Table of Contents

1. Introduction to Business Continuity Planning and Disaster Recovery

2. Business Continuity Planning vs. Disaster Recovery: What is the difference?

3. Developing Disaster Recovery and Business Continuity Plans
   - Key Considerations

4. The Four Steps to Business Continuity Planning
   - Risk Assessment
   - Business Impact Analysis
   - Plan Development and Implementation
   - Plan Testing & Maintenance

5. A Disaster Recovery Checklist

6. RFP Questions DR & BCP

7. Selecting a Service Provider
Disasters can take many forms. In the past, firms only needed to plan for and protect themselves against natural disasters such as flooding, fires and computer viruses. In today’s world, firms need to plan and protect themselves from cybercrime and terrorist threats to their businesses as well. In the hedge fund and investment industry there is no room for downtime.

Business continuity planning and disaster recovery have individual focuses, but they ultimately share the same goal: preparing businesses for potential disasters and ensuring those businesses are able to recover quickly and sustain minimal loss.

**Business Continuity Planning (BCP)**

A business continuity plan focuses on the development, planning and testing of the infrastructure plan designed to address the people, operational processes and business aspects. A hedge fund business continuity plan should identify the steps necessary to get operations up and running as they relate to business functions and personnel. BCP plans are intended to identify mission-critical services, communication strategies, employee recovery procedures and training methods.

There are four critical business continuity planning steps hedge funds and investment firms must follow:
1. **Identify what you need to protect.** The simplest way to do this is to conduct a Business Impact Analysis (BIA). 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.

2. **Determine how you are going to protect.** Developing recovery strategies is a great way to plan out your procedures. Identify two or three different scenarios and your corresponding responses. Establish specific communication strategies for each. Be sure to include strategies for both internal and external communications.

3. **Educate employees.** Set up employee information sessions and table top exercises so that everyone is on the same page and understands the policies and procedures. Develop resources to distribute, including emergency contact information, wallet cards and other vital materials.

4. **Validate and test.** Test your alternate site and remote access locations to ensure your business operations will resume quickly and efficiently.

*Want to know more about the 4 steps to Business Continuity Planning? Skip ahead to Page 10!*
Disaster Recovery (DR) is directly related to the technology and infrastructure that supports business operations. In developing a disaster recovery strategy, hedge funds typically examine what applications and services they have in production and which ones are mission-critical. File shares, email, accounting and trading applications and voice capabilities are often the first that come to mind, but firms should evaluate which are most essential to them.

The two most important factors associated with DR planning are the recovery point objective (RPO) and the recovery time objective (RTO).

**Recovery Point Objective**
The point in time to which you must recover data as defined by your organization

- **RPO = 24 hrs**
  - Nightly Backups

- **RPO < 4 hrs**
  - Snapshots

- **RPO = 0**
  - Continuous Replication

**Recovery Time Objective**
The duration of time within which a business process must be restored after a disaster

- **RTO > 24 hrs**
  - Restore from Backups

- **RTO < 4 hrs**
  - Hot Standby

- **RTO = 1 hr**
  - High Availability
The figure above illustrates the different layers of a business, as well as where and how disaster recovery and business continuity planning fit overall.
Developing Your DR & BCP Plans—Key Considerations

There are many key factors hedge funds should consider when developing their disaster recovery and business continuity plans.

**Capital Cost**
Every hedge fund’s business-specific requirements will vary. Some funds will use a long-only strategy that has fewer trading requirements. Other firms will pursue technical and sophisticated strategies to exploit inefficiencies, requiring fast, high-volume trades. Your firm’s preparations for disaster recovery should reflect your underlying business requirements, including strategy (long-only, high frequency, etc.), which will directly shape your budget decisions.

