# Market Intermediary Business Continuity and Recovery Planning

# Consultation Report


**THE BOARD OF THE**
**INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS**

| | |
|---|---|
| **CR04/2015** | **APRIL 2015** |

Copies of publications are available from:
The International Organization of Securities Commissions website www.iosco.org


Certain authorities may consider rule proposals or standards that relate to the substance of this report. These authorities provided information to IOSCO or otherwise participated in the preparation of this report, but their participation should not be viewed as an expression of a judgment by these authorities regarding their current or future regulatory proposals or of their rulemaking or standards implementation work. This report thus does not reflect a judgment by, or limit the choices of, these authorities with regard to their proposed or final versions of their rules or standards.

## Foreword

The Board of the International Organization of Securities Commissions (IOSCO) has published for public comment this consultation report on *Market Intermediary Business Continuity and Recovery Planning* (Consultation Report). The Consultation Report provides background on the project and the work undertaken by IOSCO's Committee on the Regulation of Market Intermediaries (C3) on business continuity and recovery planning by market intermediaries. It also proposes two standards[1] for regulators and sound practices[2] that regulators could consider as part of their oversight of market intermediaries and such intermediaries may find useful in the development and implementation of their business continuity plans. Not every sound practice will be appropriate or equally effective for all market intermediaries. However, IOSCO would still encourage individual market intermediaries to consider these sound practices where relevant to their activities. A final report will be prepared after consideration of comments received from the public in response to this Consultation Report.

## How to Submit Comments

Comments may be submitted by one of the following two methods **on or before Saturday 6 June 2015**. To help us process and review your comments more efficiently, please only use one method.

**Important:** All comments will be made available publicly, unless anonymity is specifically requested. Comments will be converted to PDF format and posted on the IOSCO website. Personal identifying information will not be edited from submissions.

- **Email**
  - Send comments to Mohamed Ben Salem, IOSCO General Secretariat, at consultation-2015-04@iosco.org
  - The subject line of your message must indicate *Business Continuity and Recovery Planning*.
  - If you attach a document, indicate the software used (*e.g.*, Microsoft WORD, ASCII text, etc.) to create the attachment
  - Do not submit attachments as HTML, PDF, GIFG, TIFF, PIF, ZIP or EXE files.

- **Paper**

Send three copies of your comment letter to:

---

1 Standards describe how regulators should implement the IOSCO Objectives And Principles of Securities Regulation.

2 Sound practices consist of practices that regulators could consider. Such practices would not be reflected in the methodology for the implementation of the IOSCO Objectives And Principles of Securities Regulation as they do not represent a standard that IOSCO members are necessarily expected to implement or be assessed against.

**Mohamed Ben Salem**
International Organization of Securities Commissions (IOSCO)
Calle Oquendo 12
28006 Madrid Spain

Your comment letter should indicate prominently that it is a "*Comment on Business Continuity and Recovery Planning*".

*This Consultation Report has been prepared by IOSCO's Committee on the Regulation of Market Intermediaries. The proposed market intermediary sound practices, analysis and conclusions in this Consultation Report do not necessarily reflect the view of any one IOSCO member.*

## Table of Contents

## I. Executive Summary

In 2013, the IOSCO Board approved a project specification for C3 entitled *Intermediary Business Continuity and Recovery Planning*. The project specification provided that a questionnaire would be developed for both regulators and intermediaries in order to gain an understanding of the regulatory frameworks and approaches taken by regulators for business continuity and disaster recovery for intermediaries, as well as of the arrangements currently in place at intermediaries. In addition, the project mandate contemplated that C3 would convene roundtables with intermediary and other expert industry representatives for the purpose of identifying existing and emerging threats to intermediaries. As part of this work, C3 would solicit information concerning experiences and viewpoints pertaining to, among other things, what constitutes effective business impact analysis, recovery strategies, and business continuity plan(s) (BCP),[3] as well as information concerning existing programs for testing, training, awareness, communication and crisis management. The group also considered disaster recovery plan(s) (DRP),[4] which are generally a subset of BCPs. Therefore, for purposes of this report, the term "BCP" includes DRP.

The project specification contemplated that a summary of the questionnaire responses and key information acquired at the roundtables would be prepared, including a description of current intermediary business continuity practices and relevant regulatory frameworks. The project specification also contemplated the development of a range of sound practices to address potential disruptions and possible weaknesses in BCPs and recovery strategies.

C3 completed the following work in developing this Consultation Report:

- A survey of IOSCO member jurisdictions.
- A survey of market intermediaries in IOSCO jurisdictions.
- Hosting roundtables with the major market intermediaries in Rome (Dec. 2013) and Morocco (Apr. 2014).

C3 used the results of the two surveys and the feedback from the roundtable attendees to prepare this Consultation Report.

---

[3] A BCP is a comprehensive written plan of action that sets out the procedures and systems necessary to continue or restore the operation of an organization in the event of a disruption. A BCP is a component of business continuity management (BCM), *i.e.*, a whole-of-business approach that includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. The purpose of BCM is to minimize the operational, financial, legal, reputational and other material consequences arising from a disruption. See "*High-level principles for business continuity*," a report of the Joint Forum, infra, notes 3 and 4, available at: http://www.bis.org/publ/joint17.pdf.

[4] DRPs are more technical plans that are developed for specific groups within an organization to allow them to recover a particular business application. As part of the business continuity process an organization will normally develop a series of DRPs. A common example of a DRP is the Information Technology (IT) DRP.

This Consultation Report:

- Provides background to the project.
- Describes the work undertaken by C3.
- Analyzes responses from the market intermediary questionnaire and the regulator questionnaire.
- Consults on proposed standards to regulators and draft "sound practices" that regulators could consider as part of their oversight of market intermediaries, and which such intermediaries may find useful in the development and implementation of effective BCPs. IOSCO recognizes that not every sound practice will be appropriate or equally effective for all large market intermediaries. However, IOSCO would still encourage individual market intermediaries to consider these sound practices in this report where relevant to their activities.

## II. Background

### A. Previous Work: Joint Forum Report

In 2006, the Joint Forum,[5] of which IOSCO is a parent committee, published a report entitled "*High-level principles for business continuity*" (Joint Forum Report),[6] which noted that "a major operational disruption" (MOD)[7] can result from a wide range of events such as earthquakes, hurricanes and other weather-related events, terrorist attacks and other intentional or accidental acts that cause widespread damage to the physical infrastructure."[8] This Report also noted that "other events, such as technology viruses, pandemics and other biological incidents may not cause widespread damage to the physical infrastructure, but can nonetheless lead to major operational disruptions by affecting the normal operation of the physical infrastructure in other ways."

Among other things, the Joint Forum Report stated that financial supervisory authorities and financial industry participants have a shared interest in promoting the resiliency of the financial system to MODs. This interest is the result of multiple factors, including:

- The pivotal role that financial intermediation plays in facilitating and promoting national and global economic activity by providing the means for making and receiving payments, for

---

5 The Joint Forum is a group of senior financial sector supervisors working under the auspices of its parent committees: the Basel Committee on Banking Supervision, IOSCO, and the International Association of Insurance Supervisors.

6 See http://www.bis.org/publ/joint17.pdf.

7 According to the Joint Forum Report, an MOD is "a high-impact disruption of normal business operations affecting a large metropolitan or geographic area and the adjacent communities that are economically integrated with it. In addition to impeding the normal operation of financial industry participants and other commercial organisations, major operational disruptions typically affect the physical infrastructure."

8 The Joint Forum Report defines "physical infrastructure" as "those assets, facilities and services provided (…) and widely depended on by business, governments and individuals for the day-to-day activities."

borrowing and lending, for effecting transactions, for insuring risks, and for raising capital and promoting investment.

- The concentration of clearing and settlement processes in most financial systems. Disruptions of these processes can have material adverse consequences for a financial system and prevent significant market participants from completing transactions and meeting their obligations.

- Deepening interdependencies among financial industry participants within and across jurisdictions. The velocity with which money and securities turn-over on a daily basis underpins the considerable interdependencies – in the form of settlement risk and, ultimately, credit and liquidity risks – among intermediaries and investors. The result is that operations disruptions at one intermediary can cause difficulties at others. Furthermore, given the continued globalization of markets, disruptions in one jurisdiction could have serious implications for others through contagion effects.

- The possibility of terrorist or other malicious attacks targeted, directly or indirectly, at the infrastructure of the financial system.

- The importance of public confidence in the ability of financial systems to function smoothly. Repeated or prolonged interruptions to the operation of a financial system undermine confidence and could result in a withdrawal of capital from that system by domestic and global participants.

The Joint Forum Report made clear that the purpose of business continuity management (which includes DRPs) is to minimize the operational, financial, legal, reputational, and other material consequences arising from a disruption. Effective business continuity management concentrates on the impact, as opposed to the source, of the disruption, which permits financial industry participants and supervisors/regulators to concentrate on how to recover from an event versus focusing on the cause of a disruptive event. At the same time, however, organizations cannot ignore the nature/cause of the risks to which they are exposed. For example, organizations located in earthquake-prone regions commonly plan for the impact of earthquake-related MODs.

The Joint Forum Report also noted that effective business continuity management typically incorporates a number of key components,[9] including BCP and an alternate site with distinct physical infrastructure, sufficient current data and the necessary equipment and systems, and sufficient staff – in terms of number and expertise – to recover and maintain critical operations and services consistent with its recovery objectives. In light of these key components, the Joint Forum Report sets forth a number of key principles that covered seven major areas.[10]

### B. Recent Events Relevant to Intermediary BCPs

[9] These components also included business impact analyses, recovery strategies, programs to ensure the availability of the physical, technological, and personnel resources necessary to implement such plans promptly, testing, training, awareness, communication, and crisis management.

[10] The Joint Forum principles are set forth in Appendix 1.

Recent events, emerging threats and industry initiatives have highlighted the possible need for additional regulatory attention for effective intermediary BCPs and recovery strategies, including some of the potential problems and future challenges that existing intermediary backup systems face. A number of major international markets, including the U.S., the U.K. and Australia, have confronted these issues. For example:

**United States**

- In August 2014, JP Morgan Chase & Co. first announced that the firm was the subject of a cyber-attack and later confirmed that the attack compromised information from 76 million households and 7 million small businesses. While it appears that no money was stolen from customers, and that account numbers, passwords and dates of birth were not breached, the hackers had access to contact information, including name, address, telephone number and email addresses as well as internal JP Morgan information about the system users.[11]

- During the course of 2013, and continuing throughout 2014, the U.S. Federal Executive Boards in New York City and Northern New Jersey, in partnership with FEMA Region II, The Department of Health and Human Services Region II, NYC Department of Health and Mental Hygiene, Securities Industry and Financial Markets Association (SIFMA) and the Clearing House Association have sponsored a two year series of pandemic influenza continuity exercises – tabletop exercise 2013 (complete), full scale exercise 2014 – to increase readiness for a pandemic event and ensure continuity among Federal Executive Departments and Agencies, U.S. Court, state, and local jurisdictions as well as the private sector. The objectives of the exercise are to mitigate vulnerabilities during a pandemic influenza outbreak; to identify gaps or weaknesses in pandemic planning or in organization pandemic influenza continuity plans, policies, and procedures; and encourage public and private organizations to jointly plan for, and test, their pandemic influenza plans. Pandemic influenza is unique in that, unlike many other catastrophic events, it will not directly affect physical infrastructure. While a pandemic will not damage power lines, banks, or computer networks, it will ultimately threaten all critical infrastructures by its impact on an organization's human resources causing a loss of essential personnel from the workplace for weeks or months.

