iad
INTERNAL AUDITORS DIVISION
An Affiliate of SIFMA™

Internal Audit Guidelines

Business Continuity Plan

August 2007

The Audit Guidelines (the "guidelines") are intended to provide members of the Internal Auditors Division (“IAD”), an affiliate of the Securities Industry and Financial Markets Association (“SIFMA”) with information for the purpose of developing or improving their approach towards auditing certain functions or products typically conducted by a registered broker-dealer. These guidelines do not represent a comprehensive list of all work steps or procedures that can be followed during the course of an audit and do not purport to be the official position or approach of any one group or organization, including IAD or any of its divisions or affiliates. Neither IAD, nor any of its divisions or affiliates, assumes any liability for errors or omissions resulting from the execution of any work steps within these guidelines or any other procedures derived from the reader's interpretation of such guidelines. In using these guidelines, member firms should consider the nature and context of their business and related risks to their organization and tailor the work steps accordingly. Internal auditors should always utilize professional judgment in determining appropriate work steps when executing an audit.

INTERNAL AUDITORS DIVISION
A Division of SIFMA

TABLE OF CONTENTS

iad INTERNAL AUDITORS DIVISION

A Division of SIFMA

I. Introduction and Background

I. INTRODUCTION AND BACKGROUND

A. Overview

A Business Continuity Plan ("BCP") enables a Firm and its employees to survive a disaster and to re-establish normal business operations within the timeframes set out by the business heads. In order to sustain business, we must assure that critical operations can resume normal processing within these reasonable timeframes. A disaster could result in short-term or long-term delays in production processing. Both types of delays could result in different recovery methods (i.e., normal backup / recovery vs. invoking "hot-site" recovery).

A BCP should ensure:

- The development, implementation, testing and maintenance of business continuity and emergency response plans enable the business to protect its assets and meet its business recovery objectives.

- Prevention and mitigation activities reduce the likelihood and impact of a disruption.

- Management provides an employee awareness program.

- The Information Technology ("IT") contingency plans (i.e., mainframe and distributed) support the business recovery objectives.

- Addresses a process for reconstruction of physical locations needed to continue operations in the event that a primary location is destroyed or uninhabitable for a long period of time.

B. Backup and Recovery

Back-up and recovery procedures should be in place to ensure that the company can recover from any form of failure, whether it is the loss of one record or the entire computing facility. The procedures for backup and recovery need to be reviewed from the standpoint of day-to-day backup and contingency planning.

Backup and recovery are the day-to-day processes in place to enable us to recover from short-term, localized processing errors, or loss of equipment or data. Back-up copies of all data should be made on a regular basis to ensure that the data can be restored in as complete a manner as possible in the event of a processing failure. Back-up copies should also be stored off-site to make sure they are not destroyed by the same disaster that requires them to be used.

In general, the following principles with respect to backup and recovery shall apply:

- All procedures should be documented.

- Short-term back-up copies of data should be made to facilitate recovery from processing failure.

- Copies should be made at regular intervals and several generations of backup should be maintained because errors are not always discovered as they occur and data may need to be recovered from some time ago.

- Full system backup should be taken to provide current copies of operating software and application systems.

- Proper storage procedures and facilities should be provided for back-up copies.

C. Examination Objective

Determine the quality and effectiveness of the organization’s business continuity planning process. These procedures will disclose the adequacy of the planning process for the organization to maintain, resume, and recover operations after disruptions ranging from minor outages to full-scale disasters. To assess the adequacy of the business continuity planning process on an enterprise-wide basis or across a particular line of business. Depending on the examination objectives, a line of business can be selected to sample how the organization’s continuity planning process works on a micro level or for a particular business function or process.

D. Management’s Role in the Audit Process

Management should establish a continuity framework which defines the roles, responsibilities and the risk-based approach / methodology to be adopted, and the rules and structures to document the continuity plan as well as the approval procedures. Management should also ensure that the IT continuity plan is in line with the overall business continuity plan to ensure consistency.

Management should ensure that a written plan is developed containing the following:

- Guidelines on how to use the continuity plan.

- Emergency procedures to ensure the safety of all affected staff members.

- Response / recovery procedures meant to bring the business back to the state it was in before the incident or disaster.

- Critical information on continuity teams, affected staff, customers, suppliers, public authorities and media.

IT management should provide for change control procedures in order to ensure that the continuity plan is up-to-date and reflects actual business requirements. This requires continuity plan maintenance procedures aligned with change and management and human resources procedures.

To have an effective continuity plan, management needs to assess its adequacy on a regular basis or upon major changes to the business or IT infrastructure; this requires careful preparation, documentation, reporting test results and, according to the results, implementing an action.

E. BCP Statutory Requirements

The audit will also focus on regulatory guidance from the NYSE Rule 446, NASD Rule 3510 (Business Continuity Plans), NASD Rule 3520 (Emergency Contact Information), and NFA 2-38. Abstracts from the relevant rules and sections are listed for reference.

NYSE Rule 446 and NASD 3510: Financial and Operational Assessments

Defines "financial and operational assessments" as "a set of written procedures that allows a member to identify changes in its operational, financial, and credit risk exposures." It also requires each member to designate a member of senior management who is also a registered principal to approve the plan and be responsible for conducting the required annual review. The review does not require the member of senior management to personally conduct all aspects of the review; however, he or she must review the final plan, including any proposed changes to the existing plan.

While a single designated member of senior management must approve the final plan, the member firm remains responsible for compliance with Rule 3510. Senior management approval is intended only to ensure that a person with proper authority reviews the plan, and not to make one person responsible for a member's compliance with Rule 3510.

NYSE Rule 446 and NASD 3510: Critical Business Constituent, Bank, and Counter-Party Impact

Members must have procedures that assess the impact that a significant business disruption would have on critical business constituents (businesses with which a member firm has an ongoing commercial relationship in support of the member's operating activities), banks (lenders), and counter-parties (e.g., other broker-dealers or institutional customers).

NYSE Rule 446 and NASD 3510: Client Disclosures

Requires each member to disclose to its customers how its business continuity plan addresses the possibility of a future significant business disruption and how the member plans to respond to events of varying scope. The minimum requirement is for an annual disclosure and should be done as internal reviews of the BCP occur.

NYSE Rule 446 and NASD Rule 3520: Emergency Contacts

Requires members to designate two emergency contact persons and provide this information to NYSE and NASD via electronic process.

NFA 2-38

Each National Futures Association ("NFA") member must establish and maintain a written business continuity and disaster recovery plan that outlines procedures to be followed in the event of an emergency or significant business disruption. The plan shall be reasonably designed to enable the Member to continue operating, to reestablish operations, or to transfer its business to another Member with minimal disruption to its customers, other Members, and the commodity futures markets.

Each Member must provide NFA with the name of and contact information for an individual who NFA can contact in the event of an emergency, and the Member must update that information upon request. Each Introducing Broker ("IB"), Commodity Pool Operator ("CPO"), or Commodity Trading Advisor ("CTA") member that has more than one principal and each Futures Commission Merchant ("FCM") member must also provide the NFA with the name of and contact information for a second individual who can be contacted if NFA cannot reach the primary contact, and the Member must update that information upon request. These individuals must be authorized to make key decisions in the event of an emergency.

