

Business Continuity Planning for Investment Advisers

By

**Lorna A. Schnase
Attorney at Law**

August 25, 2008

This information is provided strictly as a courtesy to readers for educational purposes.

**This information does not constitute legal advice,
nor does it establish or further an attorney-client relationship.
All facts and matters reflected in this paper should be independently verified
and should not be taken as a substitute for individualized legal advice.**

**Lorna A. Schnase, Attorney at Law
713-741-8821 (p)
<http://www.40actlawyer.com>**

INTRODUCTION

Business continuity planning (BCP) should be an integral part of every adviser's compliance program. The first part of this paper addresses basic questions about BCP for advisers. The second part lists some practical ideas about testing an adviser's BCP and related procedures.

The Basics

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?

Both. BCP is sometimes called contingency planning, disaster recovery planning, business disruption planning, crisis management and various other names, but in general means planning for any foreseeable event that could cause a material disruption to a business. The aim of BCP, of course, is to avoid or minimize disruptions and to recover as rapidly and efficiently as possible from lost functionality following an event in order to continue to conduct business.

For smaller advisers, BCP should include succession planning aimed at minimizing disruption following the death or disability of a founding partner or other key personnel. For all advisers, BCP should include planning for natural disasters such as hurricanes, earthquakes, floods, pandemic illness and the like, as well as man-made disasters due to events such as terrorism, riots and strikes. Smaller scale events may be even more foreseeable and therefore should be considered in the process, such as localized power outages, building fires, unavailability or shortages of critical supplies, services or personnel.

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

What guidance has the SEC provided advisers on BCP?

- **Compliance Rules.** The SEC named business continuity as one of the 10 key areas advisers (and funds) should focus on when creating their compliance programs under the compliance rules, 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.”

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).

- **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 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.

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>.

- **Inspection Criterion.** The Staff has identified points it looks for in examining a broker-dealer firm’s BCP, as part of their review of Internal Controls and Risk Management. This can be analogized to investment advisory firms.

“Some 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.”

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>

- **ComplianceAlert.** Advisers’ disaster recovery plans was one of only 4 topics that the SEC chose to address in its first ComplianceAlert issued to CCOs in June 2007 under the CCO Outreach program. The alert focuses mainly on “lessons learned” from Hurricane Katrina and lists a number of provisions in advisers’ disaster recovery plans that appeared effective in aiding advisers to recover after a disaster. The ComplianceAlert and list can be accessed here: http://www.sec.gov/about/offices/ocie/complialert.htm#P62_10475.
- **Recovery Goals.** The SEC has set a next-business day resumption goal as a benchmark for securities firms following a wide-scale disruption, stating:

“While the Sound Practices White Paper does not address the recovery or resumption of trading operations or retail financial services, the SEC issued, on September 25, 2003, a policy statement on ‘Business Continuity Planning for Trading Markets’.[citation omitted] This release stated it was the SEC’s belief that Self Regulatory

Organizations (SROs) and Electronic Communications Networks (ECNs) should prepare for the timely resumption of trading in the event of a 'wide-scale disruption' and specified principles to be applied for business continuity planning. The SEC also stated that the establishment of a next-business day resumption goal for the SROs and the ECNs should serve as a useful resumption benchmark for securities firms as well, recognizing that this is, in essence, a matter of business judgment."

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).

Completely aside from SEC requirements, advisory firms are now finding that having an adequate BCP can become a basic, dollars-and-cents competitive issue, given that many institutional investors 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 the basic steps of BCP?

Advisers that need or want help in developing their BCP 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 certain recognized BCP certifications and who may be hired in-house or as free-lance consultants to assist firms with BCP.

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

1) BIA – 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, HR functions, back office operations, etc. Impacts might include impacts to clients or customers (or loss of clients and customers), legal or regulatory impacts (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 as to 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 plan is invoked and who is authorized/responsible for determining when those conditions exist?

So, 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, etc.) 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, 4 hours (the RTO established for that function). The adviser might then determine that in order to recover that function, it needs a minimum of 6 portfolio management personnel with on-line connectivity to specific identified brokerage firms, 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.

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.

So, 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?

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.

So, 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 on BCP?

In a 2007 industry survey, 93% of adviser respondents stated 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%)
- pandemic flu (25%)

However, advisers reported wide variability in testing of their BCPs. 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% of adviser respondents 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.