- On July 18, 2013, over sixty U.S. broker-dealers, clearing firms and exchanges working under the umbrella of the Securities Industry and Financial Markets Association (SIFMA) staged a mock cyber-attack to test their ability to cope with a Street-wide virus that seeks to invade their trading systems. Known as Quantum Dawn 2, the exercise expands upon a similar 2011 initiative where SIFMA's members gathered in one location to compare notes concerning how they addressed hacking. The new exercise was intended to portray, in a more realistic way, how communications will work in the event of a real attack through e-mails and telephone calls by requiring firms to remain in their own offices. A similar event may

[11] It is important to note that cyber-attacks (or incident response planning) and BCP are separate, but sometimes related activities. Indeed, in many instances, a cyber-attack may not affect any operational functions of the victim. This distinction is particularly important when considering data. That is, there is a trinity when it comes to data from a cyber-security perspective: confidentiality, integrity, and availability. BCP deals primarily with the latter, but cyber-security must address all three.

take place in 2015.

- U.S. national securities exchanges closed for two business days in the wake of Superstorm Sandy, a major storm that hit the east coast of the U.S. during October 2012, and which caused significant damage in lower Manhattan, among other places. Press reports stated that, while the markets planned to open on the first day of the storm (with the NYSE planning to operate under its contingency plan as an electronic-only venue), after consultation with market participants, along with the U.S. Securities and Exchange Commission (SEC) and its staff, and in light of concerns over the physical safety of personnel and the possibility of technical issues, the national securities exchanges jointly decided not to open for trading on October 29 and October 30, 2012. The market closures occurred despite the securities industry's annual test of how trading firms, market operators and their utilities could operate through an emergency using backup sites, backup communications, and disaster recovery facilities. (This test occurred on October 27, 2012, just two days before the storm). It appears that the test did not uncover issues that would preclude markets from opening two days later with backup systems, if they so choose. In its proposing release for Regulation SCI,[12] the U.S. SEC stated that it considered the impact of Superstorm Sandy on the securities markets, particularly with respect to business continuity planning and testing.

- On August 16, 2013, the U.S. Commodity Futures Trading Commission (CFTC) joined the U.S. SEC and the Financial Industry Regulatory Authority in the U.S. (FINRA) in issuing a staff advisory on business continuity and disaster recovery planning.[13] The advisory, which was the result of a joint review by these regulators, highlighted lessons learned in the aftermath of Superstorm Sandy. Specifically, the CFTC's Division of Swap Dealer and Intermediary Oversight, the SEC's Office of Compliance Inspections and Examinations (OCIE), and FINRA issued the advisory to encourage firms to review their business continuity plans so as to improve responses to and reduce recovery time after significant large-scale events.

**United Kingdom**

- In the United Kingdom, the Financial Conduct Authority (FCA) has undertaken a number of initiatives including (1) market wide exercises (running since 2003) – involving the participation and assessment of BCPs covering different scenarios over different years, *e.g.*, pandemic, severe weather, and payment services disruption; (2) a cyber and technology resilience benchmarking exercise involving the top nine U.K. banks and key exchanges, which took place in 2011;[14] and (3) *Waking Shark I*, a cyber-themed exercise undertaken in March 2011, across the investment and wholesale banking community, with a follow-up *Waking Shark II* in November 2013. As part of several policy recommendations made by the U.K.'s Financial Policy Committee in June 2013, a program of work has been established at a cross-authorities level (HM Treasury, FCA, Bank of England / Prudential Regulation

---

12 See http://www.sec.gov/rules/proposed/2013/34-69606.pdf. The rule is now final. See also http://www.sec.gov/rules/final/2014/34-73639.pdf.

13 See http://www.cftc.gov/PressRoom/PressReleases/pr6667-13.

14 The report (known as the benchmarking report) was published at the end of 2013.

Authority) to undertake a cyber assessment of the core U.K. financial systems.[15]

**Australia**

- In January 2013, a large Australian market participant that is part of a global investment bank with a European head office experienced a major system outage of its middle and back office systems due to a data corruption event. This resulted in a significant increase in settlement failures and affected financial monitoring, securities transactions, position and account ledgers, and reconciliations for the broker. The outage occurred as a result of an overseas, outsourced service provider failing to follow standard procedures for system maintenance. The BCP did not consider the mitigation of a data corruption event, which hampered the timely recovery of data. Contrary to the system developer's best practice guidelines, which recommend that a completely segregated backup system be used, the participant copied its real time data to tape, which could be used to re-create the data if required. By the time the participant discovered the data corruption it had overwritten the tape (which happened at the end of each business day) and could not recover its data efficiently.

### C. Purpose and Scope of This Project

The IOSCO Board concluded that the events described above (and others) indicate that it would be appropriate to review the 2006 Joint Forum Report. As a part of that process, the Board reconsidered the issues addressed in that Report, particularly with regard to potential disruptions at intermediaries and possible weaknesses in their current BCPs and recovery strategies. C3 therefore conducted a study (described below) of both intermediaries and regulators to address potential disruptions and possible weaknesses or gaps in intermediary BCPs and recovery strategies. Among other things, this study:

- Analyzed practices associated with establishing physical and information security and testing BCPs.

- Elicited information from market intermediaries regarding the facilities, data, and software needed for backup sites and any threats posed by systems updates across facilities.

- Considered:

    - Steps necessary to assure the availability, despite a wide-area disruption, of personnel with requisite knowledge and training to perform promptly mission-critical activities.

    - Whether it would be appropriate to examine practices associated with "geographical diversity" for purposes of business continuity planning and, if so, the range of regulatory steps that may provide greater clarity regarding factors for obtaining geographical diversity.

    - Current cyber and natural threats, the associated costs to protect critical data, along with the lessons learned from the threats the industry has recently experienced. This included

[15] See http://www.bankofengland.co.uk/publications/Documents/records/fpc/pdf/2013/record1307.pdf.

looking at the potential loss of clients' or investors' information and assets or firm assets due to cyber-attacks, and responsibility of financial institutions and authorities to ensure compliance with privacy laws with respect to customer information.

- Industry-wide testing of BCPs.
- Feasibility of cross-border testing of BCPs.
- Relationships and counterparties that could have a material negative impact on intermediaries, including the impact of any group of large intermediaries that collectively handle a majority of the securities transactions in a jurisdiction.
- Systems development processes with intermediary testing of new trading/clearing systems.
- Regulatory guidance issued for BCPs.
- Whether measures are adequate to ensure high availability and resiliency of critical systems.
- Impact of intermediary outsourcing of operations, systems, data, or network development, management and maintenance work.
- Evaluation of critical vendors on BCPs.

## III. Methodology

To carry out this project, a C3 working group developed detailed questionnaires for both regulators and intermediaries to gain a fuller understanding of the regulatory frameworks and approaches taken by regulators for business continuity and disaster recovery for intermediaries, as well as of the arrangements currently in place at intermediaries.[16] These questionnaires were supplemented by two roundtable discussions that C3 convened with intermediary representatives for the purpose of identifying existing and emerging threats to intermediaries as well as to discuss current firm practices.[17] With regard to both the questionnaire and the roundtables, C3 sought information concerning experiences and viewpoints pertaining to, among other things, what constitutes effective business impact analyses, recovery strategies, and business continuity plans, as well as information concerning existing programs for testing, training, awareness, communication, and crisis management.

After obtaining the questionnaire responses and considering the input from the roundtables, the working group analyzed the results in the context of current intermediary business continuity management practices and relevant regulatory frameworks. The results of this work are set forth in the form of a range of sound practices that regulators could consider as part of their oversight

[16] C3's work was carried out in parallel with the IOSCO Committee on the Regulation of Secondary Markets (C2), which also undertook a project on secondary market business continuity and disaster recovery planning.

[17] The roundtables were held in Rome, Italy (Dec. 2013) and Marrakesh, Morocco (Apr. 2014). Summaries of those roundtables are set forth in Appendix 2.

of market intermediaries and which such intermediaries may find useful in their development and implementation of effective BCPs and recovery strategies. IOSCO recognizes that not every sound practice will be appropriate or equally effective for all large market intermediaries. However, IOSCO would still encourage individual market intermediaries to consider these sound practices where relevant to their activities.

## IV. Study Results

### A. Current Intermediary BCPs and Regulatory Approaches

#### 1. Overview

Most IOSCO members who responded to the survey (Supervisor Respondents) have at least some requirements in place for market intermediaries to maintain BCPs (*e.g.*, rules or formal guidance that can be used to help enforce rules). For example, most Supervisor Respondents require intermediaries to have BCPs and other arrangements to ensure the continuation of business in the event of an MOD, such as natural disasters or terrorism. Some Supervisor Respondents identify, for the intermediaries they oversee, the types of disasters that firms must consider as an MOD.[18] Several European regulators emphasize the need for back-up of electronic information systems, IT, and software.[19]

Despite these requirements, however, it appears that there are relatively few jurisdictions that impose the kind of "requirements" with respect to BCPs where failure of a firm to comply might subject it to penalties. While many Supervisor Respondents note that they require market intermediaries to have BCPs in place, they did not always identify penalties associated with non-compliance. Conversely, a number of jurisdictions publish "best practices" for intermediaries, which they believe firms would optimally follow. More detailed descriptions of the requirements or guidance of IOSCO member jurisdictions are set forth in Appendix 3.

Nonetheless, the overwhelming majority of intermediaries that responded to IOSCO's survey (Intermediary Respondents) indicated that they have a written BCP.[20] A significant majority stated that they had not faced challenges in complying with regulatory requirements or special issues arising for cross-jurisdictional BCP requirements. A minority of Intermediary Respondents indicated that they had faced special challenges in complying with regulatory requirements or confronted unique issues arising from the cross-jurisdictional implementation of their BCPs.[21]

---

18 For example, Japan, and Mexico.

19 For example, France, Romania, and Turkey.

20 The majority of Intermediary Respondents confirmed that separate BCPs are maintained across each jurisdiction. Some of these respondents disclosed that the intermediary's BCP arrangements were governed by a global policy with local requirements followed within each jurisdiction.

21 Some examples of the challenges cited by Intermediary Respondents include (1) compliance issues associated with local regulations (Italy); (2) the required establishment of an alternative work site in the domestic country for "wide area disasters" (Japan); (3) requirements for systems recovery and uptime for the Swaps Execution Facilities (SEFs) as stipulated by the CFTC, together with requirements for segregated workplaces and data (including in recovery) (U.K.); and (4) restrictions by certain jurisdictions

Intermediary Respondents typically described their BCPs as consisting of two parts – (1) a series of procedures whereby the firm identifies threats to its business and critical operations, and (2) an assessment of the potential impact of those threats.[22] Firms also take into account numerous factors when determining the resources (*i.e.*, time and funds) to allocate for developing and implementing a BCP. A minority of Intermediary Respondents indicated that their BCPs are executed in part by third-party suppliers. The BCPs were also typically described as imposing required actions in an integrated manner across the firm, and as being approved and updated on a regular basis.