You will need to devote funds to server hardware, software, connectivity, other resources and training. Collectively, these represent major investments of capital. More broadly, you must consider whether outsourcing disaster recovery to a service provider or keeping it in-house is best for your business. As you make this evaluation, additional considerations include: potentially leasing the real estate and procuring, installing and maintaining all of the equipment yourself, and determining the capital budget implications of outsourcing disaster recovery versus managing it in-house.

Regardless of the approach, a disaster recovery strategy should include a “hot” or remote site that replicates your current IT environment and enables your workers to be immediately up and running in the event of an outage.

**Hot Sites and Remote Sites**
Hot site and remote site are two commonly confused terms for hedge funds looking at disaster recovery solutions. Both are technically remote sites that serve as secondary disaster recovery sites.
A disaster recovery hot site is a remote physical location where you can maintain copies of all of your critical systems, such as trading applications, data, and documents. A remote site provides a secondary instance or replica of your IT environment—without physical desks and office infrastructure—that you and your firm’s employees can securely access and use remotely, through standard Internet connections, from anywhere. How do you choose which site is best for your fund?

Begin by evaluating your hedge fund's needs:

- When would you most likely need to access the site?
- How many employees do you have?
- Is it cost-effective to book a seat at a hot site for each employee?
- In the event of a disaster, does each employee have remote locations from which they can work?

In your selection process, consider the following factors:

- **Infrastructure**: The remote or hot site must have multiple levels of redundancy designed and built into every aspect of the facility.

- **Security**: From a facilities standpoint, you want your secondary disaster recovery site to have an even higher standard of physical security than your production environment or primary data center, as the disaster recovery site may experience a constant flow of people unaffiliated with your firm. Ensure the site is set up with locked cabinets and cages housing your equipment. There should also be human security, including guards, video surveillance and visitor logs. Biometric security is another important feature. And finally, ask about perimeter and monitoring security.
• **Maintenance**: A remote site provides a more focused and efficient set of services that may be more appropriate for a hedge fund. This model provides advantages, including lower cost, assured access to dedicated IT resources and greater convenience for employees.

**Tape is Not Enough**

One of the key issues in disaster recovery is protecting one of your most crucial assets: data. Due to increased regulations, financial firms are required to maintain a vast amount of data. However, storing physical documents is not cost-effective and does not ensure the safety of your information. Your data is too valuable for you to strictly rely on unstructured backup and archiving processes with unreliable media. For many companies, tape is the attractive medium because of its low cost—and it is an appropriate choice for day-to-day restoration or long-term archiving.

However, with the many challenges that tape presents, it is wholly unsuited to the critical tasks involved in disaster recovery and business continuity planning.

Consider some of the uncertainties and questions that come with using tape:

• Have we produced a quality backup?
• Where are we storing the data? If it is not offsite, the backup may not be helpful if your data center is destroyed.
• Are the drives and equipment at the offsite location compatible with your tape format?
• Assuming you and your provider have compatible systems, will the tapes index and restore correctly to achieve a successful recovery?
• How quickly can we access our data on the tape and become operational?
Business continuity plans must consider a wide range of events and how they will affect each level of the firm and its business. A BCP, for example, must consider the potential for wide-area disasters that result in the loss or inaccessibility of office facilities or staff. Plans must also consider geographic, as well as market-based, interdependencies among investment firms and their service providers.

A comprehensive business continuity planning approach covers the complete life cycle:

**Risk Assessment**
Risk assessment is the first step firms should take when writing their business continuity plans. There are four main key components of the Risk Assessment phase:

1. Evaluate the company's risks and exposures
2. Identify single points of failure
3. Evaluate the impact of various business disruption scenarios
4. Develop a roadmap
Business Impact Analysis (BIA)
The Business impact analysis (BIA) is the most important step in the overall BCP process. A BIA is an essential component of a hedge fund’s business continuity plan; it includes an exploratory component to reveal any vulnerabilities and a planning component to develop strategies for minimising risk.

