

# Business Continuity Planning for Advisers

---

by Lorna A. Schnase

## **INTRODUCTION**

Business continuity planning (BCP) should be an integral part of every adviser's risk management effort. This article provides basic information about BCP for advisers and their compliance personnel. The first part addresses key questions about BCP, such as what SEC authority governs BCP, how advisers might go about BCP, what other advisers are doing about BCP and what other resources are available to help. The second part discusses some practical ideas about designing and testing an adviser's plan and provides a sample matrix for assessing and addressing business continuity risk.

## **RULES, GUIDANCE, RESOURCES**

***What is BCP? Does it mean what will we do if our founding partner dies or what will we do if our computer systems go down?***

It means both. BCP is sometimes called contingency planning, disaster recovery planning, business disruption planning, crisis management and various other names, but in general it means planning for any foreseeable event that could cause a material business disruption. The aim of BCP is to avoid or minimize disruptions and to recover as rapidly and efficiently as possible from lost functionality should a disruption occur.

BCP should include succession planning to minimize disruption following the death or other unavailability of a founding partner or other critical personnel. This is particularly true for smaller advisers whose very existence may depend on the continued availability of one or a handful of key individuals.

For all advisers, BCP should include planning for natural disasters such as hurricanes, earthquakes, floods and pandemic illness, as well as man-made disasters due to terrorism, civil disorder, strikes and the like. Smaller scale events may be even more foreseeable and therefore should be considered in the process, such as localized power outages, building fires and shortages of critical supplies, services or personnel.

Of course, any or all of these events could impact an adviser's computer systems, which should therefore be addressed in any BCP undertaken by an adviser. Advisers must also satisfy their obligations under the books and records requirements of Rule 204-2(g) under the Investment Advisers Act of 1940 (Advisers Act), which sets specific standards an adviser's records must meet if they are maintained in electronic form requiring, among other things, that records be reasonably protected from alteration, loss or destruction.

***What guidance has the SEC provided advisers on BCP?***

Over the years, the SEC and its Staff have provided BCP guidance in various forms:

**Compliance Rules.** The SEC named business continuity as one of the 10 key areas advisers (and funds) should consider when creating their compliance programs, stating:

“We believe 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>1</sup>

**Top Inspection Deficiency.** The SEC Staff listed “business continuity plans were not established and/or tested” as a top deficiency at the 2008 CCO Outreach<sup>2</sup> Regional Seminars for advisers and funds. This deficiency was listed under the section relating to Information Processing and Protection. Examples of specific deficiencies were:

- An adviser's BCP did not include provisions for loss of access to its facilities; and
- A small adviser did not have procedures or contingencies in the event of the death or incapacitation of the owner.<sup>3</sup>

**Inspection Criterion.** The SEC Staff listed points it looks for in examining a broker-dealer's BCP, as part of a review of the firm's Internal Controls and Risk Management, stating: “Some [BCP] areas we cover are:

- senior management involvement;
- adequacy of resources;
- review and update of the plan;
- employee training;
- testing;
- coverage of critical areas;
- back-up facilities;
- coverage of third party vendors and major counterparties and customers;
- short-term and long-term strategies;
- communication alternatives; and
- data back-up timing and capacity.”<sup>4</sup>

These points are equally relevant to an adviser's BCP.

**ComplianceAlert.** Disaster recovery was one of only four topics that OCIE (the SEC Office of Compliance Inspections and Examinations) chose to address in its inaugural ComplianceAlert aimed at advisers.<sup>5</sup> The alert focused mainly on “lessons learned” from Hurricane Katrina and listed a number of provisions in advisers' disaster recovery plans that appeared effective in aiding post-disaster recovery, including:

- having a pre-arranged remote location for short-term and possible long-term use;
- having alternate communication protocols to contact staff and clients, such as cell phones, text messaging, web-based email accounts or an Internet website;
- having remote access to business records and client data through appropriately secured means that ensure ongoing compliance with Regulation S-P (privacy regulations) and other confidentiality requirements;
- arranging temporary lodging for key staff where necessary as a result of a relocation of the firm;

- maintaining accurate and up-to-date contact information for all third-party service providers, including custodians, broker-dealers, transfer agents, pricing services and research firms;
- becoming familiar with the business continuity plans of third-party service providers;
- making contingency arrangements for loss of key personnel, such as the president or primary portfolio manager, either temporarily or permanently;
- training staff on how to fulfill essential duties in the event of a disaster, including compliance matters;
- conducting periodic testing, evaluation and revision of disaster preparedness; and
- maintaining sufficient insurance and financial liquidity to prevent any interruption to the performance of compliant advisory services.