Intermediary Respondents stated that the key components of their BCPs include, among other things:

- A dedicated, fully operational contingency site.
- Instantaneous replication and off-site storage of data also stored on the in-house network. This includes periodic backup of critical information, with real-time storage in multiple secure locations for the most critical information.
- An annual, often independent, review of the BCP.
- Defined global and regional governance bodies and executive ownership of (responsibility for) business continuity management.
- Accountability to the firm's board of directors, reporting through the audit committee, risk committee or operating committee.
- Full-time business continuity management professionals.
- The embedding of business continuity coordinators in each business line.
- Defined crisis management organizations and escalation protocols, and crisis communication strategies.
- Maintenance and review to respond to changing client requirements, emerging risks and changes to the firm.
- A training and awareness program for all staff.
- A 24-hour monitoring system and network.

---

on "what can be performed offshore by legal entities of the same group that are not licensed to perform onshore activities" (U.S.).

[22] Intermediary Respondents identified, among other things, the following as major threats and impacts considered in their BCPs: threats to or unavailability of people, premises, technology and critical vendors; earthquake; fire; power failure/outage; floods; hazardous materials; bombs or dirty bombs; terrorist activity; hurricane; cyber-attacks; transportation shutdown and strikes, and civil demonstrations which affect employee commute/access; loss of IT infrastructure, building infrastructure, staff, service from external providers or external infrastructure or production; impact on customers or firm reputation; pandemic scenarios; open positions of customers, and potential losses customers incur if the firm cannot liquidate the position; and customer losses and stop loss levels.

- The firm's relationship with clearing and settlement entities. Indeed, several respondents stated that their relationship with clearance and settlement entities is deemed "critical" or at least "very important" to their operations.

Two thirds of the Intermediary Respondents[23] stated that their firm's BCP did not include different policies or procedures for different markets. These respondents stated that their BCP polices were "global," and that BCP policy and procedural differences may occur due to variations at the country/regional level by business unit rather than by market or by product.[24]

About a third of the Intermediary Respondents stated that they update their BCP policies and procedures on an ongoing process (*e.g.*, at least annually), on an "as needed" basis, or because of new regulatory requirements.[25] About a quarter of the Intermediary Respondents indicated that, as there had not been any new regulatory requirements in their jurisdiction, they had not updated their policies or procedures.

### 2. Role of Senior Management and the Board of Directors - Corporate Governance

**Regulatory Requirements**

Most Supervisor Respondents require the intermediary's senior management, board of directors, or "management board" to be responsible for oversight of the market intermediary's BCP.[26] These requirements are structured in various ways, but generally require that the intermediary's senior management, board of directors, or management board have responsibility for the organization of the firm's BCP and/or risk and compliance structure, such as BCP policies and procedures,[27] or require senior management to approve or update the board on its BCP on a regular basis.[28]

---

23 Comprising all of the respondents from Singapore, the U.K., and the U.S.

24 When asked whether the policies or procedures described in their BCPs differ depending on the market type, about a fifth of the respondents indicated that some differences exist, depending on the connectivity type, and/or unique characteristics of certain products and markets. Some respondents advised that functions were divided at the product and process level by criticality and recovery time. A few respondents noted that procedural differences may be appropriate for certain products and markets that are highly global in nature, which requires a trading and support model that provides resiliency between locations in different jurisdictions. It was noted that for more "local" products, with proprietary trading and settlement systems that are not accessible in other jurisdictions, recovery strategies may be appropriately limited to the local work area.

25 Of these firms, a number specifically referred to regulatory changes as the impetus for the updates, such as IIROC by-law 17.19, BCM governance framework ISO 22301, MAS Technology Risk Management Notice & Guidelines v4 (effective from 1 July 2014) and new CFTC regulations.

26 Although Australia does not have specific regulatory requirements for senior management, board of director or management board oversight of a market intermediary's BCP, the market supervisor reviews, as part of its ongoing proactive surveillance of participants, exchange requirements on participants to have BCP arrangements.

27 For example, Germany, Japan, Poland, Romania, Singapore, and Turkey.

28 For example, Canada (IIROC), France, and Mexico.

Other Supervisor Respondents require senior management to bear responsibility for maintaining or monitoring appropriate standards or an appropriate system of internal controls,[29] or require the specific appointment of individuals, such as a chief operations officer, to take responsibility for all or part of the BCP.[30] In the U.S., FINRA issued a rule requiring BCPs to address ten separate elements in specific areas and requires senior management to approve the plan and conduct an annual review.[31]

Part of senior management responsibility generally includes being accessible during an MOD. Thus, several Supervisor Respondents require intermediaries to have emergency contact information (call cascades) to facilitate communication, including both internal contacts (*e.g.*, senior management) and external contacts (*e.g.*, regulators, clients). Where jurisdictions have no specific requirements for emergency communication,[32] regulators state that intermediaries are nonetheless expected to maintain contact information as part of the normal BCP process, which would include internal (staff, senior management etc.) and external (clients, regulators etc.), or that resources should be devoted to internal and external communications.

**Market Intermediary Implementation**

All Intermediary Respondents confirmed that they have a designated individual responsible for business continuity management. While the Intermediary Respondents' answers reflected their various management structures, types of operations and size, the overall governance of the various BCPs can be characterized as relating to sponsorship, accountability, governance, and operations. Each of these levels is discussed in more detail below.

***Sponsorship***

The key role for the senior management "sponsor" is to set the strategic direction, provide high-level oversight of the BCP function, and to provide strategic support for the overall BCP mandate/program. At most Intermediary Respondents, BCP sponsorship was reflected at the highest level within the market intermediary with either the board of directors or management board, Chairman, President or Chief Executive Officer (or equivalent) acting as the main sponsor.

***Accountable Executive***

The majority of Intermediary Respondents identified an "Accountable Executive," such as a member of senior management or the Chief Operating Officer. Generally, the Accountable Executive was one level below the Chief Executive Officer, although at some market intermediaries, the Accountable Executive and the Sponsorship Individual were the same. At the market intermediaries where an Accountable Executive was not specifically identified, the

---

29 For example, Hong Kong, Hungary, and Morocco.

30 Korea, Italy. Mexico requires the chief executive officer of the market intermediary to be responsible for the development and oversight of its BCP. The Brazilian Central Bank requires that a director of a financial institution be responsible for managing operational risks, including risks relating to a BCP.

31 FINRA Rule 4370, *Business Continuity Plans and Emergency Contact Information*.

32 For example, Poland and the U.K.

accountability is generally assumed by a committee, which includes senior management (such as an operating committee or a steering committee).

In addition, the majority of Intermediary Respondents also made a clear distinction in relation to BCP accountability versus "crisis management." While accountability for the BCP mandate/program is usually clearly outlined, ultimate responsibility in terms of decision making during a crisis rests at a more senior level (*i.e.*, at the CEO or senior management level). Intermediary Respondents also generally had relevant crisis management committees or teams in place with clearly articulated roles and responsibilities to manage a crisis or other major incident. The committees or teams included personnel from various departments across all levels within the organization.

***Governance and Operations***

All Intermediary Respondents stated that they have a BCP governance model in place, which included functions such as BCP policy review, governance and control, compliance and reporting of risk, and conformance and validation activities to senior management and other stakeholders (including the firm's auditors and its regulators). They also confirmed that they have a dedicated internal function (*e.g.*, operations team) with responsibility for BCP operations and crisis management. The responsibilities include the implementation and roll out of BCP strategy, policy, liaising with auditors, and testing.

At the majority of Intermediary Respondents, the BCP operations team is also responsible for carrying out crisis simulations with the crisis leadership committee or team. One Intermediary Respondent noted that only a designated crisis management team may "declare a disaster," and that a designated recovery team is responsible for determining activities that are critical, technology resource requirements, minimum number of staff and supporting requirements necessary to continue key business functions, and to confirm Recovery Time Objectives (RTO) and Recover Point Objectives (RPO) requirements.

### 3. Mission Critical Systems and Activities

**Regulatory Requirements**

Most Supervisor Respondents require that the market intermediary's recovery plans set forth recovery objectives sufficient to permit the market intermediary to return to normal operations within a reasonable time. In addition, some Supervisor Respondents[33] specifically identified IT and other critical electronic systems as mission critical objectives. Other Supervisor Respondents[34] gave market intermediaries the flexibility to determine what systems are critical in the context of their own businesses.

Some regulators have more detailed requirements:

- Several jurisdictions (Hungary, Korea, Mexico, and Singapore) establish recovery time objectives for critical systems. For example, in Korea, intermediaries (and other financial

[33] For example, Spain, Poland, Morocco, Germany, and Italy.

[34] For example, France, Italy, Mexico, and Singapore.

firms) must establish and operate a disaster recovery center (DRC) equipped with appropriate equipment and staff to ensure its business continuity in case the main computer center becomes inoperable due to any system failure, natural disaster or other event. The DRC must be located in a safe place within a certain distance from the main computer center. Further, the primary computer center must be recoverable within three hours.

- Romania requires intermediaries to maintain two back-up servers that can save data and other information on a real-time basis.

- Poland requires market intermediaries to ensure that IT systems are protected against loss of data from disruptions.

**Market Intermediary Implementation**

***How market intermediaries prioritize functions, processes and systems as critical***

Most Intermediary Respondents prioritize relevant functions, processes and systems, and deem some of them "critical," although the process varies. For instance, functions, processes and systems are often deemed to be critical based on:

- The impact on the firm if the function, process or system becomes unavailable, including expected recovery times of processes (RTOs), with the shortest RTOs given the highest priority. One Intermediary Respondent indicated that no process is deemed critical if it can be safely deferred for more than two weeks.

- The impact an outage would have from a financial, customer, reputational, legal or regulatory perspective.

- How directly the function, process or system is linked to the firm's core business. For example, one Intermediary Respondent described their recovery prioritization as follows: (1) trading and settlement functions and other "critical" systems recovered first, (2) email, workflow, and risk management are deemed "important" and recovered second, and (3) research and administration are generally "non-critical" and recovered only if warranted.

- Whether the function, process or system has been classified as "strategic." For one Intermediary Respondent, this includes trading, and front and back office operations.

Several Intermediary Respondents use a "business impact analysis" approach in prioritizing critical functions, processes, and systems. Under a business impact analysis approach, each major operating department prepares its own business impact analysis and the combined business impact analyses are used to prioritize the overall business' critical functions, processes and systems. Some Intermediary Respondents also use this approach to determine RTOs for various functions, processes, and systems.

***Tools and methods used by market intermediaries to assess their current BCPs***

Intermediary Respondents described various tools and methods they use to assess their current BCPs to ensure high availability and resiliency of critical systems in times of an MOD. These included such things as:

- Regular examination and testing of the BCPs (usually annually) for the purposes of identifying areas that require improvement and implementing necessary changes. This may include assuming the complete unavailability of key staff, utilities and critical systems, data, and service providers.

- Using a third-party consulting firm or an external information technology provider to assess the BCP.

- Reviewing whether:

    - There are multiple data centers, redundant networks, and scheduled data backups.

    - There are dependencies on technology, people and third-party service providers.

### 4. Back-up Facilities

**Regulatory Requirements**

Most Supervisor Respondents require, at a minimum, some back-up procedures or facilities to be in place. A few suggest that firms address the potential concentration risks inherent in any wide-area disruption. For example, in Singapore, the Monetary Authority of Singapore (MAS) has set out that firms' BCPs should address specifically geographic concentration and requires firms to separate geographically primary and secondary (back-up) sites, as well as critical business operations.[35] MAS expects financial institutions to implement and test backup and recovery capabilities at the individual system or application cluster level in order to strengthen recovery measures and diversify risk.

