MEDIA RELEASE

International Organization of Securities Commissions
Organisation internationale des commissions de valeurs
Organização Internacional das Comissões de Valores
Organización Internacional de Comisiones de Valores

IOSCO/MR/54/2015

Madrid, 22 December 2015

IOSCO reports on business continuity plans for trading venues and intermediaries

The Board of the International Organization of Securities Commissions (IOSCO) today published two reports that seek to enhance the ability of financial markets and intermediaries to manage risks, withstand catastrophic events, and swiftly resume their services in the event of disruption.

The report *Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity* provides a comprehensive overview of the steps Trading Venues take to manage the risks associated with electronic trading and the ways they plan for and manage disruptions through BCPs. As technology continues to evolve, leading to different ways to operate and access markets, so too will Trading Venues have to continuously consider the impact of these changes and adapt, to protect themselves, their participants and investors.

The report discusses IOSCO findings based on the surveys responses from Trading Venues and Trading Venue participants from more than 30 jurisdictions. The report makes recommendations to help regulators ensure that trading venues are able to manage effectively identified risks, such as those related to technology. It also proposes sound practices that should be considered by trading venues when developing and implementing risk mitigation mechanisms and business continuity plans aimed at safeguarding the integrity, resiliency and reliability of their critical systems. Appendix A contains the list of recommendations and sound practices.

IOSCO recognizes that not every sound practice will work for all Trading Venues. Use of any sound practice would be at the discretion of each Trading Venue.

The second IOSCO report, *Market Intermediary Business Continuity and Recovery Planning*, sets forth two standards for regulators and sound practices that regulators could consider as part of their oversight of market intermediaries. These sound practices may also prove useful to intermediaries who are developing and implementing business continuity plans. Appendix B contains the list of standards and sound practices.

As in the case of trade venues, 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

Recent disruptive events and emerging threats in major international financial markets highlighted the need to examine and identify the key measures and arrangements in place at trading venues and market intermediaries to restore their "critical" functions should a disruption occur. The reports also take into account the 2006 Joint Forum Report *High-level Principles for Business Continuity.*[1]

Both reports are based on consultation reports published earlier this year. They also draw on the results of surveys of IOSCO members and stakeholders, and feedback from roundtables organized with industry participants.

[1] In its report, the Joint Forum noted that a major operational disruption can result from a wide range of weather-related events and intentional or accidental acts that cause widespread damage to physical infrastructure. It stated that financial supervisory authorities and financial industry participants share a common interest in promoting the resiliency of the financial system to major operational disruption. The report can be found here: http://www.bis.org/publ/joint17.pdf

International Organization of Securities Commissions
Organisation internationale des commissions de valeurs
Organização Internacional das Comissões de Valores
Organización Internacional de Comisiones de Valores

A key objective of the reports is to help identify and address possible weaknesses or gaps in the business continuity plans and recovery strategies of trading venues and market intermediaries.

NOTES TO THE EDITORS

1. IOSCO is the leading international policy forum for securities regulators and is recognized as the global standard setter for securities regulation. The organization's membership regulates more than 95% of the world's securities markets in more than 115 jurisdictions and it continues to expand.

2. The IOSCO Board is the governing and standard-setting body of the International Organization of Securities Commissions (IOSCO). The Board is made up of 34 securities regulators. Mr Greg Medcraft, chairman of the Australian Securities and Investments Commission, is the chair of the IOSCO Board. The members of the IOSCO Board are the securities regulatory authorities of Australia, Belgium, Brazil, China, Egypt, France, Germany, Greece, Hong Kong, India, Italy, Japan, Kenya, Korea, Malaysia, Mexico, the Netherlands, Nigeria, Ontario, Pakistan, Peru, Quebec, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Thailand, Trinidad and Tobago, Turkey, United Kingdom and the United States.

3. The Growth and Emerging Markets Committee is the largest Committee within IOSCO, representing 75 per cent of the IOSCO membership. Mr. Ranjit Ajit Singh, Chairman, Securities Commission, Malaysia, and Vice Chair of the IOSCO Board, is the Chair of the GEM. The Committee endeavors to promote the development and greater efficiency of emerging securities and futures markets by establishing principles and minimum standards, providing training programs and technical assistance for members and facilitating the exchange of information and transfer of technology and expertise.

4. IOSCO aims through its permanent structures:

- to cooperate in developing, implementing and promoting adherence to internationally recognized and consistent standards of regulation, oversight and enforcement in order to protect investors, maintain fair, efficient and transparent markets, and seek to address systemic risks;
- to enhance investor protection and promote investor confidence in the integrity of securities markets, through strengthened information exchange and cooperation in enforcement against misconduct and in supervision of markets and market intermediaries; and
- to exchange information at both global and regional levels on their respective experiences in order to assist the development of markets, strengthen market infrastructure and implement appropriate regulation.

5. The Joint Forum was established in 1996 under the aegis of IOSCO, the Basel Committee on Banking Supervision (BCBS), and the International Association of Insurance Supervisors (IAIS) to deal with issues common to the banking, securities and insurance sectors.