**Recovery Goals.** The SEC has set a next-business day resumption goal for self-regulatory organizations and electronic communications networks, which it said should serve as a useful benchmark for securities firms as well.<sup>6</sup>

Completely aside from SEC requirements, advisers now find that having an adequate BCP is a fundamental, dollars-and-cents competitive issue, given that many institutional clients will include assessing an adviser's BCP as part of their routine due diligence in deciding whether to hire and retain an adviser.

***What are an adviser's obligations if it maintains electronic books and records?***

As referenced above, almost any business disruption could affect an adviser's computer systems, and electronic malfunctions, corruption, crashes, attacks, outages and other problems remain high on the list of potential BCP triggers.

The SEC is acutely aware of the vulnerability of an adviser's electronic records and spelled out in the Advisers Act books and records rule, Rule 204-2, specific standards an adviser's records must meet if they are maintained in electronic form. These provisions are sorely outdated (still referring to microfiche and microfilm) and often overlooked. Nonetheless, they should be taken into consideration as advisers implement their compliance programs and formulate their continuity plans.

Specifically, subpart (g) of the rule spells out the following requirements for all "micrographic and electronic" records required to be maintained and preserved by advisers under the rule.

**General requirements.** The adviser must:

- Arrange and index the records in a way that permits easy location, access and retrieval of any particular record;
- Provide promptly any of the following that the SEC may request:
  - A legible, true and complete copy of the record in the medium and format in which it is stored;
  - A legible, true and complete printout of the record; and
  - Means to access, view and print the records; and

- Separately store, for the time required for preservation of the original record, a duplicate copy of the record on any medium allowed under the rule.

Among other things, these requirements dictate that advisers consider their document storage and retrieval capabilities (note the words “easy” and “promptly” in the rule), their back-up arrangements for preserving duplicate records and their ability to *access, view and print* archived records, including those that were generated using legacy software and hardware systems that may no longer be in use.

Special requirements for electronic storage media. In addition to the above general requirements, advisers must establish and maintain procedures with regard to their electronic records:

- To maintain and preserve the records, so as to reasonably safeguard them from loss, alteration or destruction;
- To limit access to the records to properly authorized personnel and the SEC; and
- To reasonably ensure that any reproduction of a non-electronic original record on electronic storage media is complete, true and legible when retrieved.

These points are fundamental to any sound records management system and should serve to underpin the electronic records component of an adviser’s BCP.<sup>7</sup>

***What are the basic steps of BCP and where can advisers get help?***

Advisers that need or want help in developing a continuity plan have a lot to choose from these days, given that there is an entire BCP industry offering services in developing, implementing, monitoring and testing plans. Indeed there is now a recognized BCP profession comprised of individuals who may achieve professional BCP certifications and who may be hired in-house or as free-lance consultants to assist firms with their BCP.

Whether an adviser chooses to seek outside assistance or to develop a plan on its own, the basic steps of BCP will likely boil to something like this:

Step 1) Business Impact Analysis. Business Impact Analysis involves assessing and prioritizing the critical business functions within the advisory firm and determining the impact of not performing those business functions beyond the maximum acceptable outage. Critical business functions might include things like portfolio management, client communications, HR functions, back office operations and so on.

Impacts might include consequences to clients or customers (or loss of clients and customers), legal or regulatory consequences (such as missing regulatory filing deadlines), and the like. Plans are then developed to recover those critical functions within established RTOs (recovery time objectives) at established RPOs (recovery point objectives).

A well-executed Business Impact Analysis will require an adviser to think through all components of its business, not just its core client service functions, but also information technology, personnel/staffing, communications, logistics, relationships with vendors for services and supplies, and so on. Specific questions an adviser should be asking to identify and prioritize critical functions and impacts in this process include:

- Which firm functions are mission critical to serving clients’ needs on various time frames -- hourly, daily, weekly, monthly, quarterly and annually?
- What critical interdependencies exist between internal systems, applications, business processes and departments?

