

# Investment Adviser Business Continuity Planning

## Turning Compliance and Readiness into Competitive Advantage

January 3, 2008

By Scott P. Tarra  
Managing Principal  
[starra@financialreg.com](mailto:starra@financialreg.com)

### Introduction

Time is money. Unfortunately, for some investment advisers, business continuity planning and resumption strategies still appear to be an afterthought. However, in the event of a significant business disruption, whether it is measured in terms of days or hours, firms quickly learn to appreciate a high level of preparation and readiness in an effort to resume normal business operations as quickly as possible.

Significant business disruptions have the potential to interrupt and interfere with a firm's ability to effectively service investment advisory clients. From both an economic and strategic standpoint, firms that understand the regulatory requirements and prepare business continuity planning strategies around such considerations would appear to be in a better position to resume business operations. Therefore, the faster a firm can resume normal business operations, the less it will incur in recovery costs and the more it stands to gain in competitive advantage against other less equipped competitors.

### What is a Significant Business Disruption?

Since the disastrous events of September 11, 2001, terrorism has remained in the spotlight for the financial services industry. However, terrorism is one among many significant events that can disrupt the normal operations of a business. Therefore, for the purposes of this guide, it is important to operationally define a significant business disruption. In general terms, a significant business disruption is any event that may potentially threaten the ongoing operations of an organization, and

which may require special measures to restore normal operations.<sup>1</sup> Although firms are better prepared to deal with significant business disruptions today than in the past, firms must prepare for certain natural disasters such as fires, floods, earthquakes, storms, tornadoes, and hurricanes, and certain man-made events such as theft, vandalism and terrorist attacks. Firms should also consider the likely residual effects of both events such as possible power failure or other utility outages.<sup>2</sup> However, the most common business disruptions are less sensational to include theft, employee sabotage and equipment failures.

### Regulatory Framework

Establishing, maintaining and testing business continuity planning strategies in accordance with applicable rules can potentially increase an investment adviser's ability to resume normal business operations following a wide-scale disruption. One of the first steps in recognizing the importance of an effective business continuity plan is to understand the regulatory framework behind the requirements. The regulatory framework for establishing and maintaining a business continuity plan is addressed in the following federal, state and self-regulatory organization rules and regulations, as well as industry guidelines and best practices:

SEC Rule 206(4)-7 of the Investment Advisers Act of 1940 ("Advisers Act"). In accordance with Rule 206(4)-7, investment advisers required to be registered under

<sup>1</sup> PACE Business Continuity Planning Guide First Edition (May 1998)

<sup>2</sup> Id.; Business Continuity Planning Guidelines Texas Dept. of Information Resources December 2004

section 203 of the Investment Advisers Act of 1940 must: (i) adopt and implement written policies and procedures reasonably designed to prevent violation of the Investment Advisers Act of 1940 (“Act”) and any adopted rules thereunder; (ii) conduct an annual internal review on the adequacy of the policies and procedures and the efficacy of their implementation; and (iii) designate a chief compliance officer responsible for administering the adopted policies and procedures.

SEC Release Nos. IA 2044; IC-26299 Final Rule: Compliance Programs of Investment Companies and Investment Advisers.

When outlining the minimum requirements for developing policies and procedures, the SEC provided further clarification by recommending that advisers first conduct an internal analysis to identify any conflicts, risks and other compliance factors related to each firm’s specific size, scope and operations. Once established, firms can then develop policies and procedures that are truly customized to a firm’s compliance needs. At a minimum, the SEC outlined ten areas that firms should address when developing policies and procedures that include a business continuity plan. The SEC provided further clarification by stating that “...an adviser’s fiduciary obligation to its clients includes the obligation to take steps to protect the clients’ interests from being placed at risk as a result of the adviser’s inability to provide advisory services after, for example, a natural disaster or, in the case of some smaller firms, the death of the owner or key personnel. The clients of an adviser that is engaged in the active management of their assets would ordinarily be placed at risk if the adviser ceased operations.”<sup>3</sup>

Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System. On April 7, 2003, the Federal Reserve, the Office of the Comptroller of the Currency, and SEC issued the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System in an effort to identify certain business continuity planning

practices for key market participants. As a result of the new risks posed in the post 9/11 risk environment, the paper emphasized three new business continuity objectives for all financial institutions:

- Rapid recovery and timely resumption of critical operations following a wide-scale disruption;
- Rapid recovery and timely resumption of critical operations following the loss or inaccessibility of staff in at least one major operation location; and
- A high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible.<sup>4</sup>

The paper also identified four sound practices with a focus on minimizing the immediate effects of a wide-scale disruption on critical financial markets:

- Identification of clearing and settlement activities in each critical financial market in which a firm is a core clearing and settlement organization or plays a significant role. *Firms should conduct an internal assessment of its systems that serve a significant role in the performance of clearing and settlement activities.*
- Determination of appropriate recovery and resumption objectives for clearing and settlement activities in support of critical markets. *Emphasis is placed on the relative consistency and reliability related to recovery-time objectives for clearing and settlement activities, with considerations for circumstantial factors including time, scope and severity of disruption. Core clearing and*

<sup>3</sup> SEC Release Nos. IA-2044; IC-26299 Final Rule: Compliance Programs of Investment Companies and Investment Advisers

<sup>4</sup>Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System April 7, 2003; SEC Release No. 34-47638; the agencies concluded that all financial firms have a role in improving the resilience of the financial system because of the interdependence in the network of interrelated markets and participants and therefore should review their business continuity planning and incorporate these objectives to the fullest extent practicable.

*settlement organizations should be able to resume clearing and settlement activities within the business day on which the disruption occurs with the overall goal of achieving recovery and resumption within two hours after an event.*<sup>5</sup>

- Maintenance of sufficient geographic dispersion of resources to meet recovery and resumption objectives. *Firms should maintain sufficient distance between primary and secondary or other back-up locations related to operations and data centers. Although specific proximity between office locations is not discussed, back-up locations should be sufficiently distant from the primary office to avoid being subject to the same risks and to avoid relying on the same infrastructure components (e.g., transportation, telecommunications, water supply, and electric power).*
- Routine use or testing of recovery and resumption arrangements. *Adviser firms are encouraged to periodically test primary and back-up facilities with markets, core clearing and settlement organizations, and third-party service providers to ensure connectivity, capacity, and the integrity of data transmission.*

SEC Policy Statement: Business Continuity Planning for Trading Markets. On September 23, 2003, the SEC issued a policy statement which recommended basic principles to business continuity planning for self-regulatory organizations operating trading markets (SRO Markets) and electronic communications networks (ECNs). Because the trading markets are an instrumental component to the overall financial sector, the SEC and other financial regulators have focused their attention on the need for more rigorous business continuity planning to address problems of wider geographic scope and longer duration than those previously addressed.

Although primarily focused on trading markets, this Policy Statement can also benefit investment advisers as part of the overall financial sector. And because investment advisers may be affected by a protracted disruption to trading markets, the following recommended principles can assist in providing a prompt and smooth resumption of trading following a wide-scale disruption:

- Each SRO Market and ECN should have a business continuity plan that anticipates the resumption of trading, in the securities traded by that market, no later than the next business day following a wide-scale disruption.
- There must be geographic diversity between primary and backup sites and these sites should not rely on the same infrastructure components (e.g., transportation, telecommunications, water supply, and electric power).
- The SRO Markets also should assure the full resilience of important shared information systems, such as the consolidated market data stream generated for the equity and options markets.
- The effectiveness of back-up arrangements should be confirmed through ongoing testing.
- Each SRO Market and ECN should implement plans reflecting these principles by the end of 2004.

The Financial Planning Association Template Investment Adviser Compliance Policy Manual. As an additional tool for investment advisers, in 2005, the FPA designed a template policy manual<sup>6</sup> to help FPA-member firms who wish to create their own investment adviser compliance policy manual and to comply with the SEC's requirements for advisers registered under the Investment Advisers Act of 1940. As part of the template policy

---

<sup>5</sup> Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System April 7, 2003

---

<sup>6</sup> The Financial Planning Association Template Investment Adviser Compliance Policy Manual Fall 2005

manual, the FPA included the following key minimum topics to consider when preparing a disaster recovery/business continuity plan:

- Roles and responsibilities of employees;
- Procedures for evacuating employees in the event of a disaster, including identification of a central meeting place;
- Procedures for contacting clients and key service providers (including, maintenance of client contact information outside of the office);
- Procedures for accessing “mission critical systems” (e.g. access to client accounts and trading systems);
- Procedures for back-up and recovery of electronic and paper records (e.g. maintenance of a back-up of all critical electronic and paper records in a fire proof safe outside of the office); and
- Alternative location to conduct business (often, an employee’s house – or, preferably, the option of two employees’ houses); and
- Business continuity matters (i.e. what will the firm do in the event an owner retires or passes away?).

