ICSA

INTERNATIONAL COUNCIL of SECURITIES ASSOCIATIONS

Business Continuity Planning Guidelines

for Securities Firms

March 5, 2004

ICSA International Council of Securities Associations

Business Continuity Planning Guidelines

for Securities Firms

The members of the International Council of Securities Associations (ICSA)[1] consider that it is in the interest of all firms involved in the financial services sector to develop and maintain suitable business continuity programs so that they are able to recover quickly and effectively from any unanticipated market disruption. Accordingly, ICSA has endorsed the general guidelines for business continuity planning set out below.[2] Although individual firms in different jurisdictions will need to develop specific business continuity programs that take into account local law and regulations and their own unique circumstances, these guidelines are intended to provide a framework for business continuity planning that can be followed by all firms regardless of their specific needs and circumstances. ICSA members encourage their member firms to take account of these guidelines when drawing up or reviewing their business continuity plans.

---

[1] The membership of the International Council of Securities Associations (ICSA) includes self-regulatory and trade associations for the securities industry in ten countries as well as a number of international trade associations. ICSA members represent and/or regulate the overwhelming majority of the world's equity, bond and derivatives markets. ICSA's objectives are to encourage the sound growth of the international securities market by promoting harmonization in the procedures and regulation of those markets and to promote mutual understanding and the exchange of information among ICSA members. A list of the individual members of ICSA is attached to this document.

[2] These guidelines are based on the *Best Practices for Business Continuity Planning* developed by the Securities Industry Association (SIA).

Best Practice Guidelines for Business Continuity Planning[3]

1. Each firm should have in place a business continuity program that:

    - Facilitates the development, implementation, testing and maintenance of business continuity and emergency response plans that would enable the business to protect its assets and meet its business recovery objectives in the event of a severe disaster;

    - Includes plans for prevention and mitigation activities that would reduce the impact of a disruption; and,

    - Includes an ongoing employee awareness program.

2. Each firm should have a business continuity policy document which provides the framework for its business continuity program and the development of business continuity and emergency response plans. Business continuity plans should be documented and readily accessible to those who need access to them in an emergency.

3. As part of its contingency planning preparation, each firm may wish to carry out a business impact analysis (BIA) that will help it to understand the likely impact of potential disasters so that it can quantify the potential losses and various other unwanted effects that could result.

4. Each firm should have an executive and corporate group responsible for overseeing the business continuity plan.

5. Business managers should be responsible for the review, implementation, funding and sign-off of business continuity plans and associated exercise results.

6. Recovery exercises for critical business functions should be conducted no less than annually and as warranted by changes in the business and/or information system(s) environment. Firms should participate meaningfully in any industry-wide resiliency tests as well as any testing sponsored by regulators, core clearance, exchange and settlement organizations or other critical infrastructure providers.

---

[3] These guidelines are intended for firms that have sufficient resources so that they would be able to remain in operation in the event of a major market disruption. It is recognized that some firms with limited resources may not be able to fully implement these guidelines. In such cases firms must ensure at a minimum that their customers will have access to their funds and securities in the event of a severe market disruption and will know whom to contact for information about their accounts.

7. Business continuity plans should be reviewed and updated no less than annually and as warranted by changes in the business and/or information system(s) environment.

Recovery Objectives and Strategies

1. The primary objective of the business continuity plan should be for the firm to have the capacity to resume operational effectiveness within a specified period of time after the onset of a disaster or other market-disrupting event. Operational effectiveness is defined as the operational level that would enable the individual firm to continue or resume its most critical operating, service and technology functions in order to:

    - Meet service level commitments to customers;
    - Meet fiduciary requirements;
    - Meet legal and/or regulatory requirements;
    - Minimize financial exposure; and
    - Meet other defined recovery objectives.

2. A firm's recovery strategy should be based on a hypothetical event that involves a severe disruption or destruction of transportation, telecommunications, power, or other critical infrastructure components or which results in a wide-scale evacuation or inaccessibility of the population within normal commuting range of the disruption's origin.

3. Firms may wish to determine a specific recovery time for the resumption of operational effectiveness. Recovery-time objectives provide concrete goals to plan for and test against. However, these objectives cannot be regarded as hard and fast deadlines to be met in every emergency situation since various external factors, such as the scope of disruption and status of critical infrastructure, will affect actual recovery times.

Critical Elements of a Business Continuity Plan

1. Firms should have the capability to communicate with employees, customers and counterparties during an emergency using multiple methods of communication. For ongoing contact with staff, whenever possible firms should establish a specific facility, such as a place on their website or an emergency phone number, that would provide general information for staff members.

2. Each firm should have pre-defined business continuity teams with detailed management structures and clearly defined roles and responsibilities for each team member.

3. Firms should be cognizant of the geographic diversity of critical staff and production applications data or data centers when developing their business continuity programs.

4. Each firm should have a human resources plan as part of its overall business continuity program. The human resources plan could include, among other items, a plan for the provision of emergency services for employees such as grief counseling and financial assistance as well as basic payroll services.

5. To the greatest extent possible recovery facilities should be located at a sufficient distance from the primary site in order to avoid being subject to the same risks as the primary location and should be supported by separate infrastructure components (e.g., transportation, telecommunications, water supply and power).

6. Firms should ensure that critical business applications and computing facilities in the recovery center and other supporting locations are sufficient to meet their business recovery objectives.

7. Firms should ensure that essential staff members are trained and capable of performing multiple business functions at the recovery location.

8. The effectiveness of back-up arrangements in recovering from a wide-scale disruption should be confirmed through testing. A comprehensive testing program should consider all aspects of the back-up plan, including systems connectivity, staff relocation and communications.

9. Business continuity plans should take into account the potential impact of a significant market disruption on key internal and external business partners (including telecommunications, energy, water, transportation, operations, technical support, clients, vendors, regulators, exchanges and clearing corporations) in order to ensure that acceptable levels of operational connectivity can be resumed within recovery objectives.

10. Business units should ensure that redundant copies of vital records are stored in a secured and geographically diverse location and are available for use during an emergency.

The members of ICSA are as follows:

Association Française des Entreprises d'Investissement, France
Australian Financial Markets Association, Australia
Bond Exchange of South Africa, South Africa
The Bond Market Association, United States
Chinese Taiwan Securities Association, Taiwan
Italian Association of Financial Intermediaries, Italy
International Banks and Securities Association of Australia, Australia
International Primary Market Association, United Kingdom
International Securities Market Association, Switzerland
Investment Dealers Association of Canada, Canada
Japan Securities Dealers Association, Japan
The Korea Securities Dealers Association, Korea
London Investment Banking Association, United Kingdom
NASD, United States
Securities Industry Association, United States
Swedish Securities Dealers Association, Sweden