- What specialized equipment is required and how is it used?
- How would a particular function work (or not) if the mainframe, server, network and/or Internet were not available?
- What single points of failure exist and how significant are those risks?
- What are the critical outsourced relationships and dependencies?
- How are responsibilities divided between the adviser and its outsourced providers in the service agreement between them?
- What is the minimum number of critical staff and amount of space that would be required at a recovery site?
- What mission critical equipment and communications systems would be necessary to operate from a recovery site?
- What is the impact if the same recovery site provider is serving multiple businesses all located in the same geographic area?
- Can mission critical employees operate adequately from home or another off-site location if necessary? Is that dependent on their having access to servers or other equipment, files, systems or other items located at the principal office?
- Have employees been cross-trained in back-up functions and roles so they can cover in the event of unanticipated unavailability of key personnel?
- Are the personal and family needs of personnel being adequately considered?
- What critical cash management and liquidity needs are likely in the event of a crisis?
- What conditions must exist before the continuity plan is invoked and who is authorized/responsible for determining when those conditions exist?

For example, an advisory firm might identify managing and trading client accounts as one of its critical business functions. It might also identify loss of account value (and resulting loss of fees, loss of client goodwill and the like) as an impact that could occur if the adviser were not able to perform that account management and trading function beyond a maximum outage of say, four hours (the RTO established for that function). The adviser might then determine that in order to recover that function, it needs a minimum of three portfolio management personnel with on-line connectivity to specific identified brokerage firms, trading venues, market monitoring databases and so on. The adviser can then plan the steps necessary, in the face of a disruption, to have those personnel relocated to an off-site RPO, with the identified on-line connectivity within the established RTO.

Step 2) Risk Assessment. This step goes hand-in-hand with Step 1 and involves evaluating the Business Impact Analysis under various potential threat scenarios. Potential threats should be prioritized based on probability of occurrence and severity of impact. Threats could include natural disasters, man-made threats or threats of an unknown cause.

For example, a firm located in a hurricane zone would identify hurricanes as a potential threat, with a reasonably high likelihood of probability and a potentially severe impact. Then the firm would determine whether the BCP procedures it intends to use in Step 1 for maintaining critical functions within established RTOs is adequate in light of the identified hurricane threat, asking questions such as is the off-site recovery location sufficiently far from the hurricane zone as to allow for smooth recovery within the critical time period?

Step 3) Risk Management. This step includes on-going management of the risk of a business disruption through techniques such as development and dissemination of a written plan, ensuring that the plan is reviewed and updated routinely, continually assessing potential threats and interdependencies within the firm, and pursuing mitigation strategies, including appropriate training and drilling of personnel.

For example, a firm would make sure that all its employees know what the firm's BCP entails and what their roles are in the plan. It would have employees participate in training exercises and/or drills on a regular basis aimed at ensuring smooth functioning of the plan in the event of a real disruption. On an ongoing basis, the firm might pursue basic mitigation strategies such as:

- protecting its computers from viruses, spyware and hackers;

- continually upgrading the stability of its data systems and remote operating capabilities;
- maintaining state-of-the-art fire suppression systems in its offices;
- routinely updating its calling tree and employee contact database;
- establishing back-up or redundant service provider relationships; establishing back-up or redundant power supplies; and
- maintaining back-up inventories of critical equipment.

### ***What are other advisers doing about BCP?***

In a 2007 industry survey,<sup>8</sup> 93% of adviser respondents indicated that they had a written business continuity plan, covering areas such as:

- facility-wide outages (electrical, fire) (92%)
- temporary interruption of discrete services (Internet, telephone, server) (89%)
- natural disasters (flood, earthquake, hurricane) (85%)
- terrorist attack (50%)
- death or disability of key personnel (succession planning) (47%) and
- pandemic flu (25%).

However, advisers reported wide variability in testing of their plans. Some firms conducted full tests annually (28%) or only every few years (5%). Others conducted only partial tests on a periodic basis (annually 25%, quarterly 9%, monthly/rolling 8%). Some 18% indicated that they take BCP into account when assessing vendors.

While most adviser respondents (90%) said they had established a back-up site, over a third of them (37%) had not yet tested a physical shift of operations and personnel to that site. Similarly, 89% of respondents had established an employee communications system, although 49% had not tested the system.