### **State Regulatory Requirements**

In an effort to increase uniformity with investment adviser regulation and align with recently adopted and long-standing SEC rules and interpretations, certain states have proposed or adopted rules pertaining to business continuity planning.

To check on specific state requirements for business continuity plans, adviser firms are encouraged to review state specific rules and regulations which are typically available on each state’s Website. A useful resource for facilitating this review is the North American Securities Administrators Association (NASAA) website<sup>7</sup> which

includes *Contact Your Regulator*<sup>8</sup> for a list of state regulatory agency contact information and the *Directory of Securities Laws & Regulations*<sup>9</sup> which allows access to websites of NASAA members containing information about individual state, provincial, or territorial securities laws, rules and regulations.

For example, in the State of California, the Commissioner of Corporations proposed certain rules under the Corporate Securities Law of 1968 (“Corporate Securities Law”) relating to the regulation of investment advisers which included a proposal for business continuity plans.<sup>10</sup>

*Section 260.238.4 of Title 10 of the California Code of Regulations. This proposal requires an investment adviser to adopt and implement a business continuity plan. The plan must specify how an investment advisory business would respond to emergencies of varying scope. In general, the business plan may be tailored to the size and scope of the investment advisory business. The plan must be in writing and must specify how an investment adviser would address situations that disrupt the advisory business (e.g., alternative communications channels between an investment adviser and its clients). The plan must also provide certain specified safeguards for clients in the event of death or incapacitation of the investment adviser. For example, the investment adviser must specify how clients will be notified in the event of death or incapacitation of the investment adviser. Finally, the investment adviser would be required to disclose the nature of the plan to clients. This rule is necessary to protect the interests and assets of clients in situations that disrupt the investment advisory business of the investment adviser.*

<sup>8</sup> [http://www.nasaa.org/about\\_nasaa/2062.cfm](http://www.nasaa.org/about_nasaa/2062.cfm)

<sup>9</sup> [http://www.nasaa.org/Industry\\_\\_\\_Regulatory\\_Resources/Directry\\_of\\_Securities\\_Laws\\_\\_\\_Regulations/](http://www.nasaa.org/Industry___Regulatory_Resources/Directry_of_Securities_Laws___Regulations/)

<sup>10</sup> The California Corporations Commissioner extended the public comment period through February 1, 2008 for proposed changes to the rules under the Corporate Securities Law of 1968 relating to the regulation of investment advisers.

<sup>7</sup> <http://www.nasaa.org>

## Considerations for Dual Registered Firms (FINRA Member Broker-Dealers)

NASD Rule 3510—Business Continuity Plans. In accordance with Rule 3510, FINRA member firms must; (i) create and maintain a written business continuity plan identifying procedures to be followed in the event of an emergency or significant business disruption. The business continuity plan must be made available immediately upon request to the NASD staff; and (ii) conduct an annual assessment on the efficacy and functionality of its business continuity plan to determine whether any modifications are necessary in light of changes to the firm's operations, structure, business and/or location.

The general requirements for the creation of a firm's business continuity plan are flexible enough to allow for certain customization based on a firm's size, scope and operational function. However, in accordance with NASD Rule 3510, Release No. 34-46444 and Notice to Members (NTM) 02-23, 04-37, 05-57, and 06-31, FINRA requires that all member firms meet a minimum of basic standards. The following is a list of the minimum standards for addressing critical issues in the preparation and implementation of business continuity planning and procedures:

1. Data back-up and recovery (hard copy and electronic). *The process and frequency under which the firm conducts back-up copies of its critical customer data should be properly disclosed. A firm should set clear frequency guidelines for conducting back-up copies of all relevant client information on a daily, weekly, quarterly and/or annual basis, based on its size, scope and operation function. All client data should be stored on a firm's computer server/tape or through other electronic format. Firms are encouraged to save back-up tape that should be appropriately labeled and serialized for proper recording and organization of each back-up file.*
2. All mission critical systems. *Firms should analyze internal systems that*

*are considered necessary to ensure prompt and accurate processing of securities transactions, including, but not limited to, order taking, order entry, execution, comparison, allocation, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts and the delivery of funds and securities.*<sup>11</sup>