Examples of additional regulatory approaches include Hungary, where the regulator's guidelines require intermediaries to consider the storage of back-up information and the establishment of back-up facilities that are geographically separated from primary operations sites, while Italy requires regulated intermediaries to identify in their BCPs key emergency response employees in different geographic locations.

In the U.S., an interagency paper was published that set out four sound practices pertaining to the appropriate back-up capacity for operations sites and data centers for the recovery and resumption of clearance and settlement activities in critical financial markets.[36] Supervisor Respondents noted an array of additional requirements applicable to back-up facilities.[37]

---

35 Principles 6 and 7 of the MAS Business Continuity Management Guidelines.

36 *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, Securities Exchange Act Release No. 47638 (April 7, 2003).

37 Various Respondent Supervisors impose, among others, the following types of requirements: (1) an external contingency site for back-up files and a requirement that files be sent to this site on a daily basis; (2) that the BCP address specifically in their BCP physical backup locations (*e.g.*, that are sufficiently secure to safeguard the firm's material resources and documents or that there be at least two back-up systems in different locations); and (3) that back-up facilities and infrastructure be established in accordance with recognized information technology security and continuity standards.

Finally, a few Supervisor Respondents specifically address (through guidance or some form of requirements) assumptions that underlie an intermediary's BCP, such as that alternative facilities will remain accessible and operational. One jurisdiction (U.S. SEC/FINRA) does not require market intermediaries to explicitly state underlying assumptions, but notes that it is good practice. Another jurisdiction (Singapore) specifies that market intermediaries should challenge all strategic and planning assumptions regularly to assess their applicability. Finally, Italy requires annual testing of assumptions.

**Market Intermediary Implementation**

About half of the Intermediary Respondents stated that they established back-up facilities in connection with their BCPs.

***Data and software requirements used by market intermediaries at back-up sites***

Intermediary Respondents generally take one of two approaches to data and software requirements at their back-up sites. Approximately 40% of the Intermediary Respondents advised that their "independent" (*i.e.*, leased) back-up sites mirror their primary business operation sites (*i.e.*, there are no special or different data or software requirements in place at their back-up sites). Most of the remaining Intermediary Respondents indicated that they had special data and software requirements in place at their leased back-up sites. A small number of Intermediary Respondents indicated that they relied on operational business sites owned and controlled by them (both local and offshore) to assume the work of any center made non-operational by an MOD.

***Location of back-up sites relative to primary business operation sites***

Most Intermediary Respondents[38] consider geographical diversity as part of their business continuity planning. This includes those that have remote login capability (via VPN) to log on to their data centers as one means of encouraging geographic diversity.

The policy of a majority of Intermediary Respondents is to have a minimum distance of 20 kilometers between their back-up site and their primary business operations site, although the minimum distance ranged from 10 to 1,000 kilometers. Some Intermediary Respondents locate their back-up sites further away to ensure they are on different communication and power grids, thus building their network redundancy capability in the case of an MOD,[39] although others place their back-up sites closer to the primary business operation in order to be able to meet intra-day commitments. In addition, a few Intermediary Respondents also consider key access routes as part of their planning for location of back-up sites, locating them close to major access routes and/or public transportation.

***Regulatory hurdles faced by market intermediaries in setting up back-up sites***

Most Intermediary Respondents stated that they faced no regulatory hurdles in setting up back-up sites, largely due to the fact that operational and back-up sites were located a minimum

[38] For example, Brazil, Canada, Korea and U.S.

[39] For example, one market intermediary in Brazil has a back-up site 600 kilometers away from its primary business operation site, one in Canada was 50 kilometers away, and one in Japan was 40 kilometers away.

distance from each other (albeit in the same jurisdiction). Some Intermediary Respondents noted, however, that when potential back-up sites are considered, they must seek to ensure that the choice would permit them to comply with data privacy laws and regulations. For example, securities regulators in the European Union (EU) generally do not permit cross-border migration of data. In addition, firms within the EU face specific regulatory hurdles when data is shared or transmitted outside of the EU and are required to incorporate "safe harbor principles" and "EU model clauses" whenever information or data is shared with firms providing outsourced services.

### 5. Protection of Data and Assets, Including Security Measures

**Regulatory Requirements**

In general, Supervisor Respondents are of the view that security controls should be implemented and extend to both information and facilities, under both normal operating conditions and MODs. However, most Supervisor Respondents do not have specific rules applicable to how a market intermediary's BCP should address the firm's physical and information security. In addition, although some Supervisor Respondents have general rules in place that require intermediaries to safeguard information and comply with privacy laws, only two of them require applying those rules specifically in the context of the triggering of a BCP in the case of an MOD. In addition, although a number of Supervisor Respondents mentioned physical security as a requisite for alternative or back-up sites in order to preserve critical documentation and equipment, they do not impose any specific requirements in this regard.

**Market Intermediary Practices**

Most of the Intermediary Respondents confirmed their commitment to protecting the privacy of the firm's clients and of its associated data. A majority of Intermediary Respondents have general global and/or regional privacy policies and procedures in place to identify and manage privacy risks and to ensure compliance (or prevent breaches) with relevant privacy laws and protection of assets.

It is unclear, however, whether many Intermediary Respondents' BCPs include specific policies and procedures regarding data privacy and asset protection. The security controls implemented by Intermediary Respondents extend to the protection of physical facilities, information (*e.g.*, in order to comply with privacy laws), to guard against cyber-attacks and to ensure data back-up. Moreover, all Intermediary Respondents confirmed that they had a defined security and IT policy in place outlining appropriate controls (technical, logical and administrative) to restrict access to physical assets and information. Yet not all Intermediary Respondents appear to have assigned specific roles and responsibilities to staff that would be triggered in case of an MOD.

Security policies in place at Intermediary Respondents for general application are set as a global mandate, but not necessarily tailored to apply in the context of triggering a BCP in case of an MOD. That is, such policies are not in all cases applied to data and assets *maintained for recovery purposes* (*e.g.*, backup data and recovery facilities).

In addition, most Intermediary Respondents confirmed that they have an array of specific procedures in place (sometimes including testing) to address "cyber risks" that could lead to client or investor information and asset loss. These range from comprehensive cyber-attack

policies to limited policies (*e.g.*, only related to data leakage or privacy policy guidelines and incident escalation policies).

### 6. Critical Personnel

**Regulatory Requirements**

Different regulatory efforts have been made at an international level to ensure the availability of critical personnel within the context of business continuity plans. One of the most common requirements noted by Supervisor Respondents is that firms must have critical and qualified personnel available to address an MOD effectively, *i.e.*, the personnel must have the appropriate training and be prepared to respond in case of any event of any foreseeable MOD. Other requirements that were noted include requirements (1) for an intermediary to staff a fully operational disaster recovery center, and (2) that the intermediary must have in place an internal organization structure that can handle effectively any reasonably foreseeable MOD. Some of the Supervisor Respondents have set minimum personnel qualifications and/or issued guidelines describing an optimal training level for critical personnel in order for them to respond effectively to an MOD.

**Market Intermediary Practices**

Most of the Intermediary Respondents confirmed that they have policies and business continuity plans in place to ensure critical personnel are available in the event of an emergency. Steps they have taken to help ensure such availability include the following:

- 68% confirmed they have alternate worksites and workstations available;
- 23% identified their staff had remote access solutions that would allow employees to work from their homes;
- 3% confirmed that their employees have access to the firm´s mobile devices to keep them in contact;
- 53% designate key positions and personnel;
- 28% have designated back-up personnel or alternate personnel; and
- 8% have call trees or automatic email messaging in place.

### 7. Relationships with Third Parties

A number of Supervisor Respondents identified as an important issue relationships with third parties (*e.g.*, a supplier, or a subcontracted supplier whether located in the domestic jurisdiction or abroad), who may be unable to provide contracted services during an MOD, thus threatening the effective implementation of the intermediary's BCP. Some regulators believe that risks to intermediaries derived from outsourcing operations to third parties, including networks and data storage and recovery, must be anticipated during the development of BCPs. The financial industry may be potentially vulnerable to collective 'supplier concentration risk,' whereby the majority of the firms rely on a few core suppliers for certain services. For example, in the U.S., under FINRA rules, an intermediary must address in its BCP the firm's existing relationships

with other intermediaries and counterparties. In addition, under FINRA requirements, each BCP must address, among other things, critical business constituent, bank and counterparty impact related to an emergency or significant business disruption.

As IOSCO has stated in the past, an outsourcing market intermediary, including its management and its governing authority, retains full legal liability and accountability to the regulator for any and all functions that the firm may outsource to a service provider to the same extent as if the service were provided in-house.[40] IOSCO has defined intermediary outsourcing "as an event in which a regulated outsourcing firm contracts with a service provider for the performance of any aspect of the outsourcing firm's regulated or unregulated functions that could otherwise be undertaken by the entity itself."[41] It is intended to include only those services that were or can be delivered by internal staff and management. A regulator may impose sanctions and penalties on an intermediary in its jurisdiction for violations of statutory and regulatory requirements that result in whole or in part from the failure of a service provider (whether licensed or unlicensed) to perform its contractual obligations for the intermediary.

A number of the Supervisor Respondents specifically stated that intermediaries are required to identify outsourcing arrangements.[42] Most respondents described regulations that otherwise govern intermediaries' third-party dependencies, including how to address the impact that such relationships may have on the intermediary. In some jurisdictions,[43] intermediaries are specifically required to maintain responsibility over the actions of any third parties on which they rely. Canadian market intermediaries must ensure that third-party service providers have adequate safeguards for, where appropriate, disaster recovery capabilities. They should also develop and test a business continuity plan to minimize disruption to the firm's business and its clients if the third-party service provider does not deliver its services satisfactorily.

Certain jurisdictions impose more unique requirements. For example, Italy requires market intermediaries to identify all outsourcing firms and that they enter into an agreement with the outsourcing firm that requires the firm to "guarantee" a minimum level of operation in emergency crisis and identifying suitable, tailored and detailed business continuity solutions. Italy also requires that the intermediary have access to any information held by the third party that might be necessary to assess the quality of their services and possible corrective actions.

In India, intermediaries must have separate contingency plans for each outsourcing arrangement and submit them to the regulator. In Poland, Singapore, and Spain, intermediaries are required to ensure that outsourcing arrangements are viable and that the third parties have the requisite skill and knowledge to undertake duties on behalf of the intermediary. Singapore provides details, requiring intermediaries first to "identify the interdependencies and the extent of reliance on third parties by their critical business functions" and then to assess the business continuity preparedness of these third parties. Furthermore, Singapore requires intermediaries to ensure that third parties develop and establish disaster recovery contingency frameworks, to review, evaluate

---

40 See IOSCO's Final Report *Principles on Outsourcing of Financial Services for Market Intermediaries* (Feb. 2005), available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD187.pdf.

41 *Id*.

42 For example, Brazil, Canada, Hungary, Italy, Mexico, and Singapore.

43 For example, Australia, Canada, Italy, and Morocco.

and test regularly BCPs. The MAS also sets out that intermediaries should have contingency plans based on "credible worst-case scenarios in third parties."

France's domestic regulations provide that (1) the continuity and quality of services provided by the market intermediary should not be impacted if outsourcing services are interrupted, and (2) firms must ensure that external service providers implement contingency mechanisms in the event of a serious problem affecting the continuity of the service or factor into their own BCP the eventuality that an external service provider may fail to carry out its tasks.

