7 Steps to Create a Business Continuity Plan

EzeCastle INTEGRATION

Table of Contents

Overview

When confronted with unexpected business disruptions, firms must react swiftly, methodically and successfully – or else risk significant financial, regulatory, and reputational losses. This level of response requires in-depth business continuity planning to ensure all aspects of a firm's business are evaluated and ready to recover at a moment's notice.

To preface, it's important to know what a Business Continuity Plan is and why your firm needs one. A Business Continuity Plan (BCP) is typically a document that illustrates how your firm will respond when confronted with unexpected business disruptions, such as weather, downtime of critical software or applications or even natural disasters.

While having a Business Continuity Plan can be required by regulators, all firms should consider implementing a BCP, as the process can provide specific insight into the organization. Additionally, having a BCP can proactively mitigate financial loss and other negative effects of disruptions in strategic plans, market position, operation, and reputation.

This eBook is designed to help you understand the key considerations your firm should take when developing a Business Continuity Plan as well as testing, maintenance, and training required for a comprehensive plan.

Step 1: Perform a Regulatory Review and Landscape

The first step to creating a Business Continuity Plan is to perform a regulatory review, as all businesses have requirements coming from oversight bodies. Some examples of regulators include:

- International Bodies, EU General Data Protection Regulation (GDPR)
- Federal Agencies, Securities Exchange Commission (SEC) and Financial Services Authority (FSA)
- State Agencies, MA's PII Regulation (201 CMR 17.00)
- Industry Oversight, FINRA and National Futures Association (NFA)

There are also self-imposed industry standards and expectations that come from external stakeholders including:

- Investors, who will have standard due diligence questionnaires and reporting expectations
- Auditors, who will have frameworks to be followed
- External Partners, who may have a stake in the continuity of your firm

Step 2: Perform a Detailed Risk Assessment

Next, you should perform a risk assessment on your firm. At a high level, this process includes identifying and prioritizing potential business risks and disruptions based on severity and likelihood of occurrence.

Through this process, your firm will need to understand the risks to the operation as well as the functions, reputation, and organizational assets of the firm. It's also a balance of what risks are acceptable, and which you would want to take actions against, whether it be mitigating these, creating contingency plans, or simply accepting risk.

When evaluating the potential risks and exposures of the company, be sure to look at the people, company culture, technology, and business office locations. Some offices might experience snow storms where others may experience earthquakes. Some companies expect employees at the office while others allow employees to work from home. All of these factors can have an impact on the risk assessment.

Conducting a risk assessment typically includes the following steps:

You want to identify and prioritize the risks into a register or database. The registry can and should include other areas of the business that might cause disruption such as cybersecurity risk, staffing shortages, single points of failure, or other potential exposures.

Step 3: Business Impact Analysis

A Business Impact Analysis (BIA) is beneficial from not only the Business Continuity Plan standpoint, but if you're looking to understand the company and how the different business units function, what is critical to them, and the different tools they have and what their dependencies are, this information is valuable.

A BIA is designed to identify any gaps your firm may have such as costs linked to failures, loss of cash flow, replacement of equipment, or salaries paid to catch up with a backlog of work and loss of profits. A BIA report quantifies the importance of business components and suggests appropriate fund allocation as measures to protect them. The BIA will also prioritize the recovery process and recommend the maximum allowable downtime.

A BIA should include each functional area of your business (i.e. finance, operations, trading, human resources, etc.). This will help you acquire detailed information about each function's business requirements – both during normal business hours and during a disaster. Other key pieces of information to gather are the recovery point objective (RPO) and the recovery time objective (RTO). Recovery objectives may be different unit it to unit, so it's important to ensure where recovery is most critical.

PRO TIP

Compiling your BIA into a master list can be helpful from a wholistic standpoint, as well as helpful in identifying pain points throughout the organization.

Step 4: Strategy and Plan Development

It is important to complete a Risk Assessment (RA) as well as a Business Impact Analysis (BIA), and once these are complete, it's a good time to start thinking about the overall strategy and begin to organize and develop the plan.