3. Financial and operational assessments. *Firms should prepare a set of written procedures that include the identification of changes in its operational, financial, and credit risk exposures.*<sup>12</sup>
4. Alternate communications between customers and the member. *Firms should ensure that its customers have some form of alternate contact information to facilitate the communication process in the event of a significant business disruption.*
5. Alternate communications between the member and its employees. *Firms should ensure that all key or essential personnel have the proper means of communication, such as cellular phones or other acceptable electronic and/or mobile communications, to facilitate the communication process in the event of a significant business disruption. Email lists and cellular phone numbers and other relevant contact information pertaining to all key and essential personnel will be programmed and documented to facilitate access and enhance connectivity between critical staff and key personnel. Some of the various methods of communication can be e-mail, two-way text messaging, instant messaging, and/or other portable messaging devices.*
6. Alternate physical location of employees. *Firms should ensure that all key or essential personnel are informed of all alternate locations and*

<sup>11</sup> 17 C.F.R. § 240.15b7-3T(g)(1) (2001); NASD Notice to Member 02-23

<sup>12</sup> Release No. 34-46444; File No. SR-NASD-2002-108

are assigned to specific alternate locations to promptly resume business operations.

7. Critical business constituent, bank, and counter-party impact. *Firms should adequately address and analyze the potential impact of a significant business disruption might cause to existing business constituents (i.e. any business entity that maintains a business relationship with the firm regarding the support of the firm's operational activities), banks, and counter-parties (i.e. other broker/dealers or institutional customers).*
8. Regulatory reporting. *Certain regulatory filings are maintained on the CRD system for future use and retrieval purposes. In the event that a firm experiences a significant business disruption, it may attempt to access the IARD system through its User Name and Password information within a certain time period to ensure the CRD system is in operating order. Each firm should also maintain copies of each current Form BD, U4/U5 and other relevant filings appropriate schedules for future use.*
9. Communications with regulators. *Each FINRA member firm should maintain telephone and Internet access capabilities at the main office and the designated off-site facility. This may facilitate any required communications with federal, state and/or self-regulatory organization (SRO) agencies. As an alternate method, firms should also maintain an electronic (CD) and hardcopy list of all SEC regional offices, State securities agencies and any other regulatory agencies that firms may be affiliated with such as the FINRA, CFTC, NFA etc.*
10. How the member will assure customers' prompt access to their funds and securities in the event that the member determines that it is unable to continue its business. *Firms should focus on establishing alternate written procedures and operational processes*

*for accessing customer funds and/or securities in the event that the firm is unable to continue normal business operations.*

**NASD Rule 3520—Emergency Contact Information.** In accordance with Rule 3520, FINRA member firms must: (i) report to FINRA emergency contact information for the member including designation of two emergency contact persons. Each emergency contact person shall be a member of senior management and a registered principal of the member; and (ii) promptly update its emergency contact information in the event of any material change, and must review and, if necessary, update its emergency contact information, including the designation of two emergency contact persons, promptly, but in any event not later than thirty days following any change in such information, as well as to review and, if necessary, update the information within seventeen business days after the end of each calendar year to ensure the information's accuracy.<sup>13</sup>

### **Business Continuity Plan Life Cycle**

When preparing a business continuity plan, it is equally important to understand the five stages of a business continuity plan life cycle. Investment advisers should incorporate all five stages which include analysis, design, implementation, testing and maintenance. Each stage provides the foundation for the overall business continuity plan process which includes the regulatory framework and minimum regulatory requirements under SEC examination process.

1. **Analysis.** As the first stage in developing a sound business continuity plan, investment advisers should conduct an internal risk analysis that includes a thorough assessment of all associated risks and exposure to its external and internal environment. Such assessment should also include a business impact analysis that includes potential costs and damages incurred by a particular business disruption (high vs. low impact). Other considerations should include recovery resources and

<sup>13</sup> FINRA Regulatory Notice 07-42, SEC Approves NASD Rule 1160 Regarding Firm Contact Information; effective December 31, 2007

strategies that support the organization's mission and mitigate risks to an acceptable level. These include a prioritization of internal systems and processes, personnel responsibilities, resource requirements, and primary and alternate recovery strategies.