Not surprisingly, the firms most likely to have not established or tested a system were smaller firms (1-5 employees). But notably, some 25% of all survey respondents had not tested any aspect of their BCP at all, although many of those indicated that they intended to be testing within the next year and therefore presumably have by now.

Under the lead of SIFMA (Securities Industry and Financial Markets Association), the securities industry conducts periodic industry-wide emergency preparedness tests.<sup>9</sup> These tests include participants from the major exchanges, clearing banks, payment systems, market data providers and service bureaus. However, an overwhelming majority (96%) of the adviser respondents in the 2007 industry survey indicated that they had not participated in any industry-wide disaster preparedness drills.

### ***What other BCP resources are available?***

There are numerous other BCP resources available to help firms plan. Many of these resources are aimed at the financial services industry, such as:

- The Investment Adviser Association makes available to its members a Guide to Establishing and Implementing a Compliance Program for Investment Advisers.<sup>10</sup> One section of the Guide is devoted to Contingency Planning and Procedures. It discusses key items such as:
  - Forming a business continuity committee.
  - Distributing and training personnel on the BCP.
  - Communications with employees during a crisis.
  - Workplace recovery.
  - Back-up communications and records storage.
  - Utilities, including phone, Internet and so on.

- Communications with clients and other key contacts (landlord, emergency services and so on).
  - Pricing/valuation of portfolios, particularly if disaster is widespread and affects markets.
  - Loss of key personnel.
  - Third-party service provider relationships (brokers, custodians, sub-advisers, pricing services, transfer agents, administrators and the like) and assessing their readiness.
- The MFA (Managed Funds Association) has issued Sound Practices for Hedge Fund Managers addressing Business Continuity and Disaster Recovery in Chapter 7.<sup>11</sup>
  - The SEC posted “Spotlight on: Business Continuity Planning” on its website,<sup>12</sup> providing links to numerous other SEC materials concerning business continuity planning at the SEC, with the exchanges and with various financial institutions in the aftermath of 911 and Hurricane Katrina.
  - FINRA (Financial Industry Regulatory Authority, the SRO for broker-dealers) has a Business Continuity Planning webpage,<sup>13</sup> which includes a BCP template for a small introducing firm and a Case Study aimed at helping a small firm ask questions and frame its business continuity planning.
  - SIFMA (Securities Industry and Financial Markets Association) has posted on its website a document addressing areas to consider when validating a BCP and suggesting methodologies to use to measure the capabilities of the plan.<sup>14</sup>
  - FFIEC (Federal Financial Institutions Examinations Council) has posted extensive BCP information and links on its website.<sup>15</sup>
  - DRI International is a non-profit organization founded to develop a knowledge base concerning contingency planning and the management of risk, with numerous resources, educational opportunities and materials available on its website.<sup>16</sup>
  - FEMA has posted an Emergency Management Guide for Business and Industry, which includes a step-by-step guide on how to conduct BCP and hazard-specific information.<sup>17</sup>
  - OSHA has issued How to Plan for Workplace Emergencies and Evacuations (2001 revised), which includes specific steps for emergency planning.<sup>18</sup>
  - The SEC, Federal Reserve System and Treasury Department issued an Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.<sup>19</sup>

## **PRACTICAL IDEAS FOR DESIGNING AND TESTING A BUSINESS CONTINUITY PLAN**

### ***What are some key elements advisers should include in their BCP?***

BCP has many key elements in common with every other procedure adopted as part of an adviser’s compliance program, such as:

- Management’s buy-in is helpful, if not critical.

- Input from as many employees as is practical is important when formulating the plan.
- The process should tie into the firm's overall risk assessment, identifying and prioritizing risks and their potential consequences to the adviser and its clients.
- Procedures should be focused on addressing the higher priority risks, with appropriate but less urgent focus on lower priority risks.
- Roles and responsibilities for implementing and executing the plan should be made clear as part of the plan.
- The plan should be disseminated to all employees and training should be made available to ensure everyone understands the plan.
- The plan should be tested routinely.
- The plan should be reviewed and updated routinely.

### ***How might an adviser go about testing its plan?***

The aim of testing an adviser's plan is to achieve a high level of confidence that critical internal and external continuity arrangements are effective and compatible. Of course, it is better to identify weaknesses and gaps in the plan in a test situation rather than in a real crisis where the well-being of the adviser's personnel or clients may be at stake.