F. NYSE Recommendations on Pandemic Planning

NYSE Rule 446(b): Evolving Circumstances and the threat of a Pandemic from Avian Flu

According to Exchange Rule 446(b), "member organizations must conduct, at a minimum, a yearly review of their business continuity and contingency plan to determine whether any modifications are necessary in light of changes to . . . operations, structure, business or location." The Exchange has advised that "risk assessment is an essential component of business continuity planning. When preparing, updating, and maintaining a BCP, . . . member organizations must dedicate resources to periodically assess risk factors so that plans remain viable and effective in light of evolving circumstances." At present, member organizations should assess the unique risks posed by a pandemic flu to determine whether their BCP would be viable in the event that the avian flu were to give rise to a pandemic.

Due to the unique nature of this threat a separate section of the audit guideline was created to determine if member firms have a BCP that adheres to the recommendations in the NYSE letter on this subject, an extract of the relevant section follows. In conducting this type of assessment, member organizations should consider utilizing the Federal government's Business Pandemic Influenza Planning Checklist, available at www.pandemicflu.gov/plan/pdf/businesschecklist.pdf. This checklist was used to develop the audit guidelines.

Some questions that firms should consider in light of the risks a pandemic poses to their operations include:

- Many health officials believe that a best practice would be to have a multi-tiered response determined by various pandemic-related trigger points. So, for example, if human to human transmission occurred abroad, that would trigger the firm to implement certain contingencies, whereas if an occurrence of the outbreak occurred in the U.S., which would trigger implementations of additional contingencies. Has the firm established escalating contingencies for various trigger points?

- Do the firm and/or firm service providers have the technological infrastructure and capacity in place to support widespread telecommuting and/or operations from back-up sites?

- BCPs may call for the activation of one or more back-up sites in response to certain events. The conventional use of a back-up site is as a response to a geographically localized event. Firms should consider whether a back-up site would be a viable option in the event of a pandemic. If the firm uses a vendor to provide back-up space, has the firm evaluated whether the vendor is capable of providing space in the event that multiple customers require usage simultaneously?

- Has the firm considered the impact of requiring employees to work at a remote location over a long timeframe?

- Has the firm conducted tests, including telecommuting and teleconferencing capabilities, to evaluate its ability to execute both the technological and the logistical aspects of its BCP?

- Does the firm have supervisory, surveillance, and record-keeping systems in place to permit employees to work from home for prolonged periods? Has the firm tested the functionality of such systems? Does the firm have procedures for supervising employees who work from home for prolonged periods?

- Business continuity planning for the financial industry has historically focused particular attention on firms' clearing and settlement functions as well as on trading operations, both of which are viewed as critical. Does the firm have contingencies in place that ensure functioning of these critical operations in the event of conditions including, but not limited to, limitations on travel and on public gatherings?

- Do any components of the firm's BCP involve activities or the suspension or modification of business practices that will require regulatory approval? If so, firms should start a dialogue with regulators.

- Has the firm considered the Human Resources implications of a pandemic? Such considerations include, but are not limited to, the operational and financial impact of a significant percentage of the staff being absent or taking short-term disability leave.

- The Federal government has recommended that firms establish partnerships with other members of their sector to provide mutual support and maintenance of essential services during a pandemic. Has the firm identified critical business partners, and has each party determined what it expects of the other during the various conditions that may arise in the event of a pandemic, to ensure that clearing, trading, and other critical functions remain operational? If a firm were to determine, for example, that a critical supplier does not have an adequate BCP or the capability for ensuring supply in the event of a certain trigger, the firm should investigate whether it would require alternative business partners or whether it would be able to consolidate its transactions with fewer business partners.

- How will the firm respond to a shutdown of national mass transit? Has the firm evaluated how to prevent employees from becoming stranded, or how to respond if they are stranded, in the event of a mass transit shutdown while employees are traveling on business?

- Educational programs are important tools that can help businesses remain functional in the event of a pandemic. Has the firm initiated a program to educate its employees about the potential pandemic and firm contingency plans? When considering responses to various pandemic scenarios, firms may want to read "High Level Principles for Business Continuity," which was prepared by the Joint Forum of the BASEL Committee on Banking Supervision, The International Organization of Securities Commissions, and the International Association of Securities Supervisors. Annexes II and III are Case Studies on the impact of the 2003 SARS outbreak on the Hong Kong and Canadian securities markets, respectively. Additional information is available on various government and health organization websites.

Potential Regulatory Relief

NYSE Regulation, Inc. has provided short-term relief from certain regulatory requirements during prior business interruptions. NYSE Regulation, Inc. anticipates that, in the event of a pandemic or other public health emergency, a flexible approach to regulatory requirements will be appropriate. Some of the areas of potential regulatory relief currently under consideration by NYSE Regulation, Inc. include the following:

- extensions of time for standard filing requirements;
- flexibility with respect to office space arrangements;
- delays in real-time supervision where technology monitoring is feasible;
- additional time for reconciliations;
- extensions of time relating to licensing requirements; and
- flexibility with respect to compliance with certain provisions of clearing agreements.

Further guidance as to regulatory relief will be issued by the NYSE as circumstances warrant.

G. Additional Resources

The following external resources are available as supplemental information for BCP planning by member firms and as reference material for audits of the BCP.

The 2007 Edition of the American National Standard for Disaster/Emergency Management and Business Continuity Programs (NFPA 1600).
http://www.nfpa.org/newsReleaseDetails.asp?categoryID=488&itemID=33516&cookie%5Ftest=1

SEC Interagency Paper on Sound Practices to Strengthen the Resilience of the U. S. Financial System.
http://www.sec.gov/news/studies/34-47638.htm.

NYSE Statement on Pandemic Preparations
http://www.theassetmanager.com/docs/BCP_NYSE_050506.pdf

Federal Financial Institutions Examination Council's BCP Workbook
http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf

H. Audit Scope

The scope of the audit will be established by focusing on those factors that present the greatest degree of risk to the institution and at a minimum will include the following areas:

- Business continuity policy.
- Executive sponsorship for accountability, ownership, and awareness.
- Roles and responsibilities (i.e., BCP teams, BCP committee).
- Investment / Funding.
- Employee education and awareness.
- Methodology for the development, implementation, and maintenance of the BCP.
- Contingency sites / alternate site processing.
- Vendor management (i.e., external business partners).
- Technical requirements including backup / recovery and offsite storage.
- BCP testing / recovery exercises.