2. **Design.** The second stage is the preparation of a business continuity plan that is customized to an investment adviser's size, scope and operations while also meeting regulatory requirements and industry best practices. The customization process should consider associated risks, business impacts, and recovery resources and strategies and their interconnectivity under the current regulatory framework.
3. **Implementation.** Once designed, firms must work to implement its planning and processes to ensure prompt resumption of business operations in the event of a disruption. This typically includes top-down support from senior executives, mid-level managers and frontline employees alike to implement planning directives in accordance with internal analysis and design.
4. **Testing.** The fourth stage, and an ongoing process, is for firms to routinely test its business continuity and resumption planning and processes to ensure that critical internal and external continuity arrangements are effective and compatible. The testing should incorporate all associated back-up systems and facilities to include telecommunication firms, third-party service providers, and securities exchanges. Proper testing of a business continuity plan, to include simulations, may also detect possible flaws in the planning and execution stages that may require necessary adjustments.
5. **Maintenance.** In today's constantly changing regulatory environment, it is not enough to simply prepare business continuity plan. Firms must work to provide ongoing updates and maintenance to remain relevant and up-to-date with material changes in key personnel, advances in technology, communications, and infrastructure. A business continuity plan should also be inclusive of current material changes in SEC, FINRA and/or

applicable state rules and regulations and industry best practices. Therefore, the establishment of a business continuity plan should be viewed as a dynamic document subject to a periodic and routinely scheduled review and maintenance.

### **Business Continuity vs. Disaster Recovery**

While most disaster recovery plans tend to address data recovery processes and technology access, they do not adequately address the total needs of the organization. A business continuity plan, which includes a disaster recovery plan, focuses on the total procedures and alternative processing for critical business functions; "it keeps key operations operating while systems are recovered."<sup>14</sup> Therefore, business continuity planning suggests a more comprehensive approach to ensuring productivity through the maintenance of critical business operations.<sup>15</sup>

### **Business Continuity Planning vs. Succession Planning**

While most succession plans tend to address the replacement of top executives and/or key personnel involved in the decision making process of critical business functions, they also do not adequately address the total needs of the organization. A business continuity plan, which generally includes a succession plan, focuses on the overall operations of the organization and the importance that key personnel play in maintaining critical business functions. Therefore, business continuity planning suggests a more comprehensive approach to ensuring productivity through the cross training and positioning of key personnel involved in the decision making process.

### **Regulatory Expectations and the SEC Examination Process**

For federal covered investment advisers, the SEC is reviewing business continuity plans as part of assessing operation risk under their Internal Controls and Risk Management examination. During SEC routine examinations, requests for business continuity plans have become a standard practice with a focus on meeting general regulatory requirements, while also addressing more specific

---

<sup>14</sup> Business Continuity Planning: Are You Prepared? By Jonathan Nobis & Dennis Bagley Security Assurance *Universal Advisor*, 2004 Issue No. 1

<sup>15</sup> CSO Fundamentals: The ABCs of Business Continuity and Disaster Recovery Planning (May 1, 2006)

areas and processes in light of a firm's scope and complexity. However, both SEC and state registered investment adviser firms stand to benefit from understanding the regulatory expectations and minimum requirements of business continuity plans. This typically includes a review of the following areas and processes:

- Senior Management Involvement. The commitment and support of management is critical to the success of a firm's business recovery effort.<sup>16</sup> This typically includes top-down support from senior executives, mid-level managers and frontline employees alike to properly implement a firm's business continuity planning initiatives. Members of senior management should work with all departments including personnel, information technology, trading and operations, to foster an integrated or "shared" approach toward business continuity and recovery.
- Adequacy of Resources. Firms must maintain certain resources such as people, equipment, processes, and supplies necessary for the recovery of core business operations.<sup>17</sup>
- Review and Update of the Plan. Once prepared, firms must continually review and provide ongoing updates to remain current with changing regulatory requirements as well as the inevitable changes in growth and functionality of the firm. A business continuity plan should also include material changes in applicable state rules and regulations and industry best practices.
- Employee Training. Firms are encouraged to establish an ongoing training program to promote firm-wide awareness of business resumption processes and recovery functions. Creating awareness may take the form of holding training presentations, discussing planning topics during employee training and new hire orientation, interviewing staff and management, issuing articles, memos or other relevant materials, and working with auditors and risk managers to provide a true snapshot on a

firm's level of readiness. Training should include (i) necessary action to be taken by staff in the event of a significant business disruption; (ii) detailed assignments and clear responsibilities of staff members; (iii) emergency procedures of essential systems and operations; (iv) procedures for back-up locations; (v) ongoing communications with management and staff; and (vi) action required to restart operations.<sup>18</sup>