Most Intermediary Respondents indicated that they have entered into Service Level Agreements (SLA) and Non-Disclosure Agreements (NDA) with their providers. However, some Intermediary Respondents indicated that they have decided to reduce outsourcing to a minimum, thus avoiding delegating critical processes as much as possible.

## 8. Other Aspects

### Business Impact Analyses, Including Financial and Operational Assessments

A significant number of regulators stated that they required a business impact analysis (BIA).[44] Most regulators note that completing a business impact analysis is important to ensure that intermediaries consider all relevant risks and have appropriate controls in place with a view to minimizing overall exposure to risk. A few jurisdictions (Australia and the U.K.) do not specifically require a business impact analysis, but provide guidance to intermediaries regarding these issues. Where the regulatory framework does not provide for specific requirements, intermediaries are assessed on their effectiveness of the plans based on internationally accredited standards, *e.g.*, ISO standards.

### Communications: Regulatory Reporting, Public Disclosure and Internal Structure

#### *Reporting to Regulators*

Regulatory reporting requirements or guidelines vary across IOSCO members. Most Supervisor Respondents do not require their intermediaries to provide them with a copy of the firm's BCP (with the exception of France), but BCPs may be reviewed upon request or as part of the on-site inspection of the intermediary (*e.g.*, U.S. and Hungary). In a few jurisdictions (*e.g.*, Italy), firms must provide the regulator with periodic updates to the BCP (and in the event of a major change, the disclosure must be made "promptly").

A few jurisdictions have specific supervisory guidelines either suggesting or requiring that an intermediary report any incidents/operational disruptions to the regulator,[45] such as to report promptly any serious emergency, or a summary of IT breakdowns in bi-annual reports (Poland). Some Supervisor Respondents also require intermediaries subject to their regulation to (1) notify

---

[44] For example, Brazil, Canada (IIROC), France, Germany, Hong Kong, Hungary, India, Italy, Japan, Mexico, Poland, and Singapore. A BIA seeks to identify which business units/departments and processes are essential to the survival of the entity, how quickly essential business units and/or processes are able to resume full operation following a disaster situation, as well as the resources required to resume business operations. The BIA does not address recovery solutions.

[45] For example, France, Italy, Japan, Morocco, Mexico, and Singapore.

the regulator of a potential or actual breach of customers' information and/or of illegal activity, (2) address in their BCP communication channels with counterparties, authorities, vendors and the media and/or (3) impose upon the intermediary´s CEO the ultimate responsibility for developing and implementing a proper communications policy.[46]

Korea requires prompt reporting of a serious accident that relates to the suspension or delay of computer operations, financial incidents related to manipulation of computer data or programs, and information processing system failures. Both Turkey and Romania require intermediaries to notify regulators about certain changes to their BCPs. In the U.K., the regulator has issued guidance that it expects to be notified if (1) a firm identifies a significant operational exposure, (2) a firm invokes its BCP, or (3) a significant change to a firm's organization, infrastructure, or business environment occurs. Regulators in Turkey and the U.S. (FINRA) require that emergency contact information be reported to them.

***Public Disclosures***

BCP public disclosure obligations vary widely. In some jurisdictions, regulators have specific rules under which intermediaries must disclose BCP requirements to their clients/customers and outline the firms' plans to respond to significant business disruptions (*e.g.*, Japan and U.S. (SEC/FINRA)). Others do not.[47]

Singapore requires senior management to attest to the Board that it is aware of and accepts the residual risks and allows the intermediary to decide whether to disclose information to customers and counterparties. In Turkey, intermediaries must either provide disclosure about workflow procedures and contingency plans to customers when they open an account or make them available online. In Canada, the IIROC does not require disclosure of its BCP to clients.

Whether addressed in the BCP or not, the majority of Intermediary Respondents make some disclosures concerning their BCPs to clients or other stakeholders. However, it should be noted that due to confidentiality concerns, the BCP information provided is often general in nature (*e.g.*, posted on the intermediary's Web site, provided to the client during the client onboarding process), or provided only upon request (*e.g.*, to institutional clients conducting due diligence). Those firms that do not make such disclosures referred to confidentiality issues as the main reason.

A minority of the Intermediary Respondents addressed the question regarding disclosure of an MOD to clients or the market generally, or to their regulator. Those respondents who indicated that they disclosed information regarding an MOD indicated that they did so pursuant to a formal crisis communications plan to key stakeholders, to regulators for any "material" MOD and whenever mandatory, and/or to clients affected by the MOD. Some of the Intermediary Respondents indicated that such disclosures appear to have a positive "marketing" effect when a client is selecting a firm, or may engender trust in that firm.

---

[46] For example, Australia, Singapore, the U.K. and Japan. Germany is currently considering such requirements.

[47] In Mexico and Hungary, BCPs are considered confidential and do not need to be publicly disclosed. In Mexico, the information may be provided to authorities in accordance with relevant federal law protecting information.

### *Internal Communication Policies*

The majority of Intermediary Respondents disclosed that their formal BCPs included documented procedures for internal and external communications with clients, service providers, regulators and other stakeholders (*e.g.*, media). Most Intermediary Respondents also use call cascades and call trees, which are procedures that firms use to handle communication to critical personnel in case of an MOD, regardless of possible automated emergency notification systems that could be implemented. Some intermediaries utilize dedicated crisis management and/or communication teams or rely on senior management for the dissemination of BCPs and/or MODs related information internally and externally, and often rely upon templates or draft messages to prepare information for external release. A few Intermediary Respondents[48] stated that their compliance team communicates with the regulator(s) in relation to BCP/MOD issues.

### *Customer access to funds and securities, if an intermediary determines that it is unable to continue business*

Numerous Supervisor Respondents identified requirements that ensure protection of customer funds and securities in the event an intermediary determines that it is unable to continue business.[49] Some jurisdictions have no specific requirements, but have published principles aimed at protecting client funds.[50]

### *Training: BCP awareness, crisis management training for leadership/management*

A large number of the Supervisor Respondents require, or suggest through guidelines, that firms implement staff training.[51] Turkey noted that employees needed to be informed of their responsibilities in light of the BCP and provided with written procedures laying them out. Some regulators also require intermediaries to have succession plans for critical staff and senior management.

Training critical personnel is important for 74% of the Intermediary Respondents; most of them use mock drills, business continuity plan or disaster recovery testing, training exercises and simulations, as well as "tabletop" exercises or tabletop simulations.[52] 24% create staff awareness of business continuity plan policies and procedures by disseminating material for reading, such as online training, distribution of hardcopies of critical information, pamphlets, information cards or the BCP plan itself. 25% confirmed that they use seminars, lectures or meetings to train staff.

---

48 For example, Australia, Singapore, and U.S.

49 For example, Canada (IIROC), France, Hungary, Italy, Japan, Mexico, Morocco, Poland, Spain, Turkey, and the U.S. (SEC/FINRA/CFTC). In Spain, Poland, Turkey, and the U.S. (SEC/FINRA/CFTC), funds may be transferred from the failing firm to another intermediary.

50 Australia and Morocco both reported that there is a specific guarantee fund structure to ensure that customers are made whole in the event a business fails.

51 For example, Brazil, Canada, Germany, Hungary, India, Italy, Japan, Korea, Mexico, Singapore, the U.K., and the U.S. (SEC/FINRA/CFTC). However, a few jurisdictions stated in response to the IOSCO survey that they have no specific requirements (*e.g.*, Australia, Morocco).

52 A "table top" exercise, also known as a "walk through," plays out scenarios "on paper" with no actual enactment of the BCP.

## B. Testing/Mock Scenario Drills and Exercises

### Regulatory Requirements

Almost all Supervisor Respondents require testing by market intermediaries of their BCPs on a regular basis. Some regulators require that testing be conducted on an annual basis[53] while others require (either by rule or guidance) regular or periodic testing but do not specify precise timelines for testing.[54] In addition, some regulators require larger market intermediaries to conduct testing of their BCP plans more often than smaller intermediaries.

As part of their on-site inspections, some regulators (*e.g.*, Hungary) examine whether the market intermediary has completed testing of its BCP by, for example, completing mock drills and other exercises. In addition, some regulators (*e.g.*, Singapore) also conduct industry-wide mock drills at regular intervals to assess sector-wide responses to potential MODs.

### Market Intermediary Implementation

The majority of Intermediary Respondents conduct testing of their BCPs annually while others conduct testing quarterly, semi-annually or bi-annually. Intermediary Respondents indicated that the frequency of BCP testing depends on, among other things, the:

- Criticality of the business function and supporting technologies.
- Existing regulatory requirements.
- Potential issues identified during previous BCP testing.

In addition, two-thirds of Intermediary Respondents indicated that they participate in industry-wide or cross-border testing of their BCPs with other market intermediaries, such as during the U.S. Securities Industry and Financial Markets Association's (SIFMA) annual industry-wide test.

Areas tested at least annually by most market intermediaries through stress testing based on different scenarios[55] include, among other things:[56]

- Crisis/emergency communications (including call tree/notification to ensure employee can be reached).
- Information technology infrastructure resilience and recovery capability.
- Workplace, data center and critical function recovery capability.

---

53 For example, Canada (IIROC), Germany, Italy, Korea, Mexico, Romania, Singapore, Turkey, and the U.S. (SEC/FINRA).

54 For example, Australia, France, Germany, Japan, Poland, Spain, the U.K., and the U.S. (CFTC).

55 Other types of scenario tests performed by market intermediaries include "table top," and "walk-through" exercises and data center "switching" tests. *See also* note 52, above.

56 Less frequently, Intermediary Respondents report that they will also test less critical applications.

- Back-up site operating capability.

- Alternative data center availability and functionality.

Most Intermediary Respondents summarize test results in a report, which is reviewed and/or signed off by one or more responsible parties.[57] The results of BCP testing or mock testing are generally used to assess whether changes are needed to the market intermediary's BCP. In addition, if a test "fails," some Intermediary Respondents indicated that they repeat it again after appropriate changes are made to the BCP.

### C. Oversight of Intermediary Business Continuity Plans

**Overall Review Process**

A number of Supervisor Respondents[58] gather information about market intermediary BCPs as part of their routine supervisory oversight and risk assessment processes. In two markets -- Hong Kong and Singapore – regulators also conduct industry-wide surveys to gauge the extent of the adoption and implementation of sound BCP principles.

Other jurisdictions have more regimented oversight programs, which assess and evaluate the processes and internal controls of all member intermediaries.[59] For example, in Brazil, the BSM[60] analyzes BCP documentation and visits alternative work sites. It also evaluates tests performed by the intermediaries that it supervises. In France, the ACPR[61] requires its regulated firms to complete a BCP questionnaire. In addition, the ACPR has a specific IT risk assessment unit within its on-site inspection corps, which periodically carries out wide-ranging supervision of firms' business continuity and disaster recovery planning. In the U.S., should a BCP be triggered, the SEC and FINRA may examine the underlying disruptive event and consider the "in-practice" effectiveness of the BCP. The CFTC requires that futures brokers (futures commission merchants) have their BCPs reviewed every three years by an independent party.

The consequences of routine supervisory review of BCPs vary. In the U.K., for example, market intermediary BCPs are scored based on the potential risk of non-compliance with the FCA's objectives. Similarly, in Australia, firms are also risk-rated on a number of categories, including the BCP. For virtually all jurisdictions, however, the survey results made clear that in those jurisdictions where BCPs appear to be inadequate, regulators contact and engage proactively with firms to improve the plans.

