterparties, and other broker-dealers during an emergency or significant business disruption. The rule also requires firms to review and update their BCPs when there are changes to operations, structure, or location.

### Components of a Business Continuity Plan

A business continuity plan provides a framework for returning to normalcy. The planning process identifies hazards associated with a disaster and mitigates the devastating effects should an event occur. The plan includes three components, each addressing a specific planning phase: risk assessment and mitigation, emergency response, and business recovery.

**Risk Assessment and Mitigation** planning considers the types of events that might compromise your business, assesses the hazards facing your company, and identifies steps to eliminate or minimize the impact of those hazards. Taking measures to prepare for a disaster improves your ability to protect employees, safeguard assets, and minimize financial consequences.

**Emergency Response** planning develops procedures that enable you to respond to a disaster. The emergency response plan is activated when an unexpected event occurs (such as a fire or contamination of a cleanroom) or when a forecasted event (such as a hurricane or flood) is imminent. The plan responds until people are safe and there is no threat of property damage or bodily injury.

**Business Recovery** planning addresses your company's critical business functions and defines procedures that facilitate the restoration of research, sales, production, and operations to pre-disaster levels. If operations are disrupted for too long, the organization may suffer irreparable consequences.

### Eight Steps to a Plan

1. **Program Management**

   Just as your organization depends on committed top management, successful business continuity plans begin with commitment and support from top management and a designated person responsible for overseeing the process. Developing the plan requires a core team of individuals from research and development, production, human resources, quality, finance, safety, facilities engineering, and other critical business areas.

2. **Risk Assessment and Mitigation**

   To best protect your organization, you must first understand what makes it vulnerable. A risk assessment identifies and ranks the types of events or hazards most likely to threaten your business. The categories addressed within this risk assessment include facility construction, fire protection, technology resources, staffing, past events, supply chain, specialized and vulnerable equipment, climate, security, and utilities. Supply chain risks from single and sole source suppliers may substantially extend recovery time frames.

   The extent of vulnerability can be assessed by determining the likelihood, potential impact, and currently established resources related to disasters. Immediate steps may be available to reduce these vulnerabilities significantly.

3. **Impact Analysis**

   The philosophy of a business continuity plan is to recover the most critical functions first and then, over time, restore all business processes. A business impact analysis (BIA) ranks functions from highly critical to important. This step requires input from all areas of your business, including confirmation from top management.

   Most business functions today rely heavily upon technology resources. A strategy for replacing the equipment and data should be spelled out within the business continuity plan. Your firm should review the possibility of quickly procuring replacement equipment from your vendors. Backup data files

should be stored off-site and accessible within a few hours. Arranging backups between multiple data centers can be helpful.

4. **Resource Management**

   Financial institutions must determine the minimum resources needed to perform the critical functions identified in the business impact analysis. These resources include staff, equipment, materials, and space. Determining what is available and what is needed based on the strategies that have been selected is crucial. Part of resource management is determining this gap and planning for future investments as needed to ensure resources are available in the event of a disaster.

   Managing resources also involves setting up alternatives for critical functions such as mutual aid agreements, identification of alternate sources of materials, and updating space requirements based on new processes within the organization.

5. **Plan**

   It is important to document systematic procedures. Most plans do not require expensive business continuity planning software—they can be written using basic word-processing programs.

   Once the critical functions have been identified, business units need to recommend strategies that allow for functional recovery within a prescribed time frame. This is known as recovery time objectives (RTO). Top management should review these recovery strategies since they require a commitment of funding and staff.

   Elements of the plan, such as the business impact analysis (BIA), should be verified on at least an annual basis.

6. **Training**

   Training should be completed by all individuals involved in the business continuity process. It should also involve all staff members to some degree so that they are aware of the process and expectations of both themselves and the company. This process also includes the distribution of the plan to the stakeholders within the organization and committee members to ensure that they understand their roles and responsibilities in the event of an incident. The material distributed should be concise and pointed to their role. Not all individuals within the company will need access to the plan, as there might be sensitive material.

7. **Exercise and Test the People/Plan**

   To verify that your choices for recovery strategies are valid, testing the plan is essential. These tests may be as simple as a tabletop exercise where company staff discuss the steps required to respond to a disaster scenario. From these discussions, it may be apparent that prescribed strategies may not work. A testing timetable will help your firm track the required testing.

   A common test scenario would be to assume that the main location is not available for a period of 30 days. With this assumption in place, the business continuity plan can address steps to operate from a temporary or secondary location. It is better to assume a worst-case scenario and be ready if something less severe happens.

8. **Program Revision**

   The business continuity plan is a living document and must evolve to keep pace with the organization. Revisions to the plan should be made at least annually to reflect any changes within the organization. Additionally, after each test of the plan/staff suggestions, improvements, and critiques should be incorporated.

## A Worthy Investment

Business continuity planning is not a static SOP (standard operating procedure). It is a continuous dynamic cycle that evolves and grows with your organization. An effective BCP requires continual reviews, updates, and adjustments based on changes to your business operations. This may appear time-consuming and costly, but the investment is essential to maintaining a comprehensive, effective plan and is often imperative to the viability of your company.

Once you engage in this process, your staff will better understand your company's vulnerabilities. Your company will then have in place the tools needed to:

- Control recovery costs.
- Increase productivity during the recovery period.
- Protect research data, materials, and scientific animals.
- Mitigate lost production capacity.
- Minimize lost revenue.
- Minimize regulatory impact.
- Increase competitive advantage.

How quickly a financial institution can recover from a devastating incident depends on effective planning and education before the incident occurs. Invest time in your business continuity plan now to preserve your organization and maintain regulatory commitments when disaster strikes.

## Resources

Financial Industry Regulatory Authority (FINRA), www.finra.org/rules-guidance/rulebooks/finra-rules/4370

The Federal Reserve, www.frbservices.org/financial-services/ach/business-continuity.html

Federal Financial Institutions Examination Council (FFIEC), ithandbook.ffiec.gov/it-booklets/business-continuity-management

ISO 22301: Security and Resilience – Business Continuity Management Systems – Requirements

NFPA 1600: Standard on Continuity, Emergency, and Crisis Management

## Learn More & Connect

For more information on protecting your business, contact your local risk engineer, visit the Chubb Risk Consulting Library, or check out www.chubb.com/riskconsulting.