- Testing. Firms should routinely test its business continuity and resumption planning and processes to ensure that critical internal and external continuity arrangements are effective and compatible. The testing should be conducted on a periodic and regularly scheduled basis. Firms are recommended to conduct testing no less frequently than annually and more frequently if a firm experiences material changes to any critical component to its business continuity plan.
- Coverage of Critical Areas. Firms should conduct a thorough analysis to define specific critical areas and core business processes and resources needed to minimize the impact of interruption. Some critical areas include key personnel, information systems and technology, trading and operations, financial and accounting systems, and telecommunications. Firm should include a focus on cross training key staff to ensure sufficient continuity of critical functions related to systems and operations.
- Back-up Facilities. A back-up facility is an alternate location operated by the firm, or contracted via a company that specializes in disaster recovery services. In the event of a significant business disruption, a firm must make the transition to alternate facilities and resume business functions and support services at those alternate facilities. There are generally three main types of back-up facilities, including cold, warm and hot sites with the difference between each site determined by the costs and effort required to operate each alternate location.

---

<sup>16</sup> Business Continuity Planning Guidelines Texas Dept. of Information Resources December 2004

<sup>17</sup> Business Continuity Planning: Are You Prepared? By Jonathan Nobis & Dennis Bagley Security Assurance *Universal Advisor*, 2004 Issue No. 1

---

<sup>18</sup> PACE Business Continuity Planning Guide First Edition (May 1998)

- Cold Site- a cold back-up site requires the least amount of costs and operational effort. It generally does not include back-up copies of data or information from the firm's original location, nor does it include pre-established hardware. However, because there is no pre-existing set-up of technology or operations, a cold site requires the most time to operate at normal capacity after a significant business disruption.
- Warm Site- a warm back-up site is a location that already maintains technology hardware and software similar to the firm's original location but does not maintain back-up copies of data or information.
- Hot Site- a hot back-up site is a location that is a duplicate of the firm's original location to include fully redundant information technology systems, communication systems, as well as complete back-ups of user data and information. Hot sites exist to facilitate the relocation of offices with minimal loss to normal operations. Although most expensive to operate, hot sites provide the best opportunity to resume normal operations within the shortest time period.<sup>19</sup>
- Coverage of Third Party Vendors and Major Counterparties and Customers. Although a disruption might not affect a firm directly, it may affect one or more third-party service providers that a firm relies on to conduct its day-to-day operations. Therefore, it is not only important for a firm to maintain its own business continuity plan, but also from third-party service providers that are considered instrumental in the firm's normal operations. Additionally, firms should conduct an analysis on how a loss of

operations to selected third-party services providers may impact its business by identifying the level of reliance on each third-party and the types of functions that require third-party involvement. The ultimate objective is to "identify those tangible and intangible assets and relationships that are susceptible to compromise during an emergency situation."<sup>20</sup>

- Short-term and Long-Term Strategies. Firms are encouraged to establish a two-tiered approach to business resumption planning in terms of short-term and long-term strategies. This two-tiered approach provides certain consideration for the type and level of business disruptions, and creates a recovery timetable for resuming business operations in light of varying degrees of business impact. Critical timing elements for short-term strategies may range from several hours to five days, while long-term strategies may range from several weeks or months. Short-term and long-term strategies may also affect the use of select back-up facilities such as cold, warm or hot sites based on the duration of the disruption and available resources necessary to continue normal operations.
- Communication Alternatives. Similar to FINRA requirements, firms should ensure that all key or essential personnel have the proper means of communication, such as cellular phones or other acceptable electronic and/or mobile communications, to facilitate the communication process in the event of a significant business disruption. Email lists and cellular phone numbers and other relevant contact information pertaining to all essential personnel should be documented to facilitate access and enhance direct communications. Some acceptable methods of communication include phone, e-mail, internet, two-way text messaging, instant messaging, and/or other portable messaging devices.
- Data Back-up Timing and Capacity. The more critical the data and electronic media, the more frequently the back-up process.