A BIA is designed to identify costs linked to failures, such as loss of cash flow, replacement of equipment, 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 for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts on safety, finances, marketing, legal compliance, and quality assurance. Where possible, impact is expressed monetarily for purposes of comparison.

Plan Development and Implementation
With the first two steps done, the next stage in developing your business continuity plan is streamlining the business function recoverability ratings and threat findings and presenting the information to management for executive sign-off.

There are two main considerations to think about:

- What types of outages do you need to prepare for? Classify them by the extent and type of impact they have – the recovery strategies available to you necessarily depend on what you must recover from.

- What types of solutions do you require based on differing breadths of coverage? Implementing alternative solutions provides a greater level of flexibility.
Plan Testing and Maintenance
Business Continuity Plans should be regularly tested using predefined strategies. Your strategy should include testing objectives and associated measurement metrics and test schedules.

A full test should be completed at least once a year, with less disruptive testing of subcomponents performed throughout the year. If a certain part or system that is to be tested depends upon another part, then that other part or system should also be tested at the same time. This will allow for a full understanding of interdependencies, and produce tests that are as realistic as possible to reduce the potential that people will freeze or an unanticipated event may occur in a real emergency.

Business continuity plans must be reviewed and updated annually to help ensure they account for changes within the firm, as well as changes in threat scenarios. As part of the maintenance process, firms must conduct annual comprehensive business impact analyses or risk having an outdated plan that does not appropriately protect the firm’s assets. It is important to ensure that your BCP accurately reflects your firm’s most current requirements and environment.
A Quick Checklist for Your Infrastructure and Disaster Recovery

- Analyze voice and data systems and determine RPOs and RTOs for each
- Identify key performers requiring earliest access
- Identify remote-site provider candidates
- Establish service level agreements (SLAs) with service providers
- Assess the provider’s data/voice and physical facility security
- Assess the provider’s testing plans
- Ensure the provider has 24-hour manned security at the DR facility as well as cameras and digital monitoring
- Are there backup power generators?
- Is there onsite fuel to run those generators? You’ll want onsite fuel that can last a few weeks.
- Check whether your remote or hot site provider has “N+1” availability, a system configuration in which multiple components have at least one independent backup component to ensure system functionality continues in the event of a system failure
Request For Proposal Questions

Below are some RFP questions you should consider when selecting a technology vendor:

- Does your company have a written policy and program for business continuity and disaster recovery?

- Have your company’s policies and programs for business continuity and disaster recovery been fully implemented? If not, discuss those areas in detail and explain any plans to address them.

- Does your business continuity and disaster recovery policy include the implementation of the following actions? (Be sure to address all parts.)
  - Personnel requirements, including emergency management contacts and all operations personnel
  - The restoration of service to clients in a prioritized manner
  - Capability and support of multiple client recovery events
  - Geographically dispersed recovery locations to allow diversity of data centers, utilities, transportation, telecommunications, etc.
  - Full security controls (for operating systems, hardware, software, user access) activated at time of system recovery, same as in a normal state
  - Timely and ongoing client status reports as part of emergency response procedures
• How often does your company test its business continuity and disaster recovery plans to ensure their effectiveness?

• Does your company use unaffiliated service providers for recovery services?

• Are the recovery services dedicated or shared?

• Is your fund at risk of being preempted in a disaster? If yes, please explain.

• Did your most recent business continuity and disaster recovery test meet its stated objectives?
Selecting a Service Provider

When evaluating technology service providers, there are eight important factors to consider.

1. **Breadth of Solutions**
   Does the IT provider offer all of the solutions and services necessary to encompass all aspects of the technology foundation required to help your firm operate effectively and efficiently?

   These can vary depending on your firm's specific business requirements, but may include such solutions as backup & recovery services, business continuity planning, disaster recovery, email & IM archiving, telcom services, cloud services, application hosting, consulting and project management.