Understanding the needs of the individual business units and functions in order to ensure that they can operate efficiently is crucial. Ask yourself the following questions:

Do you have a contingency plan for each department? If a system is down, how long can each department go without having it up and running?

If a system is down for an extended period of time, what is the contingency plan to continue business operations?

Validate that the recovery times that you have stated in your plan are obtainable and meet the objectives that are stated in the BIA. They should easily be available and readily accessible to staff, especially if and when a disaster were to happen.

In the development phase, it's important to incorporate many perspectives from various staff and all departments to help map the overall company feel and organizational focus. Once the plan is developed, we recommend that you have an executive or management team review and sign off on the overall plan.

Step 5: Create an Incident Response Plan

It's not if, but when, an incident will happen. So having a proper, realistic incident response plan in place specifically for your firm is crucial.

If an incident does occur that disrupts day-to-day business, you'll want to ensure that responsibilities and specific actions are assigned to specific employees, and the employees are aware of their role in the incident response plan.

On occasion, we do see incident response plans that are very light and do not provide specific scenarios, which may not be applicable when the unexpected happens. When planning, assume that the incident will occur in the future, and that the plan is both realistic to your firm specifically, and to the vendors that may have a stake in your response.

When creating the incident response plan, be sure to involve departments throughout your organization and engage with other parties both internally and externally.

Internally, you should include employees from operations, personnel, HR, General Console and any IT or partners who will respond to events. Everyone should understand the strategic plan and what their responsibilities are within the plan.

From an external stand point, reach out to the different vendors that you work with and see how they plan to respond to the incidents that may arise. In doing so, this will allow you to understand the impact it will have on not only your firm itself, but your clients as well.

PRO TIP

Having these conversations both internally with staff and externally with third parties in advance is crucial. Ensuring that all parties understand their roles and responsibilities can impact the success of your response and recovery.

Step 6: Plan Testing, Training and Maintenance

Business continuity exercises are an essential and ongoing initiative. Your plan must be regularly tested using the predefined strategies developed. Testing focuses can vary depending upon which detail, conditions, frequency, business functions, or supporting information processing you wish to test.

The testing strategy should include testing objectives and associated measurement metrics, scenario scripts, summaries, post mortem and improvement planning. Firms should look to set up a schedule of testing throughout the year, we recommend looking at the Business Continuity Plan at least once to twice a year.

Be sure that your firm is able to provide instructions or scripts to follow to ensure the test progresses as it should.

Conducting tabletop exercises and simulation exercises is recommended. These can be in-person or virtual seminars, but should involve department representatives across the firm to open up communication and verify planning process in the event of a business-impact scenario.

Step 7: Communication

The final and one of the most critical aspects of a Business Continuity Plan is communication. It is crucial to be able to communicate with key personnel quickly and efficiency during an incident.

Your firm likely has a wide variety of counterparties to communicate with regularly, and during a disruption, keeping parties abreast of ongoing activity will be crucial.

Your business continuity plan should determine who will be responsible for contacting necessary parties (including employees, investors, service providers and regulators) and how they will maintain those communications.

Many organizations use an automated mass notification system to expedite the communication process. But, what if email or Internet is down? Ensure responsible parties have contact information readily accessible and clear plans for getting the word out in a timely manner.

PRO TIP

Test communication procedures in various settings and scenarios.

Communication isn't easy to master but practice make progress and helps identify gaps.

Be sure to communicate internally with your organization, and externally with the general public, regulators, investors, vendors, or other third parties.

About Eze Castle Integration

Eze Castle Integration is a leading provider of managed IT, cloud and cybersecurity solutions to more than 650 firms worldwide.

We are uniquely positioned to support today's firms with our broad portfolio of managed services, including:

Outsourced Technology Services
IT Support | Staff Augmentation | Global 24x7x365 Help Desk

Cybersecurity Solutions & Training
Vulnerability Assessments | WISP Development | Active Threat Protection | Managed Phishing/Training

Hybrid & Private Cloud Solutions
Application Hosting | Infrastructure as a Service | Managed DR | Hosted Voice

Business Resiliency & Contingency Planning
Disaster Recovery | Business Continuity Planning | Backup & Recovery | Email & IM Archiving

www.eci.com/bcp