<sup>19</sup> Records Management Services (2004, July 15). Vital Records: How Do You Protect And Store Vital Records? Retrieved from the UW Records Management Web site: <http://www.washington.edu/admin/recmgt/vital.store.html>; Haag, Cummings, McCubbrey, Pinsonneult, and Donovan (2004). Information Management Systems, For The Information Age. McGraw-Hill Ryerson

<sup>20</sup> Contingency Planning And Rule 206(4)-7 By Oren Chaplin and Thomas Giachetti; Financial Advisor Magazine October 5, 2004

Loss of critical and sensitive data can ultimately delay the recovery process which tends to result in a loss of time and money. Data and electronic media should be thoroughly analyzed and categorized by frequency of back-up (e.g. daily, weekly, monthly, quarterly, annually and periodic).

By understanding the regulatory framework, following the various stages of the life cycle, and meeting the regulatory expectations and minimum requirements for business continuity plans, investment advisers will be well positioned to resume business operations after a significant disruption, and to mitigate compliance deficiencies resulting from a regulatory examination.

### **Use of Consultants**

As an additional resource, when outsourcing or co-sourcing certain functions of the business continuity plan life cycle, the use of consultants is often a good idea in an effort to save time, money and expertise by providing a clear guidelines and focal points based on current regulatory requirements. The three key benefits of using consultants to assist in the preparation of a business continuity plan are as follows:

Time. The coordination of key principals and/or staff to prepare a business continuity plan often takes a considerable amount of time away from normal assigned tasks and therefore may be analyzed in terms of a utility cost to the firm. To facilitate this process, consultants often work from an existing business continuity plan framework which addresses both regulatory requirements and industry best practices and will obtain necessary client information to include in its existing framework to provide for a customized version based on a firm's internal processes.

Cost. From an economic perspective, the allocation of personnel to prepare a business continuity plan may be analyzed in terms of a utility cost to the firm, which is a measurable metric. Additionally, for more complex firms with several departmental layers, the allocation of key personnel specializing in particular areas such as technology and information systems, trading, back-office, and operations, may take even longer to organize each respective section and manage the

production of the final product. Therefore, to reduce the costs associated with preparing a new business continuity plan, certain consultants provide a ready-made approach for a reasonable price as an economically feasible alternative.

Expertise. Because the financial industry is dynamic and subject to constant regulatory change, the use of consultants becomes a value added consideration due to a consultant's ability to provide up-to-date information by focusing on ongoing regulatory updates to SEC, state and other applicable rules and regulations. Additionally, a consulting firm or individual consultant who participates in regulatory examinations, and who maintains a national presence with clients across other districts and regions will have the insight of leveraging unforeseen regulatory focal points, changes and expectations as they occur during the examination process. Once learned, consultants will often apply these newly learned requirements to their procedures in anticipation future regulatory requirements and/or expectations.

### **Conclusion**

Today's investment advisers are inextricably bound to technology in an effort to improve operations and become more efficient. The byproduct of greater efficiency is greater profitability. However, some investment advisers address business continuity strategies by focusing solely on technology, while others focus on personnel issues. Regardless of the scope and complexity of the operations, investment advisers should balance these two general considerations for the completion of a well designed plan that will facilitate the restoration of normal business operations.<sup>21</sup>

Investment advisers should also work toward improving operations and efficiency by mitigating disruptive events which could impede its growth and expansion efforts. Successful investment adviser firms focus on both opportunities and risks associated with its business operations. Recognizing and properly planning for threats to an organization's ongoing operations can help mitigate

---

<sup>21</sup> Contingency Planning And Rule 206(4)-7 By Oren Chaplin and Thomas Giachetti; Financial Advisor Magazine October 5, 2004 Business Continuity Planning: Are You Prepared? By Jonathan Nobis & Dennis Bagley Security Assurance *Universal Advisor*, 2004 Issue No. 1

risk while building trust and confidence among investment advisory clients. Investment advisers that are well equipped and better prepared to restore business operations over their competitors will be in a better position to serve tomorrow's advisory clients.

---

Mr. Tarra is a Managing Principal with Financial Registrations, Inc., a compliance management consulting firm providing registration and compliance advisory services to securities broker/dealers and registered investment advisers. For more information on this topic or other compliance related matters, please contact:

Scott P. Tarra  
Managing Principal  
[starra@financialreg.com](mailto:starra@financialreg.com)

Financial Registrations, Inc.  
25602 Alicia Parkway #107  
Laguna Hills, CA 92653  
[www.financialregistrations.com](http://www.financialregistrations.com)

Toll-free (800) 641-1818  
Direct (949) 770-6154  
Fax (949) 770-6198