---

57 This could be the BCP sponsor, internal audit, external auditors, senior management, and/or the board of directors/management board.

58 For example, Australia, Germany, Hong Kong, Hungary, India, Mexico, Morocco, Netherlands, Poland, Spain, and the U.K., and the U.S. (SEC/FINRA and CFTC).

59 For example, Brazil, Canada, France and the U.S. (CFTC).

60 The BSM is the Brazilian self-regulatory organization in charge of BM&FBOVESPA market surveillance and supervising market participants.

61 The ACPR (*Autorité de contrôle prudentiel et de resolution*) is responsible for supervising the banking and insurance sectors in France.

Four of the Supervisor Respondents identified "significant issues" that they found as a result of their BCP review process and that market intermediaries needed to address.[62] In Australia, for example, ASIC identified a few intermediaries that either did not have a BCP in place, or had not tested the BCP. In Mexico, the CNBV discovered that at some intermediaries neither the board of directors nor senior management acted as "sponsors." That is, neither was involved in setting the strategic direction or providing high-level oversight of the BCP function. As a result, plans were developed that only addressed disaster recovery and not business continuity. Reviews in Romania revealed backup servers that did not provide real-time backup for data and information. Moreover, the backup server was not located on the authorized premises of the firm, or in a location that specialized in disaster recovery as required by regulation. Finally, in the U.S., FINRA identified failures to disclose to customers how the firm's BCP addressed the possibility of a significant business disruption, and how the firm planned to respond to events of varying scope.[63]

**Systemically Important Intermediaries**

The IOSCO survey to regulators sought to determine whether regulators make distinctions in their oversight of BCPs for those intermediaries that are deemed to be systemically important. Fourteen Supervisor Respondents indicated that their laws did not distinguish systemically important intermediaries from non-systemically important institutions.[64] The BaFin (Germany) noted, however, that its oversight programs follow the principle of proportionality, *i.e.*, systemically important institutions receive more supervisory attention than less important institutions. This also applies to inspections in connection with BCPs.

There was an exception, however, to the above findings. In Italy, systemically important intermediaries are subject to more stringent requirements to establish robust and reliable BCPs. These requirements include:

- Requiring that risk scenarios triggering the BCP be identified in writing and updated.
- Subjecting recovery sites *i.e.*, back-up infrastructures to enhanced requirements, including geographic diversification and stringent recovery time.
- Documentation of all human, IT and logistics resources and processes and subjecting those to more stringent requirements.
- Mandatory annual testing of the intermediary's business continuity measures.

---

62 For example, Australia, Mexico, Romania, and the U.S. (SEC/FINRA and CFTC).

63 Other weaknesses uncovered by FINRA as part of its examination process included the failure by several firms to (1) review and update their BCP at least annually, (2) file current emergency contact information with FINRA, and (3) address adequately all required components in the firm's BCP.

64 These jurisdictions were Australia, Brazil, Canada, Hong Kong, Korea, Mexico, Morocco, Netherlands, Poland, Romania, Singapore, Spain, Turkey, and the U.K.

## D. Lessons Learned from Material Disruptions

In some jurisdictions, the supervisor will examine the underlying disruptive event and consider the "in-practice" effectiveness of BCPs.[65] Most Supervisor Respondents expressed the view that in those few instances in the recent past where intermediaries needed to trigger their BCP, the plan effectively dealt with the disruption[66] and facilitated the resumption of operations. Therefore, in the view of most Supervisor Respondents, no major changes to their regulations are necessary. However, some Supervisor Respondents believe that their participation in BCP testing has led to improvements in the quality and scope of data used by market intermediaries to assess the effectiveness of their BCPs.

A number of Intermediary Respondents that experienced MODs and needed to trigger their BCPs in response were able to use the opportunity to identify weaknesses and improve the BCP and expressed the view that ongoing updating of the BCP is critically important. Based on the experiences over the last years, Intermediary Respondents identified, among other things, the following "lessons learned" that should in their view be considered when developing/modifying a BCP:

- Indirect events and chain reactions caused by third parties are not always anticipated;[67]
- Staff safety and welfare should be a key priority;
- Cybercrime and malware could impact an entire region, not just a single jurisdiction;
- Communications during an MOD need to be clear, concise and ongoing;
- Analysis of past MODs, by the firm itself or other firms or regulators, should be considered because they can help to improve existing BCPs;
- Electronic trading is very sensitive to connectivity losses, which is the most common incident;
- Vendors must be considered as part of recovery processes;
- Work-from-home strategies are not sufficient/efficient in all cases;
- Essential staff must be identified, prepared and ready to deal with an MOD;
- The need to develop a practice of collecting information and news on an ongoing and continuous basis in order to anticipate certain events (*e.g.*, storms, social disruptions, political crisis, strikes);

---

65 U.S. (SEC/FINRA and CFTC).

66 Floods, rain, snow and ice storms, typhoons, hurricanes, earthquakes, civil unrests, and strikes have occurred and impacted the operation of firms for periods as long as two weeks.

67 For example, the event of January 2013, described above (p. 13), where a large Australian market participant that is part of a global investment bank with a European head office experienced a major system outage of its middle and back office systems due to a data corruption event.

- Each department of the firm must have its own tailored BCP;

- The need to consider outside factors that are not necessarily part of the firm's business but can materially impact the ability of a firm to implement its BCP, *e.g.*, the effect of an MOD on public/mass transportation systems; and

- The need to recognize that back-up data can be corrupted and that the BCP should take this into account.

## V. Guidance

Based upon a review of current regulatory requirements and firm practices, we believe there is broad consensus for the following standards applicable to supervisors with regulatory oversight responsibility over market intermediaries:

### Standards for Regulators

1. *Regulators should require market intermediaries to create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption.*

2. *Regulators should require market intermediaries to update the business continuity plan in the event of any material change to its operations, structure, business or location and to conduct an annual review*[68] *of it to determine whether any modifications are necessary in light of changes to the member's operations, structure, business, or location.*

### Guidance for Intermediaries

As indicated above, we believe that all market intermediaries should be required to have written BCPs and review them at least annually to determine whether modifications are necessary. However, the specific components of any single market intermediary's BCP will vary depending on the nature of the firm's activities and the market(s) in which it operates.

Upon reviewing current firm practices and regulatory requirements, we believe that there are a number of sound practices associated with current BCPs that merit consideration by all intermediaries as they develop their BCPs and/or consider revisions to their current BCPs. We describe these below.

The proposed sound practices are intended to allow for a wide range of application, taking into account necessary adaptation by market intermediaries in different jurisdictions. Regulators could consider these sound practices as part of their oversight of market intermediaries and such intermediaries may find useful in the development and implementation of their BCPs. Not every sound practice will be appropriate or equally effective for all market intermediaries. In particular, market intermediaries may conclude that a particular practice is not relevant to them because of the characteristics of their specific regulatory framework or the nature of the market intermediary's activities, or other factors. Market intermediaries may therefore incorporate these sound practices on a selective basis or in a manner best suited to their circumstances and national

[68] This recommendation is not intended to restrict the ability of a regulator to require, at its discretion, more frequent reviews.

legal frameworks. However, IOSCO would still encourage individual market intermediaries to consider these sound practices where relevant to their activities.

## A. Sound Practices

The elements that comprise a comprehensive BCP are flexible and may be tailored to the size and needs of an intermediary. Sound practices for such a BCP that merit consideration include:

### 1. For Components of a Market Intermediary's BCP

a) Identify the business functions and systems that are critical to continue operations in the face of an MOD, along with primary and backup staff.

b) Identify the major threats and impacts posed to the firm. As part of the BCP development process, consider risks like fire, floods, severe weather, pandemics, local protests, terrorism, or cyber-attacks, *i.e.*, anything with the potential to have broad impact on the physical access to buildings and staff.

c) Assess the potential impact of an MOD through qualitative analysis (*e.g.*, evaluating image reputation, legal and regulatory risks) and quantitative analysis (*e.g.*, assessing potential financial and operational impacts of outages, and regulatory reporting).

d) Consider whether the BCP needs to be modified based upon market disruptions that have impacted the industry.

e) Take steps that seek to ensure clients' prompt access to their funds and securities in the event of an MOD.

f) Consider the unique aspects of regional operations, if it is a globally active firm. For example, consider the need to have separate BCPs for different markets in which the firm operates.

g) Where appropriate, address a firm's operational dependencies on clearing and settlement entities and other third-party constituents.

h) Include documented procedures for internal and external communications with employees, clients, service providers, regulators and other stakeholders (*e.g.*, media), including policies and procedures that establish specific call cascades or trees.

i) Establish back-up sites for critical operations that have the same basic capabilities of primary sites. Consider the need for geographic diversity of back-up sites.

j) Establish an appropriate internal corporate governance structure that will be capable of implementing the BCP successfully in the event of an MOD. This could include having the firm designate certain individuals who are responsible for business continuity management.

k) Establish policies and procedures to ensure that critical personnel (or their back-ups) are available in the event of an MOD.

l) Assess, on a periodic basis, the current robustness of their BCPs, including critical outsourcing suppliers, to ensure high availability and resiliency of critical systems in times of an MOD, including the testing of the market intermediary's BCP on a periodic basis. Whenever possible, participate in industry-wide or cross-border testing with other intermediaries and stakeholders, and conduct mock drills (simulation exercises) to test the effectiveness of the BCP plan. Senior management should review results of BCP assessments.

m) Evaluate funding access and liquidity of the firm during an MOD.

n) Conduct BCP training exercises to help ensure that the BCP operates as intended should it be triggered by an MOD.

   i. Document the training exercises (ideally in an executive-level memo), and note any observed problems or weaknesses in staff execution of the BCP.

   ii. Require follow-up with any concerns addressed by responsible parties in advance of any subsequent testing.

**2. For Protection of Data, Systems and Client Privacy, including against Cyber-Attacks[69]**

a) Whether as part of the BCP or otherwise, address the need to protect data and client privacy, particularly from cyber-attacks. This would include measures to address the risk of potential loss or compromising of the firm's and investors' information or assets due to cyber-attacks. Aspects to consider include:

   i. Establishment of a defined security and IT policy outlining the appropriate controls (technical, logical and administrative) to restrict access to physical assets and information, particularly during an MOD, including procedures (*e.g.*, security controls, encryption) that address both the frequent back-up and recovery of hard copies and electronic information;

   ii. Whenever appropriate, consideration of the use of offsite storage facilities or backup data centers for electronic data or hardcopies, as applicable, and/or encryption of the electronic information that are backed up; and

   iii. The use of:

      A. Firewalls.

      B. Internet security (anti-virus, -spyware and –malware tools).

      C. Third-party vendors for IT services and systems protection and monitoring.

[69] This section does not aim to address all aspects of cyber security controls, but addresses the protection of data and privacy from a BCP perspective, including cyber security as relevant in this specific context.

## Appendix 1:

## Joint Forum BCP Principles

**Principle 1: Board and senior management responsibility**

Financial industry participants and financial authorities should have effective and comprehensive approaches to business continuity management. An organisation's board of directors and senior management are collectively responsible for the organisation's business continuity.

**Principle 2: Major operational disruptions**

Financial industry participants and financial authorities should incorporate the risk of a major operational disruption into their approaches to business continuity management. Financial authorities' business continuity management also should address how they will respond to a major operational disruption that affects the operation of the financial industry participants or financial system for which they are responsible.