iad INTERNAL AUDITORS DIVISION
A Division of SIFMA

II. Audit Guidelines

II. AUDIT GUIDELINES

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
A. Overall Scope		
Lack of awareness around factors that present the greatest degree of risk to the institution with respect to continuity of operations and the need for business continuity planning.	Determine examination scope and approach for reviewing the business continuity planning program.	• The scope, objectives, and approach will be discussed with management prior to commencing the review. • When documenting the system, diagrams will be useful to understand the environmental features of the site, such as building layout, position of security features and fire protection measures. • Testing controls will generally be by inquiry, observation and inspection with corroboration that control procedures are being applied. However, some sample testing of physical and logical access procedures may be required. • Determine if there are regulatory and statutory requirements. • Review past reports for outstanding issues or previous problems. Consider: • Regulatory reports of examination; • Internal and external audit re-ports, including SAS 70 reports; • Business continuity test results; and • Organization’s overall risk assessment and profile. • Review management’s response to issues that rose since the last examination. Consider: • Adequacy and timing of corrective action; • Resolution of root causes rather than just specific issues; and • Existence of any outstanding issues.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Interview management and review the business continuity request information to identify: • Any significant changes in business strategy or activities that could affect the business recovery process; • Any material changes in the audit program, scope, or schedule related to business continuity activities; • Changes to internal business processes; • Key management changes; • Information technology environments and changes to configuration or components; • Changes in key service providers (technology, communication, back-up/recovery, etc.) and software vendor listings; and • Any other internal or external factors that could affect the business continuity process. • Determine management's consideration of newly identified threats and vulnerabilities to the organization's business continuity process. Consider: • Technological and security vulnerabilities; • Internally identified threats; and • Externally identified threats (including known threats published by information sharing organizations). • All audit issues raised during the current examination will be discussed and approved with management and include responses prior to report issuance.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
B. Existing Business Continuity Plans		
Lack of an existing plan. • Unable to sustain business operations during disasters that affect the business site. • Deteriorating performance and user discontent. • Loss or revenue. • Loss of clients. • No contingency. • Lack of information and knowledge to support business during disasters.	Determine the existence of an appropriate enterprise-wide business continuity plan. A Business Continuity Planning strategy has been documented which defines the level of business required to be recovered in the event of a disaster, and the various types of failures BCP is intended to cover (scenarios).	• Determine if the management has established an enterprise-wide business continuity planning process appropriate for the size and complexity of the organization which defines the organization's business continuity strategy. • Determine if there is a written BCP policy that clearly defines the need and importance of a BCP. • Determine if an objective of the BCP has been formally defined and documented. • Confirm that there is a process in place to ensure that the business continuity plan is reviewed on a regular basis and approved by a registered principal. Confirm when the plan was last reviewed and when the next review is scheduled. • Review the plan to ensure that the procedures for declaring a disaster and steps to follow in the event of a disaster are clearly stated. • Obtain a copy of the business continuity plan and confirm that it caters for scenarios resulting in partial or total loss of supported systems, services and facilities. • Confirm that the branches and/or departments each have a clear BCP plan with short-term/long-term goals that conform to the goals of the whole firm, and are in compliance with SMART principles. • Review the written BCPs of each branch and/or departments to verify that they address the recovery of each business unit/department/ function with respect to the following: • According to its priority ranking in the risk assessment;

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		- Considering interdependencies among systems; - Is consistent with the overall plan; - Law enforcement; - Security; - Media; - Shareholders; and - Include(s) all aspects of emergency preparedness and crisis management as defined throughout the remainder of this section.
C. Management Support for BCP		
Lack of management interest in and support of business continuity plans. - Funding – Management has not provided adequate funding for the creation and testing of BCP planb. - Implementation - Management has not defined project plans to implement the recovery strategy for the business.	Determine the quality of BCP oversight and support provided by the board of directors and senior management, and the roles and responsibilities of those involved in the execution of the plan are well defined. The BCP strategy has been approved by the appropriate executives, boards, and committees.	- Determine whether there is an Executive sponsorship for accountability and ownership. - Determine if an owner has been given the responsibility for the development and maintenance of the plan. - Determine if there are business owners who are responsible for their areas recovery requirements / testing. - Determine if the plan or decision to develop and maintain a BCP has been discussed and approved by executive management. - Ensure that there is constant employee awareness and education for the BCP. - Determine if there are communications established for the employees, their families, key suppliers, headquarters, and other critical parties. - Determine whether there is sufficient investment / funding for the Firm's BCP efforts.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Review the Firm's BCP plan to determine if it: ◦ Clearly identifies the management individuals who have authority to declare a disaster; ◦ Clearly defines responsibilities for designated teams or staff members; ◦ Communicates the contingency locations for each business area; ◦ Explains actions to be taken in specific emergency situations; ◦ Documents each business area's BCP plan and includes an up-to-date Business Impact Analysis ("BIA"); ◦ Defines the conditions under which the backup site would be used; ◦ Has a procedure for notifying employees; ◦ Establishes processing priorities to be followed; ◦ Identify business units without a BCP; ◦ Clearly defines responsibilities and decision-making authorities for designated teams and/or staff members; ◦ Explains actions to be taken in specific emergency situations; ◦ Defines the conditions under which the back-up site would be used; ◦ Has procedures in place for notifying the back-up site; ◦ Designates a public relations spokesperson; and ◦ Identifies sources of needed office space and equipment ◦ Provides a list of key vendors (hardware, software, communications, etc.). • Ensure that the BCP plans are available and accessible at both the production and the contingency site. Obtain the websites' IP addresses and attempt to connect to both locations.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Determine if senior management periodically reviews and prioritizes each business unit, business process, department, and subsidiary for its critical importance and recovery prioritization. If so, determine how often reviews are conducted. • If applicable, determine if senior management has evaluated the adequacy of the BCPs for its service providers, and ensured the organization's BCP is compatible with those service provider plans, commensurate with adequate recovery priorities.
D. Risk Assessment		
Loss of service that could seriously impact the business. • Impact – Management is not aware of or fully informed of the business impacts that may result for loss of operations.	Determine if an adequate business impact analysis ("BIA") and risk assessment have been completed.	• Interview management and review the business continuity request information to identify: ◦ Any significant changes in business strategy or activities that could affect the business recovery process; ◦ Any material changes in the audit program, scope, or schedule related to business continuity activities; ◦ Changes to internal business processes; ◦ Key management changes; ◦ Information technology environments and changes to configuration or components; ◦ Changes in key service providers (technology, communication, back-up/recovery, etc.) and software vendor listings; and ◦ Any other internal or external factors that could affect the business continuity process. • Determine management's consideration of newly identified threats and vulnerabilities to the organization's business continuity process. Consider: ◦ Technological and security vulnerabilities; ◦ Internally identified threats; and ◦ Externally identified threats (including known threats published by information sharing organizations).

