



Business Continuity Plan
Summary

Last updated: January 2010

I. Overview of This Document

Advisors Asset Management, Inc. (AAM) maintains a comprehensive Business Continuity Plan (BCP). The BCP is an internal document that is not available to the public. This document, the Business Continuity Plan Summary is intended to provide our customers and other interested parties with information regarding our BCP.

II. Contacting Us

If after a significant business disruption you cannot contact us as you usually do at (800) 697-7220, you should call our alternative number (800) 347-5128, or go to our web site at www.aam.us.com. If you cannot access us through either of those means, you should contact our clearing firm; Pershing, at (201) 413-3635, or www.pershing.com, for instructions on how they may assist you with some types of security, cash disbursement, and security transfer transactions for your customers.

III. Firm Policy

Our firm's policy is to respond to a Significant Business Disruption (SBD) by safeguarding employees' lives and firm property, making a financial and operational assessment, quickly recovering and resuming operations, protecting all of the firm's books and records, and allowing our customers to transact business with minimal disruption.

Significant Business Disruptions (SBDs)

Our plan anticipates two kinds of SBDs, internal and external. Internal SBDs affect only our firm's ability to communicate and do business, such as a fire in our building. External SBDs prevent the operation of the securities markets or a number of firms, such as a terrorist attack, a city flood, earthquake, or a wide-scale, regional disruption. Our response to an external SBD relies more heavily on other organizations and systems, especially on the capabilities of our clearing firms, Pershing or NFS.

It is impossible to list every type of event that might trigger an SBD. Generally speaking, any event that disrupts any of our branches could become an SBD. The senior corporate managers together with managers at an affected branch will determine on a case by case basis the expected extent of the disruption in order to decide whether or not to begin execution of this plan.

Examples of potential SBDs include fire, earthquake, flood or other events that can destroy or incapacitate one of our offices. Also, power outages and loss of communications that last longer than an hour could become an SBD. In many cases it may be difficult to determine whether or not an outage should trigger our Business Continuity Plan. In the event of a power outage or communications failure, our CEO and/or COO will determine whether or not to implement this plan based on the expected duration of the outage, the time of day, and all other information available to them at the time.

Note that we do not consider a computer failure to be an SBD. All critical servers are backed up on-site and off-site, and standby servers are maintained on-site and off-site. Therefore, although a server failure might cause a short disruption of service, it should not cause an SBD.

The AAM Internal Backup and Recovery Plan documents all of our servers, and the backup and recovery plans in place.

IV. Customers' Access to Funds and Securities

Our firm does not maintain custody of customers' funds or securities, which are maintained at our clearing firms, Pershing and National Financial Services LLC (NFS). In the event of an internal or external SBD (if telephone service is available) our registered persons will take customer orders or instructions and contact our clearing firms on their behalf. If Web access is available, our firm will post on our Web site instructing Retail customers that they may access their funds and securities by contacting Pershing at 201-413-3635 or 213-624-6100 extension 500. AAM will make this information available to customers through our disclosure policy.

V. Data Back-Up and Recovery (Hard Copy and Electronic)

Electronic Data

Our primary data center is in our San Diego branch. Our database servers and other mission critical servers are all located in our San Diego data center.

Data on all of our mission critical servers is backed up to backup servers either throughout the day or at least each night (depending on the type of data and its importance). Data is also backed up onto tape drives at geographically separated locations. In addition, all mission critical data on our servers is backed up to our San Antonio backup data center either throughout the day or in a batch each night.

Data on our servers in each of the other branches is backed up to our San Diego data center each night. Therefore, at any given point of time, we can recover data from our branch offices as of the previous night.

In the event of an SBD in any of the branches other than San Diego, the San Diego data center will provide a backup system for the affected branch. In the event of an SBD in our San Diego branch, we will shift to our backup data center in our San Antonio branch.

Our recovery objectives address Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO). Our RPO for critical data is 5 minutes, meaning that we should not lose more than 5 minutes of transactions in the case of an SBD at our data center. Our RTO is 4 hours, meaning that if we have to shift to our backup data center in San Antonio, our goal is to have our critical systems operational within 4 hours. Our goals are based on an SBD that is local to our office area. Widespread disruptions such as terrorist attacks or national communications disruptions could adversely affect our ability to continue processing from our backup data center.

Hard Copy

Our firm maintains its primary hard copy books and records at our Monument branch. Important documents are kept in a fireproof vault with offsite copies kept at a storage facility.