**Principle 3: Recovery objectives**

Financial industry participants should develop recovery objectives that reflect the risk they represent to the operation of the financial system. As appropriate, such recovery objectives may be established in consultation with, or by, the relevant financial authorities.

**Principle 4: Communications**

Financial industry participants and financial authorities should include in their business continuity plans procedures for communicating within their organisations and with relevant external parties in the event of a major operational disruption.

**Principle 5: Cross-border communications**

Financial industry participants' and financial authorities' communication procedures should address communications with financial authorities in other jurisdictions in the event of major operational disruptions with cross-border implications.

**Principle 6: Testing**

Financial industry participants and financial authorities should test their business continuity plans, evaluate their effectiveness, and update their business continuity management, as appropriate.

**Principle 7: Business continuity management reviews by financial authorities**

Financial authorities should incorporate business continuity management reviews into their frameworks for the ongoing assessment of the financial industry participants for which they are responsible.

## Appendix 2

### Summary of Roundtables held in Rome, Italy (Dec. 2013) and Marrakesh, Morocco (Apr. 2014).

## ROME ROUNDTABLE

### Firm 1

The firm has around 20 different legal entities in Italy, with a total of approximately 19,000 employees.

### Topics covered:

#### Best practices; lessons learned

*Superstorm Sandy*: Key matters were (1) anticipation of the event; and (2) communication. We learned that when you have a weather forecast you cannot underestimate it, even if the threat is slight. You need to react. Check for availability for hotel rooms with cancellation possibility because you will need those rooms. Second: communication is key; it must be prompt. The firm's messages must be promptly distributed and be consistent with messages sent out by authorities. Firms must coordinate both with authorities and the media. You must take account of the fact that power outages will impact phones and other lines of communication that you rely on. Governance must be prepared in advance and roles and responsibilities and strategic priorities must be distributed early on in an event. HR, facilities, security must all be governed on an ongoing basis. Otherwise people will not be in a position to do the right things. The dedication and commitment of key personnel to continue operations is critical. Only in this way are teams able to anticipate problems and act. The BCP must account for the need for external work stations, including a desk and PC, and that these stations must be able to maintain contact with your primary site. The firm can own or outsource the site. The risk with outsourcing (*e.g.*, having a contract with a third-party provider to rent space to you in case of an event) is that the space is also "sold" to other clients. The weakness of this outsourcing model is that if the provider provides the alternative work site on a first come first served basis, the last people to come in may not have a workstation. Thus, in the firm representative's view, dedicated alternative stations owned by the firm are a better option. You need a robust set of working tools, including from home. The representative notes that some firms during the crisis had in advance a large number of users working remotely; backstop reliance is best. Those firms that planned the best (*e.g.*, providing accommodations for and transportation of people) did the best.

#### Geographic diversity

The Bank of Italy has BCP rules that require firms to take account of the probability of disaster with your alternative sites. You must make a risk assessment with regard to the geographic characteristics. How might regulators help? We need to understand telecom and electricity providers (*e.g.*, the topography of their installation). Regulators should make (or seek to make) this topography transparent, imposing providers rules of transparency on telecom and electricity covering the installations and networking on which intermediaries' buildings depend. This allows intermediaries to certify the independence of sites physically distant. There cannot be interdependencies between two sites. In addition, they cannot permit both sites (primary and

alternative) to be potentially affected at the by the same phone lines or power infrastructure. Ideally, a securities regulator would be in a position to make clear to regulated entities as to whether any alternative sites proposed by firms will have the services they need in a crisis.

**Activity transfer (solution) to face a wide area disaster**

One solution that might help: utilization of people outside your jurisdiction. This can be a cost efficient alternative when you have two offices in two jurisdictions that have the same functions. You must do an analysis ahead of time to determine whether there are cross-border legal impediments before relying on this option. Perhaps this is an area where regulators can help? The firm's BCP takes these legal issues into account. There is generally a recovery agreement between the two locations. So they were granted a provisional license. Systems are usually not an obstacle at all. "Activity" testing between the two sites is conducted at least once a year. Calendars must be synchronized. Cross location recovery can also be done by transferring employees to a separate location, generally outside the geographical scope, to recover businesses or other defined functions and processes. That also requires training, preparation and maintenance.

**Approaches to be applied to small firms**

The Bank of Italy has declined to issue special rules for smaller firms. Firm actions should match the level of risk they pose. You must put sufficient resources into the BCP based on the risks you face. Even when a smaller firm is subject to the same requirement as a larger firm, the level of risk and therefore the appropriate actions should be firm specific and proportionate to its size and relative criticality. Every firm must do this analysis.

**Firm 2**

The presenter is the firm's BCP planner and spends 100% of his time on the issue. He is a member of the firm's information security unit.

The company is an "investment firm" in Spain, South America and the United States. It is also engaged globally in insurance, with its main insurance company headquartered in Spain. It is active in 46 countries and has 45,000 employees worldwide.

In the representative's view, the most important thing is that you must engage everyone in the company in the BCP (he spends 100% of the time on BCP). Info and tech people are the most important for BCPs. They also believe there should be some international standards. Some of their BCP standards are broadly applied and apply to most company affiliates.

A good BCP has two main drivers: senior management and regulation. As to the first, there is a crisis committee headed by a VP of the firm. In May 2013, they conducted a "major crisis" test; and the firm's senior management committee was involved. With regard to regulation, there are specific committees that address BCPs and useful on a day-to-day basis. Senior management pressure along with legal requirements play an important role in motivating a firm and its employees to dedicate the resources they need to develop effective BCPs.

How does one assess whether a BCP is well implemented? The firm focuses on testing, as this is the most important (although not only) indicator. Sometimes non-tested portions, when

implemented, are the best indicator of how things work. Firms must take into account geographic diversity. You must protect information. Safety of information is key. People do not always focus sufficiently on the quality/quantity of information protection; they sometimes focus too much on the time to recover.

Testing: firms must test for all possible scenarios (*e.g.*, you will no longer have the "right telephone number" if headquarters is destroyed). The most important part of testing is that it should tell us how we are doing and identify problems…and then lead to new testing until it works. The key: identify the problem and then test again!! Testing helps to foster a BCP 'culture' in the firm. You should know the things you will need in a real disaster. But you can't test everything. So we test parts of the plan periodically. In the representative's view, "this is a long distance race." Every test should be better than the last one, but not as good as the next. The firm's first test was in 2003.

The firm conducts two major BCP tests per year, involving nearly 100 people. In a real disaster, more would be involved. It is very important that business users are involved in the testing. For the first time, in June 2013, under the auspices of the Spanish authorities, the main objective was to react in case of a cyber-attack.

The firm has a primary data center and headquarters. They have a secondary data site and alternative offices and centers and administrative officers. A key challenge when trying to implement a BCP is your email and agreement for service. Service agreements are fine (*e.g.*, you might get discounts if the service goes down), but that does not help you in a crisis. You need the service! Two days down would be a disaster for the firm. So these agreements are worthless and do not help you…a problem we find with any service provider. He notes that there's "lots of regulation for financial firms," but we rely on these service providers and they are NOT so worried about BCPs. This reliance on external parties is a problem (email service, electricity, phone, etc.).

**Group Discussions (Q&A)**

**Regulator (R) 1:** An observation regarding Sept. 11: things worked well at foreign offices.

**R2** asks representative of Firm 2 about a real life experience. He cites two examples. With regard to a major earthquake in Chile, the BCP worked correctly…people went to alternative site. But some unexpected things happened. Firm employees were too busy to give money out to customers! The firm needed to call other people from other countries to go to Chile to support the business process and give the service to the customers. The second crisis was in November 2013, in a Brazilian new call center where there was a fire. It was supposed to have fire extinguishers, but they did not work. So the building burned. No one injured. But the BCP had not been updated. They were lucky because Friday was a non-working day. So Saturday and Sunday permitted them to recover. They were also lucky because information technology was not at the burnt location.

**R3:** Regulators have lots of rules. But things don't always work. No matter how much how guidance we give, there are still problems. How can we make firms more aware than they currently are? What more can and should be done from a regulatory perspective? The representative from Firm 1 commented that regulators in the banking industry have already

acted, and the firm already has the regulatory guidance it needs. The problem is with the providers who are not part of the securities industry…and are not regulated (phone, electricity, email service providers). Can regulators help there?!! She also commented that regulators should differentiate between different types of crisis, *e.g.*, liquidity or counterparty default risk.

**R4:** Can some of these problems be solved via comprehensive outsourcing arrangements? Response: They do outsource, but you have to do a very good impact analysis and if you decide to outsource; you must assess the risk of non-performance given the type of disaster(s). But for really critical activities, you should not outsource. But that can be very costly! This choice cannot be made in a simple way. The firm must engage in a cost-benefit analysis. With regards to electric power and telecom systems, the key is transparency so that BCPs can be accordingly written. The firm must ask itself: Where does the affected grid extend to? How can you plan for alternative sources of electricity in areas that will not be affected?

**R5:** Lessons learned? Cyber is a risk. We know fire, we know earthquakes, and we know better how to prepare for those. But cyber-attacks are new and a real risk. But we don't know the probability or the potential impact. We are facing something new that we cannot measure. But we do have people prepared to react. The presenters suggested that regulators might require firms to prepare for cyber-attacks very specifically.

**R6:** How hard is it for you to get the budget ($$) you need? What is the role of the regulator there? Response: Regulatory requirements DO assist the BCP planners to get the resources they need. But risk analysis is really important. If a risk is high, then the senior management will be more willing to provide the necessary resources.

**R6:** Fiber optic lines are critical to effective BCPs and this is relevant to the presenters' concern about electricity and telecom. But perhaps asking for transparency about capabilities really is the best that we as regulators can do.

**MARRAKESH ROUNDTABLE**

**Firm 1**

The firm has global coverage that allows its staff to operate in other locations such as London, Australia, or Boston. Employees have remote access of their work and the testing is performed on a monthly basis. In the firm's home jurisdiction, the BCP is primarily subject to bank regulation and the BCP is ingrained in the business practice and culture of the firm. In one of the firm's primary offices, there are 2-3 people who are involved in the BCP program and these employees are part of the regional and global BCP groups. It was noted that many intermediaries have outsourced back-office operations to another foreign jurisdiction.

**Firm 2**

The firm fulfills its BCP obligations by conducting operational risk management meetings and identifying outsourcing risk. A key step taken by the firm to maintain an effective BCP includes on-site visits by responsible staff on a semi-annual basis, including the COO. Documentation has also been enhanced recently compared to the past. There is also an open information exchange of these outsourced divisions/entities with the home regulator.

A regulator asked a question concerning cross jurisdiction concerns. It was explained that in Europe, cross jurisdictional issues are a bit easier to address due to the European passports, which permit employees to travel freely to another European jurisdiction to resume work. Another example is the Fukushima disaster in Japan. The Japanese licensed staff came to Hong Kong and the SFC expeditiously processed the necessary licensing registration. Similarly, licensing accommodations were made during Hurricane Katrina in the U.S among the state regulators.