Often advisers need to get creative in testing their plan because full-scale testing can itself cause a disruption and is not always practical. However, testing just individual components of the plan can be effective and conducted with less risk of unwarranted disruption.

In addition, testing of the plan as a whole can be undertaken in varying degrees of intensity. One less intensive type of testing is known as a "**tabletop exercise**" where key players attend a meeting to discuss BCP and walk through various components of the plan. Roles and responsibilities are discussed and refined. Potential issues and problems are identified and addressed in a less time-critical and stressed situation. While this type of testing can be an effective planning tool, it is not a high-level type of testing and is generally not considered a substitute for more "real-life" testing.

A more intensive type of testing is referred to as a "**walk-through drill**" or simulated test. In this type of test, a particular scenario is chosen for participants to simulate under the plan. This involves wider employee participation and can be helpful to identify functional response capabilities, demonstrate knowledge and skills, test employee interactions and hone decision-making capabilities. Role playing can be used to practice critical steps. Recovery teams can be mobilized to practice coordination and cooperation without invoking the actual recovery process.

Yet another level of intensity is involved in an actual "**functional drill**" or parallel test. This involves actually mobilizing personnel to other sites in order to test availability, functionality, coordination and communications, with a real-time test of any redundant, back-up or recovery systems utilized under the plan. The more employees this type of test involves, the better the test will be to ensure smooth functioning in a real-life situation. Participants can get real-time experience with command and control, evacuation routes and procedures for employee accountability. Team leaders can get practice in assessment, operations and implementation. Varying degrees of actual – as opposed to simulated – recovery and back-up systems can be mobilized.

The highest level, most intensive test is the "**full-interruption/full-scale**" test. This type of test simulates a full-scale emergency, as close to real-life as possible, and is usually not undertaken until full planning and testing at lesser levels of intensity have been successfully completed. All or virtually all personnel are required to participate, with internal and external coordination with other teams of emergency personnel, including where appropriate local emergency management or law enforcement personnel. All back-up and recovery systems are tested, off-site locations activated and evacuation routes practiced. While this type of test may be best suited to identifying potential weaknesses in the plan as applied to a real-life situation, it can also put personnel and clients' interests at risk so should be planned and executed with due care.

Of course, whenever an adviser experiences a real-life business interruption triggering its business continuity plan, the plan is effectively tested. At an appropriate time after that test, a rigorous analysis should be conducted to determine how well the plan functioned and how it could be improved.

***How might an adviser document its BCP process?***

The sample matrix in Appendix A spells out various risks an adviser might face when developing a business continuity plan, what procedures might be used to address those risks and various ways those specific procedures might be tested short of a full-scale test of the entire plan. This is one way an adviser might document the process by which it assessed, designed and tested its plan.

The matrix does not constitute a complete business continuity plan and might not be suitable for every adviser given how widely firms vary in their needs. However, it is offered as an illustration of how an adviser might think through these steps in the BCP process.

**CONCLUSION**

No adviser is immune from the risk of a significant business disruption, as both natural and man-made disasters in the last decade have underscored. To mitigate the effects of a disruption, advisers should adopt a business continuity plan tailored to their circumstances. The information in this article will help advisers better understand how to design, implement and test such a plan.

\* \* \*

*The information in this article is provided strictly as a courtesy to readers for educational purposes. It does not constitute legal advice, nor does it establish or further an attorney-client relationship. All facts and matters reflected in this article should be independently verified and should not be taken as a substitute for individualized legal advice.*