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Determine if all functions and departments were included in the BIA. • Review the BIA to determine if the identification and prioritization of business functions are adequate. • Determine if the BIA identifies maximum allowable downtime for critical business functions, acceptable levels of data loss and backlogged transactions, and the cost and recovery time objectives associated with downtime. • Review the risk assessment and determine if it includes scenarios and probability of occurrence of disruptions of information services, technology, personnel, facilities, and service providers from internal and external sources, including: ◦ Natural events such as fires, floods, and severe weather; ◦ Technical events such as communication failure, power outages, and equipment and software failure; and ◦ Malicious activity including network security attacks, fraud, and terrorism. • Verify that the risk assessment and BIA have been reviewed and approved by senior management. • Verify that reputation, operational, compliance, and other risks are considered in plan(s). • Determine if the continuity strategy includes alternatives for interdependent components and stakeholders, including: ◦ Utilities and telecommunications; ◦ Third-party technology providers; ◦ Key suppliers/business partners; and ◦ Customers/members.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Verify that the firm has taken steps to prevent a disaster and/ or minimize the damage. For example, backup generators for power outages, redundant power sources, fire suppression equipment, fire safety training, hand-held fire extinguishers. • Determine if requirements for new office space and equipment, such as, square feet, number of offices, telephones, electrical requirements, etc. have been developed and are stored offsite. These would be used for reconstruction of physical locations needed to continue operations in the event that a primary location is destroyed or uninhabitable for a long period of time.
E. Incident Management		
Failure to initiate the business continuity plan and coordinate with appropriate authorities resulting in a delay to resuming normal operations.	Determine if the firm has developed an incident management system to direct, control, and coordinate response and recovery operations.	• Determine if the incident management system describes specific organizational roles, titles, and responsibilities for each incident management function. • Review established applicable procedures and policies for coordinating response, continuity, and recovery activities with stakeholders directly involved in response, continuity, and recovery operations. • Review established applicable procedures and policies for coordinating response, continuity, and recovery activities with appropriate governmental authorities and resources, including activation and deactivation of plans, while ensuring compliance with applicable statutes or regulations. • Determine if emergency operations/response are guided by an incident action plan or management by objectives. • Verify that incident management plans include provisions for wide scale disruptions, systemic failures, critical financial market failures, and pandemic crises in addition to the firms' individual BCP.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
F. Communication		
Clients, staff, and other external resources (vendors, suppliers, etc) are unaware that business operations are continuing during a disaster.	Determine that proper communication with affected staff, clients, and other external resources are planned for and that the redundant facilities needed to effect communication are in place and operational.	• Verify that alternate communication procedures for customers are documented and disclosure to customer. • Obtain the alternate communication procedure for customers; • Determine whether the firm's contact information can be easily accessible by customers; and • Determine whether there is a backup for contact information. e.g., hotlines, websites links, etc. • Verify that alternate communication procedures for employees are documented and properly communicated to all employees. • Obtain the alternate communication procedure for employees; • Determine whether the firm's client contact information can be easily accessible by employees; • Determine if all key personnel have copies of the plan; • Determine the procedure for communicating with staff during a disaster and for activating the plan; • Determine whether tasks are assigned to different personnel and there is backup in case of absence; • Verify that it has an accurate employee/manager contact tree; and • Determine if personnel are adequately trained as to their specific responsibilities under the plan(s) and whether emergency procedures are posted in prominent locations throughout the facility.
G. Risk Management		
Proper preparation of or destruction, loss, or corruption of business continuity plans.	Determine if appropriate risk management over the business continuity process is in place.	• Determine if external audit involvement in the business continuity program is needed and if so determine if it includes the following: • Audit coverage of the business continuity program; • Assessment of business continuity preparedness during scheduled line(s) of business reviews;

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Audit participation in testing in an observer role; and • Audit review of testing plans and results. • Determine if there are adequate processes in place to ensure the plan(s) are maintained to remain accurate and current. • Designated personnel are responsible for maintaining changes in processes, personnel, and environment(s); • The management reviews and approves the plan(s) annually and after significant changes and updates; and • Process includes notification and distribution of revised plans to personnel and recovery locations.
H. Alternate Facilities		
Lack of alternate physical facilities to carry out business operations during a disaster.	Determine if an appropriate alternate work site has been established for use in the event one or more of the primary work centers are inaccessible.	• Determine if alternate locations and capacity have been provided for: • Data centers and computer operations; • Back-room operations; • Work locations for business functions; and • Telecommunications. • Obtain the alternate physical locations for employees. • Determine whether employees know where to go in case of an emergency. • Determine if the plan identifies recovery sites for each critical business and support function. • Ensure the business unit has a predetermined meeting place in case of an evacuation of their facilities. • Determine if satisfactory consideration has been given to geographic diversity for: • Alternate processing locations; • Alternate locations for business processes and functions; and

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		- Off-site storage. • Determine if plans and/or agreements with peers are in place for Mutual Aid/Assistance to share facilities in the event that one member's primary work center is not available.
I. IT Business Continuity Plans		
Lack of an IT BCP plan. • Increasing inability to support the dependent applications. • Deteriorating performance and user discontent. • Expensive recovery costs. • No contingency. • Lack of information and knowledge to support operations.	Determine if the information technology environment has a properly documented BCP that complements the enterprise-wide and other departmental BCPs.	• Determine if the IT component of the BCP has a properly documented contingency plan. Verify that the IT contingency plan properly supports and reasonably reflects the goals and priorities found in the BCP. • Obtain access to the DR procedures. Review the documented IT continuity plans to ensure they include all critical business units and that they identify their system and service requirements in a disaster situation. • Ensure appropriate policies, standards, and processes address business continuity planning issues including: - Systems Development Life Cycle, including project management; - The change control process; - Data synchronization, back up, recovery; and - Employee training and communication planning. • Review the written IT continuity plan(s) and determine if the plan(s) addresses the back-up of the systems and programming function (if applicable), including: - Back-up of programming tools and software; and - Off-site copies of program and system documentation. • Determine if the plan addresses how backlogged transactions and other activity will be brought current.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Determine if there are plans in place that address the return to normal operations and original business locations once the situation has been resolved and permanent facilities are again available.
J. Hardware Backup and Recovery		
Loss or corruption of physical processing equipment and/or data center needed to support business operations.	Determine whether the BCP(s) include(s) appropriate hardware backup and recovery.	• Verify Back-up of: ◦ Data; ◦ Operating systems; ◦ Applications; ◦ Utility programs; and ◦ Telecommunications. • Verify Off-site storage of: ◦ Back-up media; ◦ Supplies; and ◦ Documentation, e.g., BCP(s), operating and other procedures, inventory listings, etc. • Verify Alternate power supplies: ◦ Uninterruptible power supplies ("UPS"); and ◦ Back-up generators.
K. Data and Application Backup and Recovery		
Loss or corruption of data or mission critical software needed to support business operations.	Determine whether the business continuity process includes appropriate data and application software backup and recovery.	• Obtain the backup and recovery procedure for the Firm's data. Understand the process for backing up databases from the production site to the contingency site. Determine if operating systems and production programs are available both on and offsite locations. • Determine whether data is backed up real-time (i.e., via replication), daily, weekly, monthly, incrementally, etc. • Understand the process for storing backups at an offsite location. Determine if backup media (disks or tapes) is rotated off-site according to a predefined schedule.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Determine if the off-site storage facility is: • Sufficiently remote from the processing facility; and • Accessible within a reasonable time frame, if backups are needed. • Access to data files should be logged in and out to prevent release to unauthorized individuals. A log of the contents, time of the backup and location of the off-site backups must be maintained and stored both locally and at the offsite location. • Determine whether a tape management system is in place. • Identify what prevents the mounting and use of the wrong tape. Identify what prevents the inadvertent use of an active tape as a scratch tape. • Verify that the tape library (used for on-site storage) is a sufficient distance from the computer room and adequately protected to ensure that if a disaster befell the computer room, the tape library would be able to service, and vice versa. • Determine if all critical resources and technologies are covered by the BCP(s), including voice and data communication networks, customer delivery channels, etc. • Determine if the BCPs include the entire network and communication connections. • Determine if the BCP establishes processing priorities to be followed in the event not all applications can be processed. • Describe the arrangements for alternative processing capability in the event any specific hardware, the data center, or any portion of the network becomes disabled or inaccessible, and determine if those arrangements are in writing.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• If the organization is relying on in-house systems at separate physical locations for recovery, verify if the equipment is capable of independently processing all critical applications. • If the organization is relying on outside facilities for recovery, determine if the recovery site: • Has the ability to process the required volume; • Provides sufficient processing time for the anticipated workload based on emergency priorities; and • Allows the organization to use the facility until it achieves a full recovery from the disaster and resumes activity at the organization's own facilities.
L. Alternate Data Center		
Alternate data center is unable to support running of mission critical applications due to lack of backed up date, required applications, or type and size of equipment needed.	Determine whether the BCP(s) include(s) appropriate preparation to ensure the alternate data center recovery processes will work as intended.	• Verify that the plan describes arrangements for alternate processing capability in the event the data center or any portion of the work environment becomes disabled. • Determine that there is a designated back-up computer hardware system, and that it is a practical site for back-up operations until current equipment can be repaired or a new computer can be installed. • Determine how customers would be accommodated if simultaneous disaster conditions were to occur to several customers of the backup facility provider. • Determine whether the Firm is kept informed of any changes at the recovery site (e.g., hardware or software upgrades or modifications) that might require adjustments to the Firm's software or to the recovery plan. • Determine if the plan provides physical security at the recovery site. Determine whether there is a guard present and a sign in/out log for