2. **Depth & Quality of Staff**
   When selecting an outsourced IT provider, it is crucial to understand who you will potentially be working with. Is the organization led by a seasoned, reputable management team? Do they employ a skilled technical staff of engineers and analysts to assist with all stages of your infrastructure build-out and maintenance? What pertinent technical certifications do they hold?

   In addition to ensuring that the provider has a top quality team, it is also important to note the depth of that staff. In other words, do they have a team of engineers and analysts that is large enough to ensure that someone will be available to assist you 24x7x365 if necessary?
3. **Experience in Deployment**  
Does the service provider have deep experience in deploying these types of solutions and services in an investment management environment? Do they have experience working with funds of all sizes, from small start-ups to large, well-established firms? There are numerous outsourced IT providers out there, but be sure to select one that is experienced in deploying systems that are specific to your industry and has a solid understanding of your business environment.

4. **Project Management Experience**  
Will your firm receive the benefits of a dedicated project manager and accompanying staff to ensure that your initiatives are coordinated, designed, and implemented to your exact unique requirements? For instance, if you choose to relocate offices, does the provider have the expertise and experience to facilitate this process?

5. **Hosted/Private Cloud Infrastructure Options**  
Cloud computing has emerged as the prominent trend in investment technology this year. Look for a provider that offers a robust, scalable and secure cloud infrastructure model. Also, ensure that the infrastructure is maintained by a team of highly trained and certified professionals with experience in financial services operations. Tier III data centers (or higher) that are SAS70 certified should be used to host your firm’s critical data.

6. **Disaster Recovery Policies & Procedures**  
Does the provider maintain contingency plans or disaster recovery plans with proper risk controls designed to allow continued performance and availability at all times? How will the provider ensure that your data is secure, protected, and accessible even in the event of a disaster?
7. **Vendor Relationships**
Does the organization have strong vendor relationships in place that will allow them to leverage the benefits of best-in-class third party providers on your behalf? Strategic partnerships with top-tier technology companies are crucial to maintaining a world-class IT environment for your firm.

8. **Geographic Reach**
Does the provider have offices dispersed in different areas of the country and around the world? Do they employ staff in different time zones to ensure that assistance is available to you 24x7x365? If your firm has multiple offices, or is considering opening more in the future, ensure that you will be able to use that provider to service all regions, thereby streamlining costs and increasing efficiency.
Founded in 1995, Eze Castle Integration is the market leader in IT services, technology and consulting for hedge funds and investment management firms.

Over 600 hedge funds, managing more than $300 billion in assets, entrust their technology operations to us and for good reason. We employ the industry's best and brightest technology professionals. Our business processes are mature and our premier customer service is tailored to match the unique requirements of our hedge fund clients. Plus, we have helped launched over 1,000 hedge funds and have a deep partner network that ensures clients gain preferred access to the industry's best solutions.

On top of all that, we offer the industry's broadest portfolio of hedge fund-specific Solutions and Services including: Outsourced IT, Private Cloud Services and Managed Services, Project & Technology Management, Professional Services, Disaster Recovery and Business Continuity Planning, Archiving, Storage, Colocation and Telecommunications.

We also have offices around the world.

Contact us at:
US: +1.800.752.1382
UK: +44 207 071 6802
www.eci.com
<table>
<thead>
<tr>
<th>Founded</th>
<th>1995</th>
</tr>
</thead>
</table>
| Website & Blog| [www.eci.com](http://www.eci.com)  
[www.eci.com/blog](http://www.eci.com/blog) |
| Contact Us    | Phone:  
US: +1.800.752.1382  
UK: +44 207 071 6802  
Website:  
[http://www.eci.com/contact/index.html](http://www.eci.com/contact/index.html)  
Twitter:  
[www.twitter.com/EzeCastleECI](http://www.twitter.com/EzeCastleECI)  
Facebook:  
[www.facebook.com/EzeCastle](http://www.facebook.com/EzeCastle) |
This eBook is for general information purposes only and does not constitute Eze Castle Integration advice as to any particular set of facts.