MEDIA ENQUIRIES

Carlta Vitzthum	+ 34 91 787 0419
Outside office hours	+ 34 697 449 639
Email:	carlta@iosco.org
Website:	www.iosco.org
Follow IOSCO on Twitter	@IOSCOPress

MEDIA RELEASE

International Organization of Securities Commissions
Organisation internationale des commissions de valeurs
Organização Internacional das Comissões de Valores
Organización Internacional de Comisiones de Valores

Appendix A:

Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity

(Recommendation and sound practices)

Recommendations to Regulators

1. *Regulators should require Trading Venues to have in place mechanisms to help ensure the resiliency, reliability and integrity (including security) of critical systems.*

2. *Regulators should require Trading Venues to establish, maintain and implement as appropriate a BCP.*

Sound Practices for Trading Venues

A. Managing technology to mitigate risk

Trading Venues should consider:

1.1 Establishing and implementing policies and procedures that provide for the identification, monitoring and addressing of risks to their critical systems, including risks that may arise by third party access to the Trading Venue's critical systems.

1.2 Establishing policies and procedures related to the development, modification, testing and implementation of new, or changes to, critical systems.

1.3 Implementing mechanisms for its critical systems that relate to capacity management, stress testing, application controls, system development methodologies, the use of metrics to monitor performance, security related to systems access and systems reviews.

1.4 Establishing, maintaining and implementing a governance model for the management of critical systems, including governance for the development of new critical systems or changes to critical systems. The governance model could include that senior management or the Board retains an overarching decision-making role with respect to critical systems.

1.5 Performing objective systems reviews on a periodic basis (such as, for example, on an annual basis) of the Trading Venue's critical systems and their compliance with all applicable regulatory requirements. These reviews could include:

a. Having an objective internal auditor or third party conduct the systems review.
b. Establishing policies and procedures to analyze the results of the review, which may include reporting the results to senior management.
c. Establishing policies and procedures to address any deficiencies identified by the systems review.
d. Notifying regulators, whenever appropriate, of the review, including any deficiencies identified and the steps it is taking to address them.

1.6 Establishing and implementing incident management procedures that address system incidents. This could include internal coordination and communication protocols, reporting to regulators and, where appropriate, to participants.

1.7 Establishing and implementing communication protocols that govern the sharing of information regarding the introduction of new, or changes to, critical systems. For example, a communication protocol could include information about the timing of implementation for new critical systems or changes to existing critical systems so that Trading Venue participants are given sufficient lead time to make the requisite systems changes or adjustments.

B. Managing external risks to critical systems

Trading Venues should consider:

2.1 Establishing and implementing:

a. Mechanisms to monitor Trading Venue participant compliance with the rules of the Trading Venue.
b. Pre-trade controls, such as price and volume controls or filters.
c. Post-trade monitoring of trading.
d. The ability to suspend trading by a Trading Venue participant.
e. Measures to provide for a "cooling off" period, such as through a trading halt or pause, where there are sudden price movements, including collars on price movements, and volatility measures.

2.2 Establishing, implementing and updating robust cyber-security programs to protect the Trading Venue's critical systems against cyber-attacks, including:

a. Governance practices that include consideration of appropriate controls to restrict access to critical systems and identification of responsible personnel.
b. Appropriate escalation and communication procedures.
c. Penetration and vulnerability testing.
d. Data storage and integrity safeguards, including, for example, the use of off-site storage facilities or back-up centers, encryption, passwords and network segregation, anti-virus and malware software.
e. Policies and procedures to monitor for suspicious network activity, including, for example, intrusion detection, firewalls, and audit trails regarding access to critical systems.

C. How to plan for disruptions: business continuity plans

Trading Venues should consider:

3.1 Establishing objectives and strategies in terms of business continuity planning, which should include allocation of adequate human, technological and financial resources to the development, maintenance, updating and testing of the BCP;

3.2 Establishing an appropriate governance structure for the approval of the BCP and any updates.

3.3 Conducting assessments of the potential impact of material operational disruptions, particularly to critical systems, and taking account of these in developing the BCP.

3.4 Updating the BCP, as necessary.

3.5 Having the BCP include, among other things:

a. Clear and comprehensive communication protocols and procedures for both external and internal communications.
b. Escalation procedures.
c. Recordkeeping, including logs of all tests and deficiencies.
d. Redundancy in software and hardware, where appropriate.
e. Consideration of the possibility that the services of a supplying firm (i.e., a firm to which critical systems have been outsourced) may become unavailable and setting forth in the SLA the obligations of the supplying firm, should its services become unavailable, and if

possible, providing for access to information by the Trading Venue of the supplying firm's own BCP, if any.

3.6 Testing the operation of the BCP on a periodic basis. BCP testing could include assessments of the Trading Venue's ability to recover from incidents under predefined objectives and the ability of a Trading Venue to resume trading within the target recovery time. In addition:

a. Documenting and recording the testing results and submitting them promptly to the Board of Directors or other competent management body.
b. Making the results available to the regulator upon request.
c. Coordinating, as appropriate for its market structure, the testing of its BCP with participants and with other venues.

3.7 Making the BCP available to the regulator, upon request.

International Organization of Securities Commissions
Organisation internationale des commissions de valeurs
Organização Internacional das Comissões de Valores
Organización Internacional de Comisiones de Valores

Appendix B:

Market Intermediary Business Continuity and Recovery Planning

(Standards and sound practices)

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 their business continuity plan in the event of any material change to operations, structure, business, or location and to conduct an annual review[2] of it to determine whether any modifications are necessary in light of changes to the market intermediary's operations, structure, business, or location.*

Sound Practices for Intermediaries

A. 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.[3]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).

---

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

3 A firm may of course also consider more broadly the potential impact of an MOD on the market and how that might affect the firm.

d) Consider whether the BCP needs to be modified based upon market disruptions that have impacted the industry, including similarly situated market intermediaries.

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 practical and useful, 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.

B. For Protection of Data, Systems and Client Privacy, including against Cyber-Attacks[4]

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.

[4] 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.