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		all visitors. • Determine the extent of vendor arrangements in the event of an emergency. • Review the contract between applicable parties, such as recovery vendors. • Determine how the recovery facility's customers would be accommodated if simultaneous disaster conditions were to occur to several customers during the same period of time. • Determine whether the organization ensures that when any changes (e.g., hardware or software upgrades or modifications) in the production environment occur that a process is in place to make or verify a similar change in each alternate recovery location. • Determine whether the organization is kept informed of any changes at the recovery site that might require adjustments to the organization's software or its recovery plan(s). • Determine if the BCP(s) addresses communications and connectivity with technical service providers in the event of a disruption at the institution. • Determine if: ◦ Duplicates of the operating systems are available both on- and off-site; ◦ Duplicates of the production programs are available both on- and off-site, including both source (if applicable) and object versions; ◦ All programming and system software changes are included in the back up;

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		- Back-up media is stored off-site in a place from which it can be retrieved quickly at any time; - Frequency and number of back-up generations is adequate in view of the volume of transactions being processed and the frequency of system updates; - Duplicates of transaction files are maintained on- and off-site; and - Data file back-ups are taken off-site in a timely manner and not brought back until a more current back-up is off-site. • Determine if the BCP(s) addresses communications and connectivity with technology service providers ("TSPs") in the event of a disruption at the service provider's facilities. • Determine if there are documented procedures in place for accessing, downloading, and uploading information with TSPs, correspondents, affiliates and other service providers, from primary and recovery locations, in the event of a disruption. • Determine if the institution has a copy of the TSP's BCP(s) and incorporates it, as appropriate, into their plans. • When testing with the critical service providers, determine whether management considered testing: - From the institution's primary location to the TSPs' alternative location; - From the institution's alternative location to the TSPs' primary location; and - From the institution's alternative location to the TSPs' alternative location. • Determine if institution management has assessed the adequacy of the TSP's business continuity program through their vendor

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		management program (e.g., contract requirements, SAS 70 reviews).
M. Security		
Lack of appropriate physical security at either primary or alternate site causes disruptions in or loss of ability to conduct business operations.	Determine that the BCP(s) include(s) appropriate security procedures.	• Determine whether adequate physical security and access controls exist over data back-ups and program libraries throughout their life cycle, including when they are created, transmitted/delivered to storage, stored, retrieved and loaded, and destroyed. • Determine if appropriate physical and logical access controls have been considered and planned for the inactive production system when processing is temporarily transferred to an alternate facility. • Determine if the intrusion detection and incident response plan considers resource availability, and facility and systems changes that may exist when alternate facilities are placed in use. • Determine if the methods by which personnel are granted temporary access (physical and logical) during continuity planning implementation periods are reasonable. • Evaluate the extent to which back-up personnel have been reassigned different responsibilities and tasks when business continuity planning scenarios are in effect and if these changes require a revision to the levels of systems, operational, data, and facilities access. • Review the assignment of authentication and authorization credentials to determine if they are based upon primary job responsibilities and if they also include business continuity planning responsibilities.
N. Outsourced Business Activities		
Mission critical outsourced activities fail to run during a disaster or suffer a disaster in their own right.	The risks in outsourcing information, transaction processing, and settlement activities	• Identify critical outsourced activities and determine whether a BCP exists for each service provider. • Review each service provider's contract to verify it includes detailed

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
Reliance on third-party providers, key suppliers, or business partners may expose financial firms to points of failure that may prevent resumption of operations in a timely manner.	include threats to the security, availability and integrity of systems and resources, to the confidentiality of information, and to regulatory compliance. In addition, when a third party performs services on behalf of the institution, increased levels of credit, liquidity, transaction, and reputation risk can result.	business recovery timeframes that meet the business continuity planning needs of the firm and call lists necessary for contacting key individuals at the service provider's primary and recovery locations. • Review and understand each service providers' BCP and ensure critical services can be restored within acceptable timeframes based upon the needs of the firm. The firm's own BCP should also address how it will be exchanging information with its service providers should the firm be operating from an alternative location, e.g., transmission via a branch facility that has redundant telecommunications links with the service provider. • Review third party contracts to determine if they address the service provider's responsibility for maintenance and testing of disaster recovery and contingency plans and the firm is provided testing results. • Review third party audits and BCP test results to determine the adequacy of plans and the effectiveness of the testing process and if the firm participated in the service provider's testing process.
O. Regulatory Compliance		
Failure to comply with regulatory, financial, and reporting requirements results in sanctions that impair business operations.	Determine if the firm is in compliance with all regulatory, financial, and reporting requirements.	NYSE Rule 446 and NASD 3510: Mission Critical System The term "mission critical system," for purposes of this Rule, means any system that is necessary, depending on the nature of a member's or member organization's business, to ensure prompt and accurate processing of securities transactions, including order taking, 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. • Mission critical systems should be complete and up-to-date.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Obtain the list of Mission Critical Systems. • Determine the procedure assessing mission critical system. NYSE Rule 446 and NASD 3510: Financial and Operational Assessments Defines "financial and operational assessments" as "a set of written procedures that allows a member to identify changes in its operational, financial, and credit risk exposures." Operational risk focuses on the firm's ability to maintain communications with customers and to retrieve key activity records through its "mission critical systems." Financial risk relates to the firm's ability to continue to generate revenue and to retain or obtain adequate financing and sufficient equity. In addition, an eroding financial condition could be exacerbated or caused by deterioration in the value of the firm's investments due to the lack of liquidity in the broader market, which would also hinder the ability of the firm's counter-parties to fulfill their obligations. A firm would be expected to periodically assess changes in these exposures, quickly assess the situation, and take appropriate action relative to a significant business disruption. Members' procedures should be written and implemented to reflect the interrelationship among these risks. • Obtain financial and operational assessments procedure. • Determine whether the procedure contains sufficient guidelines that allow the Firm to identify changes in its operational, financial, and credit risk exposures. NYSE Rule 446 and NASD 3510: Critical Business Constituent, Bank, and Counter-Party Impact Members must have procedures that assess the impact that a significant business disruption would have on critical business constituents (businesses with which a member firm has an ongoing commercial relationship in support of the member's operating activities), banks