Under the lead of SIFMA (Securities Industry and Financial Markets Association), the securities industry has conducted a number of industry-wide emergency preparedness tests. See <http://www.sifma.net/bcp/index.shtml>. These tests included participants from most of the major exchanges, clearing banks, payment systems, market data providers and service bureaus. Not surprisingly, 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.

The 2007 Investment Management industry survey referenced above can be accessed here: <http://www.investmentadviser.org/public/2007%20IM%20Testing%20Report.pdf>.

BCP was also mentioned in the latest edition (2008) of the Investment Management survey, as one of the compliance areas that advisers had most commonly amended since the beginning of 2007. The 2008 survey can be accessed here: http://www.investmentadviser.org/public/compliancetestingurvey_report-2008.pdf.

What other resources are available?

- IAA Guide to Establishing and Implementing a Compliance Program for Investment Advisers, section on Contingency Planning and Procedures, available in the password protected members-only section of the IAA website at <http://www.investmentadviser.org/>. This 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, etc.

- Communications with clients and other key contacts (landlord, etc.).
 - 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, etc.) and assessing their readiness.
- Managed Funds Association, Sound Practices for Hedge Fund Managers, at <http://www.managedfunds.org/downloads/Sound%20Practices%202007.pdf> (see Section 7 on Business Continuity, Disaster Recovery and Crisis Management).
 - SEC Spotlight on: Business Continuity Planning, at <http://www.sec.gov/spotlight/continuity.htm>, with links to numerous other SEC materials concerning business continuity planning at the Commission, with the exchanges and with various financial institutions in the aftermath of 911 and Hurricane Katrina.
 - FINRA, Business Continuity Planning resources webpage at <http://www.finra.org/RulesRegulation/IssueCenter/BusinessContinuityPlanning/index.htm>, including a BCP Template for a small introducing firm at <http://www.finra.org/RulesRegulation/IssueCenter/BusinessContinuityPlanning/p006464> and a Case Study, aimed at helping a small firm ask questions and frame its business continuity planning at http://www.finra.org/web/groups/rules_regs/documents/rules_regs/p006467.pdf.
 - SIFMA Business Continuity Planning Committee, Best Practices Subcommittee compiled “Testing Methodologies for Validating Business Continuity Plans” at http://www.sifma.org/services/business_continuity/pdf/SIFMA-Testing-Methodologies.pdf.
 - Federal Financial Institutions Examinations Council, Business Continuity Planning, IT Examinations Handbook, March 2008 at http://www.ffiiec.gov/ffiecinfbase/booklets/bcp/bus_continuity_plan.pdf.
 - Disaster Recovery Institute, an organization founded to develop a knowledge base concerning contingency planning and the management of risk, at <http://www.drii.org/DRII/>
 - FEMA Emergency Management Guide for Business and Industry, which includes a step-by-step guide on how to conduct BCP and hazard-specific information at <http://www.fema.gov/business/guide/toc.shtm>.
 - OSHA How to Plan for Workplace Emergencies and Evacuations (2001), which includes specific steps for emergency planning at <http://www.osha.gov/Publications/osha3088.pdf> .
 - Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, SEC Release No. 34-47638; File No. S7-32-02, at <http://www.sec.gov/news/studies/34-47638.htm>.

Practical Ideas for Testing an Adviser's BCP

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

- 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.

Testing. The aim of testing an adviser's BCP 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 BCP because full-scale testing itself can cause a disruption and is not always practical. However, testing just individual components of the BCP can be effective and helpful and usually undertaken with less risk of unwarranted disruption.

In addition, testing of the BCP 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 the 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 BCP. 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 BCP. 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 BCP 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.

* * *

BCP Matrix

Following is a sample matrix that spells out various risks an adviser might face in BCP, 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 BCP. The matrix does not constitute a complete BCP 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 go about thinking through these steps in the BCP process.

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 backed 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>

<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 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>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>	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.
Loss of access to office facility due to natural or man-made disaster	<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>
Loss of ability to communicate in-person with firm personnel due to disaster	<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, call 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>	Test a "dry run" of the calling tree, attempting to communicate a particular instruction or message throughout the firm during non-working hours.

<i>What risk is being addressed?</i>	<i>What procedure might address that risk?</i>	<i>How can the procedure be tested?</i>
Financial strain or capital inadequacy due to business interruption event	<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>	At least annually, get assurances from firm insurance agent, broker or consultant that insurance coverage is still adequate.
Loss of critical third-party provided service due to interruption affecting that party	<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>