## Appendix 3

### IOSCO Member Requirements or Guidance Relating to Intermediary BCPs

**Australia:** Australia reported that there are no specific requirements under the Corporation Act for the majority of market intermediaries ("AFS licensees") to implement a business continuity plan. However, market intermediaries are required to have adequate risk management systems under applicable law, which requires risks to be kept at an acceptable minimum. Moreover, regulators have provided guidance to entities on what constitutes an "adequate level" of risk management. This guidance specifically asks whether the AFS licensee has a business continuity plan as part of its risk management framework. This guidance identifies what the regulator believes is adequate for AFS licensees' risk management systems. This guidance states that these systems should (i) be based on a structured and systematic process that takes legal obligations into account; (ii) be able to identify and evaluate risks that face the business; (iii) establish and maintain controls to manage and mitigate the risks; and (iv) be fully implemented and monitored. In addition to regulatory guidance, exchanges require their market intermediary participants to have adequate BCPs and back-up plans for each of its systems that support order entry, order routing, execution and trade reporting. Clearing and settlement facilities also require adequate business continuity arrangements.

**Brazil:** The Brazilian Central Bank follows Basel Committee principles with regards to business continuity and requires that all financial institutions, including market intermediaries, have proper BCPs in place. In addition to the requirements of the Central Bank, organized markets (*e.g.*, BOVESPA) require that intermediaries comply with basic guidelines set forth in the Operational Qualification Program as a condition to participate in the market. Under the Operational Qualification Program, market intermediaries with electronic brokerage activities must set forth contingency plans in the event online systems come to a halt. In addition, the intermediaries must develop, implement, and test a BCP designed to ensure the continuation of operations. This includes settlement continuity, back-up processes, and annual testing. Moreover, the Operational Qualification Program sets forth requirements for physical and information security. These entities must submit a yearly audit report to the regulator.

**Canada:** Canadian regulation is harmonized among the various jurisdictional regulators and requires that intermediaries establish a compliance system that ensures the system complies with securities law and manages business risks. In addition, there is a companion policy that states that intermediaries should maintain internal controls to mitigate risks and protect the firm and assets. Canadian regulation is principles-based (coupled with prescriptive SRO rules) and allows intermediaries to adopt an appropriate compliance structure.

**France:** The French response refers both to EU and French law. MiFID requires firms to maintain an adequate business continuity and recovery policy. The Capital Requirements Directive provides that such policies must ensure the firm's ability to operate on an ongoing basis and limit losses in the event of a severe business interruption. Domestic regulations require that (1) firms ensure the effectiveness of BCPs in line with objectives set by senior management and/or the board, (2) that back-up IT procedures enable business operations to continue notwithstanding an event, and (3) that the integrity and confidentiality of information is preserved in the event of a serious systems failure.

**Germany:** German law requires intermediaries to have an appropriate and effective risk management system including a business contingency plan overseen by the members of the management board. In addition, German regulators published administrative instructions, which specify requirements for adequate risk management as set out under the law. These instructions set forth minimum requirements for addressing events that could materially interrupt business. These requirements are not limited to IT systems, but address all sources of potential critical interruptions of business. The business contingency plan must seek to mitigate damage and set out back-up systems in the event of disruption. German regulation also requires regular testing and communication of the plans to all relevant employees.

**Hong Kong:** The regulators have issued a code of conduct and guidelines addressing business and operational risk. These require that an intermediary employ the necessary resources for its business activities and implement an effective BCP appropriate to the size of the firm, including impact studies, identification of potential scenarios, and regular testing.

**Hungary:** The IT Supervision Department of the Magyar Nemzeti Bank (Central Bank of Hungary) provides detailed guidance on disaster recovery and Business Continuity Management. This guidance is not legally binding, but is based on the underlying legal requirements of Hungarian law that require tested BCM to be in place. The regulators review compliance with the guidance and the related legal requirements by supervised financial institutions during on-site inspections.

**India:** Indian regulators have issued guidelines and provisions for BCP and disaster recovery for intermediaries. The guidelines require depositary participants to ensure that there is continuity for electronic data and effective back-up systems. Stock exchanges also direct their members to review risks and put BCPs into place. Registrars and transfer agents are required to maintain information in off-site back-up facilities. Indian regulation also contains provisions for these entities to have systems to maintain data and appropriate hardware and software back-up systems. In addition, there are requirements for regular drills and testing and policies must be put in place to handle many events. Exchanges and depositaries have also been asked to submit their plans to regulators.

**Italy:** Italian law requires intermediaries to maintain a BCP that ensures continuous operation, limits loss, preserves data and essential functions, and guarantees continuity of service. There is a detailed framework with which intermediaries must comply.

**Japan**: The Supervisory Guidelines require securities companies (etc.) to establish Business Continuity Management (BCM) and prepare a BCP. From a governance perspective, the BCM should be reviewed by an independent body such as internal or external auditors, and the board of directors should be involved in preparing and revising the BCP (*i.e.*, whether a firm obtains an approval from the board of directors when the firm adopts the BCM and makes material revisions). The BCP should ensure that the firm can continue the business activities that are essential for maintaining the function of the financial system while both recovering promptly from emergencies such as damage caused by acts of terrorism, large-scale disasters or other events and cooperating with the relevant parties.

**Korea:** Korean intermediaries are subject to two key regulatory requirements. First, firms are required to prepare a BCP, among other things, in order to gain authorization for an investment

business. Second, the law sets out the details for BCPs and seeks to ensure the security and reliability of electronic financial transactions.

**Mexico:** Mexican regulators have issued specific rules regarding BCPs as part of the internal control for intermediaries.

**Morocco:** Market intermediaries must provide a BCP to the regulator.

**Netherlands:** Market intermediaries are required to implement BCPs, but the regulations are not prescribed in great detail. The Dutch use guidelines to cover the various areas.

**Pakistan:** Pakistan stated that while no formal regulatory system was in place, market intermediaries are encouraged to put mechanisms in place in line with international best practices. There is a plan to issue specific regulation with broad guidelines to implement BCPs.

**Poland:** Investment firms are required to ensure the security and continuity of brokerage services and the protection of customers' interests as well as protect confidential information.

**Romania:** Romanian regulation requires investment firms to have a BCP that ensures the safekeeping of data, operational continuity and recovery of data. The BCP should also govern the security and control of IT systems to ensure confidentiality of information. The BCP should be reviewed and updated annually.

**Singapore:** The Singapore regulator has issued the Business Continuity Management Guidelines, Notice on Technology Risk Management and Technology Risk Management Guidelines which set out requirements for financial institutions including market intermediaries to maintain BCPs.

**Spain:** Under the Spanish Securities Markets Act, intermediaries are required to develop a BCP that addresses potential damage/disruption in operations in the event of catastrophe and that ensures continuity and regularity in the performance of their services and activities, including controls and resources designed to ensure the safekeeping of information systems. The regulator does not, however, prescribe a specific implementation plan.

**Turkey:** Intermediaries must implement BCPs in more specialized areas as in the case of leveraged transactions on forex and precious metals.

**U.K.:** Market intermediaries' BCPs may be covered by either the FCA or by the FCA and the Prudential Regulation Authority (PRA). Although each Authority has a separate handbook which comprises both Rules (requirements) and Guidance (should have); the actual text the handbooks is the same. The handbooks contain high level Rules requiring BCPs and some Guidance as to the coverage and testing of BCPs but they do not include detailed or prescriptive requirements. Market intermediaries are subject to the same requirements derived from EU legislation under MiFID and the Capital Requirements Directive as other EU members such as France. Guidance in the handbook includes having a robust process in place to assess and mitigate business continuity risks as part of its overall risk management and take reasonable steps to ensure continuity and regularity. The intermediary should also assess the likelihood and impact of potential disruptions. For high impact firms, guidance is applied on a "comply or explain"

basis.[70] The handbook also sets forth Rules regarding the notification to regulators of major BCP events and Guidance to ensure the regulators are informed of material changes in BCPs, tech systems and failures of any systems.

**U.S. (CFTC):** The CFTC has issued regulations and rules requiring market intermediaries to establish effective risk management policies and procedures that cover business continuity. Intermediaries are required to establish and maintain a written BCP that enables the intermediary to resume operations by the next business day with minimal disturbance to its counterparties and the market and to recover all necessary documentation. Some elements that must be in the plan are a mechanism to identify data, key personnel, a communication plan, procedures for back-up facilities and infrastructure, and a procedure to review these policies among other things. A firm's BCP must be reviewed at least every three years by an independent third party and a report issued thereon. The National Futures Association (NFA), the self-regulatory organization for the U.S. futures industry, has a rule with similar requirements.

**U.S. (SEC/FINRA):** Broker-dealer members of FINRA must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption. Such procedures must be reasonably designed to enable the member to meet its existing obligations to customers and to comply with FINRA rules. In addition, such procedures must address the member's existing relationships with other broker-dealers and counter-parties. The business continuity plan must be made available promptly upon request to FINRA staff. Plans must be updated in the event of any material change to the member's operations, structure, business or location. Each FINRA member must also conduct an annual review of its business continuity plan to determine whether any modifications are necessary in light of changes to the member's operations, structure, business, or location. FINRA rules also require broker-dealer BCPs to contain certain minimum elements.

[70] "Comply or explain" is a regulatory approach used in the United Kingdom, Germany, the Netherlands and other jurisdictions in the field of corporate governance and financial supervision. Rather than setting out binding laws, government regulators (in the U.K., the Financial Reporting Council, in Germany, under the *Aktiengesetz*) set out a code, which listed companies may either comply with, or if they do not comply, explain publicly why they do not. The purpose of "comply or explain" is to "let the market decide" whether a set of standards is appropriate for individual companies. Since a company may deviate from the standard, this approach rejects the view that "one size fits all," but because of the requirement of disclosure of explanations to market investors, anticipates that if investors do not accept a company's explanations, then investors will sell their shares, hence creating a "market sanction," rather than a legal one. The response to the above is generally public. For example, the Financial Policy Committee in the U.K. can give "comply or explain" recommendations.

## Appendix 4

## Survey Tables

*TABLE 1: List of Regulators Participating in this study*

| | Country | Regulator |
|---|---|---|
| | | |
| 1 | Australia | ASIC |
| 2 | Brazil | CVM |
| 3 | Canada | OSC and QAMF (combined response) |
| 4 | Germany | BaFin |
| 5 | France | AMF |
| 5 | Hong Kong | SFC |
| 6 | Hungary | MNB (Central Bank) |
| 7 | India | SEB |
| 8 | Italy | CONSOB |
| 9 | Japan | FSA |
| 10 | Korea | FSS |
| 11 | Mexico | CNBV |
| 12 | Morocco | CDVM |
| 13 | Netherlands | AFM |
| 14 | Pakistan | PSEC |
| 15 | Poland | PFSA |
| 16 | Romania | RFSA |
| 17 | Singapore | MAS |
| 18 | Spain | CNMV |
| 19 | Turkey | CMB |
| 20 | U.K. | FCA |
| 21 | U.S. | CFTC |
| 22 | U.S. | SEC |

*TABLE 2: Market intermediary responses by jurisdiction*

| **Jurisdiction** | **Number of Responses** |
|---|---|
| Australia | 5 |
| Brazil | 2 |
| Canada (OSC and Quebec AMF) | 12 |
| Germany<br>France | 3<br>1 |
| Hong Kong | 1 |
| Italy | 4 |
| Japan | 4 |
| Korea | 5 |
| Morocco | 5 |
| Romania | 3 |
| Singapore | 4 |
| Turkey | 5 |
| U.K. | 2 |
| U.S. | 6 |
| | |
| **TOTAL** | **60** |
| | |