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		(lenders), and counter-parties (e.g., other broker-dealers or institutional customers). In addition, members must provide for alternative actions or arrangements with respect to their contractual relationships with business constituents, banks, and counter-parties in the event of a material business disruption to either party. In short, the Rule requires a member to assess the effect of a significant business disruption on its business constituents, banks, and counter-parties and decide appropriate actions if faced with any such situation. The Rule, however, permits each member to adopt an approach in dealing with its business constituents, banks, and counter-parties that is best suited to the member's particular operations, structure, business, and location. • Determine whether the BCP addresses "critical constituent, bank and counter-party impact". • Determine how the Firm assesses the impact on significant business disruption. Procedures for regulatory reporting should be in placed and procedures for communication with the regulators should be in placed and updated periodically. • Obtain the procedure for regulatory reporting. • Determine whether the procedure covers all regulatory reporting. • Obtain the procedure for communication with regulators. • Determine whether contact information is accurate and up to date. <u>NYSE Rule 446 and NASD 3510:</u> Requires each member to disclose to its customers how its business continuity plan addresses the possibility of a future significant business disruption and how the member plans to respond to events of varying scope. In addressing the events of varying scope, NYSE and NASD

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		believes that each member should: (1) provide specific scenarios of varying severity (e.g., a firm-only business disruption, a disruption to a single building, a disruption to a business district, a city-wide business disruption, and a regional disruption); (2) state whether it plans to continue business during that scenario and, if so, its planned recovery time; and (3) provide general information on its intended response. The disclosure must, at a minimum, be made in writing to customers at account opening, posted on the member's Web site (if the member maintains a Web site), and mailed to customers upon request. Members must disclose the existence of back-up facilities and arrangements. Members, however, need not disclose the following factors: the specific location of any back-up facilities; any proprietary information contained in the plan; and the parties with whom the member has back-up arrangements. Members may include cautionary language in their business continuity plans indicating that such plans are subject to modification, that updated plans will be promptly posted on the member's Web site, and that customers may alternatively obtain updated plans by requesting a written copy of the plan by mail. • Verify that BCP is disclosed to customers via the following ways: • New account form; • Website; and • Physical mail. NYSE Rule 446 and NASD Rule 3520 require members to designate two emergency contact persons and provide this information to NYSE and NASD via electronic process. <u>Emergency Contact Information</u> (a) Each member shall report to NYSE and NASD, via such electronic or other means as NYSE and NASD may require, prescribed emergency contact information for the member. The emergency contact information for the member includes designation of two emergency

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		contact persons. Each emergency contact person shall be a member of senior management and a registered principal of the member. (b) Each member must update its emergency contact information, via such electronic or other means as NYSE and NASD may require, in the event of any material change, but at a minimum must review the information contained therein twice a year to ensure its accuracy. • Verify that there are two contact persons for the regulators, who must be registered principals. • Determine how often the contact information is reviewed. NFA 2-38 Each Member must establish and maintain a written business continuity and disaster recovery plan that outlines procedures to be followed in the event of an emergency or significant business disruption. The plan shall be reasonably designed to enable the Member to continue operating, to reestablish operations, or to transfer its business to another Member with minimal disruption to its customers, other Members, and the commodity futures markets. Each Member must provide NFA with the name of and contact information for an individual who NFA can contact in the event of an emergency, and the Member must update that information upon request. Each IB, CPO, and CTA Member that has more than one principal and each FCM Member must also provide NFA with the name of and contact information for a second individual who can be contacted if NFA cannot reach the primary contact, and the Member must update that information upon request. These individuals must be authorized to make key decisions in the event of an emergency. • Determine if the NFA is aware that the firm has a BCP plan. • Verify that there are two contact persons for the NFA regulators,

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		who must be registered principals. • Determine how often the contact information is reviewed. • Verify that a process is in place to respond to NFA requests for updated information.
P. Business Pandemic Planning		
Disruptions to business operations as a result of the impact of a prolonged health crisis (pandemic) such as avian flu and the measures government agencies may impose that would limit the movement of staff and resources. Historically, pandemics have occurred three to four times per century. Thus, regardless of whether the current avian flu causes a pandemic, there remains a substantial risk of a pandemic, involving some disease, in the not too distant future.	In light of the threat of a pandemic, or any biologically based threat, member firms should review their BCPs and make any necessary modifications. The threat of a pandemic poses unique challenges and therefore requires special planning. Because of the potential business disruption that a pandemic would cause, the securities industry should plan specifically for such an event keeping in mind the following five specific risks: (1) Pandemics can have multiple strains that arrive in separate waves. The cycles might span many months. Auditors therefore should evaluate the viability of their firms BCP	• Review the BCP plan for the impact of a pandemic on the firms business and determine if it contains the following; • A pandemic coordinator and/or team with defined roles and responsibilities for preparedness and response planning. • Identification of essential employees and other critical inputs (e.g. vendors, suppliers, sub-contractor services/products, and logistics) required to maintain business operations by location and function during a pandemic. • Training and preparation of an ancillary workforce (e.g. contractors, employees in other job titles/descriptions, retirees). • Planning for scenarios likely to result in an increase or decrease in demand for your products and/or services during a pandemic (e.g. effect of restriction on mass gatherings, need for hygiene supplies, etc). • Impact analysis of a pandemic on company business financials using multiple possible scenarios that affect different business lines and/or production sites. • Impact of a pandemic on business-related domestic and international travel (e.g. quarantines, border closures). • Sources of up-to-date, reliable pandemic information from community public health, emergency management, and other sources and the creation of sustainable communication links. • Creation of an emergency communications plan that is revised periodically. This plan should include identification of key contacts (with back-ups), chain of communications

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
	in the event that they would have to be operative for periods of weeks or months. (2) The US government has indicated that it may resort to quarantines in the event of a domestic outbreak, and foreign governments' reactions may be similar or more drastic. Auditors should evaluate the viability of their firms BCP in light of potential restrictions on travel, as well as on gatherings of large numbers of people in one location. (3) Pandemics can have a multinational or global scale. (4) Pandemics can impact large percentages of the population and of a firm's work force (as many as 30% to 40%). In addition, fear may deter healthy people from attending work.	(including suppliers and customers), and processes for tracking and communicating business and employee status. • Periodic exercises and drills to test the plan, and revise accordingly. • Review the BCP plan for the impact of a pandemic on the firms employees and clients and determine if it contains the following; • Forecasts and allowances for employee absences during a pandemic due to factors such as personal illness, family member illness, community containment measures and quarantines, school and/or business closures, and public transportation closures. • Guidelines to modify the frequency and type of face-to-face contact (e.g. hand-shaking, seating in meetings, office layout, and shared workstations) among employees and between employees and customers (refer to CDC recommendations). • Plan to encourage and track annual influenza vaccination for employees. • Evaluation of employee access to and availability of healthcare services during a pandemic, and improve services as needed. • Evaluation of employee access to and availability of mental health and social services during a pandemic, including corporate, community, and faith-based resources, and improve services as needed. • Identification of employees and key customers with special needs, and incorporate the requirements of such persons into your preparedness plan. • Review the BCP plan for the policies and plans to be implemented during a pandemic and determine if it contains the following; • Policies for employee compensation and sick-leave absences