VI. Operational Assessments

AAM has branches in four geographically separate regions, and data centers in San Diego and San Antonio. In the event of an SBD in any one city, we will be able to continue operations in the other cities. We will be able to communicate with customers using our website, email, and/or telephones. Backup data (both electronic and hard copy) will be retrieved as described above.

VII. Mission Critical Systems

Our firm's "mission critical systems" are those that ensure prompt and accurate processing of securities transactions, including order taking, entry, execution, comparison, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts, and the delivery of funds and securities. Both AAM and our clearing firms Pershing and NFS perform mission critical tasks for our customers.

A. Pershing Mission Critical Systems

Our clearing firm, Pershing, maintains customer accounts and is responsible for delivery of funds and securities to our customers. Pershing has its own Business Continuity Plan which we have reviewed, and we expect that Pershing will be able to recover from an SBD at their primary office.

Recovery-time objectives provide concrete goals to plan for and test against. They are not, however, hard and fast deadlines that must be met in every emergency situation, and various external factors surrounding a disruption, such as time of day, scope of disruption, and status of critical infrastructure—particularly telecommunications—can affect actual recovery times. Recovery refers to the restoration of clearing and settlement activities after a wide-scale disruption; resumption refers to the capacity to accept and process new transactions and payments after a wide-scale disruption. Pershing has the SBD recovery time and resumption objective of 4 hours.

B. National Financial Mission Critical Systems

Our clearing firm, NFS, maintains customer accounts and is responsible for delivery of funds and securities to our customers. NFS has its own Business Continuity Plan which we have reviewed, and we expect that NFS will be able to recover from an SBD at their primary office.

Recovery-time objectives provide concrete goals to plan for and test against. They are not, however, hard and fast deadlines that must be met in every emergency situation, and various external factors surrounding a disruption, such as time of day, scope of disruption, and status of critical infrastructure—particularly telecommunications—can affect actual recovery times. Recovery refers to the restoration of clearing and settlement activities after a wide-scale disruption; resumption refers to the capacity to accept and process new transactions and payments after a wide-scale disruption.

C. Our Firm's Mission Critical Systems

AAM uses a proprietary software system called Bailey to manage all trade related activity. Telephone orders are received by our registered reps and they enter the order into Bailey. Web orders are automatically set up in the Bailey order system. Orders are sent to our traders who allocate bonds from our inventory to the customer placing the order, or in the event where we do not already own the bonds, our trader will attempt to buy the bonds from other dealers.

Bailey handles the communications between our registered reps and our traders. When a trade is executed, Bailey sends the trade information to our clearing firms, Pershing or NFS.

In the event of an SBD, orders could still be taken by phone from one of the unaffected branches. We have registered reps engaged in customer service in multiple branches. We also have traders in multiple branches, and traders in an unaffected branch could execute trades on behalf of traders in a branch where an SBD occurred.

Our website, which could run from San Diego or from our backup facility in San Antonio, will advise our customers that a branch is experiencing an SBD. Customers will be advised to call an alternate branch for service. Our registered reps in any branch have the information and skills they need to fill in for the reps in any branch affected by an SBD.

In order to operate, Bailey requires a number of computer servers. These servers are located in our San Diego data center. The servers are backed up to standby servers in the San Diego data center and also to our alternate data center in our San Antonio branch.

In the event of an external SBD that prevents us from trading with other firms, we will enter the orders into Bailey and execute the orders by phone as soon as we and other firms are able to conduct business again.

VIII. Alternate Communications Between the Firm and Customers

We now communicate with our customers using the telephone, e-mail, our Web site, fax, and U.S. mail. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party. For example, if we have communicated with a party by e-mail but the Internet is unavailable, we will call them on the telephone and follow up where a record is needed with paper copy in the U.S. mail or fax.

IX. Critical Business Constituents

We have assessed the products and services provided to us by our critical business constituents (businesses with which we have an ongoing commercial relationship in support of our operating activities, such as vendors providing us critical services), and determined the extent to which we can continue our business relationship with them in light of the internal or external SBD. We will quickly establish alternative arrangements if a business constituent can no longer provide the needed goods or services when we need them because of a SBD to them or our firm.

X. Updates and Annual Review

Our firm will update this plan whenever we have a material change to our operations, structure, business or location. In addition, our firm will review this BCP Summary annually, in December. Any changes to the plan will be distributed to our website and interested parties by the end of January each year.

XI. For More Information

If you have questions about our Business Continuity Plan you can contact us at (800) 697-7220.