**APPENDIX A**  
**SAMPLE MATRIX FOR INVESTMENT ADVISER BUSINESS CONTINUITY PLANNING**

<i>What risk is being addressed?</i>	<i>What procedure might address that risk?</i>	<i>How can the procedure be tested?</i>
Loss of data due to computer system crash or similar internal IT problem.	<p>Establish and activate off-site servers or “mirror” sites to ensure firm’s electronic data, files and client records are backed up routinely, allowing for as close to full functionality as possible once crash occurs and off-site back-up systems are activated.</p> <p>Consider need to use redundant back-up systems located in a different part of the country, not susceptible to the same types of natural or man-made disasters that may be affecting adviser’s primary location.</p> <p>Maintain back-up inventories of critical system components – servers, monitors, PCs, laptops, PDAs, communications devices, Internet access, etc.</p>	Randomly test access to back-up files or records to ensure that they can be retrieved intact in a timely fashion.
Loss of normal power supply affecting accessibility of data and computer systems, etc.	Obtain redundant or alternative power supply, such as a UPS (uninterruptible power supply – backup battery or generator that kicks in when electrical power is unavailable) for primary and/or recovery office locations.	Arrange for cut-off of normal power supply on test basis, to make sure redundant or alternative supply kicks in as expected.
Building fire affecting availability of personnel, office location, data, client records, etc.	<p>Ensure adequate fire suppression system is in building and/or key areas within adviser’s offices.</p> <p>Train personnel on evacuation plans.</p>	<p>Request routine testing of fire suppression systems from landlord or system vendor.</p> <p>Drill personnel on announced and unannounced building evacuations.</p>
Long-term or permanent loss of key portfolio management or other personnel affecting ability to continue to assist all clients, access their records, and service their accounts, etc.	<p>Cross-train personnel in different job functions.</p> <p>Ensure that at least one other portfolio manager/advisor has a working knowledge of each client’s account.</p> <p>Ensure that appropriate firm personnel are not “locked” out of client records by passwords known only by one person.</p>	<p>Have personnel step into another employee’s position on a temporary basis, to see whether their cross-training has been adequate.</p> <p>Simulate unavailability of PM/advisor and have another PM/advisor step in to handle account for a temporary period.</p> <p>Randomly test firm’s “administrative rights” to access all areas of firm’s servers holding firm or client information.</p>

<p>Loss of founding partner, principal owner or other key personnel affecting client perception of firm as an ongoing concern and/or implicating Advisers Act "change of control"</p>	<p>Ensure that firm owners have wills, trusts or other instruments in place so that change of ownership upon death is understood by remaining personnel who can plan accordingly.</p> <p>Prepare in advance for measures necessary to replace lost personnel or continue firm with remaining personnel, including client contacts, consent to "change of control" (if applicable) and disclosure updates.</p>	<p>Randomly test checklists or "maps" providing guidance to remaining firm personnel on what to do in the case of death or long-term unavailability of founder, owner or other key personnel, to ensure they are accessible, up-to-date and understandable.</p>
<p>Loss of access to office facility due to natural or man-made disaster</p>	<p>Contract or license off-site back-up or recovery facility with enough seats or desks to accommodate all mission critical personnel.</p> <p>Ensure that principal technology systems, servers, online services, etc., can be duplicated at off-site location.</p> <p>Train personnel on how and when to access off-site facility.</p> <p>Establish employee capabilities for working from home or other ad-hoc temporary location (alternative residence, hotel, temporary office, etc.).</p>	<p>Run a table-top exercise with all personnel or, in larger firm, with key personnel by area or department, to think through the ins and outs of accessing the off-site back-up facility or other alternative remote location and make sure all the angles have been thought of in advance.</p> <p>Randomly test access to off-site back-up facility or other alternative remote location on an unannounced basis.</p>
<p>Loss of ability to communicate in-person with firm personnel due to disaster</p>	<p>Establish firm "calling tree" designating who is authorized to trigger the calling tree, which employees will be reaching which other employees and how each employee can be reached (home, cell phone or other alternative communications methods).</p> <p>Consider need for alternative methods of communications (land line, cell phone, IM/texting, Internet, etc.) in the event that ISP, cell towers or other communications systems are unavailable.</p>	<p>Test a "dry run" of the calling tree, attempting to communicate a particular instruction or message throughout the firm during non-working hours.</p>

<p>Financial strain or capital inadequacy due to business interruption event</p>	<p>Retain insurance agent, broker or consultant to help identify insurance needs and obtain appropriate coverage.</p> <p>Make sure this includes key employee life insurance in appropriate circumstances, particularly if firm has obligation to buy out surviving spouse or heirs/devisees of founder's or former owner's interest in firm.</p> <p>Plan for firm's capital reserve or borrowing needs in light of foreseeable interruption events.</p>	<p>At least annually, get assurances from firm insurance agent, broker or consultant that insurance coverage is still adequate.</p>
<p>Loss of critical third-party provided service due to interruption affecting that party</p>	<p>Consider third-party provider's own BCP when assessing them for hiring or retention.</p> <p>Establish any back-up relationships that might be needed on a reasonably foreseeable basis.</p>	<p>Participate in third-party provider's own BCP testing.</p> <p>Have third-party provider report results of its own periodic BCP testing to adviser.</p>

---

## ENDNOTES

<sup>1</sup> See Final Rule: Compliance Programs of Investment Companies and Investment Advisers, Release Nos. IA-2204; IC-26299 (December 17, 2003) at <http://www.sec.gov/rules/final/ia-2204.htm> (emphasis added).