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
	(5) A pandemic could result in the loss of multiple personnel within the same business unit (including business continuity managers). As a result, firms should consider whether their succession plan is adequately extensive.	unique to a pandemic (e.g. non-punitive, liberal leave), including policies on when a previously ill person is no longer infectious and can return to work after illness. • Policies for flexible worksite (e.g. telecommuting) and flexible work hours (e.g. staggered shifts). • Policies for preventing influenza spread at the worksite (e.g. promoting respiratory hygiene/cough etiquette, and prompt exclusion of people with influenza symptoms). • Policies for employees who have been exposed to pandemic influenza are suspected to be ill, or become ill at the worksite (e.g. infection control response, immediate mandatory sick leave). • Policies for restricting travel to affected geographic areas (consider both domestic and international sites), evacuating employees working in or near an affected area when an outbreak begins, and guidance for employees returning from affected areas (refer to CDC travel recommendations). • Plan for the authorities, triggers, and procedures needed for activating and terminating the company's response plan, altering business operations (e.g. shutting down operations in affected areas), and transferring business knowledge to key employees. • Review the BCP plan to determine if it allocates resources to protect employees and customers during a pandemic and determine if it contains the following; • Provides sufficient and accessible infection control supplies (e.g. hand-hygiene products, tissues and receptacles for their disposal) in all business locations. • Enhances communications and information technology infrastructures as needed to support employee telecommuting and remote customer access. • Ensures availability of medical consultation and advice for

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		emergency response. • Review the BCP plan to determine if it provides for communication and the education of employees and determine if it contains the following; • Programs and materials covering pandemic fundamentals (e.g. signs and symptoms of influenza, modes of transmission), personal and family protection and response strategies (e.g. hand hygiene, coughing/sneezing etiquette, contingency plans). • Plans to address employee fear and anxiety, rumors and misinformation and plan communications accordingly. • Ensures that communications are culturally and linguistically appropriate. • Disseminates information to employees about your pandemic preparedness and response plan. • Provides information for the at-home care of ill employees and family members. • Includes platforms (e.g. hotlines, dedicated websites) for communicating pandemic status and actions to employees, vendors, suppliers, and customers inside and outside the worksite in a consistent and timely way, including redundancies in the emergency contact system. • Identifies community sources for timely and accurate pandemic information (domestic and international) • Identifies resources for obtaining counter-measures (e.g. vaccines and anti-virals). • Review the BCP plan to determine if it provides for coordination with external organizations and assistance for local communities and that it includes the following; • Collaboration with insurers, health plans, and major local healthcare facilities to share your pandemic plans and understand their capabilities and plans.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Collaboration with federal, state, and local public health agencies and/or emergency responders to participate in their planning processes, share your pandemic plans, and understand their capabilities and plans. • Communication with local and/or state public health agencies and/or emergency responders about the assets and/or services your business could contribute to the community. • Sharing of best practices with other businesses in your communities, chambers of commerce, and associations to improve community response efforts.
Q. Insurance		
Money needed to recover from disasters and to implement a BCP plan.	Determine whether the firm is adequately insured to cover costs from a disaster.	• Obtain and review the insurance policy and determine whether the following is addressed: • IT equipment and facilities; • Loss resulting from business interruptions; • Errors and omissions; • Extra expenses, including backup site expenses; • Items in transit; and • Employee fidelity. • If the insurance policy requires that specific equipment be listed for coverage, determine that the listing currently supplied to the carrier is accurate. Check all big cost items in the fixed asset listing. • Verify that coverage is current and that premiums have been paid. • Examine the business-interruption coverage limits. Determine whether the Firm has made calculations of the probable actual cost of interruption during various disasters and identified the amount of interruption cost it will have to bear after insurance coverage. • Determine that an EDP rider is included in the Firm's general property insurance.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
R. Training		
Lack of staff training for execution of the BCP plan prevents a firm from recovering and continuing operations in the event of an actual disaster.	A training program should exist for all staff involved in the preparation of and execution of the BCP plan.	• Determine if the firm has developed and implemented a training and educational curriculum to support the BCP program. • Verify that the objective of the training is to create awareness and enhance the skills required to develop, implement, maintain, and execute the BCP program. • Determine the frequency and scope of training to insure that it is adequate to meet changing business needs. • Verify that staff has been trained in the firm's incident management system. • Verify that training records are maintained. • Verify that the BCP training and education curriculum complies with all applicable regulatory requirements.
S. Plan Testing		
Plan is not workable and fails to address critical business needs in the event of a disaster.	Determine whether the BCP plan includes appropriate testing to ensure the business processes will be maintained, resumed, and/or recovered as intended.	• Determine if adequate procedures are in place to ensure the BCP(s) is (are) maintained in a current fashion and updated regularly. • Determine if a senior manager has been assigned responsibility to oversee the development, implementation, testing, and maintenance of the BCP. • Determine if the management has ensured that adequate resources, including sufficient human resources, are devoted to the business continuity testing process. • Determine if the overall BCP plan is tested at least annually. • Describe the process for preparing, planning, coordinating, and testing the BCP.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		• Determine the extent of user involvement in testing. • Determine if individual business areas test their critical applications and services on a semi-annual basis. Understand and document the extent of testing performed. • Determine if the tests include: • Use of actual backup system and data files from off-site storage; • Disconnecting from the production site and accessing the contingency site; • A post-test analysis report and review process that includes a comparison of test results to the original goals; • Development of a corrective action plan for all problems encountered; and • The availability of workspace at the backup site or the ability to establish telecommunications links to the back up site to support ongoing operations. • Determine if the management reviews and approves the written BCP(s) and testing results at least annually and documents these reviews in the management minutes. • Verify that all critical business units/departments/functions are included in the testing. • Verify that tests include: • Setting goals and objectives in advance; • Realistic conditions and activity volumes; • Use of actual back-up system and data files while maintaining off-site back-up copies for use in case of an event concurrent with the testing; • Participation and review by internal audit; • A post-test analysis report and review process that includes a