<sup>2</sup> The SEC's CCO Outreach program is now known as the Compliance Outreach program.

<sup>3</sup> See the "Top Deficiencies Identified in Examinations" handout at <http://www.sec.gov/info/cco/topdeficiencies2008.pdf>. See also Speech by SEC Staff: Focus Areas in SEC Examinations of Investment Advisers: the Top 10, by Lori A. Richards, Director of the SEC's OCIE, at the IA Compliance Best Practices Summit 2008 (March 20, 2008) at <http://www.sec.gov/news/speech/2008/spch032008lar.htm>.

<sup>4</sup> See Speech by SEC Staff: Disaster Recovery and Business Continuity Planning, by Mary Ann Gadziala, Associate Director of the SEC, at Financial Markets Association 2003 Compliance Seminar (May 1, 2003) at <http://www.sec.gov/news/speech/spch050103mag.htm>.

<sup>5</sup> See the June 2007 ComplianceAlert at: [http://www.sec.gov/about/offices/ocie/complialert.htm#P62\\_10475](http://www.sec.gov/about/offices/ocie/complialert.htm#P62_10475).

<sup>6</sup> See Speech by SEC Staff: International Financial Institutions Examination Issues: A Regulatory Perspective, Annual Regulatory Examination and Compliance Seminar, Institute of International Bankers, by Mary Ann Gadziala, Associate Director, OCIE (October 31, 2006) at <http://www.sec.gov/news/speech/2006/spch103106mag.htm> (emphasis added).

<sup>7</sup> For a more general discussion of the books and records requirements for advisers, see E.J. Yerzak and Keith Marks, "Records Management for Investment Advisers," *Practical Compliance and Risk Management for the Securities Industry* (November-December 2011).

<sup>8</sup> See the Summary Report of the 2007 Investment Management industry survey listed on the IAA's website at [https://www.investmentadviser.org/eweb/dynamicpage.aspx?webcode=PN\\_RB](https://www.investmentadviser.org/eweb/dynamicpage.aspx?webcode=PN_RB). BCP was also mentioned in the 2008 edition of the Investment Management survey as one of the compliance areas that advisers had most commonly amended since the beginning of 2007.

<sup>9</sup> See <http://www.sifma.org/services/bcp/industry-testing/>.

<sup>10</sup> This is available in a password protected members-only portion of the IAA website at <https://www.investmentadviser.org>.

<sup>11</sup> See MFA Sound Practices for Hedge Fund Managers (2009 Edition) posted on the MFA's website (<https://www.managedfunds.org/>).

<sup>12</sup> See Spotlight on Business Continuity Planning at <http://www.sec.gov/spotlight/continuity.htm>.

<sup>13</sup> See Business Continuity Planning at <http://www.finra.org/RulesRegulation/IssueCenter/BusinessContinuityPlanning/index.htm>.

<sup>14</sup> See "Testing Methodologies for Validating Business Continuity Plans" (published January 2008), compiled by the SIFMA Business Continuity Planning Committee, Best Practices Subcommittee, at <http://www.sifma.org/uploadedfiles/services/bcp/sifma-testing-methodologies.pdf>.

<sup>15</sup> See the FFIEC Business Continuity Planning webpage at <http://ithandbook.ffiec.gov/resources/business-continuity-planning.aspx#>.

<sup>16</sup> See <https://www.drii.org/>.

<sup>17</sup> See <http://www.fema.gov/business/guide/toc.shtm>.

<sup>18</sup> See <http://www.osha.gov/Publications/osha3088.html>.

<sup>19</sup> See SEC Release No. 34-47638 at <http://www.sec.gov/news/studies/34-47638.htm>.