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
		comparison of test results to the original goals; and • Development of a corrective action plan(s) for all problems encountered. • Determine if interdependent departments, vendors, and key market providers have been involved in testing at the same time to uncover potential conflicts and/or inconsistencies. • Determine if the level of testing is adequate for the size and complexity of the organization. Determine if the testing includes: • Testing the operating systems and utilities (infrastructure); • Testing of all critical applications (application level); • Data transfer between applications (integrated testing); and • Testing the complete environment and workload (stress test). • Determine whether testing at an alternative location includes: • Network connectivity; • Items processing and backroom operations connectivity and information; and • Other critical data feed connections/interfaces. • Determine whether testing of the information technology infrastructure includes: • Rotation of personnel involved; and • Business unit personnel involvement. • Determine whether management considered testing with: • Critical service providers; • Customers; • Affiliates; • Correspondent institutions; and • Payment systems and major financial market participants.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
T. Exercises, Evaluations, and Corrective Actions		
Lack of periodic evaluations and follow-ups result in gaps in the BCP plan that prevent a firm from recovering and continuing operations in the event of an actual disaster.	Tabletop exercises, walkthrough evaluations, and other simulations are in place to insure that the BCP plan works as intended and gaps and issues are addressed through corrective action.	• Determine if the firm has evaluation program plans, procedures, and exercise capabilities in place that include periodic reviews, testing, and exercises. • Verify that additional reviews are conducted based on post-incident analyses and reports, lessons learned, and performance evaluations. • Verify that exercises are designed to test individual essential elements, interrelated elements, and/or the entire plan. • Determine that procedures are established to take corrective action on any deficiency identified.
U. Prior Audit Issues		
Prior and/or ongoing issues that impair a firm from resuming business operations in the event of a disaster.	Review of prior issues, resolution, and meeting of previously established target dates.	• Obtain prior BCP audit issues that related to this review and perform issue follow-up to ensure that actions are adequately resolved. • Review past reports for outstanding issues or previous problems. Consider: • Regulatory reports of examination; • Internal and external audit reports, including SAS 70 reports; • Business continuity test results; and • Organization’s overall risk assessment and profile. • Review management’s response to issues raised since the last examination. Consider: • Adequacy and timing of corrective action; • Resolution of root causes rather than just specific issues; and • Existence of any outstanding issues.

Risks to be Managed	Types of Controls to Manage/Eliminate Risks	Potential Audit Work Steps
V. Conclusions and Action Plan		
Failure to address BCP gaps that impair a firm from resuming business operations in the event of a disaster.	Discuss corrective action and communicate findings.	• Identify gaps in BCP plans. • Determine actions needed to close gaps. • Assign responsibility to action items. • Determine target date for each action. • Verify review of action items becomes part of next audit.

iad INTERNAL AUDITORS DIVISION
A Division of SIFMA

III. Glossaries

III. GLOSSARIES

The definitions in this section shall apply to the terms used in the guideline. Where terms are not defined in this section or within another chapter, they shall be defined using their ordinarily accepted meanings within the context in which they are used.

Approved- Acceptable to the authority having jurisdiction.

Authority Having Jurisdiction ("AHJ")- An organization, office, or individual responsible for enforcing the requirements of a code or standard, or for approving equipment, materials, an installation, or a procedure.

Business Continuity- An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies, recovery plans, and continuity of services.

Critical Financial Markets- Critical financial markets provide the means for banks, securities firms, and other financial institutions to adjust their cash and securities positions and those of their customers in order to manage liquidity, market, and other risks to their organizations. Critical financial markets also provide support for the provision of a wide range of financial services to businesses and consumers in the United States. Certain markets, such as the federal funds and government securities markets, also support the implementation of monetary policy.

Damage Assessment- An appraisal or determination of the effects of the disaster on human, physical, economic, and natural resources.

Disaster/Emergency Management- An ongoing process to prevent, mitigate, prepare for, respond to, and recover from an incident that threatens life, property, operations, or the environment.

Emergency Management Program- A program that implements the mission, vision, and strategic goals and objectives as well as the management framework of the program and organization.

Exercise- Tabletop exercises, walkthrough evaluations, and other simulations that recreate various disaster scenarios and the actions needed to resume business operations according to the BCP to verify that the BCP is workable.

Impact Analysis [Business Impact Analysis ("BIA")]- Analysis that identifies the impacts of losing the firm's resources.

Incident Action Plan- A verbal plan, written plan, or combination of both, that is updated throughout the incident and reflects the overall incident strategy, tactics, risk management, and member safety that are developed by the incident commander.

Incident Management System ("IMS")- The combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents.

Mitigation- Activities taken to reduce the severity or consequences of an emergency.

Mutual Aid/Assistance Agreement- A prearranged agreement between two or more firms to share resources in response to an incident.

Preparedness- Activities, tasks, programs, and systems developed and implemented prior to an emergency that are used to support the prevention of, mitigation of, response to, and recovery from emergencies.

Prevention- Activities to avoid an incident or to stop an emergency from occurring.

Recovery- Activities and programs designed to return conditions to a level that is acceptable to the firm and the conduct of its business.

Resource Management- A system for identifying available resources to enable timely and unimpeded access to resources needed to prevent, mitigate, prepare for, respond to, or recover from an incident.

Response- Immediate and ongoing activities, tasks, programs, and systems to manage the effects of an incident that threatens life, property, operations, or the environment.

Risk Assessment- Business processes and the business impact analysis assumptions are stress tested with various threat scenarios. The result is an assessment of the impact each may have on the organization's ability to continue to deliver its normal business services.

Situation Analysis- The process of evaluating the severity and consequences of an incident and communicating the results.

Stakeholder- Any individual, group, or organization that might affect, be affected by, or perceive itself to be affected by the emergency.

Standard- A document, the main text of which contains only mandatory provisions using the word “shall” to indicate requirements and which is in a form generally suitable for common reference by member firms.

Systemic Failure- Systemic failure includes the risk that the failure of one participant in a transfer system or financial market to meet its required obligations will cause other participants to be unable to meet their obligations when due, causing significant liquidity or credit problems or threatening the stability of financial markets.3 Given the complex interdependencies of markets and among participants, thorough preparations by key market participants will reduce the potential that a sudden disruption experienced by one or a few firms will cascade into market-wide liquidity dislocations, solvency problems, and severe operational inefficiencies.

Wide-Scale Disruption- A wide-scale disruption is an event that causes a severe disruption or destruction of transportation, telecommunications, power, or other critical infrastructure components across a metropolitan or other geographic area and the adjacent communities that are economically integrated with it; or that results in a wide-scale evacuation or inaccessibility of the population within normal commuting range of the disruption's origin.

The Audit Guidelines (the "guidelines") are intended to provide members of the Internal Auditors Division ("IAD"), an affiliate of the Securities Industry and Financial Markets Association ("SIFMA") with information for the purpose of developing or improving their approach towards auditing certain functions or products typically conducted by a registered broker-dealer. These guidelines do not represent a comprehensive list of all work steps or procedures that can be followed during the course of an audit and do not purport to be the official position or approach of any one group or organization, including IAD or any of its divisions or affiliates. Neither IAD, nor any of its divisions or affiliates, assumes any liability for errors or omissions resulting from the execution of any work steps within these guidelines or any other procedures derived from the reader's interpretation of such guidelines. In using these guidelines, member firms should consider the nature and context of their business and related risks to their organization and tailor the work steps accordingly. Internal auditors should always utilize professional judgment in determining appropriate work steps when executing an audit.